CAIGG

CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO

Ministerio Secretaría General de la Presidencia

GGSAI N° 3 - Versión 0.1 - 2025

Guía de Gestión y Servicios de Auditoría Interna (GGSAI) N° 3

Planificación del Trabajo de Auditoría Interna

ÍNDICE

Materia	Pág.
Índice	1
Presentación	2
I. Introducción	3
II. Objetivo del Documento	4
III. Marco Normativo Definido en las Normas Globales de Auditoría Interna	4
IV. Conceptos sobre la Planificación del Trabajo de Auditoría Interna	5
V. Marco Metodológico para la Planificación del Trabajo de Auditoría Interna – Principales Pasos	7
Paso N° 1: Desarrollar la Comprensión Inicial de la Actividad Bajo Revisión	9
1. Aspectos Generales de la Comprensión Inicial	10
Paso N° 2: Desarrollar una Evaluación de Riesgos en la Actividad Bajo Revisión	18
1. Aspectos Generales de la Evaluación de Riesgos en la Actividad Bajo Revisión	19
2. Conceptos Generales sobre Gobierno, Riesgos y Controles desde la Perspectiva de la Auditoría Interna	19
3. Modelo de las Tres Líneas del IIA	28
4. Relación entre Gobierno, Gestión de Riesgos, Control en la Planificación del Trabajo	31
5. Evaluación de Riesgos de Fraude	45
6. Evaluación de los Riesgos y Controles Clave de Tecnologías de Información en la Planificación del Trabajo	56
Paso N° 3: Establecer o Redefinir los Objetivos y Alcance del Trabajo	66
Paso N° 4: Identificar y/o Definir Criterios de Auditoría	78
Paso N° 5: Definir los Recursos Necesarios (Financieros, Tecnológicos y Humanos)	92
Paso N° 6: Formular el Memorándum de Planificación	106
Paso N° 7: Formular el Programa de Trabajo	110
Paso N° 8: Formular Planilla de Trazabilidad del Trabajo (Complementaria)	116
VI. Aspectos Relevantes de la Planificación del Trabajo en Funciones de Auditoría Interna Pequeñas	119
VII. Bibliografía	122
VIII. Anexos	124
Anexo N° 1: Comparación de Servicios de Aseguramiento y Asesoramiento según las NOGAI	125
Anexo N° 2: Relación entre Objetivos del Trabajo y Procedimientos de Auditoría	129
Anexo N° 3: Aspectos Fundamentales sobre Procedimientos de Auditoría	132
Anexo N° 4: Conceptos Generales sobre Apetito de Riesgo y Tolerancia al Riesgo	141
Anexo N° 5: Tablas Tradicionales de Valuación de Riesgos, Controles, Severidad y Exposición al Riesgo	143
Anexo N° 6: Conceptos sobre Dimensiones o Criterios Cualitativos adicionales en la Evaluación de Riesgos	150
Anexo N° 7: Aspectos Relevantes de los Procesos de Gobierno, Gestión de Riesgos y Control en la Actividad Bajo Revisión, que se deben Conocer y Analizar, previo a la Planificación del Trabajo	156
Anexo N° 8: Procesos Genéricos, Principales Riesgos, Controles Esperados	158
Anexo N° 9: Conceptos Fundamentales sobre Riesgo de Auditoría	159
Anexo N° 10: Análisis de Datos	161
Anexo N° 11: Conceptos Fundamentales sobre Fraude	164
Anexo N° 12: Muestreo de Auditoría y Análisis Estadístico	185
Anexo N° 13: Planilla de Trazabilidad del Trabajo de Auditoría Interna	188
Anexo N° 14: Modelo de Madurez para la Planificación del Trabajo en Funciones de Auditoría Interna	201

PRESENTACIÓN

En cumplimiento de las instrucciones del Presidente de la República, Sr. Gabriel Boric Font, relativas al fortalecimiento de la Política de Auditoría Interna de Gobierno, el Consejo de Auditoría Interna General de Gobierno (CAIGG), en su rol de entidad asesora del Supremo Gobierno en materias de auditoría interna, control interno, gestión de riesgos, probidad y gobernanza, presenta a la Red de Auditoría Gubernamental la Guía de Gestión y Servicios de Auditoría Interna (GGSAI) N° 3: Planificación del Trabajo de Auditoría Interna.

Esta guía ha sido diseñada como una herramienta metodológica clave para robustecer las capacidades técnicas y operativas de las funciones de auditoría interna en el sector público, promoviendo una planificación sistemática, estructurada y orientada por riesgos. Su contenido se encuentra plenamente alineado con los *Principios 12 y 13* de las Normas Globales de Auditoría Interna (NOGAI) emitidas por *The Institute of Internal Auditors (IIA)*, que exigen establecer objetivos de auditoría relevantes y planes de trabajo basados en una evaluación de riesgos, recursos disponibles y expectativas de las partes interesadas.

La fase de planificación constituye el pilar esencial de todo trabajo de auditoría interna. Su adecuada ejecución influye directamente en la calidad, pertinencia y utilidad del proceso completo, desde el desarrollo del trabajo hasta la emisión del informe y el seguimiento de las acciones correctivas. Una planificación deficiente, por el contrario, limita el alcance, disminuye el impacto del trabajo y compromete la capacidad de auditoría para agregar valor.

En este contexto, la guía entrega orientaciones prácticas y adaptables para que los equipos de auditoría interna puedan definir con claridad los objetivos del trabajo, identificar y evaluar riesgos relevantes, establecer criterios de auditoría, delimitar el alcance con precisión, estimar recursos, y elaborar un programa de trabajo coherente con el contexto organizacional y los riesgos priorizados.

Al contribuir activamente al cumplimiento de los objetivos institucionales y al fortalecimiento de la gestión pública, una planificación rigurosa y bien documentada refuerza la capacidad del Estado para crear, proteger y sostener valor en el tiempo, consolidando el rol de la auditoría interna como un agente clave en la gobernanza del sector público.

De esta forma, la guía busca orientar, profesionalizar y estandarizar la fase de planificación, asegurando que los trabajos de auditoría se desarrollen con base técnica sólida, enfoque estratégico y apego a los principios de calidad establecidos en las NOGAI.

Santiago de Chile, 2025

Daniela Caldana Fulss
Auditora General de Gobierno

I. INTRODUCCIÓN

El contenido de la guía se encentra alineado con las Normas Globales de Auditoría Interna (NOGAI), emitidas por *The Institute of Internal Auditors (IIA)*, en particular con las normas contenidas en el *Principio 13: Planificar eficazmente los trabajos*, perteneciente al *Dominio V: Desempeño de los Servicios de Auditoría Interna*. Estas normas constituyen el marco profesional obligatorio que rige la práctica de la auditoría interna, y orientan tanto la calidad técnica del trabajo como los estándares necesarios para garantizar su efectividad y valor agregado.

La guía tiene como propósito principal orientar metodológicamente el desarrollo de la fase de planificación para los trabajos de auditoría, asegurando que cada uno de ellos sea diseñado con suficiente profundidad técnica, enfoque estratégico y eficacia operativa. En esta fase, los auditores internos deben identificar los riesgos relevantes que afectan a la actividad bajo revisión, definir los objetivos, criterios y el alcance del trabajo, así como establecer en el programa las pruebas y procedimientos de auditoría necesarios para cumplir con los propósitos definidos.

El contenido de la guía se estructura en torno a los pasos esenciales para una planificación eficaz:

- El desarrollo de una comprensión inicial de la actividad bajo revisión.
- La identificación y evaluación de riesgos críticos y controles clave.
- La definición o redefinición de los objetivos y el alcance del trabajo.
- La definición de criterios de auditoría y selección de métodos.
- La estimación de recursos financieros, humanos y de tecnología.
- La elaboración del memorando de planificación, el programa de trabajo y el cronograma de ejecución.

Además, se incluyen anexos técnicos complementarios que proporcionan conceptos y herramientas de auditoría interna, tales como; tablas de evaluación de riesgos, fundamentos sobre riesgos de auditoría, técnicas de muestreo, clasificación de procedimientos, entre otros.

En síntesis, la guía busca fortalecer la calidad, trazabilidad y valor agregado de los servicios de auditoría interna en el sector público, consolidando un enfoque sistemático, transparente y basado en riesgos. Asimismo, proporciona criterios técnicos y directrices operativas para asegurar que los trabajos de auditoría estén enfocados en evaluar el gobierno (gobernanza), la gestión de riesgos y los controles institucionales.

Esta guía complementa las políticas y procedimientos aprobados por la función de auditoría interna para la planificación del trabajo. Su aplicación puede integrarse con la Planilla de Trazabilidad del Trabajo de Auditoría Interna, disponible en un archivo Excel del mismo nombre y descrita en los anexos de este documento.

Para mantener una visión integral del marco metodológico de auditoría interna y asegurar la trazabilidad del trabajo, se recomienda consultar y aplicar las Guías de Gestión y Servicios de Auditoría Interna emitidas por el CAIGG, las cuales abordan las distintas fases del proceso o ciclo de auditoría interna.

[1] La elaboración de este documento incorporó, en algunas secciones, el apoyo de herramientas de inteligencia artificial basadas en modelos de lenguaje natural para mejorar la redacción. Estas fueron utilizadas con criterio ético y bajo supervisión, manteniéndose los autores como responsables plenos de la exactitud y del contenido final.

II. OBJETIVO DEL DOCUMENTO

Establecer un marco técnico y metodológico para la planificación de los trabajos de aseguramiento y asesoramiento (en lo que corresponda). Su propósito es asegurar que el trabajo sea planificado con suficiencia técnica, con un enfoque basado en riesgos, y alineado con los objetivos de la actividad bajo revisión y de la entidad, de acuerdo con los principios y normas específicas de las Normas Globales de Auditoría Interna (NOGAI).

III. MARCO NORMATIVO DEFINIDO EN LAS NORMAS GLOBALES DE AUDITORÍA INTERNA

Una vez que el Jefe del Servicio aprueba el plan anual de auditoría interna, la función de auditoría debe aplicar un enfoque de planificación estructurado, sistemático y basado en riesgos. Este enfoque debe alinearse con las mejores prácticas profesionales y con lo establecido en las NOGAI, especialmente con las *Normas 13.1 a 13.6 del Principio 13*, que exigen una planificación eficaz del trabajo, y con la *Norma 14.6: Documentación de los trabajos*, que establece la obligación de documentar adecuadamente el desarrollo del trabajo en los papeles de trabajo.

De acuerdo con el glosario de las NOGAI, la planificación del trabajo se define como "*El proceso mediante el cual los auditores internos recopilan información, evalúan y priorizan los riesgos relevantes a la actividad bajo revisión, establecen los objetivos del trabajo y su alcance, identifican los criterios de evaluación, y crean el programa de trabajo específico de la actividad bajo revisión*."

Asimismo, las NOGAI definen trabajo como "*Una asignación de auditoría interna específica o proyecto que incluye múltiples tareas o actividades diseñadas para alcanzar un conjunto específico de objetivos relacionados. Véase también "Servicios de aseguramiento" y "Servicios de asesoramiento"*

En este contexto, el propósito de esta fase es asegurar que el trabajo sea diseñado de manera eficaz, con el fin de lograr los objetivos definidos, optimizando el uso de los recursos, respetando los plazos establecidos y cumpliendo con los estándares de calidad requeridos, permitiendo al auditor interno:

- Interactuar con los responsables de la actividad bajo revisión.
- Revisar documentación y normativa de procesos y áreas clave.
- Identificar y priorizar riesgos críticos y controles existentes.
- Definir o refinar los objetivos, alcance, criterios y metodología.
- Estimar y planificar recursos financieros, tecnológicos, humanos, así como el tiempo y la logística asociada al trabajo.
- Establecer los procedimientos y pruebas que permitirán obtener evidencia suficiente, fiable y relevante.

La planificación debe considerar no solo los aspectos operativos, sino también los factores estratégicos, normativos, estructurales, financieros, tecnológicos y de control interno, así como las condiciones del entorno externo e institucional en que opera la actividad bajo revisión y la entidad.

Requisitos fundamentales según las NOGAI

Conforme a las NOGAI, los principales requisitos de la planificación del trabajo incluyen:

- Comprender las expectativas iniciales del trabajo y los motivos de incluirlo en el Plan de Auditoría Interna.
- Evaluar los objetivos estratégicos, procesos críticos y riesgos significativos de la actividad bajo revisión.
- Analizar la gobernanza, la gestión de riesgos y los controles existentes, conforme a un enfoque basado en riesgos.
- Identificar oportunidades de mejora institucional, ineficiencias o deficiencias sistémicas.
- Documentar el entendimiento del contexto de la actividad (estructura organizacional, normativas aplicables, recursos involucrados, sistemas de información, registros clave, etc.).
- Alinear el trabajo con criterios técnicos y normativos relevantes, incluyendo marcos de control interno como *COSO, ISO 31000*, normativa presupuestaria, legal y regulatoria del sector público.
- Garantizar la suficiencia, competencia y asignación efectiva de recursos, acorde con la complejidad del trabajo.
- Elaborar un programa de trabajo formal y documentado, que defina procedimientos, responsables, pruebas de auditoría y estimación de tiempos.
- Establecer objetivos y alcances diferenciados para trabajos de aseguramiento y servicios de asesoramiento, de acuerdo con su naturaleza, propósito y expectativas.

Además, la planificación del trabajo debe adaptarse a las particularidades del sector público, integrando enfoques que permitan evaluar aspectos esenciales para la gobernanza pública, tales como:

- El cumplimiento de disposiciones legales, normativas y reglamentarias vigentes, incluyendo la probidad y transparencia.
- La economía, eficiencia y eficacia en la gestión de los recursos públicos.
- La responsabilidad fiscal y la transparencia en la administración y uso de los fondos públicos.

El programa de trabajo constituye el producto final de la fase de planificación. Este documento consolida los objetivos, el alcance, los riesgos evaluados, los criterios de evaluación y los procedimientos y pruebas necesarios para alcanzar los resultados esperados.

El programa de trabajo debe ser revisado y aprobado formalmente por el Jefe de Auditoría antes del inicio de su ejecución, y debe conservarse como parte integral de los papeles de trabajo. Cualquier modificación requerida durante su ejecución debe ser nuevamente aprobada, documentada y justificada, asegurando la trazabilidad, la supervisión continua y el cumplimiento de los requerimientos de calidad establecidos en las NOGAI.

IV. CONCEPTOS SOBRE LA PLANIFICACIÓN DEL TRABAJO DE AUDITORÍA INTERNA

La fase de planificación del trabajo constituye el eje estructural que determina la calidad, la pertinencia y la profundidad de todo el proceso de auditoría. Su objetivo primordial es diseñar un enfoque que se alinee inequívocamente con los objetivos del trabajo, que abarque los riesgos con mayor potencial de impacto y que se ejecute con la eficiencia operativa, la eficacia técnica y el rigor profesional exigidos por las NOGAI.

Si bien las directrices de las NOGAI ofrecen un marco común, la forma y el detalle de la planificación varían entre entidades públicas debido a múltiples condicionantes:

- El grado de madurez de la función de auditoría interna influye directamente en la forma en que se planifica el trabajo. Cuando se trata de una actividad a revisar recién instaurada, suele ser necesario dedicar más tiempo a comprender los procesos y levantar información básica, en contraste con otras más consolidadas que ya cuentan con antecedentes, documentación histórica y metodologías probadas previamente por la auditoría interna.

- La complejidad y criticidad de la actividad bajo revisión también son determinantes. No es lo mismo revisar una función de apoyo que revisar una actividad misional como por ejemplo la recaudación de impuestos o la distribución de beneficios sociales. En estos casos, tanto la cobertura como la profundidad del trabajo son mayores.

- La experiencia y especialización del equipo auditor permiten afinar los tiempos y enfoques. Cuando los auditores internos ya tienen conocimiento acumulado en temas como finanzas públicas, adquisiciones o ciberseguridad, pueden aplicar ese bagaje para planificar con mayor precisión y reducir tiempos de investigación inicial.

- También importa mucho la robustez del sistema de control interno. Entornos donde los controles están automatizados y bien documentados facilitan un enfoque de auditoría más centrado en pruebas de diseño y efectividad. En cambio, en contextos donde los procesos son manuales, fragmentados o poco formales, se requiere mayor esfuerzo y procedimientos más extensos para obtener evidencia válida.

- El marco normativo y regulatorio en el que opera la organización puede condicionar el trabajo. Existen leyes sectoriales, reglamentos emitidos por entes de control o estándares técnicos internacionales, como por ejemplo, los Requerimientos Temáticos del IIA, las Normas Internacionales de Contabilidad del Sector Público (IPSAS) o las Normas ISO de la Organización Internacional de Normalización, que establecen pruebas, formatos específicos de reporte y otras exigencias que el equipo de auditoría, según el caso, podría o debería incorporar desde la planificación.

- Las expectativas de los órganos de gobernanza también definen el nivel de detalle del plan. Si el Jefe de Servicio, la alta Dirección o una autoridad reguladora externa requiere información periódica o un nivel particular de granularidad, eso debe reflejarse en la estrategia y en la forma de planificar el trabajo y de comunicar los hallazgos.

- El uso de herramientas tecnológicas es otro factor clave. Cuando por ejemplo se cuenta con soluciones de analítica avanzada o automatización tales como *Robotic Process Automation (RPA), Data Analytics (DA)*, *Artificial Intelligence (AI),* es posible ampliar el universo de las pruebas, realizar revisiones continuas y reducir la dependencia de muestras manuales. Esto mejora la eficiencia y la cobertura del trabajo.

- El historial de hallazgos y observaciones de trabajos de auditoría anteriores también debe ser considerado. Si una actividad o área presenta reincidencias o ha recibido recomendaciones críticas en el pasado, es prudente ampliar el alcance del trabajo de auditoría actual y profundizar en las pruebas, si es el caso.

- Finalmente, es esencial que la función de auditoría interna se articule con las demás líneas de acción (ver Modelo de las Tres Líneas del IIA). Por ejemplo, coordinar con la Dirección Operativa y con los equipos de gestión de riesgos no solo evita duplicaciones innecesarias, sino que también fortalece la cobertura general y permite un uso más eficiente de los recursos disponibles.

V. MARCO METODOLÓGICO PARA LA PLANIFICACIÓN DEL TRABAJO DE AUDITORÍA INTERNA - PRINCIPALES PASOS

La planificación de un trabajo de auditoría interna se apoya en ocho pasos fundamentales que garantizan un enfoque sistemático, alineado con los riesgos clave y respaldado por altos estándares técnicos. Aunque estos pasos pueden presentarse de forma secuencial para su comprensión metodológica, en la práctica su aplicación es flexible e iterativa. Es común que algunos aspectos se revisen o ajusten a medida que se obtiene nueva información, cambian las condiciones del entorno o se detectan aspectos no considerados inicialmente.

El proceso comienza con la comprensión de la actividad que será objeto de revisión, conforme a lo indicado por la *Normas 13.1: Comunicación durante el trabajo y 13.2: Evaluación de riesgos del trabajo*. Esta etapa requiere recopilar información relevante sobre los objetivos estratégicos de la actividad bajo revisión, su estructura organizativa y los mecanismos de gobernanza, riesgo y control que existen. También es fundamental identificar a las partes interesadas, tanto internas como externas, y detectar cualquier restricción normativa, contractual u operativa que pueda condicionar el trabajo. Este conocimiento profundo del contexto no solo permite enfocar adecuadamente el trabajo, sino que también es clave para entender cómo y dónde pueden manifestarse los riesgos más relevantes.

Sobre esa base se construye la evaluación detallada de riesgos, tal como establece la *Norma 13.2: Evaluación de riesgos del trabajo*. Aquí se elabora o actualiza la matriz preliminar de riesgos y controles, integrando tanto los existentes como aquellos nuevos riesgos que puedan haber surgido por cambios operativos, tecnológicos o externos. La evaluación debe considerar la probabilidad y el impacto de cada riesgo, así como su alineación con el apetito institucional de riesgo. Además, es necesario detectar posibles brechas de control, eventos recientes que afecten la operación y otros elementos críticos que deban ser priorizados para asegurar un alcance del trabajo que sea realmente útil y pertinente.

Posteriormente, conforme a la *Norma 13.3: Objetivos y alcance del trabajo*, se establecen o ajustan los objetivos y el alcance del trabajo. Los objetivos deben seguir el principio *SMART*[2], es decir, ser específicos, medibles, alcanzables, relevantes y delimitados en el tiempo. Asimismo, es importante definir con claridad qué aspectos estarán incluidos o excluidos, de manera que el alcance sea transparente y esté alineado con las prioridades institucionales. Cualquier modificación o restricción significativa debe ser discutida y justificada ante el Jefe de Auditoría y/o el Supervisor, especialmente si afecta la cobertura inicialmente propuesta.

Una vez definidos los objetivos, el siguiente paso es identificar y validar los criterios de evaluación, según la *Norma 13.4: Criterios de evaluación*. Estos criterios constituyen la base sobre la cual se evaluará la información durante el trabajo. Pueden incluir normas internas, marcos regulatorios, políticas, procedimientos, contratos u otras referencias técnicas. La validación previa con la Dirección de la actividad bajo revisión es indispensable para asegurar que los criterios sean pertinentes, aceptados por ambas partes y aplicables al contexto del trabajo.

Con el enfoque definido, se procede a determinar los recursos necesarios, de acuerdo con la *Norma 13.5: Recursos del trabajo*. Esta fase implica estimar las horas de auditoría requeridas, identificar los perfiles técnicos adecuados para el equipo de trabajo, prever el uso de herramientas tecnológicas, como soluciones de análisis de datos o plataformas de monitoreo, y calcular el presupuesto operativo necesario. Dependiendo de los recursos disponibles y de la complejidad del trabajo, también puede considerarse la incorporación de expertos externos o personal especializado en áreas como ciberseguridad, tecnología u otras.

Toda esta información se consolida en el memorándum de planificación, que actúa como documento director del proceso. Este debe contener, de forma integrada, la descripción de la actividad bajo revisión, los riesgos identificados, los objetivos y el alcance del trabajo, los criterios de evaluación, la metodología elegida, los recursos asignados, así como un cronograma de ejecución claro y consistente con el alcance y los objetivos.

.

[2] Las siglas SMART representan las características que debe tener un objetivo bien formulado o una recomendación eficaz. Más adelante en la guía se explican en detalle.

También debe establecer mecanismos de coordinación con otras funciones de aseguramiento o líneas de acción internas. La aprobación formal del Jefe de Auditoría es un requisito indispensable antes de iniciar la fase de ejecución, en cumplimiento con lo dispuesto en las *Normas 13.3 a 13.6.*

Con el memorándum aprobado, se procede a formular el programa de trabajo, en línea con la *Norma 13.6: Programa de trabajo.* Esta herramienta operativa define con precisión los procedimientos y pruebas que se aplicarán: pruebas sobre el diseño y la efectividad de los controles, pruebas sustantivas, análisis de datos, procedimientos analíticos y los criterios de materialidad y muestreo, si es el caso. El programa también debe incluir hitos clave de calidad, validaciones parciales con la Dirección Operativa y mecanismos de supervisión técnica continua que aseguren la rigurosidad y trazabilidad del trabajo.

Finalmente, como paso complementario, se recomienda el desarrollo de una planilla de trazabilidad. Esta herramienta aporta valor durante todo el ciclo de planificación, ejecución, informe y seguimiento del trabajo, contribuyendo al cumplimiento de las disposiciones establecidas en los principios 11, 12, 13, 14 y 15.

Aunque su uso no es obligatorio, resulta especialmente valioso para aquellas funciones de auditoría interna que aún no disponen de un sistema de gestión integral para el ciclo de auditoría. Su implementación fortalece la trazabilidad del trabajo realizado, mejora la calidad del archivo de papeles de trabajo y facilita las revisiones internas o externas, incluyendo evaluaciones de calidad.

Estos pasos pueden aplicar tanto para servicios de aseguramiento como de asesoramiento. En **Anexo N° 1**. Se realiza una comparación entre ambos tipos de servicios, en relación con las normas y principios del *Dominio V: Desempeño de los servicios de Auditoría Interna.*

A continuación, se presenta gráficamente el marco de planificación del trabajo compuesto por ocho pasos principales. El esquema abarca desde la comprensión inicial de la actividad hasta la elaboración de una planilla de trazabilidad (complementaria), incluyendo la evaluación de riesgos, definición de objetivos, criterios de aseguramiento, asignación de recursos, formulación del memorándum y el programa de trabajo. Este enfoque integral busca asegurar que cada trabajo se planifique de manera estructurada, documentada y centrada en los riesgos críticos.

Esquema N° 1: Marco para la Planificación del Trabajo de Auditoría Interna - Principales Pasos

Fuente: Elaboración CAIGG

Paso N° 1

Desarrollar la Comprensión Inicial de la Actividad Bajo Revisión

1 Aspectos Generales de la Comprensión Inicial

a. Objetivo y alcance de la comprensión inicial

Un paso esencial en la planificación de cualquier trabajo de auditoría interna es el desarrollo de una comprensión integral de la actividad bajo revisión, conforme lo establece la *Norma 13.2: Evaluación de riesgos del trabajo*. Este paso constituye la base técnica que permite al equipo auditor alinear adecuadamente el enfoque, los objetivos, los criterios y el alcance del trabajo con el contexto y los riesgos reales de la actividad bajo revisión y de la entidad.

Esta comprensión requiere un análisis detallado de múltiples dimensiones, incluyendo las expectativas iniciales de los grupos de interés, los motivos que justifican el trabajo, y el entorno operativo, organizacional y normativo en el que se desarrolla. Es necesario identificar y analizar los objetivos estratégicos y operacionales, las técnicas de gestión, los indicadores de desempeño, así como la forma en que estos se integran con la gestión de riesgos y los controles clave existentes.

Además, el equipo auditor debe examinar aspectos específicos que influyen directamente en la efectividad del control interno, tales como la infraestructura tecnológica, los riesgos vinculados a tecnologías de la información, ciberseguridad y gestión de datos, así como los mecanismos de continuidad del negocio y recuperación ante desastres. También es importante considerar elementos relevantes de finanzas, contabilidad y control presupuestario, cuando estos forman parte de la actividad bajo revisión.

Una comprensión deficiente o superficial de la actividad puede debilitar el valor, la pertinencia y el impacto del trabajo, afectando la calidad de los hallazgos y conduciendo a una planificación incorrecta, pruebas inadecuadas o asignación ineficiente de recursos. Por ello, esta fase debe ser documentada rigurosamente como parte de los papeles de trabajo y formar la base del juicio profesional que sustenta las decisiones posteriores en el diseño del trabajo.

Esta fase de estudio y comprensión inicial no busca hacer una verificación en detalle, sino reunir y analizar la información clave que permita tener un panorama claro desde el comienzo del trabajo.

Lo primero es entender bien la estructura, las funciones, la normativa que aplica y los procesos de la actividad bajo revisión. Esto ayuda a ubicarse y conocer el funcionamiento en general de dicha actividad.

También es fundamental identificar los riesgos críticos y los controles que ya existen, para evaluarlos y determinar si son adecuados tanto en su diseño para en su aplicación. Revisar trabajos previos o hallazgos que aún no se resolvieron puede dar pistas útiles para esta tarea.

Con esa base, se pueden detectar áreas críticas que podrían requerir una revisión más profunda durante el trabajo. Al mismo tiempo, es buena idea empezar a generar contacto con los responsables operativos y con otras partes interesadas, para fomentar un ambiente de trabajo colaborativo.

Todo esto permite planificar mejor, usar los recursos de forma más eficiente y asegurar que los riesgos más relevantes estén cubiertos, en línea con los objetivos de la actividad bajo revisión y de la institución.

Temas Claves

- *Comprender a fondo la actividad bajo revisión alinea el enfoque y el alcance del trabajo con los riesgos reales.*
- *La comprensión inicial debe abarcar estrategias, procesos, controles, tecnología, riesgos críticos y antecedentes de trabajos de auditoría previas para garantizar una planificación rigurosa.*
- *Un análisis superficial reduce el valor del trabajo de auditoría; documentar la comprensión con rigor facilita asignar recursos adecuadamente y obtener hallazgos relevantes.*

b. Factores que influyen en la profundidad del análisis

La profundidad de la comprensión inicial dependerá de factores tales como:

- El tipo y complejidad del trabajo (aseguramiento, asesoramiento, combinado, seguimiento).
- La criticidad de la actividad bajo revisión en relación con los objetivos estratégicos institucionales.
- El nivel de conocimiento previo de la actividad bajo revisión por parte del equipo auditor.
- La disponibilidad, calidad y acceso a información relevante.
- La dispersión geográfica, volumen de operaciones o integración con otras unidades.

También incide si se trata de una actividad nueva a revisar o si ya ha sido objeto de trabajos recientes.

c. Elementos clave a considerar

Los auditores internos pueden analizar y revisar diversos documentos sobre la actividad bajo revisión para identificar sus objetivos estratégicos. Estos pueden incluir:

- **Mandato legal:** Para conocer las obligaciones de la actividad bajo revisión que debería estar estipuladas en los objetivos estratégicos.
- **Planes operativos**: Obtener información sobre las estrategias adoptadas por la actividad que se revisa para cumplir sus propósitos/objetivos.
- **Medidas y métricas**: Comprender cómo se supervisa el progreso y se mide el desempeño.
- **Organigrama**: Obtener la estructura general para entender cómo se interrelacionan las personas y las funciones, e identificar a los responsables de procesos específicos.
- **Mapas de procesos, matrices de riesgo o narrativas de procesos**: Obtener una visión general de los procesos y sus operaciones.
- **Descripciones de puestos**: Comprender en detalle las responsabilidades del personal.
- **Políticas y procedimientos clave**: Conocer los principios, valores y directrices que guían las decisiones y acciones.

En el caso que estén disponibles, se deben considerar si las autoevaluaciones de riesgo que hizo la actividad bajo revisión son confiables. No se trata solo de aceptar lo que el área reporta, sino de evaluar si esas autoevaluaciones reflejan la realidad.

También es importante revisar qué mecanismos existen para identificar, monitorear y manejar los riesgos y controles. Esto incluye determinar cómo se comunican internamente y si las acciones que toman son efectivas.

Otro punto para analizar y tener en cuenta son los eventos recientes que hayan tenido un impacto significativo. Estos pueden revelar fallas en los controles o riesgos que no estaban bien gestionados.

Además, se debe revisar la información del proceso de gestión de riesgos, tales como apetito y tolerancia al riesgo y la Matriz de Riesgos Estratégica de la institución u otras herramientas similares. Estas fuentes ayudan a tener una visión más completa del entorno de riesgos.

Si hay procesos interconectados o servicios de terceros involucrados, hay que evaluar los riesgos que puedan surgir de esas relaciones. No siempre están bajo el control directo de la actividad bajo revisión, pero de igual forma pueden tener un impacto importante.

Los auditores internos pueden obtener los objetivos estratégicos del propietario del proceso o de la persona responsable de la actividad que se revisa. En casos donde no existan objetivos escritos disponibles, los auditores internos deben mantener conversaciones con la Dirección para comprender lo que pretende lograr la Dirección.

Por supuesto que la cultura de la entidad y de la actividad bajo revisión también influyen. Una cultura que minimiza la visión de la gestión de los riesgos o evita reportarlos puede ser una señal de alerta.

Toda esta información debe quedar bien documentada en los papeles de trabajo. Esto sirve como respaldo de la planificación y como base para las decisiones que se tomen más adelante. También es útil para las evaluaciones interna y externa de calidad de la función de auditoría interna.

Temas Claves

- *La profundidad del análisis depende del tipo de trabajo, la criticidad, la experiencia del equipo, la calidad de los datos y la complejidad operativa o geográfica.*
- *El contexto previo varía según si la actividad se revisa por primera vez o ya fue examinada recientemente.*
- *Entre los aspectos a evaluar se debe considerar la fiabilidad de las autoevaluaciones de riesgo, la efectividad de los controles, los eventos recientes, la matriz de riesgos institucional, la dependencia de terceros y la cultura organizacional, dejando evidencia en los papeles de trabajo.*

d. Reunión de inicio

Como parte de la comprensión inicial de la actividad bajo revisión, y posterior a la notificación previa que realiza el Jefe de Auditoría, se debería realizar una reunión preliminar con los responsables operativos y otros actores clave. Para más detalles revisar la *Guía de Gestión y Servicios de Auditoría Interna (GGSAI) N° 6: Comunicación en Auditoría Interna y Formulación de Informes sobre Resultados del Trabajo.*

El propósito principal de esta reunión es presentar y discutir los objetivos, alcance, cronograma, requerimientos de información, entregables esperados y las expectativas de comunicación asociadas al trabajo, con el fin de asegurar que la Dirección Operativa comprenda claramente el enfoque de auditoría, recoger antecedentes relevantes para la planificación y facilitar los ajustes necesarios en caso de que surjan nuevas consideraciones o cambios en las condiciones del entorno evaluado. Esta instancia también permite establecer acuerdos sobre la frecuencia y modalidad de las comunicaciones futuras, así como identificar a los destinatarios de la comunicación final de resultados.

Esta instancia puede incluir entrevistas, reuniones formales o la aplicación de cuestionarios, y debe realizarse antes del inicio del trabajo de campo, especialmente si la ejecución puede interferir con las operaciones habituales de la actividad bajo revisión.

No obstante, en trabajos relacionados con temas confidenciales como investigaciones por fraude, denuncias o verificaciones sorpresivas, la comunicación previa y la reunión preliminar podrán omitirse, de acuerdo con el criterio del Jefe de Auditoría y conforme a los protocolos y procedimientos establecidos por la función de auditoría interna.

Durante la reunión de inicio se busca:

- Confirmar los objetivos, el alcance y el enfoque del trabajo.
- Coordinar tiempos, recursos y disponibilidad del personal.
- Detectar factores internos o externos que podrían afectar el trabajo.
- Acordar qué información se necesita de ambas partes.
- Definir puntos de contacto clave y su disponibilidad.
- Determinar qué documentos y registros se van a requerir.
- Identificar si se necesita acceso a instalaciones o sistemas específicos.

La información obtenida en esta reunión debe ser documentada y archivada como parte de los papeles de trabajo, y puede ser compartida con los miembros del equipo auditor para facilitar la planificación, ejecución y comunicación del trabajo

En determinados casos, esta reunión puede realizarse al inicio de la etapa de ejecución, especialmente si el trabajo involucra actividades ya revisadas recientemente o que mantienen condiciones operativas similares. En todos los casos, el juicio profesional del Supervisor y el equipo auditor debe guiar la decisión sobre su pertinencia, siempre que no se comprometa la independencia, objetividad ni el cumplimiento de los objetivos del trabajo.

Temas Claves

- *El propósito de la reunión de inicio es asegurar que la Dirección comprenda el enfoque de auditoría, recoger antecedentes para la planificación y acordar comunicaciones y necesidades de información antes del trabajo de campo.*
- *Entre los contenidos clave se encuentran: confirmar objetivos y alcance, coordinar recursos y tiempos, identificar factores críticos y puntos de contacto, y definir documentación, accesos y requerimientos.*
- *La reunión se realiza antes de la ejecución, salvo en trabajos de auditoría confidenciales (fraude, denuncias y otros similares) o cuando el juicio profesional indique que puede efectuarse al inicio del trabajo de campo, sin comprometer independencia, objetividad ni objetivos.*

e. Principales fuentes de información

Durante la fase de comprensión inicial de la actividad bajo revisión, los auditores internos deben obtener o actualizar información de antecedentes relevantes, con el fin de identificar riesgos clave, definir los objetivos, alcance y enfoque del trabajo, y anticipar posibles áreas críticas.

Mientras más compleja y extensa sea la actividad bajo revisión, mayor será la necesidad de contar con una perspectiva general y completa para planificar adecuadamente el trabajo de auditoría.

Algunas fuentes clave de información útiles para la comprensión inicial son:

Tabla N° 1: Fuentes de Información para la Comprensión Inicial de la Actividad Bajo Revisión

Fuente	¿Qué Aporta?	¿Para Qué Sirve?
Papeles de trabajos de auditoría previos	Objetivos, alcance, hallazgos y programas usados en auditorías anteriores.	Entender el contexto actual, detectar problemas repetidos, estimar tiempos y recursos.
Informes de resultados anteriores	Observaciones pasadas, impacto, y nivel de implementación de medidas correctivas.	Identificar riesgos persistentes y evaluar compromiso de la Dirección.
Seguimiento de medidas correctivas	Verificación de avances en soluciones aplicadas a problemas detectados anteriormente.	Evaluar si las acciones correctivas fueron efectivas y si hay mejora real.
Información organizacional	Estructura, funciones, responsabilidades, contactos clave, datos financieros, de cumplimiento o desempeño.	Contextualizar el entorno operativo y apoyar la evaluación inicial.
Marcos de gobernanza, riesgos y controles	Buenas prácticas y requerimientos de gestión de riesgos, gobernanza y control.	Evaluar madurez en gestión de riesgos y definir enfoques de auditoría (basados en guías del IIA u otras).

Temas Claves

- *Revisar papeles y resultados de trabajos anteriores para conocer hallazgos recurrentes y la efectividad de medidas correctivas.*
- *Verificar el avance de acciones implementadas para problemas previos, evaluando el grado de mejora alcanzado.*
- *Analizar información organizacional y de gobernanza (estructura, riesgos, controles, desempeño) para contextualizar y enfocar el trabajo.*

f. Procedimientos analíticos útiles para la comprensión inicial

Los procedimientos analíticos son una herramienta clave para que los auditores internos comprendan mejor la actividad que van a revisar. En esta etapa inicial, lo que se busca es observar, comparar y hacer conexiones entre distintos datos, ya sean financieros, operativos, técnicos o económicos, con la finalidad de detectar señales que puedan orientar el enfoque del trabajo. No solo ayudan a entender mejor la actividad bajo revisión, sino que también funcionan como una alerta temprana para decidir dónde vale la pena mirar más de cerca.

Este tipo de análisis puede mostrar situaciones que llaman la atención, como por ejemplo, cuando no hay diferencias donde sí se esperaban, o cuando las diferencias son inusuales, mucho mayores o menores en comparación con lo que se considera normal para la actividad bajo revisión o incluso con otras organizaciones.

Entre los análisis más comunes están las comparaciones de datos con años anteriores, los cruces con presupuestos o proyecciones, el estudio de relaciones entre datos financieros y no financieros o el análisis de tendencias y proyecciones.

También es útil comparar lo que ocurre en distintas unidades internas (benchmarking interno) o con datos de otras organizaciones del mismo sector público (benchmarking externo).

Estas herramientas ayudan a los auditores internos a identificar áreas que podrían requerir mayor revisión. Sin embargo, no todo hallazgo amerita profundización. Es necesario considerar su relevancia, la solidez del control interno, la confiabilidad de la información y la utilidad del análisis. Bajo condiciones normales, ciertos patrones deberían mantenerse estables; si surgen desviaciones, el auditor debe analizarlas, ya que podrían indicar desde errores menores hasta posibles irregularidades.

Temas Claves

- *Los procedimientos analíticos comparan datos financieros y operativos para detectar variaciones inusuales o tendencias anómalas.*
- *Incluyen comparaciones históricas, versus presupuesto, entre indicadores financieros y no financieros, y contra unidades internas o entidades del mismo sector.*
- *Cuando las relaciones esperadas no se mantienen, el auditor debe investigar la causa y decidir si es necesario aplicar pruebas adicionales, considerando, entre otros, la importancia del proceso, la solidez del control interno y la fiabilidad de la información.*

f.1. Algunos tipos de procedimientos analíticos

Sin perjuicio que existe una gran variedad, entre los procedimientos analíticos más útiles para aplicar en esta fase se encuentran los siguientes.

Tabla N° 2: Explicación de Procedimientos Analíticos

Procedimiento	¿En Qué Consiste?	¿Para Qué Sirve?
Análisis porcentual de estados contables	Expresar cada partida como porcentaje de un total relevante (por ejemplo, sobre ingresos o activos totales).	Identificar la composición de los estados financieros y detectar variaciones inusuales.
Análisis de ratios o coeficientes	Calcular indicadores financieros (liquidez, rotación, deudas) y no financieros.	Evaluar “salud financiera”, eficiencia operativa y detectar anomalías.
Análisis de tendencias	Comparar datos actuales con los de periodos anteriores.	Detectar patrones, desviaciones o cambios importantes en el tiempo.
Análisis comparativo con presupuestos	Contrastar resultados reales con presupuestos o proyecciones.	Medir el desempeño contra lo planificado y detectar desviaciones.
Benchmarking externo	Comparar el desempeño de la entidad con otras organizaciones similares o del mismo sector.	Evaluar posicionamiento, eficiencia y oportunidades de mejora respecto al entorno.
Benchmarking interno	Comparar resultados entre distintas áreas o unidades dentro de la misma organización.	Identificar buenas prácticas internas y áreas con bajo rendimiento.

En **Anexos N° 2 y 3** se describen mayores detalles sobre objetivos y procedimientos de auditoría.

Temas Claves

- *Los procedimientos analíticos abarcan análisis porcentual de estados, ratios financieros y no financieros, análisis de tendencias y comparaciones con presupuestos.*
- *El auditor utiliza benchmarking externo e interno para contrastar el desempeño con entidades comparables o con otras unidades de la misma organización.*
- *Estas técnicas permiten detectar desviaciones significativas y señalar áreas que requieren pruebas de auditoría adicionales.*

g. Síntesis de la comprensión inicial de la actividad bajo revisión

Cada trabajo de auditoría se enmarca en un contexto específico, con objetivos, riesgos y condiciones particulares. Por tanto, no existe un formato único para documentar la comprensión inicial de la actividad bajo revisión. Sin embargo, es altamente recomendable que el equipo auditor elabore y documente en sus procedimientos una estructura para formular una síntesis técnica que consolide los antecedentes relevantes, los riesgos identificados y los criterios utilizados para definir el alcance y los objetivos preliminares del trabajo.

Esta síntesis debe basarse en toda la información recopilada durante la etapa de análisis previo, incluyendo documentación institucional, entrevistas con responsables, resultados de procedimientos analíticos, evaluaciones previas, mapas de riesgos, indicadores de desempeño y cualquier otra fuente pertinente. Su propósito es sustentar técnicamente las decisiones tomadas, facilitar la trazabilidad del juicio profesional ejercido y proporcionar respaldo documental a la planificación del trabajo.

Si bien el contenido puede variar según la naturaleza del trabajo, se sugiere que esta síntesis contemple, al menos, los siguientes elementos:

- **Riesgos críticos y temas clave**: Identificación de los principales riesgos y justificación de su priorización, considerando su impacto potencial y la exposición residual.
- **Objetivos preliminares y alcance tentativo**: Definición inicial de los propósitos del trabajo y el perímetro previsto de revisión.
- **Metodologías previstas**: Técnicas que se planea aplicar (por ejemplo, análisis de datos, pruebas sustantivas, muestreo estadístico o no estadístico).
- **Controles clave y deficiencias potenciales**: Identificación de controles relevantes ya detectados o áreas con posibles debilidades que ameritan una evaluación más detallada.
- **Criterios para ajustar el enfoque o discontinuar el trabajo**: Factores técnicos o estratégicos que podrían justificar una modificación significativa del plan o la suspensión del trabajo.

Esta información debe formar parte de los papeles de trabajo y ser utilizada como insumo para las siguientes etapas. Además, si durante esta revisión preliminar se identifican deficiencias relevantes en la gobernanza, en el diseño o ejecución de controles clave, o en la gestión de riesgos, el equipo auditor debe informar de inmediato al Jefe de Auditoría. Este, a su vez, debe evaluar la necesidad de escalar la situación a la Alta Dirección o al Jefe de Servicio, en concordancia con lo establecido por la *Norma 11.1: Establecer relaciones y comunicarse con las partes interesadas.*

Adicionalmente, una comprensión integral de la actividad bajo revisión es esencial para asegurar la calidad del enfoque de auditoría. Esto implica entender los objetivos estratégicos de la actividad, su articulación con la gestión de riesgos, las métricas de desempeño asociadas, y los sistemas de gestión utilizados. También es fundamental incorporar una visión técnica de aspectos relevantes como tecnología de la información, ciberseguridad, continuidad operativa, recuperación ante desastres, aspectos financieros y contables, y otros riesgos comunes en procesos institucionales.

Una comprensión insuficiente puede comprometer el enfoque del trabajo, generar omisiones en el diseño de pruebas o derivar en una asignación inadecuada de recursos de auditoría. Por ello, esta etapa debe ser ejecutada con rigurosidad, metodología y documentación adecuada, asegurando su alineación con las NOGAI y los procedimientos aprobados en la función de auditoría interna.

Temas Claves

- *Elaborar una síntesis estructurada de la comprensión inicial que considere: riesgos clave, objetivos y alcance preliminar, metodologías y criterios para sustentar la planificación.*
- *Guardar esta síntesis en los papeles de trabajo como evidencia y trazabilidad de las decisiones.*
- *Comunicar de inmediato a la Dirección cualquier deficiencia de control o gestión de riesgos detectada en el estudio preliminar.*
- *Evaluar la necesidad de escalar la situación a la Alta Dirección o al Jefe de Servicio las deficiencias de control.*

Paso N° 2

Desarrollar una Evaluación de Riesgos en la Actividad Bajo Revisión

1 Aspectos Generales de la Evaluación de Riesgos en la Actividad Bajo Revisión

Entender y evaluar los riesgos es una parte central del trabajo de auditoría. Esta tarea se realiza en dos momentos clave.

- El primero ocurre durante la planificación anual de auditoría. En esa etapa se hace una evaluación de riesgos a nivel general, mirando toda la organización. El objetivo es identificar qué actividades críticas presentan mayor impacto y probabilidad de riesgo, y con eso definir qué actividades, procesos o áreas deben tener prioridad para la auditoría interna en el plan. Esta mirada estratégica permite enfocar los recursos en los temas más relevantes para la entidad.
- El segundo momento se da al comenzar cada trabajo específico. Ahí, el análisis es más profundo y se enfoca en los procesos o áreas puntuales que se van a revisar. Esta evaluación más detallada permite al equipo auditor interno definir con mayor precisión los objetivos del trabajo, el alcance, los criterios, y la metodología que se va a aplicar, todo basado en los riesgos críticos que se identifiquen en el trabajo, incluidos los riesgos de fraude.

Hacer esta evaluación a fondo ayuda no solo a diseñar procedimientos y pruebas más efectivos, sino también a asegurar que el trabajo sea útil, bien enfocado y alineado con lo que realmente importa en el contexto de la actividad a revisar.

Es posible que no se requieran evaluaciones de riesgos de la actividad bajo revisión para trabajos de asesoramiento. En tales casos, los papeles de trabajo deben describir adecuadamente el acuerdo de la función de auditoría interna con las partes interesadas relevantes.

2 Conceptos Generales sobre Gobierno, Riesgos y Controles desde la Perspectiva de la Auditoría Interna

La función de auditoría interna contribuye al logro de los objetivos organizacionales evaluando y mejorando los procesos de gobierno, gestión de riesgos y controles. Comprender estos elementos permite a la auditoría interna enfocar sus servicios con valor agregado y conforme a las NOGAI, especialmente las *Normas 9.1: Comprender los procesos de gobierno, gestión de riesgos y control y 13.2: Evaluación de riesgos del trabajo.*

a. Gobierno

Según el glosario de las NOGAI, el gobierno se define como:

“La combinación de procesos y estructuras implantados por el Consejo para informar, dirigir, gestionar y monitorear las actividades de la organización con el fin de lograr sus objetivos”

El gobierno o la gobernanza es un componente esencial de la planificación del trabajo, ya que influye directamente en cómo se gestionan los recursos, se toman decisiones estratégicas y se supervisan los riesgos y controles. Desde la perspectiva de la auditoría interna, una gobernanza sólida no solo favorece el cumplimiento normativo, sino que también incrementa la capacidad institucional para generar valor público, responder ante los ciudadanos y asegurar la sostenibilidad de los resultados.

Durante la fase de planificación, evaluar la gobernanza implica, entre otros:

- Analizar el rol y la eficacia de los órganos de Dirección y supervisión (por ejemplo, comités de auditoría, comités ejecutivos o autoridades superiores).
- Evaluar el cumplimiento de los principios éticos y valores organizacionales.
- Revisar la coherencia entre los objetivos institucionales y los mecanismos de monitoreo y control.
- Verificar la existencia de estructuras claras de rendición de cuentas y canales de comunicación interna y externa.
- Considerar el grado de madurez de la gestión de riesgos y controles como parte del marco de gobernanza, incluyendo el gobierno de TI.

Una adecuada revisión de los componentes de gobierno permite al auditor interno detectar deficiencias estructurales que pueden amplificar riesgos operativos, financieros o de cumplimiento, así como identificar oportunidades de mejora en liderazgo, transparencia y eficiencia institucional.

En definitiva, el análisis de la gobernanza proporciona una visión integral del entorno de control, facilitando que la auditoría interna focalice sus esfuerzos en procesos críticos y apoye a la entidad en el cumplimiento de su misión con integridad y eficacia.

a.1. Elementos claves del gobierno corporativo o gobernanza en el sector público

En consideración a que no existe una definición de gobierno corporativo que pueda aplicarse a todas las instituciones públicas y en todo contexto de igual forma, se puede considerar que el gobierno corporativo en el sector público, es más bien un conjunto de estructuras, normativas, prácticas y mecanismos, que dependen de una serie de condiciones propias de cada institución, entre otras; la estructura, la misión, los objetivos y el tamaño, las que tienen como objetivo alcanzar los resultados previstos para las partes interesadas y los usuarios y beneficiarios de los productos y servicios.

Entre los procesos y estructuras comunes que se identifican y destacan en las definiciones de gobierno corporativo para entidades del sector público, y que se puede adecuar a la realidad nacional, se encuentran los siguientes:

- **Estructura, roles y responsabilidades del órgano de gobierno**

  - Diseño de roles y responsabilidades organizacionales.
  - Funcionamiento y coordinación entre los órganos de gobernanza.

- **Evaluación y control de gestión**

  - Estrategia y políticas corporativas institucionales relacionadas, y toma de decisiones. (Definiciones estratégicas, Indicadores de desempeño y Balance de Gestión Integral - BGI).
  - Mecanismos de incentivo de remuneraciones (Programa de Mejoramiento de la Gestión, Metas de Eficiencia Institucional, Convenios de Desempeño Colectivo, Convenios de Desempeño Individual y Leyes específicas).
  - Proceso formulación, ejecución y control presupuestario.

- **Ética y valores organizacionales**

  - Probidad/Anticorrupción.
  - Transparencia.
  - Cumplimiento legal y regulatorio.
  - Sistemas de integridad.
  - Cultura organizacional, otros

- **Gestión del desempeño y rendición de cuentas (*accountability*).**
- **Monitoreo y vigilancia del control y la gestión de riesgos.**
- **Comunicación de riesgos y controles a las áreas adecuadas.**
- **Gobierno de TI.**

Estas estructuras, procesos, normativas prácticas y mecanismos pueden conformar un marco de referencia para las instituciones públicas, con el fin de que logren identificar y definir sus propios elementos claves de gobierno corporativo en un próximo paso.

Para más detalle sobre esta materia, se debe revisar el *Documento Técnico N° 111: Conceptos y Elementos Claves de la Naturaleza del Trabajo de Auditoría Interna: Gobierno Corporativo, Gestión de Riesgos y Control en el Sector Público,* emitido por el CAIGG.

Temas Claves

- *Una gobernanza sólida es la base para planificar y fijar el tono ético.*
- *El nivel de madurez de riesgos/controle define prioridades y profundidad de pruebas.*
- *Una adecuada revisión de los componentes de gobierno permite al auditor interno detectar deficiencias estructurales.*
- *El gobierno corporativo en el sector público es más bien un conjunto de estructuras, normativas, prácticas y mecanismos, que dependen de una serie de condiciones propias de cada institución.*

b. Gestión de riesgos

El análisis del riesgo es fundamental para definir dónde se deben enfocar los recursos de auditoría, qué procesos requieren mayor profundidad de revisión, y cómo adaptar el alcance del trabajo a las condiciones específicas de la actividad bajo revisión. La correcta identificación y evaluación del riesgo permite priorizar las áreas con mayor exposición y orientar el trabajo hacia donde pueda agregar más valor.

En este contexto, el glosario de las NOGAI define los siguientes términos como se señala a continuación:

Riesgo:

“El efecto positivo o negativo de la incertidumbre sobre los objetivos.”

Gestión de riesgos:

“Un proceso para identificar, evaluar, tratar y controlar potenciales eventos o situaciones, con el fin de proporcionar un aseguramiento razonable respecto del logro de los objetivos de la organización.”

Evaluación de riesgos:

“La identificación y análisis de los riesgos que son relevantes para el logro de los objetivos de la organización. La importancia de los riesgos normalmente se valora en términos de impacto y probabilidad.”

Riesgo inherente:

“La combinación de factores internos y externos de riesgo que existen ante la ausencia de cualquier medida de gestión.”

Riesgo residual:

“La parte del riesgo inherente que permanece después de la implementación de las medidas de gestión.”

Probabilidad:

"La posibilidad de que pueda ocurrir un determinado evento."

Impacto:

"El resultado o efecto de un evento. Dicho evento puede tener un efecto positivo o negativo con relación a la estrategia u objetivos de negocio de la organización."

Apetito de riesgo:

"Los tipos y la cantidad de riesgo que la organización está dispuesta a aceptar al perseguir sus estrategias y objetivos."

Tolerancia al riesgo:

"Variaciones aceptables en el desempeño con relación al logro de los objetivos."

En **Anexo N° 4** se describen con mayor detalle conceptos sobre Apetito de Riesgo y Tolerancia de Riesgo.

b.1. Definir y clasificar los riesgos identificados

Durante la evaluación de riesgos, el auditor interno debe definir y clasificar cada riesgo identificado utilizando un lenguaje alineado con la cultura organizacional y comprensible para quienes ejecutan los procesos. La definición del riesgo debe ser clara y estructurada, comúnmente en términos de causa y efecto.

Una vez definidos, los riesgos deben clasificarse en categorías para asegurar coherencia en su análisis y seguimiento. Si la entidad pública ya emplea un marco de gestión de riesgos, el auditor interno debe conocer y entender el apetito de riesgo, la tolerancia al riesgo, y las categorías de riesgos y controles. En ausencia de un marco, pueden usarse, previo acuerdo con la Alta Dirección y el Jefe de Servicio, las categorías estándar descritas en este documento en los **Anexos N° 5 y 6.**

Cada categoría debe considerar amenazas tanto internas como externas, y los riesgos deben vincularse directamente con los objetivos organizacionales. Esta clasificación se consolida en un inventario o universo de riesgos.

Es fundamental validar el lenguaje del riesgo con los responsables operativos, asegurando que la terminología sea coherente, comprensible y útil para la gestión eficaz del riesgo.

En el contexto del sector público, la clasificación de los riesgos identificados por la auditoría interna debe considerar que ciertas categorías, como el riesgo de cumplimiento, poseen una naturaleza legal jerárquicamente superior, ya que emanan del mandato de legalidad que rige a los órganos públicos. Esto implica que no todos los riesgos pueden ser valorados o tratados con el mismo criterio literal de severidad operacional, como se muestra en las matrices tradicionales.

El riesgo de incumplimiento normativo tiene una connotación particular en el ámbito estatal, ya que su materialización puede derivar en responsabilidades administrativas, civiles o incluso penales, además de sanciones o pérdida de fondos públicos. Por ello, durante la evaluación de riesgos, el auditor interno debe clasificar cada riesgo con un enfoque que respete la estructura legal obligatoria del sector público, priorizando aquellos que comprometan el cumplimiento normativo, que además deberían tener una tolerancia cero o cercana a cero.

Si bien se pueden utilizar categorías estándar como riesgos estratégicos, operativos, financieros o reputacionales, el tratamiento del riesgo en entidades públicas exige validar estas categorías con base en los marcos legales aplicables, y no solamente en el impacto técnico o financiero. Sin perjuicio de lo anterior, desde la perspectiva global de auditoría interna los tipos de riesgo más comunes incluyen:

Tabla N°3: Descripción de Tipos de Riesgos Globales

Tipo de Riesgo	Descripción	Causas Comunes	Consecuencias Potenciales	Ejemplos
Estratégico	Riesgos que afectan los objetivos institucionales de largo plazo y la misión de la entidad.	Planificación deficiente, decisiones mal fundamentadas, cambios externos.	Desalineación con la misión, pérdida de Dirección estratégica, incumplimiento del mandato.	Abandonar proyectos clave sin justificación; metas institucionales no cumplidas.
Operativo	Fallas en procesos internos, sistemas, o ejecución de tareas.	Procesos mal definidos, falta de capacitación, fallas tecnológicas.	Ineficiencia, errores recurrentes, interrupciones en los servicios.	Retrasos en pagos, errores en atención ciudadana, fallas en sistemas de TI.
Cumplimiento	Incumplimiento de leyes, reglamentos, normativas o políticas internas.	Desconocimiento normativo, controles débiles, falta de supervisión.	Multas, sanciones legales, procesos sumariales.	No aplicar normativa para asignación de subsidios; no cumplir con requisitos de contratación pública.
Financiero	Errores, omisiones o irregularidades en la información o gestión financiera.	Controles contables débiles, presupuestos mal gestionados, falta de monitoreo.	Información inexacta, uso indebido de recursos, pérdida de recursos públicos.	Cierre contable con cifras erróneas; desvío de fondos presupuestarios.
Reputacional	Daño a la imagen pública o confianza ciudadana por decisiones o fallas internas.	Escasa transparencia, atención deficiente, crisis mal gestionadas.	Pérdida de legitimidad institucional, escrutinio público, crisis de confianza.	Denuncias en medios; atención deficiente a usuarios; conflictos mal comunicados.
De fraude	Actos intencionados para obtener beneficios indebidos u ocultar información.	Oportunidad sin controles, presión por resultados, ética debilitada.	Pérdida económica, consecuencias legales, daño institucional, procesos sumariales.	Manipulación de licitaciones, falsificación de documentos, desvío de fondos.

Al momento de planificar un trabajo, es importante diferenciar entre dos tipos de riesgos.

- El riesgo inherente que es el riesgo propio de la actividad que se va a revisar. Es decir, es el nivel de riesgo que existe antes de aplicar cualquier tipo de control. Este riesgo depende de factores como la naturaleza del proceso, cuántas transacciones se manejan, qué tan complejo es, cuánto interviene el juicio humano y qué tan expuesto está a errores o fraudes.

- Por otro lado, está el riesgo residual o exposición al riesgo, que es lo que queda después de aplicar los controles mitigantes existentes. En este caso, se considera si existen mecanismos de prevención, detección o corrección, y si estos están funcionando como deberían.

Cuando se trabaja con un enfoque basado en riesgos, no basta con hacer una evaluación técnica. También es necesario que el auditor interno documente su propio juicio profesional, considerando no solo el nivel de exposición, sino también el impacto que podría tener en la actividad bajo revisión y en la entidad, la sensibilidad social y el contexto en el que opera la actividad bajo revisión.

Temas Claves

- *El análisis de riesgos orienta el uso eficiente de recursos en el trabajo.*
- *Definir y clasificar los riesgos en categorías uniformes mejora la comunicación y el monitoreo.*
- *Diferenciar riesgo inherente y residual asegura una cobertura adecuada del trabajo.*

c. Control

El glosario de las NOGAI define **control** como:

"Cualquier medida que tome la Dirección, el Consejo y otras partes para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos."

Los controles son los mecanismos fundamentales mediante los cuales una entidad responde a los riesgos que enfrenta. Para el auditor interno, el análisis de controles no debe limitarse a su existencia en papel, sino que debe considerar:

- **Diseño:** ¿Está bien formulado el control para mitigar el riesgo? ¿Es lógico, oportuno, específico y coherente con el proceso?
- **Implementación y funcionamiento:** ¿Está el control en operación? ¿Se aplica de forma constante y de acuerdo con el diseño? ¿Se documenta su ejecución?

Los controles operativos relacionados con la mitigación del riesgo más conocidos incluyen:

- **Preventivos:** Evitan que ocurra el riesgo (ej. límites de aprobación, validación de datos, firma dual).
- **Detectivos:** Identifican la ocurrencia del riesgo tras su manifestación (ej. conciliaciones, alertas, análisis de excepciones).
- **Correctivos:** Restauran condiciones normales o eliminan impactos (ej. recuperación de pagos, medidas disciplinarias).

También se clasifican como automáticos (integrados en sistemas), manuales (realizados por personas), o híbridos (combinación). La auditoría interna debe validar no solo su existencia, sino su efectividad en la operación para mitigar los riesgos.

Temas Claves

- *El propósito del control es constituirse en una herramienta concreta para gestionar riesgos y cumplir objetivos, ajustada al apetito de riesgo.*
- *La evaluación de auditoría interna implica revisar diseño y operación real del control para confirmar eficacia y sostenibilidad.*
- *Los tipos y clasificación del control incluyen preventivos, detectivos, o correctivos; automáticos, manuales o híbridos, según tecnología y juicio humano.*

d. Tipología de controles relevantes para la planificación del trabajo

Al momento de planificar un trabajo, no basta con identificar si existen controles: también hay que entender qué tipo de controles son, cómo funcionan y en qué contexto operan. Algunos controles tienen un rol más estratégico, otros son operativos o de respaldo, y su revisión ayuda a enfocar mejor el trabajo y aplicar un enfoque basado en riesgos de forma más eficaz.

d.1. Control clave

Una actividad diseñada para reducir el riesgo asociado a un objetivo crítico del negocio. En el sector público se puede utilizar un lenguaje más acorde con la misión y la gestión institucional para referirse al término “negocio”, por ejemplo: objetivo crítico institucional / Objetivo misional.

Ejemplo: Verificación automatizada de requisitos y antecedentes del beneficiario antes de aprobar el subsidio → Asegura que solo personas o entidades elegibles accedan a recursos públicos.

d.2. Control secundario

Una actividad diseñada para reducir riesgos asociados a objetivos del negocio que no son críticos para la supervivencia o el éxito de la organización, o bien, para funcionar como respaldo de un control clave.

Ejemplo: Revisión aleatoria de rendiciones de bajo monto una vez al año → No sustituye el control obligatorio en rendiciones de alto riesgo, pero agrega una capa adicional de revisión.

d.3. Controles de nivel superior

Estos controles los ejerce la Alta Dirección o instancias de gobernanza, y cumplen una función más estratégica que operativa. Están pensados para supervisar transversalmente el funcionamiento general de la organización y detectar desvíos importantes antes de que se conviertan en problemas.

Algunos ejemplos son:

- Reuniones ejecutivas donde se revisan periódicamente los resultados clave.
- Informes consolidados de monitoreo de procesos críticos.
- Evaluaciones realizadas por comités de auditoría o de riesgos.

Ejemplo: El comité de riesgos institucional revisa mensualmente un tablero con indicadores clave (*KPI*) de todos los departamentos. Si detecta desviaciones en presupuestos, cumplimiento normativo o incidentes operativos, exige explicaciones y propuesta de corrección formales. Este tipo de control permite anticipar problemas antes de que escalen, fortalece la cultura organizacional de control y mejora la capacidad de respuesta.

d.4. Controles compensatorios

Son mecanismos que no eliminan el riesgo directamente, pero ayudan a reducirlo cuando un control clave está ausente, es débil o no se puede aplicar. Pueden ser soluciones temporales o permanentes, siempre que mantengan el riesgo en niveles aceptables.

Para que un control compensatorio sea válido, la función de auditoría interna debe verificar que:

- Reduce la exposición al riesgo de forma aceptable, según el umbral definido por la entidad.
- Cumple, al menos en parte, la función del control principal que falta.
- Está bien documentado y se revisa periódicamente para asegurarse de que funciona.

Desde el punto de vista de auditoría interna, si se detecta que falta un control clave, se deben identificar y probar los controles compensatorios disponibles. Según sus resultados, se ajusta la valoración del riesgo residual.

Ejemplo: En una entidad pequeña, donde no es posible separar las funciones de autorización y registro de pagos por falta de personal, el jefe del área que no participa en la preparación de pagos revisa semanalmente los desembolsos, analiza la documentación de respaldo y firma un acta como evidencia. Aunque este control no elimina el riesgo de fraude, lo reduce al incorporar una revisión independiente.

d.5. Controles con diseño adecuado

Son controles bien estructurados, con funciones claras y responsables definidos. Tienen una frecuencia de aplicación establecida y tienen evidencia sistemática de que realmente se están ejecutando. Además, están directamente relacionados con los riesgos que buscan controlar y responden a una lógica operativa coherente.

Ejemplo: En el proceso de rendición de viáticos y pasajes, puede haber un procedimiento formal que exija presentar los comprobantes originales, la firma del jefe directo y una revisión por parte de finanzas dentro de un plazo de cinco días. Si además el sistema registra todo electrónicamente y emite alertas cuando se incumplen los plazos, se trata de un control con buen diseño; ya que está documentado, tiene responsables asignados, parte del proceso está automatizado y existe supervisión efectiva.

Controles como este son más fáciles de evaluar. Al estar bien definidos, permiten hacer pruebas precisas y emitir una opinión técnica sólida. Por eso, son importantes de incluir en el programa de trabajo cuando se busca validar si el sistema de control interno es realmente efectivo.

d.6. Controles afectados por cambios recientes

Este tipo de controles pueden haber perdido efectividad por modificaciones en su entorno interno o externo. Los motivos más comunes son:

- Cambios en los sistemas de información.
- Reestructuraciones organizacionales.
- Cambios en normativas o en procedimientos internos.

Ejemplo: Si se implementa un nuevo sistema de gestión documental y no se replican correctamente los permisos de acceso desde el sistema anterior, puede pasar que ciertos usuarios tengan acceso a información sin los mismos controles que antes. Esto genera una exposición que antes no existía y que puede no estar bien cubierta.

En estos casos, es necesario revisar el control en detalle. Los cambios pueden haber creado brechas o debilitado el control sin que nadie lo haya notado. Por eso, requieren atención especial para evitar exposiciones imprevistas y asegurar que el sistema de control sigue siendo efectivo frente a las nuevas condiciones.

d.7. Controles a nivel de entidad

Estos pueden dividirse en dos categorías:

- **Controles de gobernanza** y
- **Controles de supervisión de la gestión**.

Los controles de gobernanza son establecidos por el Jefe de Servicio y la Alta Dirección con el fin de instaurar la cultura de control de la organización y proporcionar orientación que respalde los objetivos estratégicos.

Los controles de supervisión de la gestión son establecidos por la Dirección en las unidades de negocio y niveles operativos de la organización, con el objetivo de reducir riesgos en dichas unidades y aumentar la probabilidad de que se logren sus objetivos.

d.8. Controles en distintos niveles organizacionales

- **Control a Nivel de Entidad (*Entity-Level Control*)**

Un control que opera en toda la entidad y, por tanto, no está limitado ni asociado a procesos individuales.

Ejemplo: El establecimiento de un Código de Ética Institucional aprobado por el Jefe de Servicio, obligatorio para todos los funcionarios públicos de la entidad.

- **Control a Nivel de Proceso (*Process-Level Control*)**

Una actividad que opera dentro de un proceso específico, con el propósito de alcanzar objetivos propios de ese proceso.

Ejemplo: Un procedimiento formal para la revisión y aprobación de solicitudes de subsidios sociales, incluyendo pasos definidos, roles, plazos y documentación requerida.

- **Control a Nivel de Transacción (*Transaction-Level Control*)**

Una actividad que reduce el riesgo asociado a un conjunto o variedad de tareas operativas o transacciones específicas dentro de una organización.

Ejemplo: La verificación automática de la identidad del beneficiario antes de emitir el pago de un subsidio mediante cruce de datos con el registro civil.

d.9. Clasificación simultánea de controles

Un mismo control puede pertenecer simultáneamente a varias categorías dependiendo de su naturaleza y función. Por ejemplo, un control puede ser a la vez:

- Un control a nivel de entidad,
- Un control clave (por su impacto en la mitigación de un riesgo crítico), y
- Un control de tipo detectivo (su función es Identificar la ocurrencia del riesgo tras su manifestación).

Sin embargo, otras combinaciones no son compatibles. Por ejemplo, un control no puede ser al mismo tiempo clave, de nivel de entidad y secundario o de transacción, ya que estas últimas categorías responden a niveles de relevancia y alcance distintos.

Aunque estas clasificaciones pueden resultar complejas, con la práctica y el análisis de controles en los procesos se adquiere una mejor comprensión de cómo interactúan y se superponen estas categorías.

Temas Claves

- *Los controles claves reducen el riesgo asociado a un objetivo crítico.*
- *Los controles secundarios reducen los riesgos asociados a objetivos del negocio que no son críticos*
- *Los controles de nivel superior implican supervisión estratégica (comités, KPIs) que alerta desvíos a tiempo.*
- *Los controles compensatorios suplen controles clave ausentes; deben reducir el riesgo a un nivel aceptable y ser monitoreados.*
- *Los controles son sensibles al diseño o a cambio. Los bien diseñados facilitan pruebas sólidas; los recién modificados pueden abrir brechas y exigen revisión prioritaria.*

3 Modelo de las Tres Líneas del IIA

El Modelo de las Tres Líneas del Instituto de *The Institute of Internal Auditors (IIA)*, que fue actualizado en 2020, proporciona un marco de referencia para definir las responsabilidades en materia de gobernanza, gestión de riesgos y control interno. Este modelo resulta especialmente útil durante la fase de planificación del trabajo, ya que permite identificar en términos conceptuales y estandarizados los actores responsables, las fuentes de información y los niveles de control en la actividad bajo revisión.

En este modelo, los roles y responsabilidades se distribuyen de la siguiente manera:

a. Primera línea: gestión operativa

Es responsable directa de la gestión de riesgos y del diseño, implementación y mantenimiento de los controles internos en sus áreas de responsabilidad. Incluye supervisores, coordinadores de procesos, jefes de unidad, entre otros.

- Ejecutan actividades que afectan directamente la consecución de los objetivos estratégicos y operativos.
- Deben ser capaces de identificar, evaluar y mitigar los riesgos en tiempo real.
- Representan la fuente primaria de información para la planificación del trabajo de auditoría.

b. Segunda línea: funciones de control y supervisión

Incluye funciones como gestión de riesgos, cumplimiento normativo, control financiero, calidad y otras áreas técnicas que desarrollan políticas, metodologías y realizan monitoreo independiente del diseño y desempeño de los controles.

- Evalúan la efectividad de los controles implementados por la primera línea.
- Proveen herramientas, formación y asesoramiento para mejorar la gestión de riesgos.
- Son una fuente clave de información para la identificación de riesgos sistémicos, normativos y de cumplimiento.

c. Tercera línea: auditoría interna

Proporciona aseguramiento independiente y objetivo al Jefe de Servicio y a la Alta Dirección respecto de la eficacia de la gobernanza, la gestión de riesgos y los controles.

- Evalúa de manera integral la eficacia del diseño, implementación y funcionamiento de los controles de ambas líneas anteriores.
- Informa sobre deficiencias y propone recomendaciones para mejorar los procesos de gestión y control.
- Aporta una visión estratégica sobre la adecuación del marco de control interno respecto de los objetivos institucionales.

Durante la planificación del trabajo, es fundamental mapear claramente las responsabilidades de cada línea, identificar su grado de madurez y su nivel de coordinación. Esta comprensión contribuye a establecer el enfoque metodológico más adecuado, determinar la profundidad de las pruebas, seleccionar las fuentes de información más relevantes y definir las actividades de verificación correspondientes.

Este modelo también sirve de base para justificar el enfoque basado en riesgos y la selección de procedimientos según la robustez del sistema de control vigente. Además, contribuye al fortalecimiento de la cultura de control y la mejora continua en la entidad.

El Modelo de las Tres Líneas del IIA aplicado al sector público distribuye la responsabilidad sobre la gestión de riesgos y el control interno de la siguiente manera:

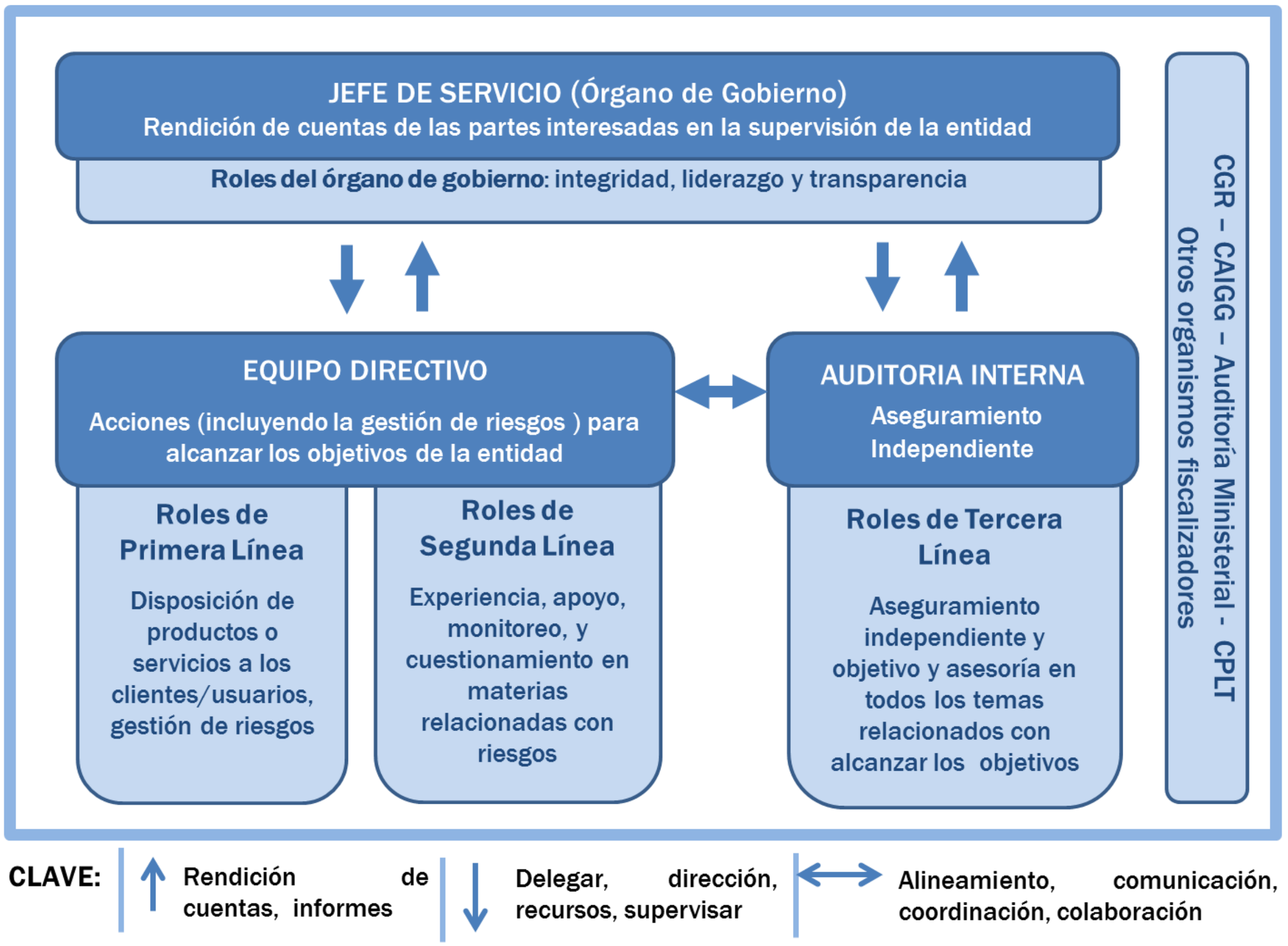
- El órgano de gobierno, en el caso corresponde al Jefe de Servicio, un consejo o directorio. Este define la estrategia, fija el apetito y tolerancia al riesgo, y exige rendición de cuentas y transparencia. Recibe informes tanto de la gestión como de la función de auditoría interna y emite directrices para la entidad.

- La gestión se divide en dos líneas. La primera línea reúne a las áreas operativas que prestan servicios al ciudadano y controlan los riesgos inherentes a sus procesos. La segunda línea está formada por unidades de apoyo especializadas, por ejemplo; cumplimiento normativo, finanzas, gestión de riesgos, tecnología, que aportan metodología, monitoreo y asesoría sobre riesgos, sin sustituir a la primera línea.

- La función de auditoría interna constituye la tercera línea. El Jefe de Auditoría y su equipo proporcionan aseguramiento y asesoramiento independientes y objetivos acerca de la gobernanza, los riesgos y los controles. Reportan funcionalmente al órgano de gobierno y cooperan con la gestión sin asumir responsabilidades ejecutivas.

- Fuera del esquema interno se ubican los organismos de fiscalización externa, como la Contraloría General de la República (CGR), CAIGG, auditorías ministeriales, etc. En general estos verifican el cumplimiento legal, la probidad y la transparencia, y sus observaciones retroalimentan el sistema de control interno, reforzando la confianza ciudadana.

Esquema N° 2: Modelo de las Tres Líneas del IIA Adaptado para el Sector Público



Fuente: Adaptación del Modelo de las Tres Líneas del IIA 2020. Una actualización de las Tres Líneas de Defensa, publicado por *The Institute of Internal Auditors (IIA).*

Temas Claves

- *El Modelo de las Tres Líneas del IIA, es un marco de referencia global para definir las responsabilidades en materia de gobernanza, gestión de riesgos y control interno.*
- *El Modelo considera: 1.ª línea gestiona y ejecuta controles, 2.ª línea supervisa y asesora, 3.ª línea (función de auditoría interna) entrega aseguramiento y asesoramiento de forma objetiva e independiente.*
- *La tercera línea proporciona servicios de auditoría al Jefe de Servicio y a la Alta Dirección respecto de la eficacia de la gobernanza, la gestión de riesgos y los controles.*

4 Relación entre Gobierno, Gestión de Riesgos, Control en la Planificación del Trabajo

Una buena planificación en auditoría no se trata solo de definir qué se va a revisar, sino de construir una lógica clara entre tres elementos clave: la gobernanza institucional, los riesgos críticos y los controles claves. Esta conexión es la base del enfoque basado en riesgos, tal como lo plantea el *Principio 13: "Planificar eficazmente los trabajos".*

Este análisis integrado le permite al auditor interno tomar decisiones más informadas y enfocadas. Por ejemplo, puede priorizar aquellas áreas donde hay un alto riesgo inherente y, además, faltan controles efectivos. Son justamente esos procesos los que presentan mayor exposición y donde la auditoría interna puede generar más valor con su análisis de causa raíz y sus recomendaciones.

También le permite evaluar si los controles clave en procesos sensibles están bien diseñados y funcionando correctamente, lo que es especialmente importante si se va a usar el riesgo residual como criterio para definir el alcance del trabajo.

Otra ventaja de este análisis es que ayuda a detectar brechas: controles obsoletos, áreas no cubiertas o mecanismos que ya no responden al contexto actual. Todos estos hallazgos pueden llevar a ajustar la metodología o ampliar el nivel de pruebas planificadas.

Durante la etapa de planificación, esta lógica se estructura y documenta conforme al procedimiento establecido para la planificación del trabajo, utilizando para ello registros tales como:

- La Matriz Preliminar de Riesgos y Controles (también llamada Matriz de Planificación de Riesgos y Controles). Incluye la priorización por exposición al riesgo, que ordena los focos de atención según su nivel de exposición. Considera los riesgos de negocio y los de fraude.
- El Mapa de Riesgos de la actividad que se va a revisar.
- Las fichas de documentación de objetivos críticos, que ayudan a enfocar el trabajo.

Es fundamental que el auditor interno deje claro, en los papeles de trabajo, por qué tomó determinadas decisiones, como por ejemplo: por qué se priorizó en base al riesgo inherente, si usó o no el riesgo residual como criterio, y qué controles clave serán revisados específicamente en terreno. Este razonamiento documentado asegura la trazabilidad técnica, cumple con las normas específicas y mantiene coherencia con el enfoque general de auditoría adoptado para el trabajo.

a. Desarrollo de la evaluación detallada de riesgos del trabajo

El Jefe de Auditoría es quien define el enfoque que se va a usar para identificar los riesgos críticos en un trabajo específico. Esta evaluación debe tener en cuenta tanto información cualitativa como cuantitativa, y también considerar cómo la propia Dirección evalúa el avance hacia sus objetivos. No se trata solo de identificar riesgos, sino de entender el contexto en el que se generan y cómo podrían afectar el cumplimiento de los objetivos y metas.

Existen varios enfoques para identificar riesgos, y cada uno se ajusta mejor a distintos niveles o tipos de trabajo:

- **Enfoque específico por actividad (*Bottom-Up*)**

Parte desde el nivel más operativo. Se identifican los riesgos de la actividad que se va a revisar a partir del conocimiento detallado de sus procesos y objetivos. Para ello, se realiza un levantamiento directo con la Dirección, conversando sobre los objetivos que persigue y los desafíos que enfrenta. Posteriormente, se asignan niveles de riesgo según su impacto y probabilidad, permitiendo priorizar donde las debilidades operativas pueden generar consecuencias significativas. Este enfoque es útil para obtener una visión contextualizada y detallada de los riesgos, especialmente en entornos complejos o áreas nuevas.

- **Enfoque basado en procesos**

Se centra en los procesos de negocio, analizándolos uno por uno con independencia de la estructura organizacional. Cada proceso se mapea desde sus entradas hasta sus salidas, identificando controles existentes y riesgos inherentes y residuales. Este enfoque permite evaluar la eficacia operativa y priorizar trabajos en procesos con alto riesgo residual, es decir, donde los controles actuales no mitigan adecuadamente los riesgos. Es especialmente útil cuando se busca fortalecer la eficiencia transversal o revisar procesos compartidos entre distintas áreas.

- **Enfoque basado en factores de riesgo (*Top-Down*)**

Este enfoque adopta una visión estratégica de la organización. Se parte del análisis de factores estructurales o contextuales que aumentan la exposición al riesgo en distintas áreas (por ejemplo, cambios normativos, uso intensivo de tecnología, rotación de personal clave, etc.). A partir de estos factores, se identifican las áreas más expuestas y se planifican trabajos que respondan a esos riesgos. Es el enfoque más apropiado para la elaboración de un plan anual de auditoría, ya que alinea la cobertura del trabajo con los objetivos estratégicos y el apetito y tolerancia al riesgo.

Según las características del contexto, es posible aplicar uno de estos enfoques de manera individual o combinarlos para obtener una visión más integral del riesgo. En esta Guía, se adoptará preferentemente un enfoque ascendente (bottom-up), dado que resulta más efectivo para una evaluación detallada de riesgos en trabajos individuales de auditoría.

Este enfoque requiere que el equipo auditor identifique inicialmente los riesgos más relevantes en función de los objetivos específicos de auditoría, el alcance y los criterios, así como su alineación con los objetivos estratégicos de la actividad bajo revisión y de la entidad. Cada riesgo deberá ser evaluado, como mínimo, considerando criterios como la probabilidad de ocurrencia y el impacto potencial en caso de materialización. En **Anexos N° 4, 5 y 6** se describen mayores detalles sobre esta temática.

a.1. Pasos globales para la evaluación de riesgos

- **Comprender los objetivos estratégicos**

Como ya se mencionó, el primer paso para comprender la actividad bajo revisión es identificar los objetivos estratégicos. Esto permite a los auditores internos obtener información sobre por qué existen la actividad y los procesos relacionados, y facilita los siguientes pasos de identificar y evaluar los riesgos y controles clave vinculados a esos objetivos.

- **Identificar objetivos**

Los objetivos estratégicos de la actividad bajo revisión son establecidos por la Dirección para alinearse con los objetivos y las metas organizacionales. Los objetivos organizacionales definen el propósito de los procesos y vinculan las operaciones diarias con el logro de las metas de la organización. Dichos objetivos pueden incluir:

- Objetivos para lograr efectividad y eficiencia operativas.
- Objetivos para cumplir los requisitos de informes internos y externos.
- Objetivos para ajustarse a leyes y regulaciones externas, así como a políticas y procedimientos internos.
- Objetivos relacionados con procesos o iniciativas específicas.

- **Integración de los objetivos estratégicos con la gestión de riesgos**

En términos conceptuales, los auditores internos deben comprender cómo la Dirección integra los objetivos estratégicos con la gestión de riesgos en la organización, lo cual se alinea adecuadamente con el componente de estrategia y establecimiento de objetivos en el *Marco Integrado de COSO de Enterprise Risk Management*. Este componente implica que la Dirección incorpore consideraciones de riesgo en cada etapa del proceso de planificación estratégica. Comienza con el análisis del entorno empresarial más amplio para entender cómo los factores externos e internos podrían influir en el perfil de riesgo de la organización.

Este análisis ayuda a definir el apetito y tolerancia al riesgo de la actividad bajo revisión y de la organización, garantizando su alineación con las metas de crear, preservar y materializar el valor institucional.

Al explorar distintas estrategias, la organización las evalúa en función de su potencial para lograr los objetivos estratégicos, así como por su impacto en el perfil de riesgo de la organización. Al establecer objetivos estratégicos en varios niveles, la organización debe considerar los riesgos asociados y asegurarse de que estos objetivos estén formulados para alinearse con las estrategias más amplias a nivel organizacional.

En el sector público, este escenario puede diferir significativamente, ya que la gestión de riesgos no siempre se encuentra plenamente integrada con la estrategia institucional ni con el proceso de definición de objetivos. Ante esta situación, es prioritario que el auditor interno comprenda cómo la Dirección articula los objetivos estratégicos, establecidos en la misión y en el marco legal que rige a la entidad, con la gestión de riesgos organizacional, a fin de evaluar su alineación, efectividad y contribución al logro del propósito institucional.

- **Indicadores clave de riesgo (*KRIs*)**

Las organizaciones con una función madura de gestión de riesgos (*Enterprise Risk Management*) pueden utilizar Indicadores de Claves de Riesgo (*KRIs*) para supervisar los objetivos, operaciones y procesos críticos. Los *KRIs* son métricas que brindan alertas tempranas sobre el aumento de los niveles de riesgos en áreas específicas críticas. A menudo se usan como indicadores que sirven para predecir el desempeño con base en insumos de procesos. Estos se complementan con indicadores rezagados (*lagging indicators*) que confirman el desempeño pasado midiendo resultados. Cuando un *KRI* muestra una tendencia preocupante o supera un umbral establecido, la Dirección puede abordar la causa raíz de manera temprana y tomar medidas correctivas antes de que se produzca algún daño significativo.

En el sector público, este escenario puede presentar particularidades relevantes, por lo que es fundamental que el auditor interno conozca y comprenda los Indicadores Clave de Riesgo (*KRIs*) existentes, y además evalúe críticamente su utilidad y pertinencia en relación con la gestión efectiva de riesgos dentro de la institución.

a.2. Identificación de riesgos y controles clave

- **Identificación de riesgos clave**

Después de desarrollar una comprensión de los procesos de la actividad que se está revisando, los auditores internos deben evaluar los riesgos clave y los controles asociados para mitigar dichos riesgos. Dado que existen riesgos en todos los procesos, el primer paso al evaluar los riesgos a nivel de proceso es identificar los escenarios de riesgo inherente que podrían afectar el logro de los objetivos.

- **Identificación de escenarios de riesgo**

Un escenario de riesgo es una descripción específica y factible de cómo un riesgo puede materializarse y afectar los objetivos de una organización. Entre otros métodos, se pueden llevar a cabo sesiones de lluvia de ideas (*brainstorming*) para identificar posibles escenarios de riesgo. Para maximizar los resultados de estas sesiones, los auditores internos pueden considerar invitar al personal involucrado en la actividad bajo revisión a participar. La sesión de lluvia de ideas puede realizarse siguiendo estos pasos:

- Centrarse en un objetivo a nivel de proceso a la vez.
- Generar ideas sobre barreras u oportunidades perdidas que podrían impedir el logro de los objetivos. Por ejemplo, no medir adecuadamente el desempeño, diseñar inadecuadamente aplicaciones tecnológicas o contar con información inexacta o inoportuna para la toma de decisiones.
- Continuar el ejercicio para los objetivos restantes a nivel de proceso.
- Categorizar y combinar escenarios de riesgo similares para facilitar la identificación de riesgos a nivel de proceso.

- **Definición de riesgos a nivel de proceso (dentro de la actividad bajo revisión)**

El uso de un protocolo de “causa y efecto” es un enfoque común y efectivo para definir riesgos a nivel de proceso. El ejercicio comienza identificando una “causa” (ej., falta de…, no lograr…) y luego determinando el “efecto” (ej., pérdida financiera, corrupción de datos). A continuación, algunos ejemplos:

- La falta de controles lógicos de seguridad efectivos podría provocar acceso, manipulación o eliminación no autorizados de datos críticos y/o sensibles.
- La incapacidad de atraer, desarrollar y retener personas competentes puede ocasionar un manejo inadecuado de ciertas tareas, dañando potencialmente el correcto funcionamiento y probidad dentro del proceso.
- La imposibilidad de procesar pagos a tiempo puede derivar en sanciones por pagos atrasados y faltas administrativas.

Una vez identificados los riesgos, ya sea mediante lluvia de ideas u otro método, los auditores internos deben vincularlos con los objetivos a nivel de proceso y luego evaluar la probabilidad y el impacto de estos riesgos sobre la capacidad de alcanzar los objetivos durante el proceso de evaluación de riesgos. El resultado de la evaluación de riesgos sirve como base para identificar los controles que teóricamente puedan mitigar los riesgos.

- **Evaluación de la probabilidad (frecuencia) del riesgo**

Consiste en estimar la probabilidad de que ocurra un evento adverso que pueda afectar el cumplimiento de los objetivos organizacionales. Esta evaluación debe estar sustentada en evidencia objetiva, como datos históricos, análisis predictivos y juicio experto, e integrar tanto factores internos (procesos, controles, historial de incidentes) como externos (entorno regulatorio, condiciones de mercado, factores sociales o tecnológicos).

- **Evaluación del impacto (consecuencia) del riesgo**

Implica analizar la magnitud del efecto que tendría la materialización del riesgo sobre los objetivos de la actividad bajo revisión y de la entidad. Estos efectos pueden ser de carácter financiero, operativo, reputacional, legal, ambiental, probidad o social. El análisis debe realizarse con base en escenarios bien definidos, considerando tanto consecuencias inmediatas como efectos de mediano y largo plazo.

- **Evaluación de otras dimensiones del riesgo**

Para lograr una visión más integral del riesgo, es posible incorporar otras dimensiones cualitativas en el modelo de evaluación del riesgo institucional, tales como:

- **Velocidad**: Tiempo que transcurre desde que el riesgo se activa hasta que genera impacto.
- **Volatilidad**: Variabilidad o cambios inesperados en la naturaleza, frecuencia o magnitud del riesgo.
- **Interdependencias**: Conexión con otros riesgos que pueden amplificar sus efectos (riesgos sistémicos o en cascada).
- **Persistencia**: Duración y sostenibilidad de los efectos una vez que el riesgo se ha materializado.
- **Impacto en el valor público**: Variable específica para el sector público. Se refiere al grado en que un riesgo puede afectar la creación, protección o sostenimiento del valor público que generan las instituciones estatales a través de sus políticas, programas y servicios.

La incorporación de estas variables dependerá del nivel de madurez del marco del proceso de gestión de riesgos adoptado por la institución.

En el **Anexo N° 6** se describen y ejemplifican cada una de estas dimensiones.

- **Determinación del nivel de criticidad del riesgo inherente (severidad del riesgo)**

Es el resultado de combinar la probabilidad, el impacto (y las dimensiones adicionales del riesgo, si así se hubiera decidió en la organización), sin considerar el efecto de los controles existentes. Esta valoración puede realizarse mediante métodos cuantitativos, cualitativos o mixtos. Se recomienda:

- Aplicar escalas consistentes y previamente definidas.
- Asignar ponderaciones cuando se desee priorizar alguna dimensión (por ejemplo, dar mayor peso al impacto).
- Documentar claramente la metodología usada, asegurando la trazabilidad y comparabilidad de los resultados.

En los **Anexos N° 5 y 6** se presentan las calificaciones o escalas para cada nivel de riesgo, según el método tradicional y avanzado, cuando corresponda.

- **Evaluación del riesgo residual o exposición al riesgo, comparación con el apetito de riesgo y respuesta al riesgo**

Una vez estimado el riesgo inherente se deben:

- Identificar los controles clave existentes para mitigar el riesgo.
- Evaluar su diseño y efectividad operativa (ver letra "*b. Evaluación del Diseño e Implementación de los Controles Clave"*).
- Determinar el nivel de exposición al riesgo o riesgo residual (riesgo remanente tras aplicar los controles).
- Este nivel se compara con el apetito de riesgo institucional, es decir, con el nivel de riesgo que la organización está dispuesta a aceptar para cumplir sus objetivos.
    - Si el riesgo residual está dentro del apetito, se considera aceptable y no se requiere acción adicional.
    - Si el riesgo residual excede el apetito, se considera no aceptable, por lo que deben tomarse medidas: reforzar controles, reformular acciones correctivas o escalar a la Alta Dirección y/o Jefe de Servicio.
- Complementariamente, deberá documentar y evaluar la razonabilidad de las respuestas adoptadas por la Dirección, asegurando que sean proporcional al nivel de exposición de los riesgos.

Temas Claves

- *Identificar y entender los objetivos estratégicos de la actividad es esencial para contextualizar los riesgos y controles. Esto vincula la revisión con las metas organizacionales.*
- *Se debe analizar cómo los riesgos afectan los objetivos estratégicos, considerando el apetito de riesgo institucional y utilizando KRIs como herramientas anticipativas de monitoreo.*
- *Se identifican escenarios de riesgo a nivel de proceso mediante técnicas como brainstorming y análisis causa-efecto, vinculándolos directamente con los objetivos afectados.*
- *Se debe analizar la probabilidad, impacto, e idealmente las dimensiones cualitativas del riesgo (como velocidad, volatilidad, interdependencia, persistencia o Impacto en el valor público), para determinar su severidad antes de considerar los controles existentes.*
- *Tras identificar controles y medir su eficacia, se estima el riesgo residual. Si excede el apetito al riesgo, se debe recomendar una respuesta (mitigar, transferir, aceptar o eliminar) y documentar su razonabilidad.*

b. Evaluación del diseño e implementación de los controles clave

b.1. Identificación de controles clave

Los controles clave están diseñados para mitigar los riesgos asociados con los objetivos estratégicos de la actividad bajo revisión. Una vez que se identifican dichos controles, se los debe vincular con los riesgos a nivel de proceso en la actividad bajo revisión. La documentación de dicha tarea puede realizarse mediante el uso de la Matriz Preliminar de Riesgos y Controles.

Los auditores internos deben considerar lo siguiente al determinar los controles clave:

- Obtener una comprensión clara de los objetivos a nivel de proceso y actividad bajo revisión.
- Evaluar las consecuencias de una ejecución inadecuada del control para determinar si una deficiencia en el control afectaría significativamente el logro de los objetivos.
- Evaluar la existencia de controles compensatorios que permitan determinar si la operación de un control clave es efectivamente tan crítica como se presume.
- Analizar el impacto que un control puede tener sobre otros, especialmente cuando su ejecución influye o condiciona la eficacia de controles adicionales.
- Considerar el efecto de los controles a nivel de entidad sobre los controles a nivel de proceso, especialmente cuando las deficiencias en los controles a nivel de entidad pueden reducir la efectividad de los controles a nivel de proceso.
- Considerar controles redundantes o menos económicos, que podrían ser modificados o eliminados.

b.2. Tipos de controles prioritarios para la evaluación

Tal como se mencionó anteriormente en esta Guía, los controles prioritarios para evaluación son:

- **Controles de nivel superior:** Son mecanismos de supervisión o revisión más transversales, útiles para detectar desvíos en niveles más agregados o institucionales.
- **Controles compensatorios:** Se vuelven clave cuando los controles principales son débiles o han fallado. Si el riesgo residual sigue siendo alto, es imprescindible verificar si estos controles alternativos están funcionando.
- **Controles con diseño robusto:** Los que, al haber sido evaluados como bien estructurados, se vuelven candidatos ideales para probar su funcionamiento en terreno.

- **Controles afectados por cambios:** En especial los controles que ha tenido modificaciones recientes en sistemas, procesos o personal. En estos casos, incluso un buen diseño puede dejar de ser efectivo si el cambio no fue bien gestionado.

b.3. Aspectos claves para la evaluación de la adecuación del diseño del control

La planificación de un trabajo conforme a las *Normas del Principio 13: Planificar eficazmente los trabajos*, debe integrar de manera estructurada la evaluación del diseño y efectividad de los controles clave.

Dicha evaluación está intrínsecamente vinculada con el análisis detallado de los riesgos, que orienta d la selección de materias a revisar, la identificación de controles relevantes y la determinación del nivel de profundidad requerido en su revisión. Este enfoque facilita la alineación de los procedimientos de auditoría con la realidad operativa del entorno bajo revisión, promoviendo un trabajo más eficaz, enfocado en la generación de valor.

Esta metodología debe estar plenamente incorporada en el procedimiento de planificación, aplicada en el programa de trabajo y sustentada en evidencia verificable, cumpliendo con los requisitos de calidad establecidos por las NOGAI. A su vez, debe reflejar en todo momento la lógica de priorización, alcance y profundidad determinada por la evaluación de riesgos específica del trabajo.

La evaluación del diseño de los controles clave tiene como objetivo verificar si esos controles están bien formulados y estructurados para cumplir la función de prevenir, detectar o mitigar los riesgos significativos que se identificaron en la etapa de análisis de riesgos (según lo establece la *Norma 13.2: Evaluación de riesgos del trabajo).*

En esta fase no se trata aún de ver si el control está funcionando en la práctica, sino de revisar si está bien pensado desde el diseño: si tiene una lógica sólida, si está alineado con el riesgo que busca cubrir, si tiene responsables asignados, criterios claros y mecanismos definidos. En otras palabras, se analiza si el control, tal como está diseñado, tiene el potencial de ser eficaz, previo a pasar a probar su funcionamiento real.

b.2.1. Aspectos a considerar para evaluar la adecuación de los controles frente a los riesgos identificados

Al evaluar el diseño de los controles, hay varios aspectos que los auditores internos deben tener en cuenta para asegurarse de que estén bien estructurados para enfrentar los riesgos identificados:

- Uno de los primeros puntos es entender cuál es el nivel de riesgo aceptable para la organización y cuál es su tolerancia al riesgo. Es decir, hasta qué punto la entidad está dispuesta a asumir un determinado nivel de exposición al riesgo con tal de alcanzar sus objetivos.

- Después, hay que evaluar si los controles que existen son pertinentes y suficientes. No se trata solo de si existen controles, sino de si realmente apuntan a los riesgos correctos y si son lo bastante sólidos, ya sea en cantidad y calidad para mantener el riesgo dentro de los límites que la organización considera aceptables.

- También es importante verificar si existen controles compensatorios. Estos son mecanismos adicionales que pueden ayudar a mitigar riesgos cuando un control principal no está funcionando o directamente no existe. En estos casos, se debe comparar su efectividad con el nivel de riesgo residual para determinar si realmente cumplen su función.

- Otro aspecto a revisar es la estructura general del proceso, no solo los controles puntuales. Hay que analizar si el diseño del proceso ayuda a prevenir errores, fraudes o ineficiencias, sobre todo en aquellas áreas que se identificaron como riesgosas desde el principio.

- Además, es necesario buscar la causa raíz para las brechas de control existentes. Esto significa identificar dónde están las debilidades en el diseño y tratar de entender por qué existen, identificando si es un problema de diseño, de implementación, de falta de recursos.

Esta información alimenta la Matriz Preliminar de Riesgos y Controles, y ayuda a ajustar el enfoque del trabajo.

En este contexto, para evaluar el diseño del control, se pueden aplicar distintas técnicas, tales como:

- **Indagación:** A través de entrevistas o cuestionarios, para conocer cómo se aplican los controles desde la perspectiva de quienes los ejecutan.
- **Observación directa:** Permite ver en tiempo real cómo funcionan los controles en la práctica.
- **Inspección de documentos y recursos:** Manuales, registros, evidencias o incluso activos físicos relacionados con el control.
- **Procedimientos de recorrido (*walkthrough*):** Consisten en seguir una transacción o proceso completo desde el inicio hasta el final para identificar los puntos de control críticos.

En forma complementaria, cuando se necesita mayor profundidad para la evaluación del control, se pueden aplicar métodos como:

- **Verificación documental:** Consiste en analizar los respaldos de operaciones y transacciones vinculadas al control.
- **Rastreo:** Permite seguir una transacción o proceso a través de todo su flujo, para comprobar que el control se activó donde debía.
- **Re-ejecución:** Es cuando el propio auditor simula la ejecución del control para comprobar si produce el resultado esperado.

Estas técnicas ayudan a tener un panorama general, pero por sí solas no suelen ser suficientes para llegar a conclusiones sólidas. Funcionan como punto de partida, pero se requiere ir más allá en la fase de pruebas en terreno.

Toda la información relacionada con análisis de los controles debe documentarse en los papeles de trabajo, incluyendo conclusiones claras sobre la solidez del diseño y posteriormente de la efectividad de la aplicación de los controles evaluados respecto del riesgo que deberían mitigar.

Temas Claves

- *La evaluación del diseño de controles clave debe formar parte integral de la planificación, orientando el esfuerzo auditor según la exposición al riesgo y ajustando el alcance y profundidad del trabajo.*
- *El análisis de diseño debe verificar si el control tiene lógica, propósito claro, responsables definidos, y mecanismos adecuados, sin aún evaluar su funcionamiento operativo.*
- *Se consideran factores como el nivel de riesgo aceptable, la suficiencia y pertinencia de los controles existentes, la existencia de controles compensatorios y posibles brechas o debilidades estructurales.*
- *Las Técnicas de evaluación aplicables incluyen indagación, observación directa, revisión documental, procedimientos de recorrido, y para mayor profundidad, verificación, rastreo y re-ejecución de controles.*
- *Toda la información y conclusiones deben quedar registradas en los papeles de trabajo, sustentando la calidad y la lógica técnica de la evaluación respecto del riesgo mitigado.*

b.4. Evaluación de la efectividad operativa de los controles claves

Una vez evaluado el diseño del control, el siguiente paso es verificar su efectividad operativa, es decir, comprobar si realmente se aplica como fue concebido (si es que está bien diseñado) y logra mitigar de manera efectiva los riesgos asociados. Esta evaluación debe basarse en evidencia suficiente, adecuada y fiable, conforme a lo establecido en *las Normas 14.1:(Recopilación de información para el análisis y evaluación* y *14.2: Análisis y potenciales hallazgos del trabajo.*

La evaluación de la efectividad del control considera revisar si el esfuerzo y los recursos requeridos para mantenerlo operativo, como tiempo, personal o tecnología, se justifican en relación con el valor que aporta en la reducción del riesgo. Esta evaluación complementa el análisis de diseño y efectividad operativa, incorporando una perspectiva de costo-beneficio, productividad y racionalidad práctica, en función de la criticidad del riesgo gestionado.

b.4.1. Aspectos clave que se deben evaluar respecto de los controles claves

Hay varios aspectos claves que se deben considerar al analizar la efectividad operativa de un control:

- **Aplicación oportuna del control**

  Hay que verificar si el control se aplica en el momento adecuado dentro del proceso. Es fundamental que esté presente justo donde el nivel de riesgo es más alto, no antes ni después. Si el control llega tarde o se aplica fuera de contexto, pierde efectividad y puede exponer a la organización al incumplimiento normativo, desviación de recursos, entre otros impactos.

- **Consistencia y responsabilidad en la ejecución**

  También es importante revisar si el control se aplica de manera constante durante todo el período evaluado y si lo ejecutan las personas responsables. Si hay cambios no autorizados, sustituciones o aplicaciones irregulares, eso puede comprometer la eficacia del control.

- **Justificación del costo del control**

  El primer paso es evaluar si la inversión que hace la organización para ejecutar ese control se justifica. Si se asignan muchos recursos a mitigar un riesgo menor, o si el costo de mantener el control supera claramente el beneficio de reducir la exposición, entonces probablemente no sea eficiente.

- **Optimización de los recursos asignados**

  Aquí se analiza si los recursos utilizados (humanos, tecnológicos, financieros) son adecuados para la complejidad del riesgo. Por ejemplo, si se usan controles manuales en procesos que podrían estar automatizados, o si hay personal muy calificado haciendo tareas básicas, hay un margen claro para mejorar.

- **Impactos no deseados**

  Algunos controles, aunque eficaces, pueden terminar generando efectos negativos: burocracia excesiva, pasos innecesarios, demoras o esfuerzos duplicados. Estos efectos pueden incluso generar nuevos riesgos o afectar el desempeño general de la entidad.

- **Comparaciones y benchmarking**

  También se puede analizar cómo se están manejando riesgos similares en otras áreas de la misma organización o en otras instituciones del sector público. Comparar permite detectar prácticas más eficientes y aplicables al contexto actual. Para esta evaluación, se pueden usar distintos métodos: procedimientos analíticos, entrevistas, observación directa y análisis de costo-beneficio, siempre enmarcados dentro de la lógica de gestión de riesgos y búsqueda de oportunidades de mejora.

En definitiva, no se trata solo de tener controles que funcionen, sino de asegurarse de que estén bien enfocados, bien ejecutados y que no cuesten más de lo que realmente aportan.

b.4.2. Alcance y oportunidad de las pruebas

Definir cómo se va a probar un control y cuándo hacerlo es una parte clave de la planificación. Estas decisiones deben basarse en criterios de riesgo, eficacia y eficiencia, considerando el objetivo del trabajo y el nivel de evidencia necesario para respaldar los hallazgos. Todo esto debe estar bien documentado y ser coherente con la estrategia definida, según lo establecen las *Normas 13.2: Evaluación de riesgos del trabajo y 14.1: Recopilación de información para el análisis y evaluación.*

Hay varios factores que deben considerarse al definir el alcance y la oportunidad de las pruebas:

- **Frecuencia (oportunidad) del control**

  Si el control se aplica de forma recurrente (semanal, mensual, etc.), lo ideal es aplicar un muestreo representativo, que permita verificar su consistencia a lo largo del tiempo.
  Si el control se ejecuta una sola vez durante el período auditado, se recomienda hacer una revisión completa, ya que una única falla podría ser significativa.

- **Confiabilidad de la evidencia**

  Cuando la evidencia es directa, objetiva y generada automáticamente (por ejemplo, por sistemas confiables), es posible reducir la cantidad de pruebas sin perder solidez.
  En cambio, si la evidencia es débil, ambigua o subjetiva, se necesita aplicar pruebas más amplias o profundas para lograr un nivel razonable de certeza.

- **Alcance total versus muestreo**

  Decidir entre revisar todo el universo o trabajar con muestras debe basarse en el nivel de riesgo, la criticidad del proceso y los recursos disponibles.
  En casos donde el impacto es alto o el control es clave en un proceso crítico, conviene optar por una cobertura total o un muestreo ampliado.

- **Oportunidad del trabajo en relación con el riesgo**

  Las pruebas deben realizarse en un momento que permita obtener evidencia válida y representativa. También deben alinearse con el ciclo operativo del proceso y con el nivel de exposición al riesgo que se quiere cubrir. Si se hacen muy temprano o muy tarde, pueden perder relevancia.

En todos los casos, las decisiones sobre el alcance y el momento de las pruebas deben quedar bien justificadas y registradas en el memorándum y programa de trabajo respectivo.

Temas Claves

- *Evaluar si el control se aplica consistentemente según lo diseñado, en el momento adecuado y por las personas responsables, con base en evidencia suficiente y fiable.*
- *Determinar si los recursos utilizados (tiempo, personal, tecnología) están justificados en relación con el valor que el control aporta en la reducción del riesgo.*
- *Detectar si el control, aun siendo efectivo, genera efectos adversos como burocracia excesiva, ineficiencia o nuevos riesgos operativos.*
- *Decidir cuánto y cuándo probar el control, basándose en criterios de frecuencia, criticidad del proceso, confiabilidad de la evidencia y nivel de riesgo.*
- *Registrar adecuadamente los criterios y resultados del análisis en el programa de trabajo, asegurando trazabilidad y coherencia con el enfoque de riesgos.*

c. “Matriz Preliminar de Riesgos y Controles” o “Matriz de Planificación de Riesgos y Controles”

La Matriz de Planificación de Riesgos y Controles permite al auditor interno documentar la identificación, análisis, valoración y priorización de los riesgos relevantes de la actividad bajo revisión, así como los controles clave destinados a mitigarlos. Esta matriz permite al auditor interno focalizar los esfuerzos en los riesgos más relevantes, priorizar actividades, y establecer una relación clara entre Objetivos estratégicos, riesgos, controles y objetivos del trabajo.

Esta matriz se construye con base en la información obtenida durante la comprensión inicial de la actividad bajo revisión y otras fuentes de antecedentes revisadas. Su elaboración permite al auditor interno enfocar el trabajo en las áreas de mayor criticidad, fortalecer la asignación de recursos y mejorar la eficacia del trabajo.

Es fundamental que dicha matriz incorpore el enfoque definido por la función de auditoría interna para la evaluación de los procesos de gobernanza, la gestión de riesgos y el control, en coherencia con los principios establecidos en las NOGAI y con base en el juicio profesional. La evaluación detallada de riesgos debe quedar documentada en los papeles de trabajo.

Para su construcción, el auditor interno debe realizar las siguientes tareas:

- Identificar los objetivos de la actividad bajo revisión.
- Identificar los riesgos relevantes que afectan dichos objetivos.
- Valorar los riesgos en términos de su probabilidad de ocurrencia y consecuencias esperadas (podrías ajustar estos elementos con variables si el proceso de riesgos es maduro).
- Determinar el nivel de riesgo inherente.
- Identificar los controles clave existentes para mitigar dichos riesgos.
- Evaluar el diseño y consistencia de los controles identificados.
- Estimar el riesgo residual tras considerar la efectividad de los controles.

Cada una de estas fases debe estar claramente descrita en la matriz y sustentada por evidencia adecuada en los papeles de trabajo. Esta herramienta también facilita la revisión por parte de supervisores y la comunicación de hallazgos preliminares al interior del equipo auditor.

El uso de esta matriz está alineado con los principios de planificación basada en riesgos establecidos en las Normas del *Principio 13: Planificar eficazmente los trabajos* y es considerado una buena práctica para asegurar que los trabajos de auditoría interna estén enfocados en los asuntos de mayor relevancia y criticidad para el logro de los objetivos organizacionales.

Esquema Nº3: Esquema de Matriz Preliminar de Riesgos y Controles - Matriz de Planificación de Riesgos y Controles

Objetivos Actividad bajo revisión	Riesgos Críticos	Probabilidad/ Impacto	Riesgo Inherente (Severidad)	Controles Claves Existentes	Evaluación de la Idoneidad del Diseño de los Controles	Riesgo Residual o Exposición	Definir Criterios de Priorización

Los elementos de la Matriz Preliminar de Riesgos y Controles se explican de la siguiente manera:

Tabla N° 4: Explicación de los Componentes de la Matriz Preliminar de Riesgos y Controles

Elemento	Descripción Técnica
Objetivos de la Actividad Bajo Revisión	Identificación de los objetivos estratégicos, operativos, de cumplimiento o de información asociados al proceso o actividad bajo revisión. Se obtienen de documentación institucional y entrevistas. Constituyen la base para evaluar la gobernanza, gestión de riesgos y controles existentes.
Riesgos Críticos	Situaciones o eventos que podrían impedir, afectar o retrasar el logro de los objetivos de la actividad. Se identifican mediante metodologías reconocidas (ej. NCh-ISO 31010 y directrices del CAIGG), considerando gobernanza, riesgos y control. Representan los riesgos con mayor relevancia para enfocar el trabajo de auditoría.
Probabilidad / Impacto	Valoración de la probabilidad de ocurrencia del riesgo y el impacto o magnitud de sus consecuencias (financieras, operativas, legales, reputacionales u otras). Se utilizan escalas predefinidas para determinar la significancia relativa del riesgo. Insumo clave para priorizar riesgos relevantes.
Riesgo Inherente (Severidad)	Nivel de riesgo estimado antes de considerar controles mitigantes. Se determina combinando probabilidad e impacto (se pueden agregar otras variables). Permite comprender la severidad natural del riesgo y enfocar el esfuerzo de auditoría en los asuntos más críticos para la organización.
Controles Claves Existentes	Controles clave implementados para mitigar los riesgos identificados, ya sea reduciendo probabilidad y/o impacto. Su identificación requiere revisión documental, entrevistas y juicio profesional. Se enfocan en aquellos vinculados con riesgos de mayor severidad.
Evaluación del Diseño del Control	Análisis de la idoneidad del control: si está correctamente estructurado, asignado, documentado y alineado con el riesgo. Se evalúa suficiencia, pertinencia, controles compensatorios, brechas y causas raíz. Deficiencias deben comunicarse oportunamente al Jefe de Auditoría y responsables.
Riesgo Residual / Exposición al Riesgo	Nivel de riesgo que permanece luego de considerar la efectividad del diseño del control. Representa la exposición actual para la entidad y sirve para definir las prioridades del programa de auditoría y la profundidad de las pruebas.
Criterios de Priorización	Ordenamiento de riesgos y controles a revisar según su severidad, riesgo residual y tolerancia institucional al riesgo. Permite definir alcance, objetivos, focalización de pruebas y asignación eficiente de recursos de auditoría.

En el **Anexo Nº 5** se incluyen criterios y escalas sugeridas para valorar la adecuación del diseño de los riesgos y controles clave de acuerdo con el método tradicional.

c.1. Definir criterios de priorización

Tras la identificación y análisis de los riesgos, y la evaluación del diseño de los controles clave, el auditor interno debe priorizar los aspectos que serán incluidos en el memorándum de planificación y en el programa de trabajo. Esta priorización debe basarse en criterios definidos y justificados, como el riesgo inherente, el riesgo residual, la magnitud del impacto o la sensibilidad de los programas institucionales, según corresponda.

La selección del criterio dependerá del juicio profesional del auditor, la confianza en los controles evaluados, la severidad de los riesgos identificados y las particularidades de la actividad bajo revisión.

Es fundamental que esta decisión esté debidamente documentada en los papeles de trabajo de planificación, especificando tanto el criterio aplicado como la justificación técnica que respalda su uso.

Ejemplo de justificación en papeles de trabajo

“Se seleccionaron los puntos críticos en base al nivel de riesgo inherente, dado que se trata de un riesgo de imagen elevado para la actividad bajo revisión y por ende para la entidad. Si bien los controles revisados presentan un diseño adecuado, no fueron verificados durante la fase de compresión inicial ni en trabajos de aseguramiento previos. Por tanto, se requiere confirmar su implementación y funcionamiento conforme al diseño en terreno.”

Al definir los criterios para la priorización de áreas en la planificación del trabajo, pueden considerarse, entre otras, las siguientes situaciones:

- **Controles con diseño adecuado, pero exposición significativa**

  Cuando el auditor interno concluye que los controles presentan un diseño apropiado, puede aplicarse el criterio de riesgo residual como base para la priorización. Este enfoque permite focalizar el trabajo en aquellas áreas que, pese a contar con controles bien diseñados, mantienen una exposición relevante debido a la naturaleza del riesgo, la complejidad operativa o el impacto potencial para la actividad o entidad.

- **Alta sensibilidad institucional o ciudadana**

  En casos donde la actividad bajo revisión, aun con un diseño de control adecuado, tiene alta sensibilidad en términos de reputación institucional, por ejemplo, por tratarse de servicios públicos esenciales o por el perfil de los beneficiarios, es recomendable aplicar el criterio de riesgo inherente, poniendo especial atención al nivel de impacto. Este enfoque es especialmente pertinente en áreas como salud, educación, programas sociales o servicios críticos, donde una falla podría comprometer gravemente la imagen o legitimidad institucional.

- **Antecedentes de fallas reiteradas**

  Si la actividad en revisión presenta historial de eventos adversos o deficiencias recurrentes, también corresponde aplicar el criterio de riesgo inherente. La persistencia de debilidades sugiere una exposición sostenida, posiblemente relacionada con fallas en la implementación, sostenibilidad o monitoreo de los controles, lo que justifica su inclusión prioritaria en el trabajo de auditoría, independientemente de la calidad del diseño actual.

- **Riesgos relevantes no tolerables sin control o con controles deficientes**

Es fundamental destacar que, si durante el desarrollo del trabajo el auditor interno identifica un riesgo relevante no tolerable que carece de controles o cuenta con controles significativamente deficientes, debe comunicarlo de forma inmediata al Supervisor o al Jefe de Auditoría. Este, a su vez, deberá informar al responsable de la actividad bajo revisión, a la alta Dirección o al jefe del servicio, según la magnitud y criticidad del asunto detectado (escalamiento). Esta acción oportuna no excluye la posibilidad de realizar pruebas selectivas en la fase de ejecución del trabajo, con el fin de verificar si dicho riesgo se ha materializado como consecuencia de las deficiencias observadas.

- **Riesgos con nivel de exposición al riesgo bajo pero estratégicamente relevantes**

La identificación de un riesgo con bajo nivel de exposición no implica, en ningún caso, su exclusión automática del conjunto de riesgos críticos a evaluar. Puede tratarse de riesgos con alto impacto potencial para la actividad bajo revisión y para la entidad, cuyo nivel de exposición se ha reducido debido a la existencia de controles sólidos en diseño. No obstante, por su relevancia estratégica, es recomendable incluirlos en el programa de auditoría para verificar que dichos controles han sido implementados correctamente y que operan de manera efectiva en la práctica.

El Jefe de Auditoría debe reunirse con el Director de la actividad bajo revisión, la Alta Dirección y el Jefe de Servicio, si corresponde (proceso de escalamiento), para asegurarse de que exista un entendimiento mutuo de los resultados de la evaluación de riesgos y para abordar cualquier diferencia significativa en las percepciones del nivel de riesgo.

En **Anexo N° 7** se describen aspectos relevantes de los procesos de gobierno, gestión de riesgos y control que se deben conocer y analizar, previo a la planificación del trabajo y en **Anexo N° 8** se identifican procesos genéricos en la organización, sus principales riesgos y los controles esperados en términos teóricos.

De forma complementaria, el auditor interno debe identificar y evaluar los riesgos asociados a la propia realización del trabajo de auditoría interna, tales como por ejemplo; riesgos de independencia, objetividad o errores en la recolección de evidencia. Esta materia se describe con mayor detalle en el **Anexo N° 9.**

Temas Claves

- *La matriz de riesgos y controles debe considerar de forma articulada los procesos de gobernanza, gestión de riesgos y control, conforme a las NOGAI y el juicio profesional del auditor.*
- *Es clave diferenciar y documentar los riesgos inherentes y residuales, valorando probabilidad e impacto, y sustentando con evidencia objetiva.*
- *Se debe analizar si los controles son adecuados, suficientes y pertinentes para mitigar los riesgos, identificando posibles brechas.*
- *La selección de áreas a auditar debe basarse en factores como impacto institucional, recurrencia o sensibilidad, más allá del riesgo residual.*
- *Cualquier riesgo crítico sin control adecuado debe comunicarse de inmediato a la Dirección y/o Alta Dirección para acción urgente.*

5 Evaluación de Riesgos de Fraude

a. Enfoque general

El riesgo de fraude debe ser considerado siempre como parte central en la planificación y ejecución de cualquier auditoría interna tal como lo establecen las NOGAI especialmente las *Normas 9.4: Plan de Auditoría Interna y 13.2 Evaluación de riesgos del trabajo.*

Aunque no es responsabilidad del auditor interno detectar todos los fraudes que puedan ocurrir, sí lo es evaluar razonablemente la exposición al fraude, mantenerse alerta ante señales de advertencia y actuar frente a condiciones que puedan facilitarlo.

En este contexto, según las NOGAI el fraude se entiende como "*Cualquier acto intencional caracterizado por engaño, ocultación, falta de honradez, apropiación indebida de activos u información, falsificación o violación de confianza, perpetrado por individuos u organizaciones con el fin de asegurarse ventajas injustas o ilegales en beneficio propio o de negocio.*"

b. Rol del auditor interno ante el riesgo de fraude

Durante el trabajo, el auditor interno debe asumir un rol activo frente a este riesgo. Específicamente, debe:

- Mantener una actitud de escepticismo profesional, es decir, no dar por hecho que todo funciona bien, especialmente en áreas sensibles.
- Evaluar señales de alerta (también llamadas banderas rojas) que puedan sugerir la existencia o posibilidad de fraude.
- Evaluar con mayor atención los controles en áreas de riesgo alto, como manejo de efectivo, adquisiciones, contratos, beneficios sociales o subsidios.
- Analizar oportunidades de fraude, sobre todo en procesos críticos que presentan controles débiles o inexistentes.
- Verificar si existen programas preventivos, como políticas antifraude, canales de denuncia o capacitaciones, y si realmente se aplican, evalúan y ajustan de forma regular.

Si durante el trabajo se detectan fallas de control importantes o indicios de fraude, el auditor interno debe informar de inmediato al Jefe de Auditoría. A su vez, este debe elevar el caso al Jefe de Servicio u otra autoridad competente, según la gravedad de la situación. No se debe esperar al informe final para comunicar estos hallazgos, ya que cualquier demora podría permitir que el problema continúe o incluso se agrave.

Temas Claves

- *El análisis de riesgo de fraude debe incluirse en el trabajo de auditoría según las NOGAI, aunque no sea su objetivo principal.*
- *El auditor interno debe identificar señales de fraude y evaluar controles en áreas de alto riesgo.*
- *Los indicios relevantes de fraude deben reportarse de inmediato a la alta Dirección y/o al Jefe de Servicio sin esperar el informe final.*

c. Análisis y evaluación del riesgo de fraude

El análisis del riesgo de fraude debe abordarse con el mismo nivel de exigencia que cualquier otro tipo de riesgo. Se puede integrar como parte de la Matriz Preliminar de Riesgos y Controles o tratarse por separado, dependiendo del enfoque del trabajo. En ambos casos, hay tres pasos fundamentales que conviene seguir:

- **Identificación del riesgo inherente de fraude**

Lo primero es identificar qué tipos de fraude podrían presentarse en la actividad que se está revisando. Para ello, se revisan esquemas de fraude comunes según el tipo de proceso, y se consideran factores como presiones internas o externas, incentivos personales o institucionales, oportunidades dentro del sistema, y posibles justificaciones que alguien podría usar para cometer fraude.

En este análisis también deben incluirse riesgos tecnológicos, sobre todo en entornos digitales o automatizados, donde pueden existir vulnerabilidades específicas que faciliten el fraude.

- **Evaluación de probabilidad e impacto**

Una vez identificado el riesgo, se debe estimar su probabilidad de ocurrencia y el impacto que podría tener. Esto se hace a partir de antecedentes (como historial de casos), entrevistas con responsables, revisión de los controles existentes y análisis de su efectividad.

El impacto se evalúa no solo en lo financiero, sino también en términos operativos, legales o reputacionales, dependiendo de la naturaleza del fraude y del contexto institucional.

- **Respuesta institucional**

Finalmente, se analiza cómo ha respondido la institución frente a ese riesgo. Esto implica revisar qué medidas han adoptado el Jefe de Servicio y los responsables operativos: si han implementado controles preventivos, correctivos o detectivos, si se ha hecho algún análisis de costo-beneficio de esas medidas y si hay decisiones de no aplicar controles que estén debidamente justificadas y documentadas.

Este análisis ayuda a entender no solo el nivel de exposición al fraude, sino también si la organización está actuando de forma responsable frente a ese riesgo. Para el auditor interno, permite ajustar el enfoque del trabajo, profundizando en los puntos donde el fraude no solo es posible, sino donde podría tener un impacto crítico.

d. Aplicación en la práctica

En el trabajo de campo, el auditor interno tiene que ponerse en el lugar de quien podría cometer un fraude. Eso implica hacer preguntas incómodas pero necesarias: ¿cómo se podrían evitar los controles?, ¿qué debilidades permitirían encubrirlo?, ¿hay posibilidad de que dos o más personas se pongan de acuerdo para burlar el sistema?

No hace falta que el fraude se haya producido para actuar. Si hay señales de alerta o se detectan riesgos que la organización no debería aceptar, aunque no haya pruebas concretas, hay que ir un paso más allá. A veces se requiere hacer pruebas específicas, revisar patrones de comportamiento, entrevistar a personas clave o aplicar técnicas que ayuden a confirmar o descartar sospechas.

Lo importante es no dejar estos indicios sin seguimiento. Todo lo que se descubra debe quedar bien registrado: qué riesgos se identificaron, qué controles se revisaron, qué se concluyó y, si corresponde, qué se recomienda hacer, ya sea investigar más a fondo o mejorar la prevención.

Temas Claves

- *El riesgo de fraude debe evaluarse con el mismo nivel técnico que otros riesgos, considerando entre otros factores; incentivos, oportunidades y tecnología.*
- *Se debe valorar el impacto del fraude y revisar si la institución ha justificado adecuadamente decisiones sobre controles.*
- *Si hay riesgos no tolerables, se deben aplicar pruebas adicionales y documentar todo en los papeles de trabajo. Sin perjuicio de escalarlos si a los niveles adecuados, si es necesario.*

e. Documentación de la evaluación del riesgo de fraude

La evaluación del riesgo de fraude debe ser documentada de forma clara, completa y trazable en los papeles de trabajo del auditor interno, conforme a lo establecido en las *Normas 13.4: Criterios de evaluación* y *14.6: Documentación de los trabajos*. Esta documentación no solo respalda el juicio profesional aplicado, sino que también constituye evidencia de cumplimiento de los requisitos de planificación y ejecución adecuados en relación con la gestión del riesgo de fraude.

Una de las herramientas clave para esta finalidad es la “Matriz Preliminar de Riesgos y Controles”, la cual permite al auditor interno:

- Identificar y describir los riesgos de fraude relevantes asociados a la actividad bajo revisión.
- Relacionar dichos riesgos con los controles existentes, sean estos preventivos, detectivos o correctivos.
- Evaluar el diseño y efectividad potencial de dichos controles frente a los riesgos identificados, incluyendo aquellos relacionados con colusión, acceso indebido, manipulación de información o conflictos de interés.

Esta matriz que debe ser elaborada durante la fase de planificación del trabajo, junto con los riesgos operativos o en forma separada, también puede ajustarse en función de los hallazgos obtenidos durante la ejecución del trabajo. El análisis debe incluir juicios sobre el nivel de riesgo inherente, la exposición residual al riesgo, y cualquier vacío de control que justifique pruebas adicionales o alertas tempranas.

A continuación, se presenta un esquema de Matriz Preliminar de Riesgos y Controles para la evaluación del riesgo de fraude, el cual puede ser utilizado como referencia y ajustado según el contexto específico del trabajo de auditoría.

Esquema Nº 4: Esquema de Matriz Preliminar de Riesgos y Controles para Fraudes

Identificación de Riesgos y Esquemas de Fraude	Probabilidad/ Impacto del Riesgo de Fraude	Riesgo Inherente de Fraude (Severidad)	Cargo o Unidad Sujeto al Riesgo de Fraude	Controles Anti fraude Existentes	Evaluación Idoneidad del Diseño de Controles Anti fraude	Riesgo Residual o Exposición	Definir Criterios Priorización

Esta estructura también puede ser parte de la Matriz Preliminar de Riesgos y Controles.

Tabla N° 5: Explicación de los componentes de la Matriz Preliminar de Riesgos y Controles para Fraudes

Elemento	Descripción
Identificación de Riesgos y Esquemas de Fraude	Se debe elaborar una lista detallada de los potenciales riesgos y esquemas de fraude aplicables a la actividad bajo revisión. Esta identificación será distinta en cada actividad y/o entidad y puede originarse en fuentes como investigaciones sectoriales, análisis de casos previos, entrevistas con personal, sesiones de análisis estratégico, revisiones documentales y canales de denuncia anónimos.
Probabilidad e Impacto del Riesgo de Fraude	Cada riesgo identificado debe evaluarse considerando la probabilidad de ocurrencia y el impacto potencial si llegase a materializarse. Se recomienda utilizar la misma escala de valoración cualitativa o cuantitativa empleada en la evaluación de riesgos operativos institucionales, para facilitar su integración al modelo de gestión de riesgos corporativo, considerando siempre, el nivel de apetito de la institución en esta materia, que debería ser bajo o cero.
Riesgo Inherente de Fraude (Severidad)	Corresponde al nivel de exposición al fraude antes de aplicar controles. Se calcula considerando la combinación de la probabilidad y el impacto del riesgo. Esta medida permite visualizar qué tan crítica es una amenaza por sí sola, y justifica su análisis más profundo en la planificación.
Cargo o Unidad Sujeto al Riesgo de Fraude	Es clave identificar a las personas, cargos, unidades internas o externas que podrían ser objeto, actores o facilitadores del riesgo de fraude. Este análisis permite diseñar respuestas específicas, ajustar controles, definir niveles de responsabilidad y asegurar una adecuada segregación de funciones o autorizaciones.
Controles Antifraude Existentes	Se deben registrar y mapear los controles actualmente implementados para mitigar los riesgos de fraude detectados. Esto incluye controles preventivos, detectivos y/o correctivos, tanto formales como informales. También deben considerarse controles compensatorios, si su aplicación es relevante ante la ausencia de controles clave.
Evaluación del Diseño de los Controles Antifraude	Implica valorar si los controles existentes están bien diseñados y son apropiados para mitigar el riesgo de manera efectiva. Esta evaluación debe responder preguntas tales como: ¿el control está alineado con la naturaleza del riesgo?, ¿opera en el momento adecuado?, ¿es específico o general?, ¿es suficientemente robusto frente a esquemas de fraude complejos como la colusión?
Riesgo Residual o Exposición al Riesgo	Se refiere al nivel de riesgo que permanece después de aplicar los controles existentes. El riesgo residual debe ser evaluado para decidir si es necesario realizar pruebas adicionales, reforzar controles o escalar el riesgo a la Dirección. Si es alto o excede el apetito, puede deberse a controles mal diseñados, inexistentes, no implementados o que operan de manera inefectiva.
Definir Criterios de Priorización	Es necesario definir claramente los criterios para priorizar los riesgos de fraude que deben incluirse en el programa de auditoría. Estos criterios pueden basarse en: nivel de exposición residual, impacto institucional, sensibilidad reputacional, obligación legal, recurrencia histórica, entre otros. La priorización debe estar documentada en los papeles de trabajo de planificación.

Temas Claves

- *La evaluación del riesgo de fraude debe registrarse de forma completa y trazable en los papeles de trabajo.*
- *La matriz de riesgos y controles para fraude permite identificar riesgos, evaluar controles y estimar el riesgo residual.*
- *Los riesgos a evaluar deben priorizarse con criterios técnicos y documentarse en la planificación del trabajo.*

f. Algunas herramientas para detectar fraudes

La selección de herramientas y procedimientos para detectar e investigar posibles fraudes debe estar basada en el tipo de trabajo de auditoría, las características específicas de la entidad y los resultados de la evaluación de riesgos desarrollada durante la planificación. Las NOGAI establecen que el auditor debe aplicar debido cuidado profesional y diseñar procedimientos adecuados a la complejidad del contexto y la naturaleza del riesgo identificado.

En la práctica, hay varias herramientas que se pueden aplicar, según el caso:

- El análisis de datos y la minería de información son especialmente útiles cuando se trabaja con grandes volúmenes de transacciones. Ayudan a detectar anomalías, pagos duplicados o patrones que se salen de lo normal y que podrían estar ocultando fraudes.
- Las entrevistas y la observación directa siguen siendo herramientas muy efectivas, sobre todo cuando se trata de detectar desviaciones intencionales en la operación diaria o comportamientos sospechosos que no aparecen en los registros formales.
- Con las técnicas de revisión cruzada de documentos, se pueden descubrir inconsistencias entre diferentes fuentes, ya sean internas o externas, que revelan fraudes administrativos o financieros que, a simple vista, podrían pasar desapercibidos.
- La revisión de accesos y permisos en sistemas informáticos ayuda a identificar fraudes tecnológicos, tales como usuarios con privilegios indebidos, accesos no autorizados o manipulaciones internas que vulneran la seguridad de la información.
- Las listas de verificación y el análisis de banderas rojas sirven como guías para detectar señales de alerta en procesos sensibles, como compras, nóminas o asignación de subvenciones. No prueban nada por sí solas, pero ayudan a enfocar la atención.
- Los procedimientos analíticos comparan lo que se espera que ocurra con lo que realmente muestran los datos. Si hay diferencias sin explicación razonable, pueden estar apuntando a una manipulación.
- Por último, las técnicas de muestreo y estadística permiten revisar grandes volúmenes de información sin necesidad de analizar todo. Se enfocan en los subconjuntos más riesgosos o donde hay indicios de anomalías.

Ahora bien, los auditores internos deben ser conscientes de los límites de sus conocimientos. En contextos más complejos, como análisis forense, ciberseguridad, fraude ambiental o uso avanzado de inteligencia artificial, puede ser necesario recurrir a especialistas, ya sean internos o externos. Dependiendo del caso, esto puede incluir expertos en informática, ingenieros, peritos forenses o asesores legales.

Si se incorpora apoyo técnico especializado, esa colaboración debe cumplir con las políticas y los procedimientos de la función de auditoría interna y quedar claramente documentados en los papeles de trabajo: quién participó, cuál era su perfil, por qué se le involucró, qué hallazgos se obtuvieron y cómo contribuyeron al resultado final de la auditoría.

f.1. Análisis de datos y minería de información

Cuando se trata de detectar posibles fraudes, el análisis de datos es una de las herramientas más potentes. Permite revisar grandes volúmenes de información en poco tiempo y detectar irregularidades que, a simple vista, pasarían desapercibidas. La clave está en buscar patrones extraños, inconsistencias o comportamientos que se salgan de lo normal.

Para aplicar esta técnica, los auditores internos pueden apoyarse en herramientas de análisis de datos, hojas de cálculo avanzadas, software de auditoría asistida por computador, plataformas de visualización de datos o lenguajes de programación orientados al procesamiento de información.

Estas tecnologías permiten realizar distintos tipos de análisis, por ejemplo:

- Detección de duplicados, como pagos repetidos, facturas ingresadas más de una vez o registros duplicados de proveedores o funcionarios.

- Análisis de excepciones, como transacciones hechas fuera del horario habitual, montos que se salen del promedio o compras a proveedores no registrados con anterioridad.

- Búsqueda de correlaciones inusuales, como empleados que aparecen también como proveedores, cambios frecuentes de cuentas bancarias o direcciones que se repiten en distintos registros.

- Análisis de secuencias, que ayuda a detectar saltos en numeración de documentos, fechas invertidas o desajustes cronológicos que podrían indicar manipulación.

Este tipo de análisis es especialmente útil en áreas como compras, pagos, manejo de inventario o gestión de nómina, donde el volumen de operaciones y el riesgo de fraude suelen ser más altos.

Como siempre, es fundamental que todo el trabajo esté bien documentado, especialmente se debe describir qué criterios se usaron, de dónde se obtuvieron los datos, cómo se procesaron y cuáles fueron los hallazgos relevantes. Esta trazabilidad no solo respalda el juicio del auditor, sino que fortalece la validez de cualquier conclusión o recomendación.

En **Anexo N° 10** se describen mayores detalles sobre esta materia.

f.2. Entrevistas y observación directa

Cuando se busca detectar posibles fraudes, las entrevistas y la observación directa son herramientas clave, sobre todo en entornos donde los procesos no están automatizados y gran parte del funcionamiento depende de las personas.

Las entrevistas, ya sean estructuradas o más flexibles, permiten al auditor interno obtener información valiosa directamente de quienes están involucrados en el proceso. A través del diálogo con actores clave, se pueden identificar percepciones sobre riesgos, debilidades o incluso prácticas informales que no están reflejadas en la documentación oficial.

Por otro lado, la observación directa permite ver con los propios ojos cómo se realizan realmente las tareas. Muchas veces, lo que está escrito en un protocolo o procedimiento no se aplica tal cual en la práctica. Esta técnica ayuda a detectar diferencias entre lo que “debería pasar” y lo que “realmente ocurre”. Por ejemplo, controles informales, pasos que se omiten, funciones que se acumulan en una misma persona sin justificación, entre otros indicios.

Todas estas técnicas deben aplicarse con profesionalismo, manteniendo la ética, la confidencialidad y el escepticismo profesional. Cualquier señal de alerta debe registrarse cuidadosamente, y si surgen dudas relevantes, se puede extender el trabajo a procesos o áreas relacionadas. Estas técnicas, aunque cualitativas, aportan evidencia crucial para entender el contexto real y tomar decisiones informadas durante la auditoría.

f.3. Técnicas de revisión documental cruzada

La revisión cruzada de documentos es una técnica muy útil cuando se busca detectar fraudes, inconsistencias o manipulaciones en los registros. Consiste en comparar información que proviene de distintas fuentes o sistemas, con el objetivo de encontrar datos que no coinciden y que podrían estar señalando un problema.

Este tipo de análisis permite detectar, por ejemplo:

- Pagos sin respaldo o sobrefacturaciones, al comparar órdenes de compra con facturas y los documentos que acreditan la recepción de bienes o servicios.
- Transferencias indebidas, al cruzar registros de pagos con los listados oficiales de proveedores autorizados, para identificar si se hizo algún pago a un tercero no habilitado.
- Información falsa o incompleta, al validar datos entregados por beneficiarios o contratistas con fuentes externas, como registros de renta, bases de datos públicas o sistemas de morosidad.

Aplicar esta técnica ayuda a verificar la trazabilidad de la información, detectar documentos que podrían haber sido alterados, y confirmar que las decisiones se tomaron con base en datos legítimos. Es un enfoque muy efectivo para comprobar la integridad de los procesos y reforzar la calidad de la evidencia en la auditoría.

f.4. Revisión de accesos y permisos en sistemas de TI

Una de las formas más efectivas de detectar posibles fraudes tecnológicos es revisar cómo se están gestionando los accesos y permisos en los sistemas informáticos de la institución. Esta técnica permite identificar vulnerabilidades que, si no se controlan, pueden ser aprovechadas para cometer irregularidades sin dejar rastro claro.

Algunos focos de atención comunes incluyen:

- Usuarios con permisos excesivos, como aquellos que pueden crear y aprobar transacciones dentro del mismo proceso, lo que elimina cualquier barrera efectiva de control.

- Cuentas de usuarios que ya no deberían tener acceso, como funcionarios que cambiaron de área, están inactivos o incluso dejaron la institución, pero siguen habilitados en el sistema.

- Cuentas compartidas o genéricas, que dificultan saber quién hizo qué, lo que debilita la trazabilidad y puede encubrir conductas indebidas.

- Análisis de los registros del sistema (*logs*), para detectar accesos fuera de horario, acciones no autorizadas o movimientos sospechosos que no encajan con el rol del usuario.

Este tipo de revisión es especialmente relevante en áreas sensibles como finanzas, recursos humanos, adquisiciones o plataformas de atención ciudadana, sobre todo cuando se utilizan sistemas integrados de información. Un mal manejo de accesos puede dejar expuestos procesos críticos y facilitar fraudes internos difíciles de detectar por otros medios.

f.5. Aplicación de listas de verificación y banderas rojas

El uso de listas de verificación (*checklists*) con indicadores de alerta, también conocidas como banderas rojas, es una herramienta práctica para que los auditores internos identifiquen condiciones que podrían estar relacionadas con fraude. Estas listas se elaboran a partir de estudios previos, normativa vigente y la experiencia acumulada por la función de auditoría interna.

Se estructuran por área o ciclo de negocio y permiten al auditor interno detectar situaciones que, aunque no prueban por sí solas la existencia de fraude, ameritan atención o revisión más profunda. Algunos ejemplos comunes por tipo de proceso incluyen:

Estas listas no reemplazan otros procedimientos, pero son especialmente útiles tanto en la planificación como durante la ejecución del trabajo. Pueden usarse como guía inicial y luego complementarse con entrevistas, análisis de datos y observación en terreno, según el caso. Detectar una bandera roja no significa que haya fraude, pero sí indica que hay que mirar más de cerca.

Para una comprensión más detallada, se recomienda consultar el **Anexo N° 11**, el cual presenta ejemplos de banderas rojas clasificadas por ciclo de negocio, tales como; cuentas por cobrar, tesorería, gestión de personal, seguridad, ciberseguridad y administración de accesos.

f.6. Procedimientos analíticos

Los procedimientos analíticos son una herramienta poderosa para detectar señales tempranas de fraude, ya que permiten identificar relaciones extrañas o inconsistencias en la información financiera, operativa o técnica de la entidad. Al comparar datos de distintas fuentes o periodos, se pueden revelar patrones que no cuadran con el comportamiento esperado.

Estas técnicas se basan en el análisis de información contenida en planillas, bases de datos o registros manuales, y ayudan a detectar desviaciones, ausencias o anomalías. Por ejemplo:

- Cuando no hay diferencias donde sí deberían existir (como costos constantes pese a aumentos en volumen),
- Cuando hay diferencias exageradas en comparación con periodos anteriores o con entidades similares del mismo sector.

Ejemplos prácticos en la entrega de subsidios

- Comparar montos entregados por región o comuna en función del número real de beneficiarios registrados. Si una zona muestra un monto elevado con pocos beneficiarios activos, podría indicar asignaciones irregulares o ficticias.
- Cruzar registros de beneficiarios con bases de datos externas, como registros de defunciones, ingresos tributarios o beneficios duplicados. Esto puede revelar subsidios entregados a personas fallecidas, con ingresos incompatibles o que ya reciben otro subsidio similar.
- Analizar tendencias de pagos mensuales, para detectar aumentos inusuales en ciertas fechas (por ejemplo, antes de cierres presupuestarios), lo cual podría ser indicio de manipulaciones para ejecutar fondos de forma acelerada y poco controlada.
- Comparar subsidios asignados con criterios establecidos en la normativa vigente. Si se detectan excepciones sistemáticas o cambios en el patrón de asignación sin respaldo, puede haber discrecionalidad indebida.
- Verificar si hay direcciones repetidas entre beneficiarios, lo que podría sugerir agrupación artificial de personas para simular hogares o núcleos familiares que no existen.
- Revisar patrones de solicitudes aprobadas por ciertos funcionarios, para identificar si hay tasas de aprobación anormalmente altas vinculadas a un evaluador específico.
- Aplicar modelos predictivos o análisis de regresión, comparando la asignación de subsidios con variables como desempleo, pobreza o escolaridad por zona. Desviaciones relevantes sin justificación podrían indicar distorsiones o favoritismos.

Este tipo de análisis no reemplaza las pruebas sustantivas, pero sí permite dirigir mejor los esfuerzos de auditoría, priorizando áreas de mayor riesgo. Lo importante es que todo hallazgo sea bien documentado y evaluado en profundidad, ya que puede ser una señal temprana de fraude, uso indebido de recursos o fallas graves en el control del proceso.

Temas Claves

- *Los procedimientos analíticos permiten identificar relaciones inusuales que pueden alertar sobre posibles fraudes.*
- *También permiten detectar diferencias superiores o inferiores a las encontradas en organizaciones similares.*
- *Se deben analizar indicadores financieros, técnicos y operacionales frente a indicadores históricos, capacidad instalada o parámetros del mercado.*

f.7. Técnica de muestreo de descubrimiento

El muestreo de descubrimiento es una técnica especialmente útil cuando el objetivo no es calcular cuántas irregularidades hay, ni cuánto cuestan, sino simplemente comprobar si existe al menos un caso de fraude, error grave o situación anómala dentro de un proceso.

La lógica es simple: *si se encuentra una sola desviación, ya es suficiente para descartar la idea de que el proceso está limpio y justificar una revisión más profunda, o incluso una auditoría completa*. Es una técnica que cobra especial valor en procesos donde no debería haber ningún error, como pagos duplicados, adjudicaciones directas sin justificación o ingresos no depositado, porque la sola existencia de un caso es crítica.

Este enfoque se usa cuando se parte del supuesto de tolerancia cero al error, y donde cualquier hallazgo representa un riesgo elevado. Por eso, es ideal para áreas sensibles como:

- Transferencias de fondos, subsidios, programas, proyectos o ayudas directas.
- Contrataciones públicas y adjudicaciones por trato directo.
- Procesos de recaudación y manejo de ingresos.
- Pagos por caja chica o rendiciones de cuentas.
- Nómina y contratación de personal a honorarios.

Por ejemplo, si en una muestra de pagos aparece una factura emitida por una empresa vinculada a un funcionario, ese único hallazgo basta para desechar la hipótesis de que el proceso es correcto, activar alertas y, si corresponde, escalar la situación a un nivel superior.

Lo importante de esta técnica es que no busca calcular porcentajes ni extrapolar resultados. Su propósito es detectar. Si aparece algo, se actúa. Y si no aparece nada, se fortalece la confianza en el proceso evaluado.

No obstante, esta técnica debe aplicarse con criterio, lo que implica definir adecuadamente el tamaño de la muestra en función del nivel de confianza requerido. El objetivo es asegurar que, si existiera al menos una irregularidad, el diseño muestral ofrezca una probabilidad razonable de detección. Asimismo, en caso de identificarse hallazgos, esta técnica por sí sola no es suficiente y debe complementarse con pruebas más específicas, entrevistas o análisis detallados, según la naturaleza y gravedad del caso.

En **Anexo N°12** se describen mayores detalles sobre esta materia.

f.8. Técnica de análisis de Ley de Benford, análisis digital, o análisis de frecuencias digitales

El análisis de la Ley de Benford, también conocido como análisis digital o análisis de frecuencias de dígitos, es una técnica que se utiliza en auditoría para detectar posibles manipulaciones numéricas, especialmente en grandes volúmenes de datos financieros o administrativos.

Su valor está en que se basa en un principio estadístico natural: en conjuntos numéricos reales, los dígitos no aparecen al azar ni con la misma frecuencia. Por ejemplo, los números que comienzan con el dígito 1 tienden a aparecer mucho más seguido (alrededor del 30% del total), mientras que los que empiezan con 9 aparecen con mucha menos frecuencia (menos del 5%).

Cuando los datos provienen de procesos normales y no han sido manipulados, tienden a seguir este patrón. Pero cuando hay fraude o intentos de alterar cifras, los números suelen desviarse de esa distribución natural, lo que puede levantar una alerta.

Resulta especialmente útil cuando se trabaja con grandes bases de datos que contienen montos; listas de facturas, órdenes de compra, registros de ingresos diarios, pagos, rendiciones o gastos por ítem, entre otros. Al aplicar la Ley de Benford a estos datos, el auditor interno puede identificar rápidamente si hay alguna distribución inusual que justifique un análisis más profundo.

Si bien esta técnica no permite confirmar por sí sola la existencia de fraude, sí constituye una herramienta eficaz para identificar alertas tempranas que podrían indicar posibles manipulaciones de cifras o registros con bajo grado de fiabilidad.

Tabla Nº 6. Distribución esperada del Primer Dígito según la Ley de Benford

Primer Dígito	Distribución Esperada
1	30,1 %
2	17,6 %
3	12,5 %
4	9,7 %
5	7,9 %
6	6,7 %
7	5,8 %
8	5,1 %
9	4,6 %

La Ley de Benford no se limita al análisis del primer dígito de un número; también puede aplicarse al estudio de los dos o tres primeros dígitos, siempre que se disponga de una base de datos lo suficientemente amplia como para que el análisis sea estadísticamente significativo.

En un trabajo de auditoría, por ejemplo, es posible tomar una muestra extensa de transacciones, como todos los pagos realizados en un año o todas las facturas vinculadas a un proveedor y analizar la frecuencia de los dígitos iniciales de los montos utilizando herramientas de análisis de datos. Si la distribución observada se desvía significativamente de la esperada según la Ley de Benford (por ejemplo, si se detecta una frecuencia anómala de importes que comienzan con 5, 6 o 7), no es posible concluir directamente la existencia de fraude. Sin embargo, este comportamiento constituye una señal de alerta que justifica la aplicación de procedimientos adicionales o pruebas más específicas para profundizar la revisión.

Este tipo de análisis es especialmente útil en trabajos relacionados con:

- Ingresos institucionales
- Procesos de compras públicas o licitaciones
- Pagos por caja chica o fondo fijo
- Rendiciones de cuentas de proyectos
- Contrataciones y pagos a honorarios

Ejemplo: En una auditoría de viáticos, si se detecta que muchos montos comienzan con 7 u 8, podría ser una señal de que los valores fueron ajustados artificialmente para coincidir con ciertos topes o justificar gastos que no ocurrieron. Ante esa alerta, el auditor podría decidir hacer una revisión más detallada, como por ejemplo, examinar respaldos originales, entrevistar al personal responsable o cruzar la información con otras fuentes.

Consideraciones adicionales

- Tamaño de la muestra: Funciona mejor con conjuntos grandes de datos (más de 100 registros).
- Función como filtro: No reemplaza pruebas sustantivas, pero sirve para priorizar áreas de riesgo.
- No concluyente de forma aislada: si bien no debe utilizarse como única base para emitir juicios, constituye una herramienta eficaz para orientar el enfoque de auditoría y optimizar el uso de los recursos disponibles.

Temas Claves

- *El Muestreo de descubrimiento se aplica cuando se espera que no haya errores; basta encontrar uno para justificar una revisión más profunda.*
- *La Ley de Benford detecta posibles manipulaciones en registros numéricos grandes, útiles para enfocar auditorías en transacciones sospechosas.*
- *El uso combinado de ambas técnicas funciona como alertas tempranas que orientan al auditor hacia áreas donde puede haber fraude y requieren pruebas adicionales.*

6 Evaluación de los Riesgos y Controles Clave de Tecnologías de Información en la Planificación del Trabajo

a. Escenarios generales sobre riesgos y controles de TI

Durante la fase de planificación de un trabajo de auditoría, uno de los pasos fundamentales, conforme a lo establecido en la *Norma 13.2: Evaluación de riesgos del trabajo*, es lograr una comprensión clara y profunda de la actividad bajo revisión, así como de los riesgos que pueden afectarla.

Dentro de esta evaluación, los riesgos asociados a la tecnología de la información (TI) adquieren un papel central. Esto se debe a que, en la actualidad, prácticamente todos los procesos de una entidad ya sean de carácter operativo, financiero, normativo o estratégico, dependen directa o indirectamente del uso de sistemas informáticos. Por tanto, omitir el análisis de estos componentes tecnológicos puede comprometer seriamente la integridad del trabajo de auditoría y limitar la validez de sus conclusiones.

La consideración de los riesgos y controles de TI resulta esencial, incluso en trabajos que no están orientadas específicamente al ámbito tecnológico. El auditor interno debe evaluar, como mínimo, los riesgos asociados a la disponibilidad, integridad, confidencialidad y trazabilidad de la información utilizada en los procesos bajo revisión. Esta evaluación incluye también la verificación de controles generales de TI, así como de controles específicos de aplicación que afectan directamente la fiabilidad de los datos y registros utilizados para sustentar decisiones.

Hay dos escenarios globales típicos que pueden presentarse:

- **Si el trabajo se enfoca directamente en TI**

En este caso, el enfoque tiene que ser mucho más técnico y profundo. Estamos hablando de trabajos de auditoría que examinan específicamente temas como; ciberseguridad, continuidad operativa, infraestructura tecnológica o el funcionamiento de sistemas integrados. Para este tipo de trabajos, es fundamental aplicar marcos especializados tales como COBIT, ISO, NIST o los Requisitos Temáticos del IIA. La revisión se centra generalmente en la estructura de los sistemas, su capacidad para proteger los datos, su disponibilidad, y la forma en que están gobernados.

- **Si el trabajo es más general (no especializado en TI)**

Incluso si el foco de la auditoría no es tecnológico, los riesgos asociados a los sistemas informáticos siguen siendo relevantes. En estos casos, el equipo auditor tiene que asegurarse de cubrir al menos tres aspectos esenciales:

- Detectar posibles riesgos tecnológicos que puedan afectar la calidad, integridad o disponibilidad de la información. Por ejemplo, sistemas que no validan los datos ingresados o bases de datos expuestas a accesos indebidos.
- Verificar si hay controles generales y controles de aplicación bien implementados. Esto es clave cuando los procesos revisados dependen fuertemente de datos procesados electrónicamente. Si el sistema falla, el trabajo de auditoría puede perder confiabilidad.
- Revisar que existan medidas razonables para proteger la información. Es decir, que se garantice la trazabilidad de las acciones en el sistema, que se respeten las políticas de privacidad y que los accesos estén bien definidos y controlados.

b. Relevancia del Requisito Temático de Ciberseguridad del IIA en la planificación del trabajo

En esta fase es fundamental considerar los requisitos temáticos emitidos por el Instituto de Auditores Internos (IIA), particularmente el Requisito Temático de Ciberseguridad, que ha sido adaptado para la auditoría interna del sector público de nuestro país mediante la GASIC 11 – Adaptación Requisito Temático Ciberseguridad al Sector Público. Este componente normativo tiene carácter obligatorio cuando el trabajo se orienta a identificar, gestionar y mitigar los riesgos relacionados con la ciberseguridad, así como la efectividad de los controles y procesos implementados para proteger los activos de información críticos.

La inclusión de este requisito temático desde el inicio del trabajo permite:

- Alinear la planificación con los estándares internacionales más recientes en materia de seguridad digital, protección de información crítica, y mitigación de ciberamenazas.
- Integrar buenas prácticas y controles clave vinculados a la gobernanza, gestión de riesgos y control de ciberseguridad.
- Reforzar el enfoque basado en riesgos, priorizando los dominios y procesos tecnológicos con mayor exposición a ataques cibernéticos, incidentes de seguridad, o pérdida de datos sensibles.

b.1. Aplicación específica en la planificación

Durante esta fase, el equipo de auditoría debe:

- Determinar si la actividad bajo revisión involucra sistemas críticos, información confidencial o dependencias tecnológicas significativas, lo cual justificaría aplicar el Requisito Temático.
- Analizar la exposición de la entidad a riesgos emergentes en ciberseguridad, como *ransomware*, accesos no autorizados, vulnerabilidades en redes o plataformas digitales, y uso de servicios en la nube.
- Evaluar el nivel de madurez del marco de ciberseguridad de la entidad, utilizando los seis componentes del marco de evaluación del IIA; gobernanza, inventario de activos, configuraciones estándar de seguridad, gestión de accesos, respuesta ante incidentes y monitoreo continuo.
- Identificar controles clave de ciberseguridad que serán evaluados, tales como: políticas de seguridad, cifrado de datos, *firewalls*, protocolos de autenticación y sistemas de detección de intrusos.

b.2. Importancia estratégica para la planificación

La incorporación del Requisito Temático de Ciberseguridad del IIA y la GASIC 11 del CAIGG no solo fortalecen la pertinencia técnica del trabajo, sino que aporta un enfoque proactivo y actualizado frente a amenazas digitales que pueden comprometer la continuidad operativa, la reputación institucional y el cumplimiento normativo. Su inclusión durante la planificación permite establecer criterios claros, delimitar alcances precisos y diseñar procedimientos efectivos que respondan a los objetivos específicos del trabajo, asegurando coherencia con los *Principios 13, 14 y 15* de las NOGAI.

Temas Claves

- *En todo trabajo de auditoría deben considerarse los riesgos tecnológicos, ya que impactan transversalmente los procesos.*
- *Aplicar el Requisito Temático de Ciberseguridad del IIA es obligatorio si existen sistemas críticos o amenazas digitales relevantes.*
- *Evaluar la madurez del marco de ciberseguridad permite definir mejor el alcance y enfoque del trabajo de auditoría.*

c. Evaluación de riesgos de TI

La evaluación de los riesgos vinculados a las tecnologías de la información es un paso esencial en la planificación de cualquier trabajo de auditoría interna. Esto permite asegurar una cobertura adecuada de aquellos factores que podrían afectar directamente el logro de los objetivos de la actividad bajo revisión. Dicha evaluación no debe limitarse a los riesgos específicos de TI, sino también considerar su interacción con los procesos operativos y de negocio en los que se integran.

Para cumplir con este propósito, los auditores internos deben identificar los riesgos tecnológicos más relevantes asociados a los objetivos de la actividad bajo revisión. Estos pueden incluir fallas en los sistemas informáticos, brechas en la seguridad de la información, accesos no autorizados, errores que comprometan la integridad de los datos o una dependencia excesiva de proveedores tecnológicos. Asimismo, es necesario tener presente los riesgos de fraude relacionados con la tecnología, tales como la manipulación o eliminación intencional de registros, el uso indebido de información confidencial o el abuso de privilegios de acceso.

Una vez identificados, los riesgos deben ser evaluados según su significancia, lo que implica analizar factores como la complejidad y criticidad de la infraestructura tecnológica, el nivel de exposición a amenazas cibernéticas, la presencia o ausencia de controles efectivos, el volumen y sensibilidad de los datos procesados, el uso de tecnologías emergentes como sistemas en la nube, automatización o inteligencia artificial y el grado de cumplimiento con la normativa vigente en materia de privacidad y seguridad de la información.

Para estructurar esta evaluación de manera sólida, se recomienda utilizar marcos de referencia ampliamente reconocidos. Algunos de los más utilizados incluyen *COBIT*, que permite alinear los objetivos de control de TI con los objetivos estratégicos institucionales; *NIST*, que proporciona herramientas para gestionar riesgos tecnológicos y evaluar la madurez de la ciberseguridad; e *ISO/IEC 27001 y 27002*, que establecen buenas prácticas para la implementación de sistemas de gestión de seguridad de la información. En el sector público, también son de especial utilidad las Guías de Auditoría para Seguridad de la Información y Ciberseguridad (GASIC), emitidas por el CAIGG.

En caso de que la entidad no cuente con un marco formal de gestión de riesgos tecnológicos, el auditor interno debe seleccionar o adaptar uno que se adecue al contexto institucional, de modo de garantizar una evaluación integral, coherente y trazable.

Por último, los resultados de esta evaluación deben quedar debidamente documentados como parte de los papeles de trabajo. Esto implica vincular los riesgos identificados con los controles existentes o ausentes, y relacionarlos con los objetivos de auditoría y los procedimientos que se incluirán en el programa de trabajo. Esta trazabilidad es clave para asegurar la consistencia del enfoque basado en riesgos que debe guiar la auditoría interna.

Temas Claves

- *Identificar y priorizar riesgos tecnológicos como fallas de sistema, accesos indebidos o fraudes, según su impacto en los objetivos auditados.*
- *Basarse en marcos internacionales como COBIT, NIST o ISO/IEC para asegurar una evaluación consistente y alineada con buenas prácticas.*
- *Documentar la evaluación de riesgos TI en los papeles de trabajo, vinculando riesgos, controles y procedimientos planificados.*

d. Controles clave de TI a evaluar

Dentro del trabajo de auditoría interna, la evaluación de los controles relacionados con las tecnologías de la información es fundamental para asegurar que la información procesada por la entidad sea íntegra, confidencial, disponible y confiable. Esta evaluación debe estar alineada con los riesgos tecnológicos previamente identificados, así como con los objetivos específicos del trabajo que se esté realizando.

En términos generales, los controles de TI que deben ser considerados se agrupan en cuatro categorías principales:

- En primer lugar, están los **Controles Generales de TI.** Estos se aplican de manera transversal a toda la infraestructura tecnológica de la organización y constituyen la base sobre la cual se sostiene la confiabilidad de los sistemas y la integridad de los datos. Dentro de esta categoría se incluyen aspectos como la gestión de accesos y privilegios de usuarios, los procesos para administrar cambios en sistemas y aplicaciones, los mecanismos de respaldo de información y recuperación ante desastres, así como la supervisión continua de la operación de los sistemas y la seguridad tanto física como lógica de los centros de datos.

- En segundo lugar, se encuentran los **Controles de Aplicación**, los cuales están integrados directamente en los sistemas o plataformas utilizados por la entidad y buscan garantizar que los datos sean válidos, completos y procesados de manera adecuada. Estos controles operan en tres niveles: entrada, procesamiento y salida de datos. En la entrada, se trata de validar que la información ingresada cumpla con los formatos, rangos y autorizaciones requeridas. Durante el procesamiento, se debe asegurar la correcta aplicación de reglas de negocio y la trazabilidad del flujo de información. En la salida, los controles se enfocan en proteger los reportes generados y garantizar su revisión y autorización antes de ser utilizados para la toma de decisiones.

- Una tercera categoría corresponde a los **Controles de Ciberseguridad**, que están orientados a mitigar riesgos derivados de amenazas internas o externas al entorno digital de la organización. Aquí se evalúan políticas y procedimientos de seguridad de la información, el uso de protocolos de encriptación para proteger datos tanto en tránsito como en reposo, la existencia de *firewalls* y sistemas de detección y prevención de intrusiones, la implementación de autenticación *multifactor* y segregación de funciones, así como la gestión de parches de seguridad, análisis de vulnerabilidades y pruebas periódicas como simulacros de ciberataques.

- Por último, es necesario revisar los **Controles de Privacidad de Datos**, especialmente cuando la entidad procesa información personal identificable. Estos controles buscan asegurar el cumplimiento de normativas sobre protección de datos. Se trata de verificar que exista una clasificación adecuada de los datos personales, que se obtenga el debido consentimiento para su uso, que se limite su almacenamiento y acceso según principios de necesidad y proporcionalidad, y que se apliquen medidas de anonimización o seudonimización cuando corresponda. También es relevante que existan auditorías y revisiones periódicas orientadas a evaluar el nivel de cumplimiento con las políticas de privacidad.

Todos estos controles deben ser evaluados de manera estructurada, documentados en los papeles de trabajo y relacionados directamente con el análisis de riesgos realizado durante la planificación. Su revisión no solo permite medir la efectividad del entorno de control tecnológico, sino que también proporciona evidencia clave para fundamentar hallazgos, elaborar conclusiones sólidas y formular recomendaciones con un alto valor agregado para la organización.

Para más información sobre estas temáticas, se sugiere revisar las Guías de Auditoría para Seguridad de la Información y Ciberseguridad (GASIC), emitidas por el CAIGG.

Temas Claves

- *Evaluar controles generales de TI, controles de aplicación, ciberseguridad y privacidad de datos, en relación con los riesgos tecnológicos detectados.*
- *Asegurar que estos controles garanticen la integridad, disponibilidad, confidencialidad y confiabilidad de los datos y sistemas.*
- *Documentar esta evaluación en los papeles de trabajo para sustentar conclusiones y recomendaciones.*

e. Rol del Modelo de las Tres Líneas en el Entorno de TI

e.1. Evaluación de riesgos de ciberseguridad y el Modelo de las Tres Líneas

El Modelo de las Tres Líneas, desarrollado por el Instituto de Auditores Internos (IIA), es una herramienta clave para comprender cómo se estructura el entorno de control en trabajos de auditoría centradas en tecnología de la información (TI), ciberseguridad, privacidad de datos y riesgos tecnológicos. Este enfoque permite distinguir claramente las funciones que asumen cada una de las líneas de defensa en relación con la gobernanza y los controles de TI, lo que a su vez facilita una planificación de auditoría eficaz y basada en riesgos. El IIA ha plasmado esta visión en su guía *GTAG: Evaluación de Riesgos de Ciberseguridad. Los Roles de las Tres Líneas de Defensa.*

La ciberseguridad, como disciplina, incluye el conjunto de prácticas, tecnologías y procesos destinados a proteger los activos de información de una organización frente a accesos no autorizados. Esta protección abarca sistemas, redes, aplicaciones y datos. Dado el creciente número e impacto de los ciberataques, la gestión de riesgos de ciberseguridad ha escalado a una prioridad estratégica para muchas entidades.

La *GTAG* del IIA analiza tanto amenazas comunes como riesgos emergentes que enfrentan las tres líneas de defensa, ofreciendo un enfoque ordenado y estructurado para evaluar integralmente los riesgos de ciberseguridad y los controles asociados. Dentro de este contexto, la auditoría interna cumple un rol fundamental, ya que debe analizar quién tiene acceso a la información crítica de la organización, cuáles son los activos más vulnerables frente a ataques, qué sistemas serían los más dañinos si se vieran comprometidos, y qué información sensible podría generar consecuencias legales, financieras o reputacionales si cayera en manos no autorizadas. También debe evaluarse si la Alta Dirección está realmente preparada para reaccionar de forma oportuna y efectiva ante un incidente de ciberseguridad.

Además de evaluar estos aspectos, la GTAG establece el papel del Jefe de Auditoría, quien debe liderar la función de aseguramiento y contribuir activamente a la protección de la entidad frente a ciberamenazas. El documento detalla cómo deben evaluarse los riesgos inherentes y las amenazas relevantes, cómo deben clarificarse las responsabilidades de cada una de las líneas de defensa y cómo se identifican brechas en el sistema de aseguramiento institucional. También se especifican las obligaciones de reporte que recaen sobre la auditoría interna frente a este tipo de riesgos.

e.2. La primera línea: gestión operativa de TI

La primera línea está conformada por quienes operan directamente los sistemas de TI. Se trata de equipos técnicos como personal de soporte, administradores de sistemas, desarrolladores y usuarios con privilegios especiales. Este grupo es responsable de implementar, mantener y operar los controles tecnológicos que aseguran el funcionamiento diario de la entidad. Entre sus responsabilidades se incluye garantizar la continuidad y disponibilidad de los servicios digitales, aplicar mecanismos como autenticación, respaldo de información, administración de cambios, aplicación de parches y resguardo físico y lógico de los activos informáticos. Asimismo, estos actores deben estar capacitados para identificar los riesgos tecnológicos en sus operaciones y reportarlos oportunamente.

e.3. La segunda línea: funciones de control de TI

La segunda línea la integran áreas especializadas como gestión de riesgos de TI, ciberseguridad, cumplimiento normativo, protección de datos personales, continuidad operativa y privacidad. Estas funciones actúan como soporte y supervisión de la primera línea, velando porque los controles sean adecuados, estén bien diseñados y operen de forma efectiva. Evalúan el cumplimiento de políticas institucionales de seguridad de la información, diseñan planes de respuesta ante incidentes, verifican que la clasificación de los datos y la asignación de permisos de acceso se realicen conforme al principio de menor privilegio, y monitorean indicadores clave relacionados con los riesgos tecnológicos y de ciberseguridad.

e.4. La tercera línea: auditoría interna

La auditoría interna representa la tercera línea. Su función es brindar aseguramiento independiente y objetivo respecto de la eficacia de la gobernanza tecnológica, el manejo de riesgos y los controles establecidos por las dos líneas anteriores. Esta revisión incluye el análisis de los controles generales de TI y de los controles de aplicación, así como la verificación del cumplimiento de marcos normativos, tales como; *COBIT, NIST, ISO/IEC 27001*, o regulaciones específicas en materia de privacidad. Además, la auditoría interna realiza pruebas sobre aspectos clave como la segregación de funciones, los accesos privilegiados, la gestión de respaldos y la capacidad de recuperación operativa. Con base en esta evaluación, emite recomendaciones estratégicas orientadas a reducir riesgos emergentes, como ataques de *ransomware*, interrupciones por fallos de continuidad tecnológica, o vulnerabilidades en la cadena de suministro digital.

e.5. Importancia durante la planificación del trabajo

Durante la planificación de un trabajo de auditoría con enfoque en TI, aplicar el Modelo de las Tres Líneas permite clarificar qué funciones o áreas serán objeto de revisión directa. También ayuda a detectar posibles deficiencias en el diseño de los controles o en la asignación de roles y responsabilidades, a evaluar el nivel de madurez en la gobernanza tecnológica, y a ajustar el alcance del trabajo según las responsabilidades que cada línea tenga frente a los riesgos identificados. Esta estructuración previa es clave para priorizar los recursos de auditoría y enfocar las pruebas en las áreas más críticas del entorno tecnológico de la organización.

e.6. Enfoque para evaluar riesgos y controles de ciberseguridad

El marco de gobierno de ciberseguridad descrito en la guía *GTAG: Evaluación de Riesgos de Ciberseguridad. Los Roles de las Tres Líneas de Defensa*, elaborada por el Instituto de Auditores Internos (IIA), plantea que todo sistema de ciberseguridad sólido debe sustentarse en seis elementos interdependientes. Estos componentes no solo son esenciales para diseñar controles efectivos, sino también para asegurar que su implementación y funcionamiento estén alineados con los objetivos estratégicos de la organización y con los riesgos reales que enfrenta.

La revisión periódica y el fortalecimiento constante de estos seis elementos es clave para mantener una postura de ciberseguridad robusta. En un entorno donde los riesgos tecnológicos evolucionan con rapidez, descuidar alguno de estos componentes puede comprometer la resiliencia operativa de la entidad. Por eso, la evaluación no debe hacerse de forma aislada o parcial. El auditor interno debe analizar cómo ha sido concebido cada elemento, cómo se ha implementado en la práctica y cómo interactúa con los demás dentro del sistema global de control.

Este enfoque sistémico permite detectar debilidades ocultas o inconsistencias que podrían dejar a la organización expuesta frente a amenazas cibernéticas, incluyendo ataques emergentes o sofisticados que se aprovechan de vacíos en la gobernanza de TI, en la gestión de accesos, en la respuesta a incidentes o en la protección de datos críticos.

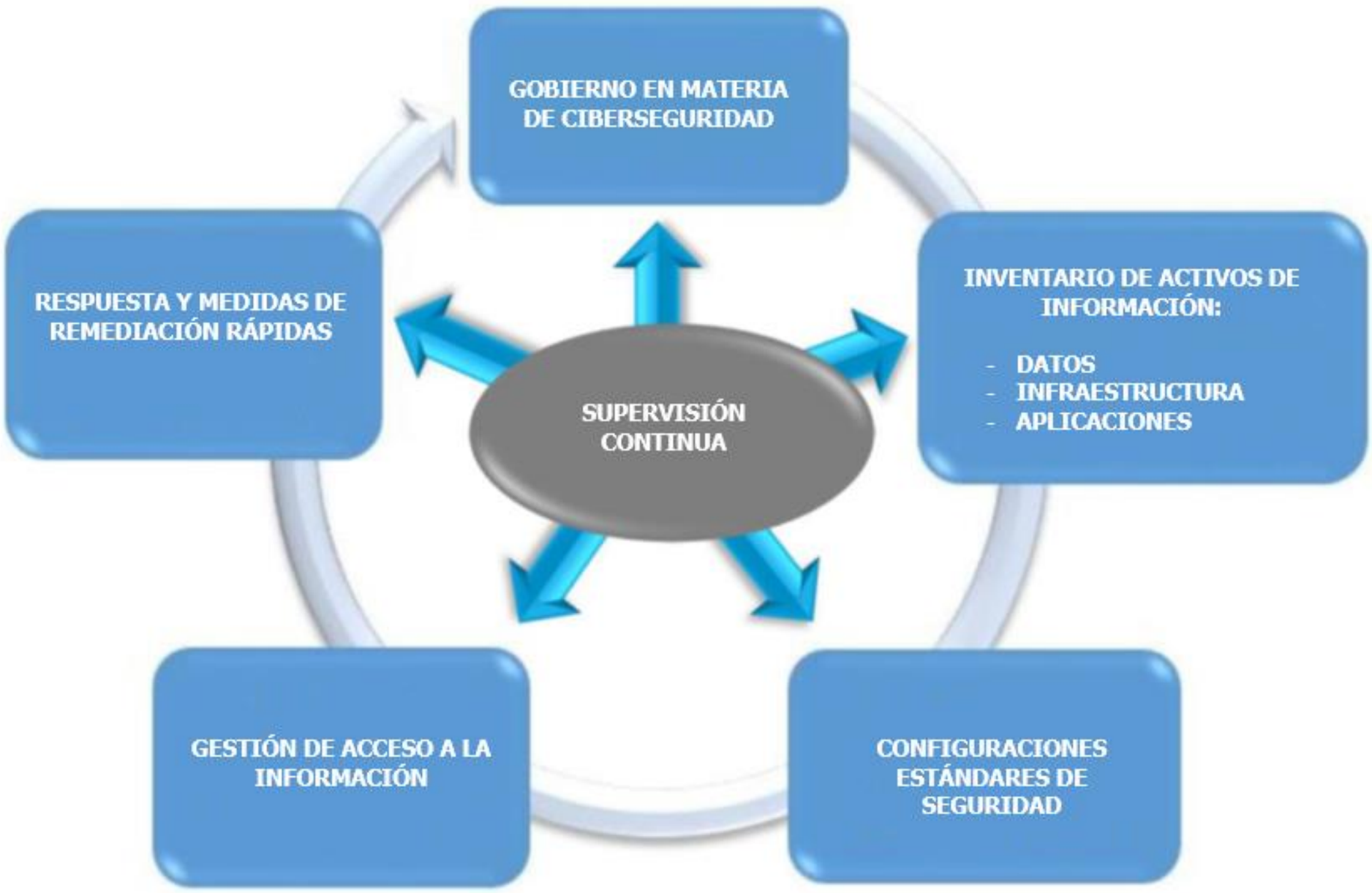
Una evaluación bien estructurada de estos seis componentes le permite al Jefe de Auditoría contar con una base objetiva y bien sustentada para emitir un juicio sobre el nivel de preparación institucional frente a los ciberataques. Si durante esta revisión se detectan fallas en el diseño o en la coordinación operativa de los elementos evaluados, se puede concluir que la organización no está adecuadamente preparada para enfrentar y responder con eficacia ante eventos de alto impacto en el entorno digital.

Temas Claves

Modelo de las Tres Líneas en el Entorno de TI:

- *Permite estructurar claramente las responsabilidades de gobernanza, control y aseguramiento en torno a la gestión de TI, ciberseguridad y privacidad.*
- *Facilita la identificación de brechas o debilidades en los controles de TI aplicados por cada línea, mejorando la planificación basada en riesgos.*
- *Apoya el ajuste del alcance del trabajo, evaluando la madurez y coordinación de roles frente a riesgos tecnológicos.*

Esquema N° 5. Marco para la Evaluación de Riesgos de Ciberseguridad



Fuente: GTAG: Evaluación de Riesgos de Ciberseguridad. Los Roles de las Tres Líneas de Defensa – Instituto de Auditores Internos Global - IIA

Temas Claves

- *La efectividad de la ciberseguridad depende de que todos los componentes del marco funcionen de manera interdependiente; una debilidad en uno puede afectar el conjunto.*
- *Es fundamental evaluar integralmente el diseño, la operación y la interacción entre los componentes para identificar posibles vulnerabilidades.*
- *El resultado de la evaluación proporciona insumos para fortalecer la preparación y resiliencia de la organización frente a riesgos y amenazas cibernéticas.*

f. Trabajo remoto versus presencial: implicancias para la planificación de auditoría

La generalización del trabajo remoto, entendido como el desempeño de funciones laborales fuera de las oficinas institucionales, plantea desafíos concretos para la auditoría interna. Estos desafíos no son menores: abarcan desde riesgos de ciberseguridad hasta barreras para acceder a procesos críticos o recolectar evidencia confiable. El uso de redes inseguras, dispositivos personales no controlados (*BYOD*) y aplicaciones no autorizadas se encuentran entre los factores que aumentan la exposición a vulnerabilidades operativas y tecnológicas.

Cuando una proporción significativa del personal trabaja a distancia, tanto la evaluación de riesgos a nivel organizacional como la evaluación específica para cada trabajo de auditoría deben incorporar explícitamente esta realidad. Ignorar el impacto del trabajo remoto en los procesos podría llevar a una planificación desalineada con las verdaderas condiciones del entorno, dejando sin cubrir áreas sensibles en materia de control interno, gestión de riesgos o gobernanza institucional.

Desde el punto de vista metodológico, y conforme a NOGAI, el auditor interno tiene la responsabilidad de ajustar el enfoque del trabajo para que refleje adecuadamente el contexto operativo. Esto implica identificar qué procesos han sido alterados por la virtualización del trabajo, adaptar la metodología para evaluar los riesgos asociados al acceso remoto y definir alternativas sólidas para recolectar evidencia sin comprometer la trazabilidad ni la calidad de los hallazgos.

Durante la planificación, es clave anticipar ciertas condiciones prácticas que podrían afectar la ejecución. Por ejemplo, debe diseñarse un plan de comunicación remota claro y estructurado, que contemple reuniones virtuales de apertura, seguimientos intermedios y revisiones de borradores en formatos que faciliten el intercambio sincrónico y asincrónico con los responsables. Las entrevistas deben programarse de manera estratégica, en sesiones breves y enfocadas, evitando cargar de trabajo innecesario a los equipos auditados.

También resulta fundamental acordar con antelación los medios de acceso a documentos y plataformas digitales, definiendo canales seguros para el envío y la consulta de información. Esto puede incluir el uso de carpetas compartidas en servidores institucionales, accesos temporales a sistemas o herramientas de escritorio remoto.

Por último, no puede pasarse por alto la preparación del propio equipo auditor. La eficacia en entornos remotos exige no solo competencias técnicas como el manejo de herramientas digitales y el análisis de datos, sino también habilidades interpersonales específicas, como la comunicación efectiva a distancia, la gestión del tiempo en modalidad virtual y la capacidad de generar confianza sin contacto presencial.

Incorporar todas estas variables en la planificación no solo fortalece la calidad del trabajo de auditoría, sino que también protege la capacidad operativa de la función frente a un entorno de control cada vez más descentralizado y tecnológicamente mediado.

Temas Claves

- *Identificar los procesos y riesgos afectados por el trabajo remoto, como uso de redes inseguras o aplicaciones no autorizadas.*
- *Ajustar la metodología y mecanismos de recolección de evidencia para mantener la calidad y trazabilidad del trabajo en entornos digitales.*
- *Garantizar competencias del equipo auditor y estrategias de comunicación remota eficaces para coordinar el trabajo con la actividad bajo revisión.*

g. Documentación y seguimiento de riesgos de TI en la planificación del trabajo

La integración efectiva de los riesgos y controles de tecnologías de la información (TI) en la planificación del trabajo de auditoría no solo mejora la calidad técnica del enfoque adoptado, sino que también garantiza su alineación con las NOGAI. Este enfoque permite construir auditorías más relevantes, normativamente sólidas y ajustadas a los desafíos actuales que enfrentan las entidades públicas.

Durante la fase de planificación, la documentación adecuada de los riesgos tecnológicos identificados constituye un elemento esencial. No se trata únicamente de enumerar amenazas, sino de dejar evidencia clara, coherente y trazable sobre las decisiones adoptadas, la lógica empleada para establecer prioridades y la conexión entre los riesgos, los controles existentes y los objetivos del trabajo de auditoría. Esta documentación debe contemplar la identificación y evaluación de los principales riesgos de tecnologías de la información (TI) relacionados con el objetivo dl trabajo de auditoría, tales como vulnerabilidades en la infraestructura, ciberseguridad, privacidad de datos, uso de plataformas digitales, dependencia tecnológica y gestión de accesos.

Asimismo, debe detallarse la existencia de controles clave, tanto generales como específicos, que busquen mitigar estos riesgos. Esto incluye desde controles generales de acceso, cambios, respaldos y monitoreo, hasta controles de aplicación sobre la entrada, procesamiento y salida de datos, además de medidas de ciberseguridad y privacidad implementadas por la entidad.

La priorización de los riesgos considerados relevantes debe estar fundamentada en criterios técnicos sólidos, tales como; impacto potencial, probabilidad de ocurrencia, exposición residual y conexión directa con los objetivos estratégicos o críticos de la actividad bajo revisión. Este análisis justifica las decisiones sobre qué riesgos serán abordados mediante procedimientos específicos y cuáles podrán ser excluidos del alcance por razones técnicas, operativas o de cobertura.

Para garantizar un enfoque estructurado y coherente, la planificación debe dejar constancia de al menos seis elementos clave: los riesgos de TI identificados y su evaluación en términos de impacto y probabilidad; los controles existentes y una valoración inicial de su eficacia; las fuentes de información utilizadas, como entrevistas, documentos técnicos, normativa vigente y auditorías previas; los marcos de referencia aplicados, como *COBIT, NIST, ISO/IEC 27001* o similares; las decisiones tomadas respecto a la inclusión o exclusión de ciertos riesgos en el alcance del trabajo; y finalmente, cualquier limitación prevista o riesgo emergente que pueda afectar la ejecución futura del trabajo.

Este enfoque permite no solo una planificación técnicamente robusta, sino también una ejecución más dirigida, una evaluación más pertinente y un proceso de seguimiento más efectivo, alineado con las mejores prácticas internacionales en auditoría de TI.

Temas Claves

- *Registrar de forma detallada los riesgos de TI, controles clave y razones técnicas de su priorización, alineados con los objetivos del trabajo y principios de las NOGAI.*
- *Asegurar que cada riesgo esté vinculado a objetivos específicos, criterios claros y procedimientos definidos en la planificación.*
- *Utilizar marcos internacionales (como COBIT, NIST, ISO 27001) y fuentes confiables para fundamentar la evaluación y anticipar riesgos emergentes.*

Paso N° 3

Establecer o Redefinir los Objetivos y Alcance del Trabajo

a. Objetivos del trabajo

Los objetivos del trabajo de auditoría responden a una pregunta fundamental: **¿qué se necesita verificar o evaluar para generar conclusiones útiles y relevantes que aporten valor a la organización?** Su formulación debe ser clara y precisa, ya que estos objetivos definen el propósito del trabajo, orientan su ejecución y permiten evaluar si se han cumplido las metas establecidas. Además, cumplen un rol fundamental en mantener la coherencia interna del informe, facilitando su lectura, discusión y seguimiento posterior.

Durante la planificación, los objetivos guían al equipo auditor en la identificación y análisis de los riesgos residuales asociados a la actividad que se revisa, ya sea un proceso específico, una función institucional o un área transversal. Esta definición no es una tarea aislada, sino que recae principalmente en el Jefe de Auditoría, quien debe trabajar de forma colaborativa con el Supervisor y el resto del equipo, asegurando que los objetivos estén bien definidos y que sean alcanzables en el marco del trabajo programado.

Cuando el trabajo forma parte del Plan Anual de Auditoría, los objetivos deben alinearse con los definidos previamente durante la etapa de evaluación de riesgos que dio origen a ese plan. En cambio, si se trata de un trabajo fuera del plan de auditoría, como un trabajo solicitado por la autoridad o derivada de una situación emergente, los objetivos deben ser definidos antes del inicio, respondiendo de forma directa al problema o situación que motivó su ejecución.

Los objetivos de auditoría pueden orientarse hacia distintas dimensiones del control interno, conforme al marco conceptual del *COSO*. Algunos estarán enfocados en evaluar la economía, eficiencia y eficacia de los procesos, así como la adecuada protección de los recursos institucionales, lo que corresponde a los objetivos operativos. Otros se centrarán en verificar la calidad, integridad, oportunidad y confiabilidad de la información financiera y no financiera, en línea con los objetivos de información. Particularmente en el sector público, una parte significativa de los trabajos de auditoría tendrá como finalidad comprobar el grado de cumplimiento de leyes, normativas, reglamentos y políticas internas, respondiendo así a los objetivos de cumplimiento.

Desde el punto de vista metodológico, los objetivos de auditoría se pueden clasificar en generales y específicos. Los generales expresan el propósito amplio del trabajo. Deben ser coherentes con el mandato institucional de la auditoría interna y, si corresponde, coincidir con lo establecido en el Plan Anual de Auditoría. Los objetivos específicos, en cambio, se definen a partir de la identificación de los riesgos clave y los controles asociados dentro del proceso o actividad bajo revisión. Estos objetivos específicos permiten establecer metas concretas que orientan directamente el diseño de pruebas, la ejecución del trabajo en terreno y la formulación de conclusiones.

Para asegurar su utilidad práctica, los objetivos específicos deben cumplir con el enfoque *SMART*, es decir, deben ser específicos, medibles, alcanzables, relevantes y acotados en el tiempo. Esta condición garantiza que puedan ser utilizados como base para diseñar procedimientos efectivos y, posteriormente, para evaluar si se alcanzaron los resultados esperados. Una buena formulación de objetivos es, en suma, la piedra angular de una auditoría interna bien ejecutada.

A continuación se explica el concepto *SMART* adaptado al contexto de la auditoría interna conforme a las NOGAI:

Tabla N° 7: Objetivos Específicos del Criterio SMART

Criterio SMART	Descripción Aplicada a Auditoría Interna	Ejemplo Aplicado
S – Específico (*Specific*)	El objetivo debe definir claramente qué aspecto del proceso o sistema de la actividad bajo revisión que será evaluado.	"Verificar la existencia y aplicación de los criterios de evaluación en las contrataciones mayores a XXX UTM."
M – Medible (*Measurable*)	Debe permitir la recolección de evidencia y comparación con un criterio definido.	"Evaluar si al menos el 90% de los expedientes contiene el acta del comité evaluador."
A – Alcanzable (*Achievable*)	Debe ser viable con los recursos, tiempo y alcance disponibles.	"Analizar la documentación de 20 contratos seleccionados aleatoriamente del año 2024."
R – Relevante (*Relevant*)	Debe estar alineado con los riesgos identificados y los objetivos del trabajo general.	"Evaluar la segregación de funciones para mitigar riesgos de fraude en compras públicas."
T – Temporal (*Time-bound*)	Debe establecer un periodo o fecha para su logro dentro del cronograma de auditoría.	"Completar la evaluación de controles clave en la primera semana del trabajo de campo."

a.1. Relación entre los objetivos de auditoría y los objetivos de la actividad bajo revisión

En el diseño de un trabajo de auditoría interna es clave entender y distinguir los objetivos propios del trabajo de auditoría respecto de los objetivos de la actividad que se revisa. Esta distinción, sin embargo, no implica separación, ya que ambos deben estar conectados de forma lógica y funcional.

Los objetivos de auditoría se formulan con el propósito de evaluar en qué medida los objetivos de la actividad bajo revisión están siendo cumplidos, si los riesgos que podrían impedir ese cumplimiento están debidamente controlados, y si existen desviaciones significativas que requieran atención. En ese sentido, los objetivos de auditoría no se crean en el vacío; responden directamente a la lógica de control y desempeño de la actividad evaluada.

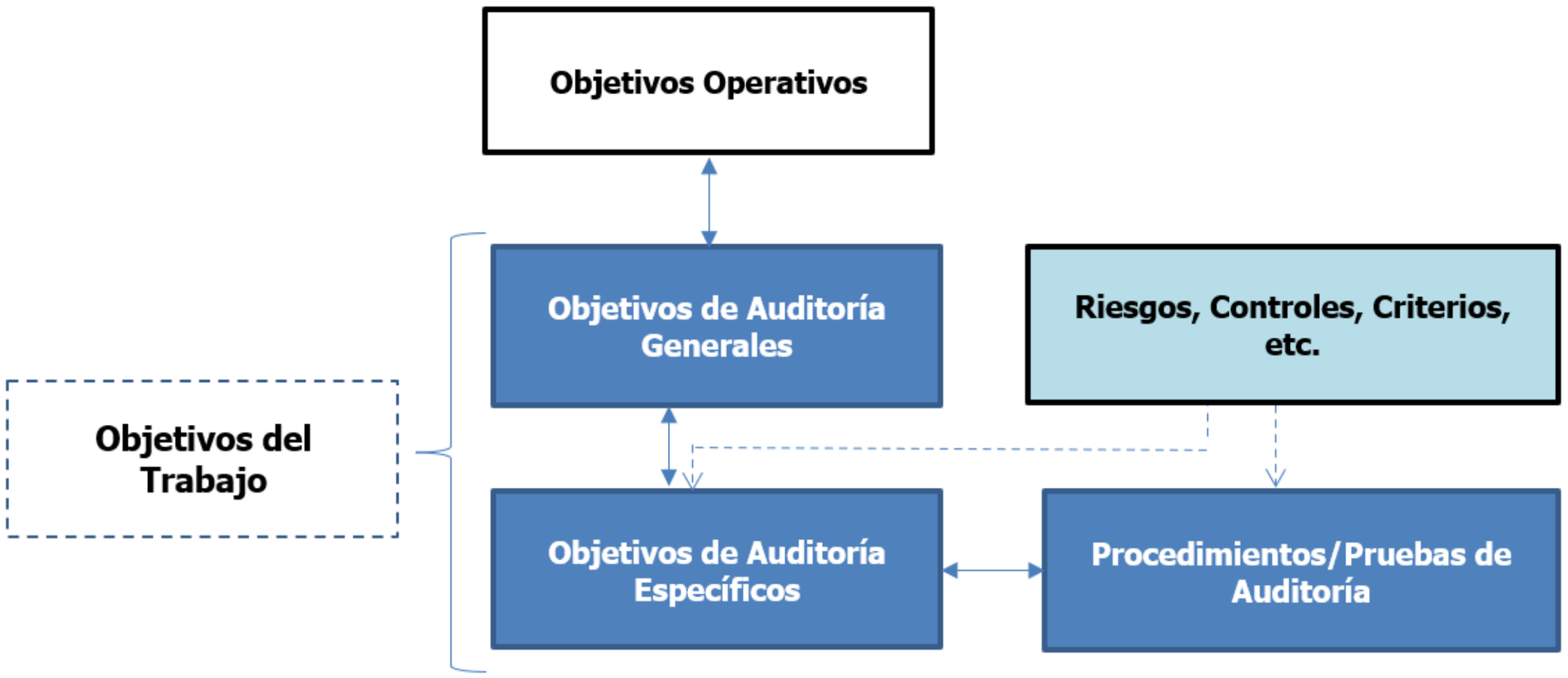
Por ejemplo, si una unidad de compras tiene como objetivo institucional asegurar adquisiciones oportunas, eficientes y a precios razonables, el objetivo específico de auditoría puede ser verificar si los sistemas y procedimientos implementados efectivamente permiten asegurar la oportunidad, calidad y razonabilidad de los precios en las adquisiciones. La auditoría no reemplaza los objetivos de la actividad, sino que los examina desde una perspectiva independiente y técnica, a fin de verificar si se están cumpliendo y si los controles existentes son adecuados para sostener ese cumplimiento.

Los procedimientos de auditoría son las herramientas concretas que permiten recolectar evidencia sobre estos objetivos. La calidad de un trabajo de auditoría no depende únicamente de aplicar muchos procedimientos o técnicas sofisticadas, sino de que estos estén bien alineados con los objetivos del trabajo. Un procedimiento, por riguroso que sea, pierde valor si no contribuye directamente a responder las preguntas clave planteadas en los objetivos de auditoría.

Aquí es donde entra en juego el juicio profesional del auditor, su experiencia técnica y su conocimiento del funcionamiento institucional. Estos elementos son indispensables para identificar cuáles objetivos son realmente relevantes, dónde están los puntos críticos, y qué procedimientos aportan evidencia útil. El auditor debe saber distinguir entre lo esencial y lo accesorio, enfocándose en los aspectos que generan valor y permiten emitir conclusiones fundamentadas.

En la fase de planificación, la relación entre los distintos elementos del trabajo de auditoría debe estructurarse de forma lógica y coherente. Los objetivos operativos de la entidad constituyen el punto de partida, a partir del cual se derivan los objetivos específicos de auditoría, ajustándolos según el nivel de riesgo identificado. Con base en estos objetivos, se diseñan los procedimientos y pruebas necesarios para obtener evidencia suficiente y adecuada que permita sustentarlos. Todo este proceso debe desarrollarse en el marco de una evaluación integral de riesgos, controles existentes y criterios aplicables, garantizando así un enfoque de auditoría sólido, alineado con los propósitos institucionales y orientado a resultados concretos.

Esquema N° 6: Relación Objetivos Operativos - Objetivos de Auditoría - Procedimientos de Auditoría



En **Anexo N° 2** se describen procesos y/o áreas comunes en una entidad, y objetivos y procedimientos de auditoría relacionados.

a.2. Lineamientos para la formulación de objetivos de auditoría

a.2.1. Características y buenas prácticas en la formulación de objetivos de auditoría

Los objetivos son el eje que sostienen un trabajo de auditoría interna bien estructurado. Su correcta formulación garantiza que el trabajo esté enfocado, sea relevante y tenga impacto. Cuando un objetivo está bien definido, orienta todas las etapas del proceso: da Dirección a la planificación, estructura la ejecución y sustenta la redacción de conclusiones en el informe final. Además, ayuda a evitar la recolección de información innecesaria, favorece la eficiencia en el uso de recursos y delimita con precisión el alcance, el enfoque y el periodo de revisión.

Para asegurar la calidad técnica de los objetivos, se recomienda seguir ciertas buenas prácticas. Una de ellas es redactarlos de manera que puedan ser verificados, ya sea como preguntas que orienten la búsqueda de evidencia, o como afirmaciones cuya validez pueda confirmarse o rechazarse. Es fundamental evitar ambigüedades, generalizaciones o expresiones vagas que dificulten la interpretación y evaluación de los resultados.

Asimismo, un objetivo bien formulado debe identificar claramente la actividad o proceso bajo revisión, señalando las unidades responsables y delimitando el alcance en función de los recursos disponibles, el tiempo asignado y la complejidad del entorno. Esta claridad no solo facilita la ejecución técnica del trabajo, sino que también promueve la transparencia y la comprensión por parte de las partes interesadas.

Otra buena práctica es asegurar que los objetivos incorporen, de manera transversal, el análisis de los procesos clave vinculados con gobernanza, gestión de riesgos y control interno. Esta integración permite que la auditoría no se limite a un análisis superficial, sino que profundice en los factores estructurales que influyen en el desempeño y en la exposición al riesgo.

Es importante validar los objetivos con el responsable de la actividad que será revisada, con la Alta Dirección o con el Jefe de Servicio, según corresponda, antes de iniciar el trabajo. Esto permite confirmar su pertinencia, su alineación con las prioridades institucionales y su capacidad para aportar valor.

En su formulación, los objetivos deben considerar la posibilidad de que existan errores, incumplimientos normativos, fraudes u otras exposiciones críticas. Al anticipar estos escenarios, se fortalece el enfoque de prevención y se amplía la utilidad del trabajo como herramienta de mejora.

Por último, debe haber una coherencia evidente entre los objetivos de auditoría definidos, los procedimientos y pruebas aplicadas, la evidencia obtenida y los contenidos del informe final. Esta trazabilidad entre los elementos clave del trabajo asegura que las conclusiones están fundamentadas en evidencia relevante, suficiente y fiable, y que responden de manera directa a los objetivos planteados.

a.2.2. Elementos a considerar al establecer los objetivos de un trabajo de auditoría

Al definir los objetivos de un trabajo, es esencial considerar varios factores que influyen directamente en el enfoque, la profundidad y la relevancia del trabajo. Estos elementos aseguran que los objetivos estén alineados con el contexto institucional, los riesgos prioritarios y los marcos normativos aplicables.

Uno de los primeros aspectos a tener en cuenta son los requisitos normativos. Si el trabajo tiene como propósito evaluar el cumplimiento de leyes, regulaciones o normas internas, los objetivos deben incorporar explícitamente esa finalidad. El cumplimiento debe evaluarse no solo desde la existencia formal de normativas, sino también desde su correcta aplicación y supervisión.

La estrategia y los objetivos institucionales también deben estar reflejados en los objetivos de auditoría. Esto permite alinear el trabajo con las prioridades estratégicas de la organización, reforzando su capacidad para generar valor y apoyar la toma de decisiones.

Otro aspecto central es el análisis de la gobernanza, la gestión de riesgos y los procesos de control. Estos tres componentes están interconectados, y cualquier objetivo bien formulado debería considerar su interacción, ya sea en términos de diseño, implementación o eficacia.

El apetito y la tolerancia al riesgo definidos por la organización son factores clave. Evaluar si los controles actuales están alineados con los niveles de riesgo aceptables permite validar si la entidad opera dentro de sus márgenes definidos o si existen exposiciones críticas no mitigadas.

Los objetivos siempre deben considerar las políticas y procedimientos internos de la actividad bajo revisión y de la entidad. No solo es necesario verificar si se cumplen, sino también si estas políticas son adecuadas, actualizadas y coherentes con el entorno operativo y los objetivos de control.

Los informes de auditorías previas son una fuente relevante para definir los objetivos. Las debilidades o riesgos que hayan sido detectados anteriormente deben considerarse, en especial si no han sido resueltos o si persisten condiciones similares que podrían reproducir problemas ya identificados.

También debe integrarse cuando sea el caso, el análisis del trabajo de otros proveedores de aseguramiento, como auditores externos o fiscalizadores. Las observaciones o hallazgos realizados por estos actores pueden revelar vacíos que el auditor interno debe abordar en sus propios objetivos, fortaleciendo así la cobertura general de aseguramiento.

A continuación, se presentan ejemplos que ilustran cómo estos elementos se traducen en objetivos concretos de auditoría interna:

Ejemplo 1

Objetivo general 1: Verificar si la Dirección de recursos humanos aplica correctamente los criterios normativos y presupuestarios para la asignación de bonificaciones al personal durante el año 2024.

Objetivo específico 1.1: Comprobar que las bonificaciones otorgadas cuentan con respaldo documental conforme a los criterios establecidos en la normativa interna.

Objetivo específico 1.2: Validar que las bonificaciones se ajustan al presupuesto aprobado para el periodo auditado.

Ejemplo 2

Objetivo general 2: Evaluar si las contrataciones directas realizadas durante emergencias se ajustan a la normativa vigente, los controles internos establecidos y criterios de eficiencia en el uso de los recursos públicos.

Objetivo específico 2.1: Revisar si las adquisiciones por trato directo en emergencias cuentan con justificación legal y técnica documentada.

Objetivo específico 2.2: Analizar si los bienes y servicios adquiridos fueron entregados y utilizados dentro de los plazos y condiciones acordadas.

Temas Claves

- *Definen el propósito ya que los objetivos establecen qué se busca lograr con la auditoría y delimitan el alcance del trabajo.*
- *Deben ser claros y medibles al ser específicos, alineados a los riesgos y redactados bajo el enfoque SMART.*
- *El Jefe de Auditoría y el equipo deben definir y validar los objetivos, asegurando coherencia con el plan de auditoría y las necesidades de la entidad.*

b. Alcance del trabajo

El alcance del trabajo de auditoría responde a la pregunta: **¿Cuáles son las áreas, procesos, actividades y períodos específicos que serán objeto de revisión y evaluación, y cuáles quedarán expresamente excluidos?**

Una vez definidos los objetivos generales y específicos del trabajo, es necesario establecer los límites técnicos, temporales y operativos dentro de los cuales se desarrollará. Este alcance debe ser claro, razonable y trazable, considerando los recursos disponibles, los riesgos evaluados y las prioridades institucionales.

El alcance constituye el marco operativo dentro del cual se desarrollará el trabajo de auditoría. Es tan relevante como los propios objetivos, ya que una delimitación imprecisa puede derivar en revisiones incompletas, difusas o excesivamente amplias. Se establece durante la fase de planificación, con base en la información recopilada hasta ese momento, y su adecuada definición permite asegurar que el trabajo sea pertinente, eficaz y enfocado en los aspectos críticos de la actividad bajo revisión.

Elementos que debe incluir el alcance

Para una formulación precisa y útil, el alcance debe abarcar al menos los siguientes aspectos:

- Temas, materias o procesos específicos incluidos en el trabajo.
- Población y muestras que se evaluarán, con su justificación técnica (criterios de muestreo, umbrales de materialidad o relevancia).
- Período de tiempo cubierto, ya sea un año calendario, un trimestre, un ejercicio presupuestario, etc.
- Unidades organizativas, áreas físicas, plataformas digitales o sistemas funcionales involucrados en la actividad auditada.
- Sistemas, registros, bienes o personal relevantes para la revisión, aun cuando estén a cargo de terceros (por ejemplo, servicios externalizados o alianzas público-privadas).
- Exclusiones deliberadas, si las hubiera, indicando con claridad los temas, procesos, unidades o periodos que quedan fuera del alcance y los motivos técnicos, estratégicos o normativos que justifican tal decisión.

Responsabilidad y documentación del alcance

El Jefe de Auditoría es responsable de definir el alcance, en coordinación con el Supervisor y el equipo auditor. Esta definición debe estar debidamente documentada en la planificación y vinculada con los objetivos del trabajo y los riesgos identificados.

Es fundamental que cualquier limitación de alcance sea identificada, justificada técnicamente y documentada de forma explícita. Estas restricciones deben comunicarse oportunamente a la Dirección o jefatura responsable de la actividad bajo revisión, con el fin de resolver o mitigar sus efectos.

Si no se logra una resolución adecuada y persiste una limitación significativa, esta debe ser escalada formalmente, por el Jefe de Auditoría a la Alta Dirección o al Jefe de Servicio, conforme a lo establecido en el procedimiento o protocolo correspondiente.

Importancia práctica del alcance

Un alcance bien definido:

- Evita desviaciones metodológicas o interpretaciones erróneas durante la ejecución del trabajo.
- Garantiza la coherencia entre lo que se evalúa y lo que se concluye.
- Protege la calidad técnica del trabajo ante observaciones internas o externas.
- Facilita la rendición de cuentas y la trazabilidad del proceso o ciclo de auditoría.

b.1. Factores que influyen en la definición o ajuste del alcance

La definición del alcance es una etapa crítica en la planificación del trabajo. Debe construirse sobre un análisis riguroso y revisarse cuando surjan factores que afecten significativamente la cobertura prevista. En este proceso, resulta esencial considerar también las expectativas de los grupos de interés respecto al propósito, objetivos y cobertura del trabajo, especialmente si se trata de trabajos de aseguramiento o asesoramiento.

El Jefe de Auditoría, el Jefe de Servicio y la Alta Dirección, si corresponde, deberían reunirse para discutir las expectativas generales de los trabajos de auditoría interna, las cuales deben reflejarse en el Estatuto de Auditoría Interna, el Mandato y el Plan Anual de Auditoría. Desde el inicio del trabajo, los auditores internos deben comprender claramente esas expectativas para garantizar su alineación estratégica con los objetivos de la actividad bajo revisión.

Durante la ejecución del trabajo, si los objetivos o el alcance cambian, es indispensable:

- Notificar de forma oportuna a los grupos de interés, a fin de gestionar adecuadamente sus expectativas.
- Documentar las razones que motivan tales cambios en los papeles de trabajo.
- Asegurar que el Jefe de Auditoría apruebe cualquier modificación significativa al alcance o a los objetivos durante la auditoría.
- Comunicar adecuadamente los cambios y su justificación técnica al Jefe de Servicio o alta Dirección, si corresponde.

Ejemplos típicos de ajustes incluyen la exclusión de una unidad que ha cesado operaciones, o la incorporación de nuevos procesos críticos no previstos inicialmente. En algunos casos, incluso podría ser necesario ampliar el alcance para asegurar que los objetivos se aborden de forma adecuada. Tarea que debe ser aprobado por el Jefe de Auditoría.

Entre los factores clave a considerar para definir o modificar el alcance se incluyen:

Tabla N° 8: Factores Definir o Modificar el Alcance del Trabajo

Categoría	Factor Específico
Historial de auditoría	• Trabajos previos realizados y antigüedad de sus resultados.
Estructura organizativa	• Cambios recientes, nuevas unidades, reorganizaciones internas.
Normativa y complejidad funcional	• Grado de regulación, existencia de marcos normativos extensos o complejos.
Tiempos y duración del trabajo	• Calendario disponible para ejecución y entrega de resultados.
Naturaleza del trabajo	• Aseguramiento, cumplimiento, desempeño, asesoramiento o seguimiento.
Muestreo	• Tipo de muestreo seleccionado: estadístico, dirigido, juicio profesional, etc.
Recursos disponibles	• Disponibilidad y competencia del equipo auditor; herramientas y soporte técnico.
Riesgo y controles	• Nivel de riesgo, control residual, efectividad de controles existentes.
Hallazgos previos	• Situaciones no resueltas o medidas correctivas en curso.
Expectativas de usuarios	• Necesidades y prioridades de quienes utilizarán el informe final.
Mandatos normativos	• Disposiciones legales o requerimientos que originan el trabajo de auditoría.
Gobernanza y control	• Presencia o ausencia de estructuras de gobernanza, gestión de riesgos y control.

Esta visión estructurada permite al equipo auditor anticipar limitaciones, detectar riesgos no considerados inicialmente y asegurar que el trabajo se mantenga relevante, enfocado y técnicamente bien fundamentado.

b.2. Elementos a documentar en la definición del alcance

Para asegurar un trabajo de auditoría efectivo, trazable y alineado con los objetivos definidos, el alcance debe documentarse desde la fase de planificación. Esta documentación debe permitir comprender con exactitud qué se va a revisar, en qué condiciones, y con qué criterios técnicos.

A continuación, se detallan los elementos mínimos que deben quedar registrados en la definición del alcance:

Tabla N° 9: Elementos a Documentar en la Definición del Alcance

Categoría	Elemento Específico
Alcance Temporal y Poblacional	• Periodo cubierto por las pruebas • Universo: tipo y volumen de transacciones
Cronograma y Duración	• Tiempo disponible para el trabajo • Fechas clave (inicio, avances, informe final)
Datos e Información	• Ubicación y acceso a registros • Volumen y confiabilidad • Necesidad de reconstrucción de datos
Selección de Unidades o Áreas	• Justificación técnica de inclusión/exclusión • Relevancia estratégica u operativa
Muestreo	• Tamaño de muestra y universo total • Criterios de selección • Restricciones metodológicas
Recursos Humanos Clave	• Personal responsable en las unidades auditadas • Equipo auditor asignado y su especialización
Expertos y Apoyos Técnicos	• Necesidad de expertos técnicos (TI, legal, ambiental, etc.)
Limitaciones Previstas	• Restricciones de acceso • Condiciones de confidencialidad • Datos no disponibles

b.3. Limitaciones de alcance observadas en el desarrollo del trabajo de auditoría

Durante el desarrollo de un trabajo de auditoría pueden surgir condiciones que impidan realizar las pruebas o aplicar los procedimientos previstos en la planificación. Estas situaciones, afectan de manera parcial o total la cobertura del trabajo y deben ser gestionadas con cuidado para no comprometer la calidad o validez de los hallazgos.

Las limitaciones más comunes incluyen:

- Falta de acceso a información clave, como bases de datos, expedientes físicos, o plataformas digitales.
- Restricciones de tiempo o recursos, que impiden ejecutar ciertos procedimientos dentro del cronograma.
- Ausencia o no disponibilidad del personal relevante para entrevistas, validaciones o entrega de antecedentes.
- Restricciones institucionales o externas, como procesos legales, revisiones en curso por otros órganos o confidencialidad de datos.
- Modificaciones impuestas por los interesados, como solicitudes de incluir o excluir ciertos elementos del alcance acordado.

Ante cualquier limitación, el auditor debe documentar la situación, sus causas y sus efectos. Primero, debe intentar resolverla directamente con los responsables de la actividad bajo revisión. Si no hay solución, el Jefe de Auditoría debe informar a la Alta Dirección o al Jefe de Servicio, siguiendo el procedimiento de escalamiento establecido, e incluir una evaluación de las implicancias sobre el trabajo.

Ejemplo:

Durante un trabajo de auditoría al proceso de contratación de servicios informáticos en una institución pública, se solicitó acceso a expedientes clave relacionados con licitaciones de proveedores estratégicos. La Dirección jurídica informó que estos documentos estaban bajo revisión de un ente externo y no podían ser liberados sin autorización formal, lo cual generaría una demora significativa.

Ante la imposibilidad de acceder a información crítica dentro del plazo definido, el Jefe de Auditoría determinó la existencia de una limitación de alcance relevante. Esta fue documentada y reportada al Jefe de Servicio. Por lo anterior, se ajustó el enfoque del trabajo y se restringieron algunas pruebas sustantivas, según lo establece el procedimiento interno.

b.4. Ejemplos de declaración de alcance

Los siguientes ejemplos ilustran cómo se puede formular de forma clara y completa el alcance del trabajo de auditoría:

Ejemplo 1 – Auditoría a compras públicas:

- El trabajo de auditoría cubrirá el proceso de adquisiciones de bienes y servicios en la Unidad de Abastecimiento del Ministerio X, correspondiente al período enero a diciembre de 2023.
- Se revisará una muestra aleatoria de 100 compras, representando el 45% del monto total adjudicado en el período.
- No se incluirán las adquisiciones por convenio marco ni las compras internacionales, debido a restricciones de tiempo y acceso documental.

Ejemplo 2 – Auditoría de controles de ciberseguridad:

- El trabajo de auditoría evaluará los controles de seguridad en la red de TI, incluyendo los protocolos de gestión de accesos y privilegios, las medidas de protección de datos, las configuraciones de *firewall* y los planes de respuesta ante incidentes cibernéticos.
- El período cubierto será del 1 de enero al 30 de junio de 2023.
- Se enfocará en el entorno corporativo central, excluyendo filiales y dispositivos personales utilizados en modalidad de teletrabajo.

Temas Claves

- *El alcance define qué procesos, unidades, sistemas y períodos serán revisados, y cuáles se excluyen, con justificación técnica.*
- *Puede ajustarse por cambios en objetivos, riesgos, recursos o expectativas de partes interesadas; los cambios deben notificarse y documentarse.*
- *Debe registrarse claramente, incluyendo muestreo, cobertura y restricciones; si hay limitaciones críticas, deben informarse y escalarse si es necesario.*

b.5. Requisitos Temáticos (*Topical Requirements*) emitidos por el Instituto de Auditores Internos (IIA)

Los Requisitos Temáticos son uno de los componentes del Marco Internacional para la Práctica Profesional (MIPP), el cual también incluye las NOGAI. Cuando la función de auditoría interna provee aseguramiento sobre un área de riesgo específica cubierta por los Requisitos Temáticos, los auditores internos deben cumplir dichos requisitos, incluso aplicándolos durante la planificación de la auditoría.

Los Requisitos Temáticos incluyen los siguientes elementos:

- Requisitos obligatorios para la evaluación de la gobernanza, la gestión de riesgos y los procesos de control.
- Consideraciones no obligatorias que facilitan la implementación de los requisitos obligatorios por parte de los auditores internos.

La aplicabilidad de los Requisitos Temáticos se determina según el Plan de Auditoría Interna, quedando claramente documentadas las limitaciones de alcance, si las hubiera. Cuando se revisa un área de riesgo, los Requisitos Temáticos sirven como referencia inicial para evaluar el desempeño del trabajo y también están sujetos a evaluación de calidad externa.

El alcance del trabajo de auditoría debe ser claramente definido y proporcionar una orientación precisa sobre si se incorporarán, cuando sean aplicables.

Consideraciones para la incorporación de Requisitos Temáticos

- **Identificación de requisitos temáticos aplicables:** Los auditores internos deben evaluar y determinar cuáles de los requisitos del IIA son relevantes para el ámbito específico de la auditoría que se va a realizar, considerando la naturaleza del negocio, los riesgos inherentes y los objetivos del área auditada.

- **Adaptación del alcance:** La inclusión de estos requisitos puede implicar la ampliación o ajuste del alcance inicial para cubrir aspectos específicos que refuercen la profundidad y el enfoque de la auditoría.

- **Documentación y justificación:** Es fundamental documentar cómo se han integrado estos requisitos, asegurando que el equipo de auditoría y las partes interesadas comprendan la relevancia y el impacto en la planificación y ejecución del trabajo.

A la fecha de emisión de esta guía existen dos Requisitos Temáticos publicados por el IIA en 2025: Ciberseguridad y Terceras Partes, así como existía uno en consulta pública: Resiliencia Organizacional. El IIA ha indicado que futuros Requisitos Temáticos podrían abordar temas como Comportamiento Organizacional (*Organizational Behavior*)

Temas Claves

- *Los Requisitos Temáticos del IIA deben aplicarse cuando el trabajo trate de áreas de riesgo cubiertas por estos.*
- *Su incorporación puede requerir modificar el alcance y debe quedar documentada y justificada.*
- *Forman parte del MIPP y su cumplimiento puede ser evaluado externamente.*

b.6. Tipo de aseguramiento y justificación

En la etapa de planificación de un trabajo de auditoría, es imprescindible dejar claramente establecido el tipo de aseguramiento que se entregará. Esta definición debe estar incluida en la sección correspondiente al tipo de auditoría y al alcance previsto, y debe formar parte integral del memorando de planificación y del programa de trabajo.

Los servicios de aseguramiento que presta la auditoría interna se clasifican, según el nivel de confianza que proporcionan, en dos categorías principales:

- **Aseguramiento Razonable**

Este tipo de trabajo se diseña para otorgar un alto nivel de confianza sobre el tema revisado. Se caracteriza por una aplicación extensiva de procedimientos, incluyendo pruebas sustantivas, de cumplimiento, entrevistas, revisiones documentales, análisis de datos y otros métodos. Es el enfoque recomendado cuando el área bajo revisión involucra procesos críticos, alto nivel de exposición al riesgo, o cuando se espera que los resultados de la auditoría sirvan de base para decisiones relevantes por parte de la Dirección.

- **Aseguramiento Limitado**

Proporciona un grado moderado de confianza. Implica una cobertura más focalizada o menos intensiva, basada en procedimientos más acotados o selectivos. Este enfoque es adecuado cuando se trata de auditorías exploratorias, revisiones temáticas de bajo riesgo o trabajos de seguimiento. En estos casos, se busca detectar señales o validar condiciones clave sin realizar una revisión completa.

- **Criterios para justificar el tipo de aseguramiento**

La elección entre aseguramiento razonable o limitado no debe basarse únicamente en criterios formales o de tiempo, sino en una justificación técnica clara, basada principalmente en los siguientes factores:

- **Alcance de los procedimientos:**

  Se debe considerar la cantidad, profundidad y tipo de pruebas que se aplicarán. A mayor cobertura y complejidad, mayor la justificación para un aseguramiento razonable.

- **Objetivo principal y Naturaleza del trabajo:**

  Las revisiones de cumplimiento, evaluaciones de control interno o revisiones financieras suelen requerir un enfoque más robusto como es el razonable. Por el contrario, las auditorías exploratorias o de seguimiento podrían ajustarse a un enfoque limitado.

- **Nivel de riesgo identificado:**

  Si el nivel de riesgo residual es alto, el aseguramiento razonable sería lo esperado. Si los riesgos son menores o controlados, puede justificarse un enfoque limitado.

- **Disponibilidad y calidad de la evidencia:**

  En contextos donde el acceso a la información es limitado o la evidencia es insuficiente, un aseguramiento razonable puede no ser viable, y se debería optar por un enfoque limitado, con las salvedades correspondientes.

Para más información sobre este tema, se recomienda ver la Tabla N° 2: Aseguramiento Razonable vs. Aseguramiento Limitado de la Guía de Gestión y Servicios de Auditoría Interna (GGSAI) N° 6: Comunicación en Auditoría Interna y Formulación de Informes sobre Resultados del Trabajo.

- **Comunicación y documentación**

La elección del tipo de aseguramiento debe documentarse en los papeles de trabajo y quedar explícita en el memorando de planificación y en el informe final. Además, esta información debe ser comunicada a los grupos de interés relevantes desde el inicio, para asegurar que comprendan el alcance y las limitaciones del trabajo, y que sus expectativas estén alineadas con el tipo de cobertura que se entregará.

Temas Claves

- *Se debe definir si el trabajo será de aseguramiento razonable (alto nivel de confianza) o limitado (confianza moderada), según el riesgo y propósito.*
- *La elección debe basarse en factores como tipo y profundidad de los procedimientos, nivel de riesgo y calidad de la información disponible.*
- *Debe documentarse y comunicarse claramente a las partes interesadas para alinear expectativas sobre alcance y resultados.*

Paso N° 4

Identificar y/o Definir Criterios de Auditoría

a. Criterios de auditoría

Los criterios de auditoría responden a la pregunta: **¿Qué debe o debería ser?**

Se trata de los estándares, parámetros o requisitos que permiten comparar la situación observada con lo que se espera según las normas vigentes, las políticas y procedimientos internos o los modelos de referencia. Constituyen la base para evaluar si un proceso, resultado o práctica es adecuada, insuficiente, deficiente, irregular o no conforme.

Son esenciales porque permiten establecer con claridad la diferencia entre lo que se observa (condición) y lo que se espera (criterio). Esta comparación es el punto de partida de cualquier hallazgo de auditoría.

Una buena definición de los criterios de auditoría garantiza que los hallazgos serán técnicamente sólidos, comprensibles, objetivos y alineados con los objetivos del trabajo.

La organización debe alinear sus procesos de gobierno, gestión de riesgos y control con marcos ampliamente utilizados. Por ello, los criterios de auditoría pueden tener diversas fuentes, entre las que destacan:

- Leyes, reglamentos y normativas externas vigentes.
- Políticas y procedimientos internos formalizados por la entidad.
- Normas técnicas, estándares o directrices emitidas por organismos especializados.
- Marcos de gobierno, gestión de riesgos y control reconocidos, como *COSO, COSO ERM, NIST, COBIT o NCh ISO 31000.*
- Indicadores institucionales de desempeño, eficiencia, calidad o cobertura (*KPIs*).
- Guías de buenas prácticas, *benchmarks* del sector o comparaciones con entidades similares.
- Dictámenes, pronunciamientos o resoluciones de organismos reguladores como la Contraloría General de la República (CGR).
- Opiniones técnicas de expertos, debidamente documentadas.

a.1. Naturaleza y origen de los criterios

La naturaleza del criterio está determinada por el tipo de auditoría que se realiza. Dependiendo del enfoque del trabajo, los criterios adoptarán una forma distinta en cuanto a su fuente, nivel de formalidad y tipo de medición esperada.

En auditorías de cumplimiento, los criterios provienen principalmente de fuentes normativas formales. Esto incluye leyes, reglamentos, decretos, resoluciones, instrucciones administrativas o manuales internos (políticas, procedimientos y protocolos) que regulan el comportamiento de las áreas y procesos de la entidad y de sus funcionarios. Son criterios obligatorios y no negociables, ya que están legalmente establecidos.

En el trabajo de auditoría de gestión o desempeño, los criterios se basan en niveles esperados de eficacia, eficiencia, economía o calidad. Estos pueden estar definidos en normas técnicas, lineamientos estratégicos, planes operativos, acuerdos de desempeño, indicadores institucionales o compromisos asumidos por la entidad. Aquí, los criterios reflejan lo que se espera como resultado del proceso auditado, más allá del mero cumplimiento formal.

En auditorías de aseguramiento general, los criterios también pueden extraerse de modelos de referencia, marcos de control interno o metodologías de gestión de riesgos. Algunos ejemplos incluyen *COSO, COSO ERM, COBIT, NIST, ISO/IEC 27001 o NCh ISO 31000*. Asimismo se pueden considerar criterios definidos por organismos especializados o en ausencia de normativa específica, recurrir al juicio de expertos con experiencia demostrada y debidamente documentado.

Los criterios pueden clasificarse además por su tipo de medición:

- **Criterios Cuantitativos:** Como porcentajes, umbrales, indicadores numéricos, tasas o metas establecidas. Son especialmente útiles para evaluar resultados de manera objetiva y directa.
- **Criterios Cualitativos:** Como normas de comportamiento, principios éticos, condiciones mínimas, estándares técnicos, descripciones funcionales o marcos de referencia. Se aplican a aspectos donde el desempeño o cumplimiento se expresa en términos no numéricos.

La selección de uno u otro tipo depende de los objetivos del trabajo, de la naturaleza de los riesgos identificados y de la disponibilidad de información medible.

En todos los casos, los criterios deben ser pertinentes, verificables, comprensibles y útiles para emitir juicios fundados sobre las condiciones observadas en la actividad bajo revisión.

a.2. Proceso de identificación y validación de criterios de auditoría

La selección de criterios de auditoría debe realizarse siguiendo una secuencia lógica, técnicamente fundamentada y validada con las partes involucradas en el proceso. Esta secuencia garantiza la pertinencia y legitimidad de los parámetros utilizados como base para emitir juicios profesionales.

Orden de prioridad para determinar los criterios de auditoría:

- **Criterios normativos o institucionales formales**

Siempre que existan leyes, normativas, regulaciones vigentes, políticas internas formalizadas, manuales o directrices emitidas por la propia entidad, estos deben ser utilizados como criterios principales. Es imprescindible que estén alineados con el objetivo del trabajo, sean pertinentes para la actividad revisada y estén documentados de manera oficial.

- **Criterios acordados con la entidad auditada**

De acuerdo con la *Norma 13.4 sobre Criterios de Evaluación*, los criterios utilizados en el trabajo de auditoría deben ser siempre evaluados respecto de su adecuación. En los casos en que no existan criterios previamente establecidos o estos resulten insuficientes, los auditores internos pueden definir criterios razonables y técnicamente sustentados en conjunto con la Alta Dirección y el Jefe de Servicio.

Dichos acuerdos deben ser formalmente documentados y respaldados con evidencia que demuestre su pertinencia, solidez técnica y alineación con los objetivos del trabajo.

- **Criterios alternativos o de referencia externa**

En ausencia de ambos anteriores, se puede recurrir a fuentes externas de validación, tales como:

- Análisis comparativos (*benchmarking*) con entidades del mismo sector o con mejores prácticas reconocidas.
- Normas técnicas nacionales o internacionales no obligatorias, emitidas por organismos especializados.
- Estadísticas o estudios confiables, producidos por organismos públicos, académicos o técnicos.
- Juicio de expertos independientes, documentado y validado con la actividad bajo revisión.

Independientemente del origen, todos los criterios seleccionados deben cumplir con las siguientes condiciones técnicas:

- **Relevancia:** Deben estar directamente alineados con los objetivos específicos del trabajo de auditoría.
- **Razonabilidad Técnica:** Deben basarse en supuestos y criterios lógicos, viables y adecuados al contexto institucional.
- **Factibilidad Operativa:** Deben ser alcanzables dentro de las condiciones reales de funcionamiento de la entidad evaluada.
- **Claridad Comunicacional:** deben estar redactados de forma clara y comprensible para todas las partes interesadas.
- **Verificabilidad objetiva:** Deben permitir la evaluación basada en evidencia contrastable entre la situación observada y los criterios definidos.

Además, los criterios deben ser medibles, tanto en términos cualitativos como cuantitativos, para servir como base para emitir conclusiones y evaluar la magnitud de los hallazgos.

- **Evaluación de la calidad de los criterios: Modelo SCRAP**

Para asegurar la validez técnica de los criterios seleccionados, los auditores deben evaluar si un criterio:

- Cubre de manera adecuada el aspecto o temática que se audita.
- Está formulado de forma clara, precisa y comprensible para todos los destinatarios del informe.
- Es lógico y apropiado dentro del contexto específico de la actividad bajo revisión y de la entidad auditada.
- Es reconocido, aceptado y compartido por las partes interesadas relevantes.
- Está directamente relacionado con el objetivo de la auditoría y permite evaluar su cumplimiento de forma objetiva.
- Es verificable mediante evidencia disponible o accesible durante el desarrollo del trabajo.
- Puede ser medido o contrastado razonablemente, ya sea de forma cualitativa o cuantitativa.

El uso del modelo **SCRAP** permite validar de manera sistemática los criterios y fortalecer la calidad técnica del trabajo de auditoría, asegurando que los hallazgos y recomendaciones se basen en estándares sólidos y defendibles.

Tabla N° 10 Cinco Características clave Modelo SCRAP

Características SCRAP	Descripción de la Característica
Específicos (S -*Specific*)	Claros, concretos y suficientemente definidos para determinar si el estado deseado ha sido alcanzado.
Comparables (C -*Produce Reliable Comparisons*)	Permiten realizar comparaciones consistentes, bajo condiciones equivalentes, entre lo observado y lo esperado.
Relevantes (R -*Relevant*)	Directamente vinculados con el objetivo evaluado y con la finalidad del trabajo de auditoría.
Alineados (A- *Aligned*)	Coherentes con los objetivos estratégicos de la entidad y con el propósito de la actividad bajo revisión.
Prácticos (P - *Practical*)	Posibles de evaluar a través de los procedimientos definidos en el programa de auditoría, utilizando evidencia observable y verificable.

Ejemplo:

"Durante la revisión de los procesos de rendición de cuentas del programa de capacitación institucional, se observó que el 40 % de los informes financieros presentados entre enero y junio de 2025 no fueron entregados dentro del plazo máximo de 15 días hábiles contados desde el término de la actividad, según lo exige la normativa interna."

Criterio de auditoría aplicado:

Los informes financieros de rendición de cuentas deben ser entregados a la Unidad de Finanzas dentro del plazo máximo de 15 días hábiles, contados desde la finalización de la actividad financiada.
(***Fuente: Instructivo Interno de Rendición de Cuentas de Programas Institucionales, Resolución Exenta N° 213/2023***)

Tabla N° 11: Evaluación del criterio según modelo SCRAP

Letra	Evaluación	Aplicación al ejemplo
S	Específico	Define con claridad el plazo máximo para rendir cuentas (15 días hábiles).
C	Comparables	Permite contrastar cada rendición contra un estándar temporal objetivo.
R	Relevante	Relacionado con la transparencia y control del uso de fondos públicos.
A	Alineado	En consonancia con las políticas de control financiero de la entidad.
P	Práctico	Puede verificarse con revisión documental (fecha de actividad vs. fecha de entrega del informe).

La idoneidad de los criterios también debe ser evaluada considerando el nivel de control existente, la tolerancia al riesgo definida por la entidad y cualquier referencia a la materialidad que sea relevante para la actividad bajo revisión. Por ejemplo, un control puede considerarse satisfactorio si un porcentaje significativo de transacciones cumple con los procedimientos establecidos o si los controles operan consistentemente como se espera.

Si los auditores internos determinan que los criterios utilizados por la Dirección son inadecuados o inexistentes, deben proponer y documentar criterios más apropiados. Esta situación también puede representar una oportunidad para que la auditoría interna realice un trabajo de asesoramiento, orientado al fortalecimiento de políticas o modelos de evaluación internos.

Finalmente, los criterios seleccionados y su justificación deben quedar claramente documentados en los papeles de trabajo, incluyendo las fuentes utilizadas, el proceso de validación realizado y cualquier discusión relevante con la Dirección o responsables de la actividad bajo revisión.

a.3. Aceptación de los criterios

Los auditores internos deben estar preparados para demostrar a todas las partes interesadas, incluyendo al Jefe de Servicio, los responsables operativos y los lectores del informe, que los criterios utilizados durante el trabajo fueron técnicamente válidos y apropiados para los temas revisados, transparentes y previamente informados en caso de haber sido desarrollados por el propio auditor, y fundamentados en evidencia y aplicables a la realidad organizacional.

Contar con criterios bien definidos, validados y documentados es fundamental para respaldar adecuadamente los hallazgos, las conclusiones y las recomendaciones del trabajo de auditoría, asegurando así la trazabilidad del juicio profesional del auditor y la utilidad del informe final.

Una vez establecidos y acordados, los criterios deben documentarse adecuadamente para evitar interpretaciones erróneas. Las NOGAI recomiendan que los auditores internos conserven evidencia documental de las discusiones sostenidas, según corresponda, con el Jefe de Servicio, la Alta Dirección y la Dirección de la actividad bajo revisión, lo que puede incluir actas de reuniones, memorandos de planificación o intercambios de correos electrónicos.

a.4. Riesgos asociados a criterios inadecuados o no consensuados

Cuando los criterios de auditoría no están claros, no fueron comunicados a tiempo, o no se acordaron con los responsables operativos, el trabajo se vuelve más complejo y el riesgo de auditoría aumenta. criterios mal definidos o impuestos sin discusión pueden hacer que una buena auditoría pierda fuerza o credibilidad. La anticipación, el diálogo y la justificación técnica son herramientas clave para evitarlo.

Las diferencias de interpretación sobre qué se está evaluando o qué se considera adecuado pueden generar cuestionamientos al informe, resistencia a los hallazgos y poca disposición a implementar recomendaciones.

Por eso, es clave que el auditor informe desde el principio qué criterios usará y escuche las observaciones que surjan. Si hay discrepancias, es importante explicar con claridad por qué se eligieron esos criterios, en qué norma, política o estándar se basan, y por qué son relevantes para el objetivo del trabajo.

Este tipo de diálogo es muy valioso, ya que permite entender cómo ve la otra parte su propia gestión, qué estándares consideran válidos, y muchas veces ayuda a reforzar la calidad del trabajo. Incluso si no se llega a un consenso completo, haber informado y argumentado los criterios de forma anticipada ayuda a reducir conflictos posteriores y a fortalecer la posición del auditor frente a la Dirección.

a.5. Tipos de Criterios de Auditoría

Aunque en la práctica los criterios pueden mezclarse o superponerse, en general se pueden agrupar en dos tipos principales: los que apuntan a los resultados y los que se enfocan en los procedimientos.

a.5.1. Criterios de resultados

Este tipo de criterios se usa cuando la auditoría busca medir si algo funcionó bien o no. Es decir, si se logró lo que se esperaba. Se aplican, por ejemplo, para revisar si una política fue eficaz, si los recursos se usaron de manera eficiente, o si se alcanzaron ciertos niveles de calidad o cobertura.

Pueden medirse con datos duros (como porcentajes, tiempos de respuesta o costos), pero también con datos más blandos, como encuestas de satisfacción o evaluaciones técnicas.

Ejemplo: Evaluar si se cumplieron las metas institucionales en cuanto a la entrega de subsidios a tiempo, si la atención ciudadana llegó al número de personas previsto, o si se redujo el tiempo promedio de un trámite relevante.

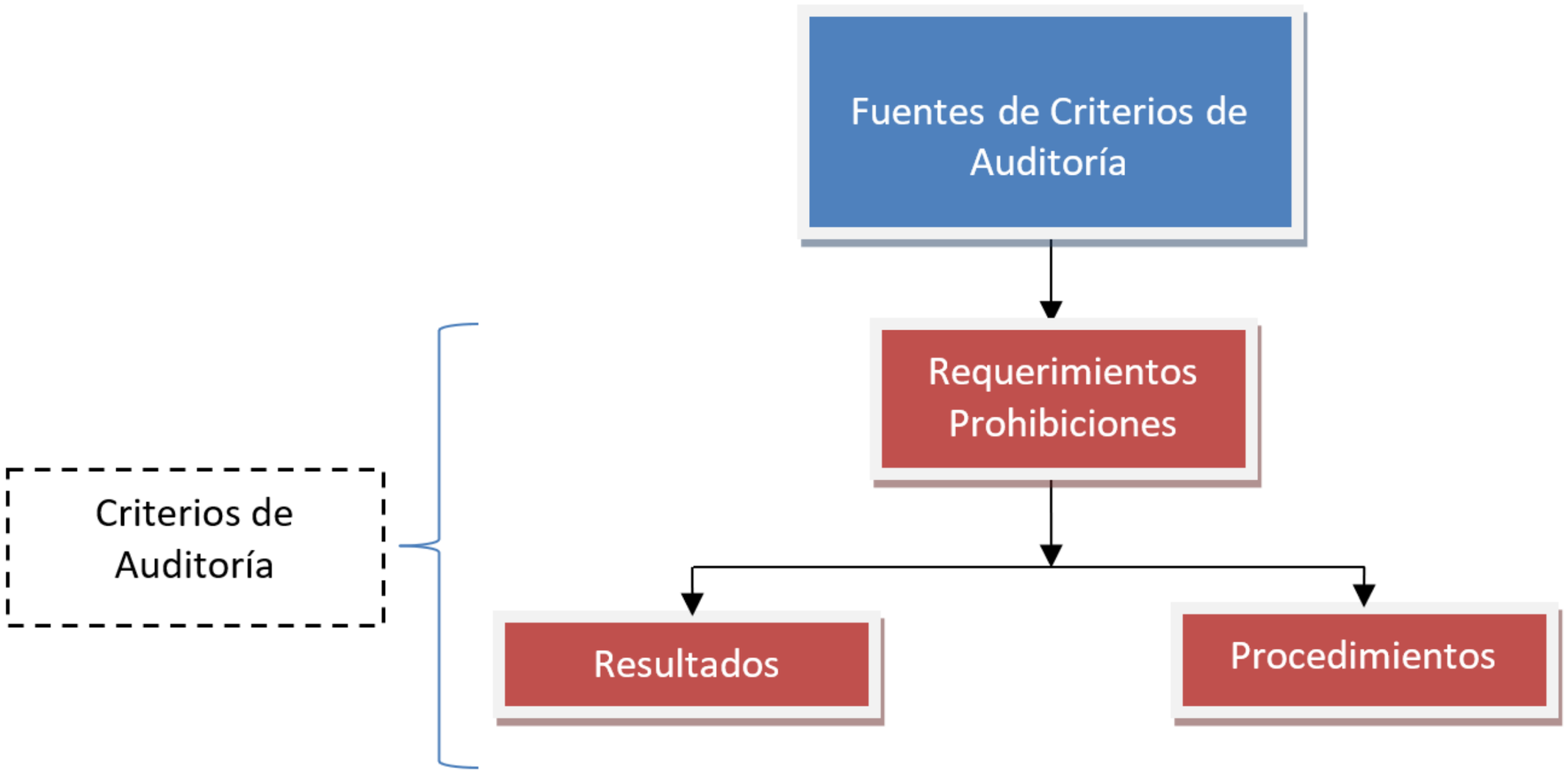
a.5.2. Criterios de procedimientos

Estos se centran en cómo se hicieron las cosas. El foco está en revisar si los pasos del proceso se siguieron como corresponde, si se cumplieron las normas y si se aplicaron los controles definidos.

En este caso, el auditor interno compara lo que se hizo contra lo que debió haberse hecho según las reglas o procedimientos internos, o según las normas externas aplicables.

Ejemplo: Comprobar si un proceso de compras públicas se ajustó a las etapas establecidas en la normativa o si, en un proceso de contratación, se cumplieron todos los requisitos legales y administrativos.

Esquema N° 7. Diagrama Relación Fuentes y Criterios de Auditoría



Temas Claves

- *El criterio define el estándar esperado contra el cual se compara la condición observada. Es esencial para formular hallazgos objetivos, relevantes y comprensibles.*
- *Deben provenir de fuentes formales (leyes, políticas, estándares, marcos de control, benchmarks). Su elección debe ser justificada, medible y documentada, aplicando principios como los del modelo SCRAP.*
- *Es clave lograr acuerdo con la Dirección sobre los criterios utilizados; de lo contrario, aumenta el riesgo de auditoría. La falta de consenso debe ser gestionada con diálogo técnico y evidencia clara.*

b. Fuentes y criterios de auditoría para evaluar el riesgo de fraude

Cuando un trabajo de auditoría contempla revisar posibles riesgos de fraude, los criterios que se aplican no siempre están escritos en una norma específica. Muchas veces, lo que guía la evaluación son señales de alerta o lo que comúnmente se llaman “banderas rojas”. Estas son situaciones que, en un contexto normal, no deberían pasar y que activan la necesidad de revisar más a fondo.

Estas señales funcionan como referencias implícitas. Aunque no estén en un manual oficial, se basan en marcos teóricos sólidos, experiencia profesional acumulada y buenas prácticas reconocidas en auditoría, ética y control interno.

Entre las principales fuentes para identificar este tipo de criterios, podemos considerar:

- Leyes y normativas formales, tanto generales como específicas.
- Instrucciones o circulares emitidas por organismos del Estado o entes reguladores.
- Modelos clásicos de análisis de fraude, como el Triángulo del Fraude o el Árbol del Fraude, que explican cómo y por qué ocurren estos hechos.
- Señales prácticas recogidas de experiencias anteriores, investigaciones internas, o trabajos realizados por órganos de control.
- Normas de ética pública, de probidad administrativa y códigos de conducta.
- Recomendaciones o alertas difundidas por instituciones especializadas en auditoría o prevención del fraude.

Estas referencias, aunque sean informales en algunos casos, pueden ser totalmente válidas como criterios para formular observaciones si están bien fundamentadas. Lo importante es que el auditor pueda explicar por qué una situación observada no es aceptable, incluso si no existe una norma específica que la prohíba.

Para facilitar este enfoque, en el **Anexo N°3** se incluye una lista de banderas rojas genéricas aplicables a distintos ciclos operativos, junto con el Esquema Global del Fraude, una herramienta visual que ayuda a entender cómo se manifiestan, evolucionan y conectan las distintas formas de fraude dentro de una organización.

Temas Claves

- *Cuando se evalúa el fraude, se consideran señales de alerta como criterios implícitos, aun si no están formalmente normadas.*
- *Los criterios pueden provenir de normativas legales, modelos teóricos de fraude, estándares éticos, y experiencia profesional previa en auditoría y control.*
- *Se recomienda utilizar herramientas como el Árbol del Fraude y listas de banderas rojas para guiar la detección de irregularidades.*

c. Principales procedimientos de auditoría para evaluar el fraude

c.1. Conceptos generales

Una vez definidos los riesgos críticos, el objetivo, el alcance y los criterios del trabajo, el siguiente paso clave es establecer cómo se va a auditar. Es decir, qué acciones concretas se llevarán a cabo para obtener evidencia relevante, suficiente y fiable que permita llegar a conclusiones bien fundamentadas.

Los procedimientos de auditoría son el conjunto de técnicas y métodos que el auditor interno aplica para revisar si los controles internos funcionan adecuadamente, si la información es confiable y si los procesos se están ejecutando como deberían. No son genéricos ni automáticos: deben construirse con precisión para cada trabajo, teniendo en cuenta el contexto y los riesgos que se buscan evaluar. No son una lista de chequeo genérica. Son herramientas estratégicas que deben construirse a medida de cada trabajo, con profundidad, sentido crítico y enfoque técnico.

Para diseñarlos bien, es importante considerar:

- Los riesgos más relevantes identificados al inicio del trabajo.
- Los criterios que se usarán como referencia para juzgar si algo está bien o mal.
- El tipo de auditoría (cumplimiento, gestión, asesoría, etc.).
- El alcance: qué procesos, sistemas, periodos y unidades van a revisarse.
- Los objetivos específicos que guían el trabajo.
- La complejidad y criticidad del área auditada.

Un procedimiento de auditoría bien formulado permite al auditor interno:

- Entender a fondo cómo funciona el proceso o sistema que está evaluando.
- Verificar si los controles internos están bien diseñados, si están en uso y si realmente funcionan en terreno.
- Detectar fallos, debilidades, errores o incluso indicios de fraude.
- Recolectar evidencia suficiente, relevante, fiable y verificable que respalde las conclusiones y resultados que contiene el informe.

Además, el diseño de estos procedimientos debe alinearse con uno de los principios clave del auditor interno: el debido cuidado profesional, tal como establecen las NOGAI. Esto implica aplicar juicio técnico, mantener una actitud de escepticismo razonable y actuar siempre con base en los riesgos detectados.

c.2 Naturaleza de los procedimientos de auditoría

No todos los procedimientos de auditoría se aplican de la misma forma. Algunos dependen directamente de la interacción del auditor interno con las personas, los documentos o los sistemas; otros se apoyan en herramientas tecnológicas que permiten revisar grandes volúmenes de información sin tener que hacerlo línea por línea. El auditor interno debe elegir con criterio qué aplicar, cuándo y por qué, siempre en función del riesgo, la complejidad del entorno y la confiabilidad de los datos disponibles.

Por un lado, están los procedimientos más tradicionales, que el auditor interno realiza manualmente: entrevistas, observación directa de procesos, revisión física de documentos, seguimiento de una operación desde su origen hasta su resultado, o simplemente repetir cálculos para confirmar su exactitud. Son útiles cuando el proceso revisado es más simple, no está automatizado o cuando se requiere una mirada directa.

Pero cuando se trata de grandes bases de datos, sistemas automatizados o ambientes tecnológicos complejos, el auditor necesita apoyarse en herramientas informáticas. Aquí entran las llamadas técnicas asistidas por computador. Con determinadas tecnologías y programas se puede analizar en minutos lo que manualmente tomaría días. Esto incluye validar transacciones, identificar patrones anormales, revisar integridad de datos o comparar registros cruzados sin intervención humana directa.

En entornos modernos, lo más común es que ambos enfoques se combinen. Los procedimientos manuales siguen siendo útiles, sobre todo para entender el contexto, detectar señales cualitativas o realizar verificaciones puntuales. Por su parte, los digitales permiten más cobertura, velocidad y seguridad.

c.3. Extensión de los procedimientos de auditoría

No basta con saber qué procedimientos aplicar; también hay que definir hasta qué punto profundizar. ¿Revisamos todo o solo una parte? ¿Hacemos un muestreo amplio o uno focalizado? ¿Analizamos con mayor o menos detalle?

La extensión de los procedimientos depende, principalmente, del riesgo. Si el área bajo revisión es crítica, si hay antecedentes de fallas, o si los controles no son del todo confiables, el auditor tendrá que ampliar la cobertura. Más muestras, más transacciones revisadas, más pruebas cruzadas. En cambio, si los riesgos no son tan críticos y el control interno es robusto tanto en diseño como en su aplicación, puede bastar con una revisión menos extensa.

Otro factor clave es la materialidad. Si los montos involucrados son altos o las consecuencias de un error son significativas, el análisis tendrá que ser más profundo. Lo mismo pasa cuando hay dudas sobre la calidad de la información o la operación de los sistemas, ya que cuanto menos confiables sean, mayor deberá ser la extensión de la revisión.

El auditor interno debe mantener un equilibrio adecuado en la obtención de evidencia, evitando tanto la insuficiencia como el exceso injustificado. Lo esencial es aplicar un juicio profesional fundado que permita determinar la cantidad y calidad de evidencia necesaria para sustentar las conclusiones con un nivel razonable de confianza.

c.4. Oportunidad de los procedimientos de auditoría

La oportunidad de los procedimientos no se trata solo de cumplir con el cronograma, sino de elegir el momento más útil y relevante para aplicar las pruebas y obtener evidencia sólida.

Desde la planificación misma, el auditor interno debe tener claro en qué momento conviene aplicar cada tipo de procedimiento. Por ejemplo, si se trata de un control que opera mensualmente, no tendría sentido revisarlo solo una vez al año. Si hubo cambios recientes en un sistema o una norma, eso puede alterar completamente el momento adecuado para evaluar ciertos riesgos o controles.

Los métodos que se pueden aplicar, entre otros, son entrevistas, observación directa, revisión documental. El valor que puede aportar el procedimiento depende del momento en que se aplican. Hacer pruebas demasiado pronto puede dejar fuera problemas que aparecen después. Hacerlas muy tarde puede significar pérdida de evidencia o condiciones que ya no existen.

Además, hay que pensar en la eficiencia. ¿Vale la pena seguir aplicando controles que cuestan más de lo que evitan? ¿No hay mecanismos duplicados? Estas preguntas también influyen en el momento en que se debe intervenir.

Todo esto debe quedar documentado en los papeles de trabajo. Si las condiciones cambian, el auditor interno tiene que estar listo para ajustar la estrategia, sin perder de vista los objetivos y la calidad del trabajo. La supervisión continua es lo que garantiza que las pruebas sigan teniendo sentido.

- **Algunos criterios técnicos para la aplicación oportuna y efectiva de pruebas de auditoría**

No basta con saber qué auditar ni cómo se hace. También hay que definir cuándo aplicar las pruebas y qué periodo van a cubrir. Esto cambia el enfoque del trabajo y la calidad de los hallazgos.

Primero, hay que ubicar las pruebas en el tiempo:

- ¿Se aplicarán en la etapa de planificación para conocer el terreno?
- ¿Durante la ejecución, mientras los procesos están en marcha?
- ¿Al cierre, cuando se debe revisar los resultados o impactos?

Luego, viene el horizonte temporal:

- ¿Se aplicarán para examinar hacia atrás?
- ¿Se revisará lo que está ocurriendo ahora?
- ¿Se proyectará si los controles van a seguir funcionando en el futuro?

Según estas interrogantes, las pruebas de auditoría se pueden dividir en tres tipos:

- **Pruebas retrospectivas**

Son las más utilizadas en la práctica de auditoría. Se aplican sobre eventos, transacciones, procesos o controles que ya han ocurrido, con el objetivo de verificar su conformidad respecto de criterios definidos (normativos, procedimentales, contractuales, entre otros). Estas pruebas permiten identificar errores, desviaciones o ineficiencias a partir del análisis de evidencia histórica, tales como registros contables, documentos contractuales, reportes de gestión o soportes de operación.

- **Pruebas concurrentes**

Se ejecutan en paralelo con la actividad en curso, permitiendo observar el funcionamiento del proceso o control mientras ocurre. Este tipo de pruebas ofrece la ventaja de detectar irregularidades o debilidades operativas en tiempo real, lo que facilita respuestas oportunas o recomendaciones inmediatas. Son especialmente útiles en contextos dinámicos o de alto riesgo, como pagos críticos, distribución de beneficios sociales, operaciones en línea o gestión de crisis.

- **Pruebas prospectivas**

Están orientadas a anticipar escenarios futuros. Evalúan si los controles, procesos o sistemas están adecuadamente diseñados para operar eficazmente frente a cambios proyectados, como transformaciones digitales, implementación de nuevas regulaciones, reformas organizacionales o ampliaciones operativas. Este tipo de pruebas requiere una comprensión profunda del diseño del control y del contexto institucional, y es clave para fomentar una cultura de mejora continua y preparación ante riesgos emergentes.

A continuación se presenta a modo de ejemplo, una tabla con descripciones generales de pruebas utilizadas generalmente para detectar fraudes, vinculadas a cada esquema de fraude de la *Association of Certified Fraud Examiners (ACFE).*

Tabla N° 12: Ejemplos de Pruebas Globales para la Detección de Fraudes en Auditoría Interna

Tipo de Fraude	Esquema de Fraude	Ejemplo de Pruebas Globales
Corrupción	Soborno	• **Revisión de pagos previos a contratos clave**: identificar desembolsos realizados a entidades o personas poco habituales antes de la firma de un contrato importante. • **Análisis geográfico de pagos**: cruzar pagos con listas de países/jurisdicciones de alto riesgo según índices de percepción de corrupción (*Transparency International, OFAC*). • Comparar condiciones contractuales con prácticas de mercado para detectar ventajas indebidas.
	Conflicto de interés	• **Cruce de base de datos de empleados y proveedores**: buscar coincidencias en direcciones, correos, números de cuenta, nombres de familiares. • **Análisis de distribución de contratos**: detectar concentración excesiva en un mismo proveedor. • **Revisión de autorizaciones**: verificar si el mismo empleado participa en varias etapas del proceso (evaluación, aprobación y ejecución).
	Gratificaciones ilegales	• **Comparación de contratos similares**: revisar diferencias en precios o términos entre contratos similares con distintos proveedores. • **Análisis de términos de pago anómalos**: identificar plazos demasiado favorables o pagos anticipados sin justificación. • **Validación de políticas de adquisiciones**: determinar si las condiciones excepcionales están autorizadas y documentadas.
	Extorsión económica	• **Análisis de archivos adjuntos en correos externos**: uso de software de monitoreo para identificar archivos confidenciales enviados a correos no corporativos. • **Análisis de patrones de comunicación sospechosa**: detectar lenguaje intimidante, amenazas veladas o coerción usando análisis de sentimiento y minería de texto en comunicaciones.

Tabla N° 12: Ejemplos de Pruebas Globales para la Detección de Fraudes en Auditoría Interna (Continúa)

Tipo de Fraude	Esquema de Fraude	Ejemplo de Pruebas Globales
Malversación	Skimming	• **Análisis de antigüedad de cuentas por cobrar**: identificar aumentos inusuales de saldos vencidos sin causa aparente. • **Comparación de ingresos en caja vs. registros contables**: identificar desviaciones. • **Verificación de segregación de funciones**: revisar si quien aprueba órdenes también procesa pagos. **Auditoría cruzada de órdenes y pagos**: validar concordancia entre condiciones pactadas y pagos realizados.
	Nómina	• **Análisis de horas trabajadas por empleado**: detectar jornadas inusuales (por ejemplo, más de 16 horas por día). • **Revisión de registros de ausencias/vacaciones**: empleados que no toman vacaciones pueden estar ocultando actividades fraudulentas. • **Evaluación de trabajadores inactivos**: verificar pagos a empleados que no aparecen en control de asistencia o supervisión.
	Reembolso de gastos	• **Análisis de reembolsos duplicados o idénticos**: mediante minería de datos, detectar repeticiones sospechosas. • **Cruce de fechas con fines de semana o feriados**: identificar viajes personales financiados como gastos laborales. • **Comparación con políticas de reembolsos**: verificar si los gastos cumplen condiciones y topes establecidos.
	Uso indebido de inventario	• **Comparación entre consumo teórico y real**: identificar desviaciones importantes respecto a estándares técnicos. • **Análisis de ajustes de inventario frecuentes o no justificados**. • **Monitoreo de acceso y requisiciones**: verificar trazabilidad en entregas de insumos clave.
	Hurto de inventario	• **Análisis de ajustes y pérdidas no atribuibles a causas normales**. • **Comparación entre reportes de recepción y uso real en producción**: diferenciar entre mermas normales y desvíos significativos. • **Revisión de videos, registros de seguridad y accesos físicos** para casos críticos.

Tabla N° 12: Ejemplos de Pruebas Globales para la Detección de Fraudes en Auditoría Interna (Continúa)

Tipo de Fraude	Esquema de Fraude	Ejemplo de Pruebas Globales
Estados Financieros	Ingresos ficticios	• **Revisión de ingresos revertidos post-cierre**: identificar registros sospechosos justo antes de cierre contable. • **Análisis lingüístico de comunicaciones de alta Dirección**: detectar presión para alcanzar metas, lenguaje agresivo sobre ingresos. • **Verificación de existencia de clientes/facturas**: confirmar si los ingresos provienen de operaciones reales.
	Corte inadecuado de ingresos	• **Cruce entre fecha de facturación y entrega del bien o servicio**: determinar si se reconocieron ingresos antes de cumplir condiciones. • **Análisis de márgenes por periodo**: detectar picos atípicos cerca del cierre que sugieran manipulación.
	Pasivos y gastos ocultos	• **Verificación de pagos posteriores al cierre contable**: determinar si deberían haberse registrado en el periodo anterior. • **Evaluación de provisiones legales**: revisar si hay litigios sin provisión contable. • **Comparación con correos y minutas legales**: detectar omisiones de pasivos conocidos.
	Sobrevaloración de activos	• **Comparación entre ingresos por ventas de activos y su valor contable**: identificar pérdidas no registradas. • **Análisis de rotación y consumo de inventario**: detectar sobreestimaciones en activos lentos o obsoletos. • **Revisión de documentación de valuaciones externas**: verificar consistencia con registros internos.

En el **Anexo N° 3** se incluye una descripción detallada sobre conceptos, técnicas y procedimientos de auditoría que pueden ser útiles para evaluar el Fraude.

Temas Claves

- *Los procedimientos para evaluar el fraude deben alinearse con el alcance, objetivos, criterios y riesgos definidos, permitiendo recolectar evidencia suficiente y confiable para evaluar controles y detectar irregularidades.*
- *Se aplican métodos manuales (entrevistas, inspección, reejecución) y asistidos por computador (TAAC), con una extensión y profundidad determinadas por la materialidad y el riesgo residual.*
- *La oportunidad (momento y horizonte temporal) de las pruebas es clave para la relevancia de los hallazgos. Se deben considerar pruebas retrospectivas, concurrentes y prospectivas, según el objetivo de evaluación.*

Paso N° 5

Definir los Recursos Necesarios (Financieros, Tecnológicos y Humanos)

a. Aspectos generales

Una parte clave al planificar cualquier trabajo es asegurarse de contar con los recursos necesarios, es decir, tiempo, personal, tecnología y presupuesto. Esta responsabilidad recae directamente en el Jefe de Auditoría, quien debe evaluar si hay suficiente capacidad para realizar adecuadamente el trabajo, dentro de los plazos y con los estándares de calidad esperados.

Planificar recursos no es solo una formalidad, tiene un impacto directo en cómo se gestiona el desempeño del equipo de auditoría, cómo se ejecuta el Plan Anual de Auditoría y qué tan eficiente es el uso del tiempo y de los recursos. Este requerimiento está alineado con el *Principio 12*, que exige medir, supervisar y mejorar la calidad del desempeño de los trabajos y de la función de auditoría interna.

Para dimensionar bien el equipo, hay que considerar no solo cuántas personas se necesitan, sino también qué tan experimentadas son, qué conocimientos técnicos tienen y si se requiere alguna capacitación adicional, sobre todo si se trata de temas nuevos o complejos.

En algunos casos, puede ser necesario recurrir a especialistas externos, por ejemplo, en áreas legales, TI, ambientales u otros ámbitos técnicos, cuando no se cuente con el conocimiento adecuado dentro del equipo de auditoría.

Además de lo anterior, resulta imprescindible contar con un cronograma claramente definido. No basta con establecer las actividades a ejecutar; es necesario asignar plazos, responsables y una secuencia lógica que determine el orden en que cada tarea debe desarrollarse. Este cronograma debería incluir

- Las principales fases del trabajo. Por ejemplo, reunión inicial, levantamiento de información, análisis de riesgos, identificación de hallazgos, reuniones intermedias, cierre, informe.
- Fechas tentativas para cada fase del ciclo de auditoría.
- Definición de quién se encarga de determinadas tareas.
- Hitos importantes, tales como entrega de avances, revisiones, versiones preliminares, etc.

Tener esto bien organizado ayuda a prevenir atrasos, gestionar imprevistos y cumplir con los tiempos, especialmente cuando el trabajo responde a mandatos externos o se trata de auditorías críticas para la institución.

b. Integración de los recursos financieros en la planificación del trabajo de auditoría

Planificar una auditoría no es solo pensar en qué revisar o cómo hacerlo. También implica definir con claridad cuántos recursos se van a necesitar y cuánto va a costar hacerlo bien. Este paso es fundamental si se quiere evitar contratiempos, usar bien el tiempo del equipo y cumplir con los objetivos sin comprometer la calidad.

Desde el inicio, el Jefe de Auditoría debe preparar un presupuesto detallado. Eso incluye no solo los sueldos del equipo, sino también todo lo necesario para ejecutar el trabajo: software, capacitaciones, traslados, viáticos, materiales, licencias o incluso apoyo externo si se requiere.

Este presupuesto debe estar en línea con el Plan Anual de Auditoría, tener coherencia con los objetivos estratégicos de la actividad a revisar y ser aprobado formalmente por el Jefe de Servicio. Durante la ejecución del trabajo, también debe mantenerse un control sobre ese gasto. Si se detectan desviaciones importantes entre lo que se presupuestó y lo que se terminó gastando, es obligatorio analizar las causas e informarlo a tiempo.

Por su parte, las metodologías (procedimientos y protocolos) de auditoría interna relacionadas con la materia deben proporcionan orientación suficiente sobre:

- Identificar los recursos requeridos para realizar el trabajo.
- Evaluar si los recursos son suficientes para lograr los objetivos del trabajo.
- Escalar la comunicación según el procedimiento o protocolo aprobado, cuando se considere que los recursos para el trabajo son insuficientes.

- **Elementos Clave para la Determinación de Recursos**

Para formular un adecuado presupuesto, hay que tener claro al menos tres elementos:

- **Diagnóstico preliminar de la actividad auditada:** Análisis del proceso, identificación de riesgos relevantes, evaluación de controles y revisión de la disponibilidad de información y documentación clave.
- **Objetivos y alcance del trabajo:** En función de la cobertura necesaria, profundidad del análisis requerido y prioridades institucionales.
- **Programa de auditoría:** procedimientos específicos a aplicar y tiempos estimados por fase (planificación, ejecución, comunicación y seguimiento).

- **Estimación Integral de Costos**

Además del tiempo y costo del recurso humano, la estimación debe incluir todos los costos financieros directos e indirectos asociados a la ejecución efectiva del trabajo. Ejemplos:

- **Gastos de viaje y viáticos:** Incluir los necesarios para visitas presenciales a unidades remotas, bodegas, sucursales u otras instalaciones descentralizadas.
- **Costos tecnológicos:** Considerar las licencias de software especializado (por ejemplo, herramientas de análisis de datos, seguridad de redes o procesamiento masivo de información). Si el presupuesto no permite su uso, se debe analizar el impacto en el alcance o considerar alternativas.
- **Suministros y equipos no rutinarios:** Estimar los materiales requeridos para condiciones específicas del trabajo (por ejemplo, vestimenta de seguridad para visitas a terreno, dispositivos de captura de datos o elementos de impresión y distribución del informe final).

La estimación debe ser completa, realista y validada por el Jefe de Auditoría, garantizando su coherencia con el plan anual de auditoría y el marco presupuestario de la entidad pública.

- **Revisión y ajuste de los recursos durante la ejecución**

La planificación de recursos financieros no es un ejercicio estático. Durante la ejecución del trabajo, deben realizarse revisiones periódicas para identificar desviaciones entre lo previsto y lo requerido en la práctica, permitiendo ajustes oportunos que mantengan la calidad técnica del servicio, sin comprometer su eficacia ni los principios de economía y racionalidad fiscal.

Temas Claves

- *Se deben definir y asignar los recursos humanos, técnicos y financieros necesarios según el alcance y complejidad del trabajo.*
- *El Jefe de Auditoría debe elaborar un presupuesto coherente con El Plan Anual de Auditoría y los objetivos estratégicos, incluyendo todos los costos relevantes.*
- *Debe establecerse un cronograma detallado y realizar ajustes durante la ejecución para asegurar calidad, eficiencia y cumplimiento de plazos.*

c. Integración de los recursos humanos en la planificación del trabajo de auditoría

Cada trabajo necesita un equipo con el tamaño justo, las competencias adecuadas y la experiencia necesaria para hacer bien las cosas desde el principio. Al planificar el recurso humano para una auditoría, lo primero es definir cuántas personas se necesitan y qué perfil deben tener, según la complejidad del trabajo, el tipo de auditoría (financiera, TI, desempeño, cumplimiento, ambiental, etc.) y el volumen de procesos o transacciones que se revisarán.

También es clave asegurarse de que el equipo cuente con los conocimientos técnicos adecuados: dominio de la normativa aplicable, manejo de marcos de control interno como *COSO* o *COBIT*, capacidad de análisis de riesgos y experiencia con herramientas tecnológicas o análisis de datos.

Las competencias profesionales blandas del equipo auditor también cuentan. Por ejemplo, buen juicio, comunicación clara, capacidad para trabajar en equipo, manejo de relaciones con las áreas auditadas y una buena dosis de escepticismo profesional. Todo esto influye directamente en la calidad de los hallazgos y en cómo se presentan los resultados.

Si el trabajo requiere habilidades muy específicas, como por ejemplo, análisis forense, evaluación de ciberseguridad, impacto ambiental o manejo de big data y no hay expertos internos disponibles, se debe considerar incorporar consultores o especialistas externos, con una adecujada justificación técnica.

Otro punto clave es el entrenamiento. Antes de iniciar un trabajo, puede ser necesario capacitar al equipo de auditoría en aspectos específicos del proceso o tecnología que se va a revisar. Esta preparación no solo mejora la calidad del trabajo, también fortalece la confianza del auditor en terreno.

La gestión del talento dentro del área de auditoría debe ser continua. No se trata solo de asignar personas a un trabajo puntual, sino de tener procesos claros para su selección, desarrollo profesional, acompañamiento y evaluación. Promover el aprendizaje continuo, dar retroalimentación constructiva y generar oportunidades de crecimiento es parte del rol de liderazgo del Jefe de Auditoría.

c.1. Equipo de auditores internos y responsable del equipo auditor

El Jefe de Auditoría tiene la tarea de asegurarse de que las personas asignadas tengan el conocimiento, la experiencia y las competencias adecuadas. No basta con cubrir una vacante, sino que se trata de garantizar que quienes participen puedan enfrentar los riesgos y la complejidad del trabajo con solvencia técnica y criterio profesional.

Esto debe quedar claramente establecido en el memorándum y en el programa de trabajo, dejando constancia de que los recursos humanos disponibles están bien alineados con lo que exige el trabajo de auditoría.

- **Estructura y asignación de roles**

Desde el inicio, debe estar claro las responsabilidades y roles de cada integrante del equipo de auditoría. Por eso, es clave documentar su composición, incluyendo por cada persona:

- Nombre completo.
- Profesión o especialidad.
- Rol en el equipo (por ejemplo, auditor junior, senior, supervisor, especialista en TI).
- Área o tema a cargo (como revisión de adquisiciones, análisis de riesgos financieros, entrevistas con jefaturas, etc.).

El auditor que lidera el equipo ya sea el Supervisor o Auditor Senior, debe tener experiencia probada en auditoría interna, criterio técnico sólido y capacidad para coordinar tanto al equipo como la relación con los auditados.

- **Justificación Técnica**

La asignación de cada integrante no debe ser arbitraria y debe estar respaldada por la naturaleza del trabajo. Debe responder a las siguientes preguntas:

- ¿Es un proceso complejo? Entonces, se necesitan perfiles con experiencia y competencias de alto nivel.
- ¿Requiere conocimientos técnicos específicos, como contabilidad gubernamental, TI, legal, o gestión ambiental? El equipo debe tenerlos cubiertos en su conjunto.
- ¿Es un trabajo de aseguramiento o asesoramiento? El enfoque también influye en qué tipo de competencias se requieren.

Tabla N° 13: Ejemplo de Composición del Equipo de Auditoría

Nombre y Apellido	Profesión Especialidad	Rol en el Trabajo	Áreas o Temas Asignados
Carla Muñoz	Contadora Auditora	Supervisora/Auditor a Líder	Supervisión general, control financiero y operativo
Jorge Vidal	Ingeniero en Informática	Auditor Especialista TI	Análisis de controles automáticos del sistema
Ana Rodríguez	Abogada	Auditora de Cumplimiento	Revisión de aspectos legales y normativos
Pedro Salinas	Auditor Interno	Auditor de Campo	Validación documental, entrevistas y pruebas en terreno

Los procesos de cierre del trabajo deben contemplar la comparación entre el tiempo y los recursos planificados versus los efectivamente utilizados en el trabajo, con el fin de identificar desviaciones relevantes. Esta información resulta clave para optimizar la planificación y asignación de recursos en futuros trabajos de auditoría.

Toda la información sobre recursos a utilizar debe integrarse a los papeles del trabajo como parte de la evidencia documental de la planificación.

Temas Claves

- *Se debe definir la cantidad, experiencia y habilidades técnicas y profesionales necesarias, considerando también la inclusión de especialistas externos si el trabajo lo requiere.*
- *Cada integrante debe tener asignado un rol claro y funciones específicas, y el Supervisor o auditor líder debe contar con experiencia para coordinar y asegurar la calidad del trabajo.*
- *La composición del equipo debe justificarse según la complejidad del objeto de la auditoría y el tipo de servicio (aseguramiento o asesoramiento), y quedar documentada formalmente.*

b. Oportunidad, periodo y estimación de horas de auditoría

Uno de los puntos clave al planificar un trabajo de auditoría es saber cuándo se va a realizar, cuánto tiempo tomará y cuántos recursos humanos se necesitarán para llevarlo a cabo con calidad. Esta definición no es solo una cuestión operativa, sino que permite asegurar que haya coherencia entre lo que se quiere lograr, la complejidad del tema que se audita y los medios disponibles. Además, se ajusta a un enfoque basado en riesgos y ayuda a optimizar el tiempo del equipo.

b.1. Oportunidad del trabajo

La oportunidad se refiere a cuándo iniciar el trabajo, para lo cual se deben considerar factores tales como:

- El calendario presupuestario o los ciclos operativos de la entidad.
- Los momentos críticos del proceso bajo revisión, como cierres financieros, licitaciones, renovaciones de contratos, etc.
- Las fechas establecidas en el Plan Anual de Auditoría o requerimientos de otras unidades.

La idea es programar el trabajo en el momento en que realmente pueda generar valor, evitar interferencias innecesarias y maximizar el impacto de los hallazgos.

b.2. Periodo de ejecución

El periodo de ejecución es el tiempo total que tomará el trabajo, desde la planificación hasta el informe final. Puede expresarse en horas, días o semanas, según la magnitud del trabajo. Pero más allá del número total, lo importante es desglosarlo en etapas, tales como:

- **Planificación**: Análisis preliminar, definición de objetivos, alcance y criterios.
- **Ejecución:** Aplicación de procedimientos, revisión documental, entrevistas.
- **Cierre:** Elaboración de hallazgos, redacción del informe, validación con las partes interesadas.
- **Seguimiento (opcional):** Incluye revisión de compromisos y acciones correctivas.

Este desglose permite distribuir la carga de trabajo de forma más ordenada, hacer seguimiento a los avances y anticipar desviaciones si el trabajo toma más tiempo del esperado

b.3. Determinación de recursos humanos y horas estimadas

Una parte clave de la planificación de auditoría es estimar cuánto tiempo tomará el trabajo y cuántos recursos humanos se necesitarán. Esta estimación no solo se hace para ordenar y priorizar la carga del equipo de auditoría, sino también para dejar constancia formal en los papeles de trabajo, de modo que haya trazabilidad, eficiencia y un uso equilibrado de los recursos.

El cálculo de horas estimadas debe considerar todas las etapas del proceso, incluyendo:

- El estudio preliminar del área a auditar.
- La identificación y análisis de riesgos y controles.
- La definición de objetivos, alcance y criterios de auditoría.
- La formulación del memorándum y diseño del programa de trabajo.
- La ejecución propiamente tal del trabajo, es decir, pruebas, entrevistas, revisión documental.
- El análisis y validación de los hallazgos.
- La redacción del informe, en borrador y versión final.
- Las reuniones formales con la unidad auditada.
- Cuando corresponda, las actividades de seguimiento posteriores al cierre.

El tiempo asignado a cada una de estas fases dependerá de varios factores, tales como qué tan complejo es el proceso en la actividad bajo revisión, cuánta información hay disponible, cuánto se puede automatizar y cuán experimentado es el equipo. También sirve mucho revisar trabajos de auditorías similares ya realizadas para tener una base comparativa.

Algunos puntos prácticos para tener en cuenta al presupuestar recursos humanos:

- El total de horas que tomará cada fase del ciclo o proceso de auditoría.
- Qué tipo de habilidades requiere el trabajo (¿se necesita un perfil TI? ¿o conocimiento contable?).
- Cuánto tiempo se tiene realmente para desarrollar cada fase, según el cronograma aprobado.
- Qué tan disponible está el equipo en términos de otros trabajos de auditoría en curso.

Además, si se van a utilizar herramientas digitales para análisis de datos o colaboración remota, eso puede reducir horas y optimizar esfuerzos. Por lo tanto, también debe ser considerado en la estimación.

b.5. Gestión de contingencias y recursos complementarios

Al planificar los recursos para un trabajo de auditoría, también es clave anticipar posibles imprevistos. Por ejemplo, la ausencia de un auditor clave, cambios inesperados en las prioridades institucionales o retrasos por factores externos pueden afectar el desarrollo normal del trabajo. En estos casos, si el presupuesto lo permite, la unidad de auditoría puede recurrir a apoyo externo, ya sea por falta de tiempo o por la necesidad de contar con habilidades especializadas que no estén disponibles en el equipo interno.

Este tipo de planificación de recursos debe estar bien documentada desde el inicio, revisarse durante la ejecución del trabajo, y mantenerse alineada con los objetivos estratégicos y el Plan Anual de Auditoría Intenta.

En muchos casos, especialmente en el sector público, no se cuenta con presupuesto para reforzar el equipo con servicios externos. Ante esa limitación, existen alternativas que podrían permitir mantener la calidad del trabajo, ajustándose a las NOGAI y a los principios de planificación estratégica (Principio 9) y mejora continua (Principio 12). Aquí algunas de las principales estrategias:

- **Priorización y reducción del alcance:** Redirigir el foco del trabajo hacia los procesos, unidades o riesgos más relevantes, dejando fuera aspectos secundarios. Posponer trabajos de auditoría de menor riesgo o transformarlos en asesorías puntuales, más acotadas.

- **Reasignación interna:** Redistribuir tareas dentro del equipo, aprovechando al máximo las capacidades disponibles. Si es viable, pedir apoyo a otras áreas de la entidad con perfiles técnicos compatibles (asegurando que se mantenga la objetividad e independencia).

- **Uso de tecnología:** Aplicar herramientas de análisis de datos existentes para cubrir grandes volúmenes de información sin necesidad de aumentar el equipo. Usar plataformas colaborativas para entrevistas, revisión de documentos y trazabilidad, reduciendo tiempos y desplazamientos.

- **Auditorías coordinadas o conjuntas:** Buscar acuerdos de colaboración con otras instituciones públicas que cuenten con especialistas disponibles, ya sea para realizar partes del trabajo o apoyarlo con conocimientos técnicos.

- **Formación interna:** Si los plazos y el presupuesto lo permiten, capacitar al equipo de auditoría en los conocimientos técnicos necesarios. Esto puede incluir cursos en normativa específica, tecnologías, análisis forense, etc.

- **Cambio de enfoque:** En lugar de realizar una auditoría completa, es posible ofrecer un servicio de asesoramiento cuando el objetivo sea entregar recomendaciones útiles sin necesidad de pruebas extensas.

Esta flexibilidad no significa bajar los estándares de calidad. Se trata de adaptar el enfoque para asegurar que el trabajo entregue valor, se mantenga dentro de lo viable y cumpla con su objetivo en un contexto de restricción en el sector público. La clave está en documentar cada decisión, justificarla técnicamente y mantener un enfoque estratégico que priorice los riesgos más relevantes.

b. Cronograma específico para realizar el trabajo

Todo trabajo de auditoría debe contar con un cronograma estimado de actividades, elaborado con base en los elementos definidos durante la planificación, tales como; objetivos, alcance, riesgos críticos, procedimientos y recursos. Este cronograma se convierte en una herramienta práctica de gestión, que permite visualizar el flujo de trabajo, anticipar posibles cuellos de botella y monitorear el cumplimiento de los plazos previstos.

Este cronograma no es simplemente una lista de fechas, representa la temporalización realista de un conjunto de acciones que deben coordinarse con precisión para lograr un trabajo eficaz, oportuno y de calidad. Debe acompañar formalmente al programa de trabajo y actualizarse cuando haya cambios sustantivos en la planificación o ejecución.

Un cronograma bien formulado permite tener el control del trabajo, tomar decisiones a tiempo y evitar tomar decisiones de última hora. También facilita el seguimiento del desempeño del equipo de auditoría, la coordinación con otras unidades y el cumplimiento con las exigencias normativas. Por eso, más que un anexo, debe considerarse como una guía dinámica que acompaña todo el proceso de auditoría interna.

b.1. Elementos comunes que puede incluir el cronograma

Aunque cada trabajo de auditoría tiene sus particularidades, muchos comparten hitos que pueden servir como base para armar el cronograma inicial. Algunos ejemplos de estos son:

- **Planificación preliminar:**

  - Incluye entrevistas exploratorias, revisión de documentación disponible, análisis de contexto, riesgos y controles, y coordinación inicial con la actividad bajo revisión.

- **Diseño del programa de trabajo**

  - Definición de objetivos específicos, desarrollo de procedimientos y definición de muestras.

- **Trabajo de campo**

  - Tiempos de traslado si se trata de trabajos de auditoría en terreno.
  - Reunión inicial con los responsables y personal de la actividad bajo revisión.
  - Levantamiento de información documental y testimonial.
  - Aplicación de pruebas de auditoría, incluyendo trabajo con muestras.
  - Supervisión continua del equipo.
  - Registro y validación de observaciones, con análisis de riesgos e implicancias.
  - Corrección o validación cruzada de papeles de trabajo.
  - Entrevistas de contraste con responsables de la actividad bajo revisión.

- **Cierre del trabajo de campo**

  - Reunión de término con responsables operativos.
  - Revisión conjunta de hallazgos preliminares.

- **Elaboración del informe**

  - Redacción de la propuesta de informe detallado y versión ejecutiva.
  - Presentación de hallazgos y recomendaciones a los responsables.
  - Incorporación de comentarios y generación de informe final.
  - Entrega oficial del informe al Jefe del Servicio.

b.2. Herramientas útiles para formular la programación de actividades y el cronograma de trabajo

Con el objetivo de contribuir a la planificación de los trabajos de auditoría o planificar la implementación de propuestas de soluciones a los hallazgos de auditoría, pueden utilizarse las técnicas *CPM (Critical Path Method* – Método de la Ruta Crítica) y *PERT (Program Evaluation and Review Technique* – Técnica de Revisión y Evaluación de Programas).

PERT

Permite visualizar gráficamente las distintas actividades involucradas en una auditoría, identificar la secuencia lógica entre ellas y calcular la duración estimada de cada fase. Es muy útil en trabajos complejos, con múltiples tareas interdependientes.

CPM

Ayuda a identificar las actividades que no pueden retrasarse sin afectar la fecha final del trabajo. Estas se denominan críticas, y su gestión adecuada es clave para mantener el proyecto dentro del tiempo estimado.

Estas herramientas son útiles cuando se requiere una adecuada planificación de proyectos o trabajos de auditoría en los que hace falta coordinar un gran número de actividades y permiten responder a un conjunto de preguntas que resultan de importancia para la gestión de dichos proyectos, la implementación de soluciones y mejoras a los procesos de la entidad. A modo de ejemplo se pueden formular las siguientes preguntas:

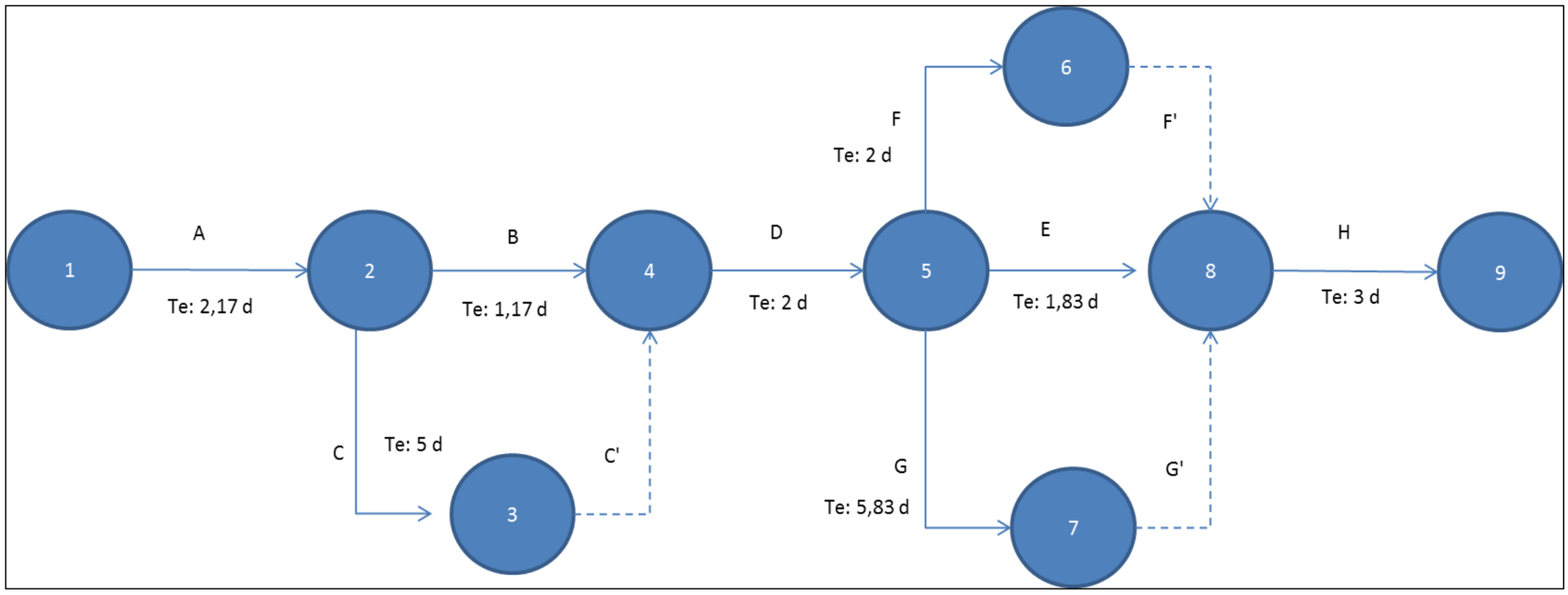
- ¿Qué actividades deben terminarse inmediatamente antes de que una actividad pueda comenzar?
- ¿Qué actividades deben seguir a la anterior?
- ¿Qué actividades deben desarrollarse de forma simultánea a esta actividad?
- ¿Cuál es el plazo mínimo para la ejecución de un proyecto de auditoría?
- ¿Cuáles son los tiempos de inicio y fin de cada una de las actividades que componen el proyecto?
- ¿Cuáles son las actividades críticas para garantizar el plazo mínimo de ejecución del proyecto de auditoría?

A continuación se presenta un ejemplo de una tabla PERT y el diagrama correspondiente.

Tabla Nº 14: Ejemplo Tabla Método PERT

Identificador	Actividades	Predecesora	Tiempo Optimista (To)	Tiempo más Probable (Tm)	Tiempo Pesimista (Tp)	Tiempo Esperado (Te)
A	Elección de temas a capacitar	-	2	2	3	2,17
B	Determinación de participantes	A	1	1	2	1,17
C	Determinar presupuesto	A	4	5	6	5,00
D	Buscar oferente convenio marco	B-C	1	2	3	2,00
E	Realizar solicitud	D	1	2	2	1,83
F	Emitir Orden de Compra y Confirmación	D	1	2	3	2,00
G	Coordinar curso con entidad y participantes	D	5	6	6	5,83
H	Realización de Curso	E-F-G	3	3	3	3,00

Esquema N° 8: Ejemplo Esquema Diagrama PERT



Al momento de organizar visualmente el cronograma de actividades para un trabajo de auditoría, una herramienta particularmente útil es el Diagrama de Gantt, también conocido como Carta Gantt. Esta herramienta, ampliamente utilizada en la gestión de proyectos, permite representar de manera sencilla y gráfica las distintas tareas, fases e hitos del trabajo, junto con sus respectivos tiempos de inicio, duración y finalización.

El principal valor del Gantt es que traduce la planificación conceptual del trabajo de auditoría en una representación visual que facilita el control, seguimiento y reprogramación, cuando sea necesario.

¿Por qué usar un Diagrama de Gantt en la planificación de auditoría?

Este tipo de representación ofrece una visión clara y estructurada del trabajo, permitiendo:

- Ver la secuencia lógica de actividades.
- Identificar tareas críticas y dependencias entre ellas.
- Estimar y visualizar duraciones reales.
- Distribuir cargas de trabajo de forma más eficiente.
- Hacer seguimiento y ajustes con mayor agilidad.

Además, al mostrar gráficamente el uso del tiempo y los recursos, el Gantt se transforma en un recurso clave para la gestión eficaz del equipo auditor y para comunicar avances de forma clara al Jefe de Servicio y a los grupos de interés.

¿Cómo se construye?

Un diagrama de Gantt se compone de dos ejes:

- **El eje vertical:** Representa la lista de actividades, tareas o fases del trabajo de auditoría (por ejemplo: planificación, revisión documental, aplicación de pruebas, redacción del informe).
- **El eje horizontal**: Corresponde al calendario o línea de tiempo (días, semanas, meses), donde se marca la duración estimada de cada tarea y su fecha de inicio y término.

Cada actividad se visualiza como una barra horizontal, lo que permite ver claramente la superposición entre tareas, los tiempos muertos, o los posibles cuellos de botella.

Aplicación práctica

En el contexto de un trabajo de auditoría, este diagrama puede incluir elementos tales como:

- Duración estimada de cada fase (planificación, trabajo de campo, análisis, cierre, informe).
- Auditores responsables asignados por fase o actividad.
- Fechas previstas de reuniones clave (inicio, cierre, presentación de hallazgos).
- Tiempo asignado para revisión de papeles de trabajo, retroalimentación y aprobación del informe.

En trabajos de auditoría más complejas, el diagrama puede complementarse con herramientas como hitos de control, colores por tipo de actividad, o incluso vincularse con matrices de recursos para verificar la disponibilidad del equipo.

Esquema Nº 9. Esquema de Carta o Diagrama Gantt

CARTA GANTT			AÑO													
			MES 1				MES ….				MES n					
Trabajo de auditoría:			SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4		
Fecha de inicio:																
Fecha de término:																
Actividades	Responsables	Duración														
ACTIVIDAD 1																
ACTIVIDAD 2																
HITO 1																
ACTIVIDAD 3																
ACTIVIDAD 4																
HITO 2																
ACTIVIDAD 5																
ACTIVIDAD 6																
HITO 3																

Temas Claves

- *Se debe definir el momento oportuno para iniciar el trabajo de auditoría, estimar su duración y calcular las horas necesarias según su complejidad.*
- *En caso de insuficiencia de recursos, se pueden aplicar estrategias como priorizar riesgos, redistribuir tareas, usar tecnología, o convertir auditorías en asesorías.*
- *Herramientas como PERT, CPM y Gantt permiten estructurar, visualizar y controlar eficazmente el cronograma y las actividades del trabajo de auditoría.*

c. Integración de los recursos tecnológicos en la planificación del trabajo

De acuerdo con las NOGAI, el Jefe de Auditoría es responsable de garantizar:

- Disponibilidad y uso efectivo de herramientas tecnológicas que apoyen el proceso de auditoría interna (software de gestión, herramientas analíticas, plataformas colaborativas, etc.).
- Capacitación del equipo auditor en el uso de dichas herramientas.
- Coordinación con áreas de TI y seguridad de la información para asegurar su correcta implementación.
- Comunicación de cualquier limitación tecnológica que pueda afectar el desarrollo del trabajo de auditoría.

Puede haber herramientas y recursos tecnológicos que ayuden a los auditores internos a realizar el trabajo de manera más eficiente y eficaz. Esto puede incluir herramientas que apoyen el análisis de datos históricos y actuales, inteligencia artificial (IA) y aprendizaje automático, y automatización robótica de procesos (RPA).

También pueden surgir riesgos específicos de la tecnología que deben abordarse como parte del trabajo, lo cual puede requerir el uso de proveedores de servicios con habilidades y conocimientos especializados, si es que el presupuesto lo permite.

El impacto de los recursos tecnológicos necesarios para el trabajo también afecta a los recursos financieros y humanos requeridos.

- **Estrategias ante la insuficiencia de recursos**

Cuando en el sector público no existen recursos disponibles para adquirir tecnologías modernas, la función de auditoría interna puede adoptar estrategias alternativas viables que permitan mantener la calidad y cobertura del trabajo sin comprometer el cumplimiento de las NOGAI.

Estas medidas deben integrarse en la planificación del trabajo, dejarse documentadas en los papeles de trabajo y evaluarse en el marco del programa de mejora continua, conforme al *Principio 12: Mejorar la Calidad* de las NOGAI.

A continuación, se detallan algunas medidas (La lista no es taxativa):

- **Uso de herramientas gratuitas o de bajo costo**

  - Explorar el uso de software libre o versiones gratuitas de herramientas de análisis de datos.
  - Aprovechar plataformas gubernamentales disponibles (como portales de datos abiertos o sistemas transversales).

- **Colaboración con otras unidades internas**

  - Coordinar con áreas como informática, contraloría, planificación o gestión de datos para aprovechar herramientas ya adquiridas por la entidad.
  - Solicitar apoyo técnico temporal de perfiles con competencias en análisis de datos dentro de la institución, sin comprometer la objetividad en trabajos futuros.

- **Optimización de técnicas manuales**

  - Reforzar el uso de muestreo estadístico, revisión documental dirigida o entrevistas estructuradas, ajustando el enfoque metodológico para obtener evidencia suficiente sin tecnología avanzada.

- **Enfoque en riesgos priorizados**

  - Ajustar el alcance del trabajo para concentrarse en procesos o transacciones con mayor riesgo, utilizando un enfoque más selectivo y estratégico.

- **Formación técnica progresiva del equipo auditor**

  - Capacitar al personal en herramientas tecnológicas accesibles (como por ejemplo, Excel avanzado con macros, Access, filtros, tablas dinámicas y funciones de validación e inteligencia artificial (IA)).
  - Desarrollar plantillas o scripts internos para análisis repetitivos, estandarizando procedimientos.

- **Gestión de alianzas externas sin costo**

  - Explorar apoyo de instituciones superiores de fiscalización, organismos reguladores, multilaterales o alianzas público-académicas que ofrecen soporte técnico o acceso a tecnología en auditorías piloto.

- **Incorporación de criterios tecnológicos en la planificación futura**

  - Documentar la necesidad no satisfecha e incluirla en el plan estratégico y/o de desarrollo de competencias de la función de auditoría interna, respaldando su inclusión en futuros presupuestos.

- **Validación y revisión continua**

  - Finalizada la planificación preliminar y definidos los objetivos y el alcance del trabajo, se debe validar que los recursos y tiempos estimados sean adecuados. En caso contrario, se debe evaluar:

    - Ajustar la planificación del trabajo.
    - Redistribuir las cargas de trabajo del equipo auditor.
    - Reformular los plazos comprometidos, sin comprometer la calidad ni la independencia.

En este contexto, el supervisor y/o el Jefe de Auditoría debe asegurar que:

- El equipo asignado esté correctamente dimensionado y cuente con las competencias requeridas.
- Se cumplan los plazos establecidos en la planificación.
- Las decisiones sobre recursos se documenten y revisen periódicamente.
- Se implementen acciones correctivas ante desviaciones significativas.

d. Limitaciones de recursos

La función de auditoría interna puede enfrentar limitaciones en el trabajo, como restricciones en la disponibilidad de recursos humanos, tiempo, presupuesto o tecnología, que pueden impedir que se logre los objetivos del trabajo.

Como se indica en las NOGAI, en situaciones en que los recursos disponibles sean inadecuados o insuficientes para completar el trabajo, el Supervisor del trabajo es responsable de escalar la situación al Jefe de Auditoría.

El Jefe de Auditoría debe discutir las implicancias de las limitaciones de recursos y determinar qué acción tomar para resolver el desafío de recursos. Entre otras opciones, podría considerar reducir el alcance del trabajo si la función de auditoría interna no puede asegurar recursos suficientes y apropiados para el trabajo.

Posteriormente, si corresponde, el Jefe de Auditoría debe comunicar al Jefe de Servicio y a la Alta Dirección, los problemas de insuficiencia de los recursos financieros, humanos y tecnológicos de la función de auditoría interna, según sea el caso.

Sin perjuicio de lo anterior, las limitaciones de tiempo que pueden justificar un ajuste en el alcance de un trabajo de auditoría, es decir, reducir la cantidad de procesos, muestras o periodos evaluados en la actividad bajo revisión, no deben afectar la calidad del trabajo ejecutado, especialmente cuando se revisan áreas o procesos de alto riesgo. Esto significa que los procedimientos aplicados deben mantenerse con el mismo nivel de rigurosidad y debido cuidado profesional exigidos en los procedimientos, garantizando que los hallazgos y conclusiones sean técnicamente válidos y útiles para la toma de decisiones.

Temas Claves

- *El Jefe de Auditoría debe asegurar el uso adecuado de herramientas tecnológicas, capacitar al equipo, coordinar con TI y comunicar cualquier limitación que afecte el trabajo.*
- *Cuando no se cuenta con tecnología suficiente, pueden aplicarse medidas como uso de software gratuito, colaboración interna, priorización de riesgos, formación progresiva del equipo y alianzas externas sin costo.*
- *Se deben revisar los recursos planificados, ajustar el trabajo si es necesario y comunicar al Jefe de Servicio y/o la alta Dirección cualquier insuficiencia, asegurando siempre que se mantenga la calidad y cumplimiento de los procedimientos aprobados en la materia.*

Paso N° 6

Formular el Memorándum de Planificación

a. Aspectos generales

El Memorándum de Planificación es un documento estratégico-operativo que constituye la documentación formal de la fase de planificación para un trabajo de auditoría. Es elaborado por el Jefe de Auditoría, o el auditor líder/supervisor y tiene como propósito principal documentar el entendimiento contextual, normativo, operativo y de riesgos de la actividad bajo revisión. Este insumo técnico sustenta y documenta la definición de objetivos, alcance y diseño metodológico del trabajo, y es el punto de partida para la formulación del Programa de Trabajo.

El Memorándum de Planificación define el "**qué**" y el "**porqué**" del trabajo de auditoría, estableciendo los objetivos, el alcance y los criterios. El programa de trabajo especifica el "**cómo**", desglosando los procedimientos, tareas, fechas y responsables para ejecutar efectivamente el trabajo en función de los lineamientos del memorándum. Ambos son fundamentales para asegurar una ejecución efectiva del trabajo de aseguramiento.

Su formular debiera comenzar durante la fase de comprensión de la actividad bajo revisión y completarse antes de la aprobación del programa de trabajo y la autorización para su ejecución.

b. Contenido general del Memorándum de Planificación

b.1. Información general del trabajo

- **Título del trabajo de auditoría:** Indicar el nombre del proyecto (ej.: "Auditoría al Proceso de Contratación de Bienes y Servicios").
- **Identificación y control**: Número de referencia, versión, fecha de emisión, vigencia, y responsables de su formulación (ej: "Versión 1.0, enero de 2024").
- **Actividad bajo revisión:** Nombre de la unidad organizativa en evaluación (ej.: "Dirección General de Abastecimiento").
- **Componente GRC:** Determinar si el trabajo abarca procesos específicos relacionados con la gobernanza, la gestión de riesgos o los controles, o si incluye los tres ámbitos de manera integral.
- **Período evaluado:** Tiempo que abarca la auditoría (ej.: "Enero a diciembre 2024").
- **Equipo asignado:** Integrantes, con su rol (ej.: "Jefe de equipo: Carla Martínez; Auditores: José Ramírez y Elena Pérez").
- **Identificación del aprobador:** Nombre, cargo y firma del Jefe de Auditoría. Fecha de aprobación.
- **Fecha estimada de inicio y fin:** Cronograma (ej.: "Inicio: 01/07/2025 - Fin: 31/08/2025").

b.2. Antecedentes y contexto

- **Tipo de objetivo de control gubernamental:** Se debe consignar si el trabajo es de tipo Gubernamental (G), Ministerial (M) o Institucional (I) o la clasificación que defina el CAIGG al momento de formular la planificación del trabajo.
- **Descripción de la actividad bajo revisión:** Se debe incluir información sobre la naturaleza del proceso, área, proyecto, antecedentes relevantes o problemas previos detectados. Esta identificación debe ser lo más precisa posible para evitar ambigüedades en la ejecución. (Ej.:"El proceso de contratación de bienes y servicios abarca desde la planificación de compras hasta la adjudicación y gestión de contratos").
- **Razones del trabajo de auditoría:** Explicar los motivos por los cuales se ha definido realizar el trabajo de auditoría, incluyendo requerimientos regulatorios, riesgos detectados o solicitudes del Jefe de Servicio. (ej.: "Identificación de riesgos críticos, hallazgos previos no resueltos, alto impacto presupuestal").

b.3. Objetivos del trabajo de auditoría

- **Objetivo general:** Definir claramente qué se pretende en general (ej.: "Evaluar el cumplimiento normativo y la eficiencia del proceso de contratación").
- **Objetivos específicos:** Detallar objetivos concretos y medibles (Ej. "Verificar la aplicación de criterios de evaluación establecidos", "Evaluar la segregación de funciones en la gestión de compras".

b.4. Alcance del trabajo de auditoría

- **Áreas, funciones o procesos específicos:** Delimitar exactamente qué unidades, departamentos, períodos de tiempo, sistemas, ubicaciones, etc., estarán cubiertos. (Ej.: "Contratos superiores a UTM XXX firmados por la Dirección General de Abastecimiento en el 2025").
- **Limitaciones o exclusiones:** Incluir restricciones conocidas, como falta de acceso a determinada información, restricciones de tiempo, recursos insuficientes, etc. (Ej.: "Contrataciones de emergencia").
- **Criterios de evaluación:** Identificar leyes, normativas, regulaciones, políticas internas, estándares internacionales, mejores prácticas, etc. (Ej.: "NOGAI, Ley de Contrataciones Públicas, Políticas internas XX").
- **Naturaleza del trabajo:** Corresponde a la relación directa o indirecta de la actividad bajo revisión donde se realizará el trabajo de auditoría, con los procesos de gobierno, gestión de riesgos y control, según lo definido previamente en el Plan Anual de Auditoría. Es importante describir cómo se vincula la auditoría con los procesos de gobierno, gestión de riesgos y control, lo que determina si se trata de una revisión de aseguramiento, una auditoría operativa, de cumplimiento, o una combinación de ellas.
- **Tipo de aseguramiento:** Aseguramiento razonable (evaluación amplia y profunda) o aseguramiento limitado (evaluación más restringida).

b.5. Enfoque y estrategia del trabajo de auditoría

- **Metodología:** Describir los procedimientos y técnicas que se usarán, como análisis documental, entrevistas, pruebas sustantivas y/o de control, revisiones por muestreo, análisis de datos, etc. (Ej.: "Entrevistas con responsables del proceso, revisión documental de expedientes, pruebas de cumplimiento").
- **Herramientas y técnicas específicas:** Uso de software especializado, entrevistas con personal clave, revisiones documentales, pruebas de control, etc. (Ej.: "uso de software para análisis de datos MT©)").
- **Estrategia de muestreo:** Si aplica, cómo se seleccionarán las muestras para las pruebas. (Ej.: "Muestreo aleatorio de contratos adjudicados superiores a UTM 100").
- **Procedimientos por tipo de aseguramiento:** Aseguramiento razonable que requiere una evaluación amplia y profunda, normalmente incluye muestreo sustantivo y pruebas de controles o aseguramiento limitado que es una evaluación más restringida, basada en procedimientos específicos previamente definidos. (Ej.: “El presente trabajo corresponde a un servicio de aseguramiento razonable, por lo que se aplicarán pruebas de control y procedimientos sustantivos para evaluar de manera integral la eficacia operativa y cumplimiento normativo del proceso de adquisiciones en el período enero a diciembre 2024.”)

b.6. Evaluación de riesgos

- **Identificación de riesgos significativos:** Riesgos potenciales relacionados con el proceso, controles débiles, riesgos tecnológicos, etc. (Ej.: "Riesgo de adjudicación indebida, colusión, pagos duplicados").
- **Consideraciones de TI:** Particular atención al entorno tecnológico, integridad de datos, seguridad de la información, acceso a sistemas, etc.
- **Evaluación de controles clave:** (Ej.: "Presencia del comité evaluador, uso de plataforma digital").
- **Matriz preliminar de riesgos y controles:** Documento con riesgos, impacto, probabilidad y controles asociados, etc.

b.7. Recursos y cronograma

- **Equipo auditor:** Roles, responsabilidades y perfiles del equipo auditor que realizará el trabajo (Ej.: "Carla Martínez, 10 años de experiencia en auditorías de adquisiciones").
- **Recursos requeridos:** Necesidades tecnológicas, acceso a sistemas, documentación, apoyo de personal de la actividad bajo revisión (Ej.: "Acceso a sistema de contrataciones, expedientes físicos y entrevistas con responsables").
- **Cronograma tentativo:** Fechas de inicio, hitos importantes, fechas de entregas y reportes, duración total estimada en horas. (Ej.: "Reunión de apertura: 01/07/2025; Trabajo de campo: del 02 al 20 de julio; Informe final: 31/08/2025").

b.8. Consideraciones éticas, confidencialidad. Independencia y objetividad

- **Declaración de independencia y objetividad del equipo:** Trabajo firmado y normas aplicables.
- **Declaración de confidencialidad:** Trabajo firmado y normas aplicables.
- **Declaración de posibles impedimentos:** (Ej.: "Auditor interno Juan Mora previamente trabajó en la actividad bajo revisión").
- **Declaración de respeto por la privacidad y la protección de datos:** Trabajo firmado y normas aplicables.

b.9. Aprobaciones y comunicaciones

- **Revisión y aprobación:** El documento debe ser revisado y aprobado por el Jefe de Auditoría y/o Supervisor.
- **Confirmación y documentación:** Es recomendable confirmar los objetivos y el alcance con la Dirección de la actividad bajo revisión y otros grupos de interés si corresponde, así como a documentar estas comunicaciones como evidencia.
- **Difusión:** Establecer cómo se comunicará oficial y formalmente el plan y programa a todo el equipo auditor y a las partes interesadas que correspondan.

b.10. Seguimiento y actualización

- **Revisión periódica:** El plan de trabajo puede ajustarse si aparecen nuevos riesgos o circunstancias imprevistas.
- **Documentación de cambios:** Cualquier modificación al plan original debe ser formalizada y comunicadas a las partes correspondientes.

c. Relevancia para las evaluaciones externas de calidad

El Memorándum de Planificación es una pieza clave del Programa de Aseguramiento y Mejora de la Calidad (PAMC). Durante evaluaciones internas o externas permite evidenciar que:

- Todas las partes tuvieron una comprensión común del trabajo realizado.
- Se estableció claramente las expectativas, límites, objetivos, enfoque y requisitos, evitando malentendidos.
- Sirve como referencia para evaluar si el trabajo de auditoría cumple con los objetivos establecidos.
- Permite anticipar y gestionar posibles obstáculos o limitaciones desde las fases tempranas del trabajo.

Temas Claves

- *El Memorándum documenta el contexto, riesgos y criterios del trabajo de auditoría.*
- *Es la base del programa de trabajo: Define el "qué" y el "porqué".*
- *Momento de formulación: Se elabora tras comprender la actividad y antes de ejecutar el trabajo*

Paso N° 7

Formular el Programa de Trabajo

a. Aspectos generales

La fase final de la planificación del trabajo consiste en la elaboración del Programa de Trabajo, también conocido como Programa de Auditoría, el cual constituye el instrumento formal que guía la ejecución ordenada, sistemática y eficaz del trabajo. Este documento sintetiza los elementos construidos en los pasos anteriores y asegura que todas las actividades estén alineadas con los objetivos de auditoría generales y específicos, previamente definidos.

El Programa de Trabajo debe ser consistente con los lineamientos del Memorándum de Planificación y la Matriz de Riesgos y Controles. Su contenido se desarrolla con base en los riesgos identificados, los objetivos definidos, el alcance, los criterios y las pruebas de auditoría, sirviendo como guía operativa para el equipo auditor.

Es recomendable vincular cada riesgo identificado con un control a revisar, y definir la técnica de prueba a aplicar. Si se va a usar muestreo, se debe especificar el tipo de muestra, número de elementos, población total y si se proyectan los resultados.

El programa siempre debe ser revisado por el Supervisor o auditor líder y aprobado por el Jefe de Auditoría antes del inicio de la fase de ejecución, así como cualquier modificación posterior, producto de hallazgos preliminares o cambios en el entorno, debe ser formalmente justificada y autorizada por el Jefe de Auditoría Interna o la persona que este designe.

Su documentación en los papeles de trabajo es obligatoria y debe conservarse como evidencia de planificación efectiva, ya que respalda la trazabilidad del proceso, justifica las decisiones adoptadas y sirve como referencia en evaluaciones de calidad internas o externas.

- **Importancia del Programa de Trabajo en la planificación**

Contar con un programa bien elaborado ayuda al equipo auditor a:

- Tener claridad sobre sus funciones y tareas, ya que cada miembro del equipo auditor sabe exactamente qué debe hacer y cuando hacerlo.
- Organizar el trabajo de forma más eficiente, al facilitar la planificación de tiempos y recursos.
- Supervisar el avance del trabajo, al permitir identificar desvíos respecto al plan original.
- Mantener la trazabilidad del trabajo realizado mediante la documentación y respaldado de cada paso planificado.
- Garantizar que se cubren los riesgos más relevantes y que los resultados del trabajo están alineados con los objetivos definidos en la planificación.

- **Relación entre el Memorándum de Planificación y el Programa de Trabajo**

El Memorándum de Planificación establece la orientación estratégica del trabajo de auditoría, definiendo sus principales lineamientos. En cambio, el Programa de Trabajo traduce esos lineamientos en procedimientos operativos específicos que deben ejecutarse para alcanzar los objetivos previamente establecidos por el equipo auditor. En este contexto se puede sintetizar la relación de los dos documentos en la siguiente tabla:

Tabla N° 15: Relación y Características: Memorándum de Planificación y Programa de Trabajo

Memorándum de Planificación	Programa de Trabajo
• Es un documento de carácter estratégico que sustenta la planificación del trabajo. • Su propósito principal es definir, documentar y comunicar los objetivos, alcance, enfoque, recursos, restricciones y criterios de evaluación. • Actúa como una herramienta de consentimiento, comunicación y autorización del trabajo de auditoría antes de su ejecución. • Es recomendable confirmar los objetivos y el alcance con la Dirección y grupos de interés correspondientes, así como a documentar estas comunicaciones como evidencia.	• Es un plan operativo y detallado, que se desarrolla a partir del Memorándum y que guía específicamente las actividades diarias y las pruebas de auditoría. • Incluye los procedimientos y pruebas específicas a ejecutar, las tareas, las fechas, los responsables y los criterios de evaluación. • Es más técnico y desglosado, orientado a la ejecución efectiva de las actividades del trabajo de auditoría.

b. Estructura y elementos del Programa de Trabajo (Programa de Auditoría)

Como ya se explicó, el Programa de Trabajo es el documento que otorga forma concreta a los elementos clave que guiarán la ejecución del trabajo. Su estructura no es rígida ni única, ya que dependerá del tamaño, complejidad y naturaleza de la actividad bajo revisión bajo revisión. Lo esencial es que contenga todos los elementos que permitan garantizar la calidad, trazabilidad y pertinencia del trabajo de auditoría.

En la práctica, sirve como una hoja de ruta que orienta las actividades del equipo auditor, ya que permite:

- Establecer qué se va a revisar (objetivos del trabajo).
- Cómo se va a hacer (métodos, pruebas y fuentes de información).
- Quién lo va a hacer (asignación de tareas y responsabilidades).
- Cuánto tiempo tomará cada tarea (estimación de duración por fase y actividad).

El programa debe estar actualizado permanentemente. Si durante el trabajo de auditoría surgen cambios relevantes, ya sea en el alcance, en los riesgos o en los procedimientos, es imprescindible revisar y ajustar el programa, con la debida autorización del Jefe de Auditoría Interna.

El programa debe elaborarse de forma específica para cada trabajo de auditoría, ya que cada actividad bajo revisión presenta riesgos, objetivos y condiciones particulares. No obstante, en ciertos contextos es aceptable emplear programas de auditoría estandarizados, por ejemplo en:

- Actividades recurrentes con baja variabilidad operativa.
- Procesos centralizados que se replican en múltiples sedes o sucursales con igual diseño.
- Revisiones periódicas bajo normativas fijas o con bajo grado de discrecionalidad.

- **Formatos que se pueden usar para formular el Programa de Trabajo**

  - **Plantillas con listas de tareas:** Documentos estandarizados con campos predefinidos que guían el desarrollo y ejecución del trabajo.
  - **Memorandos de programación:** Resúmenes escritos que presentan el enfoque del trabajo y justificación metodológica.
  - **Matrices de riesgos y controles con columnas adicionales:** Integran los riesgos, controles y pruebas en un solo documento, facilitando la trazabilidad y el seguimiento.
  - **Combinación de los anteriores:** En trabajos complejos puede ser útil usar distintos formatos para diferentes aspectos del trabajo.

- **Componentes del Programa de Trabajo derivados del Memorándum de Planificación**

Los componentes mínimos que deben considerarse para la formulación del programa de trabajo son los siguientes:

- **Objetivos del trabajo:** Claramente definidos y alineados con los riesgos y el objetivo del trabajo.
- **Alcance del trabajo:** Determina las áreas, procesos o actividades que serán objeto de revisión y las excepciones.
- **Criterios de evaluación:** Parámetros contra los cuales se evaluarán las condiciones observadas.
- **Tareas planificadas - procedimientos de auditoría:** Conjunto estructurado de pruebas, técnicas y actividades a realizar para lograr los objetivos del trabajo.
- **Asignación de recursos:** Identificación del equipo auditor, sus roles y tiempos estimados.
- **Estimación de Tiempos - cronograma de ejecución del trabajo:** Plazos y fechas clave para cada fase del trabajo.
- **Mecanismos de supervisión y revisión:** Controles internos para asegurar la calidad del trabajo realizado.

Sin perjuicio de los componentes requeridos, a continuación se detallan los elementos que es recomendable considerar en el Programa de Trabajo. Su estructura y forma de presentación podrán ser adaptadas por cada función de auditoría interna, conforme a sus características organizativas y necesidades operativas.

Tabla N° 16: Componentes Fundamentales del Programa de Trabajo

Sección del Programa	Contenido derivado del Memorándum	Explicación
Identificación del Trabajo	• Título, actividad bajo revisión, periodo, código, equipo asignado.	Datos formales que identifican el trabajo en el sistema de control de auditoría.
Tip de Servicio	• Servicio de aseguramiento razonable o limitado. • Servicio de Asesoramiento.	Define la naturaleza y características del trabajo.
Objetivos del Trabajo	• Objetivos: general y específicos.	**Requerido:** Deben estar alineados al riesgo y a los propósitos estratégicos.
Alcance del Trabajo	• Áreas, procesos y actividades incluidos y excluidos de la actividad bajo revisión.	**Requerido:** Delimita qué será examinado y permite asignar recursos adecuados.
Componente GRC	• Determinar si el trabajo abarca procesos específicos relacionados con la gobernanza, la gestión de riesgos o los controles, o si incluye los tres ámbitos de manera integral.	Garantiza la cobertura de los procesos GRC y permite trazabilidad con los resultados del trabajo.
Criterios de Evaluación	• Normas, leyes, políticas, marcos regulatorios, procedimientos, buenas prácticas, etc., y sus referencias normativas (fuentes de dónde proviene los criterios de auditoría).	**Requerido:** Sirven de referencia objetiva para calificar hallazgos.

Tabla N° 16: Componentes Fundamentales del Programa de Trabajo (continúa)

Sección del Programa	Contenido Derivado del Memorándum	Explicación
Evaluación de Riesgos y Controles	• Identificación de riesgos clave. • Controles existentes asociados. • Evaluación de efectividad de los controles. • Valoración de riesgo individuales. • Interrelación de riesgos inherentes, controles mitigantes, su efectividad y riesgo residual (matriz de riesgos y controles). • Riesgos y controles seleccionados para pruebas.	**Requerido:** Es base para seleccionar los procedimientos.
Tareas Planificadas - Procedimientos de Auditoría	Incluyen como mínimo: • Riesgo(s) relevante(s) abordado(s). • Objetivo(s) específicos de auditoría vinculado(s). • Técnica(s) de auditoría a aplicar (indagación, inspección, verificación, etc.). • Extensión, naturaleza y profundidad de la prueba (por ejemplo: muestreo estadístico, universo, documental, físico, entrevistas). • Tipo de evidencia esperada, según la técnica (documental, testimonial, física, digital). • Responsable(s) del equipo a cargo de su ejecución. • Fecha(s) estimadas para su realización dentro del cronograma general.	**Requerido:** Define las pruebas necesarias para alcanzar los objetivos de auditoría. (*Normas 13.6 y 14.1*)
Asignación de Recursos	Roles, experiencia, competencias, tiempos estimados, etc.	**Requerido:** Permite asegurar capacidad operativa adecuada.
Estimación de Tiempos - Cronograma de Ejecución del Trabajo	• Fechas clave: inicio, trabajo de campo, informe, cierre.	**Requerido:** Facilita la planificación efectiva y control de avances.
Mecanismos de Supervisión y Revisión	• Revisiones periódicas del supervisor • Validación del Jefe de Auditoría - Control de calidad.	**Requerido:** Aseguran la trazabilidad, corrección de errores y conformidad.
Control de Cambios	• Justificación de ajustes al plan • Registro de versiones • Aprobaciones	Garantiza la trazabilidad de modificaciones.
Aprobaciones	• Firmas del supervisor y Jefe de Auditoría	Formaliza la ejecución del programa conforme a lo planificado.

El cuadro a continuación representa un formato estructurado para Programa de Trabajo. Este permite establecer una relación clara y lógica entre los objetivos de auditoría, los riesgos críticos identificados, los controles clave evaluados y los procedimientos y pruebas que se aplicarán, con el fin de recolectar evidencia suficiente, relevante y confiable.

Este esquema facilita una ejecución ordenada del trabajo, alineada con un enfoque basado en riesgos, y permite monitorear el uso de recursos, tiempos estimados y responsabilidades asignadas. Asimismo, constituye una herramienta de control de calidad y trazabilidad dentro del expediente del trabajo, conforme a lo dispuesto en la *Norma 13.6 Programa de trabajo*.

Esquema Nº 10: Ejemplo Estructura de Programa de Trabajo

PROGRAMA DE AUDITORÍA PROCESO, PROYECTO, FUNCION, AREA.....

Nombre Actividad bajo revisión: …..
Tipo de Servicio: …….
Componente GRC: ……
Objetivo(s) de Auditoría General(es): ……
Objetivos de Auditoría Específicos:….

Objetivos de la Actividad	Riesgos Críticos	Controles Claves	Procedimiento Pruebas de Auditoría	Tipo de Evidencia	Responsable Auditor X	Tiempo (horas)	Evidencia de Supervisión	….
Objetivo 1	Riesgo 1	Control 1.1 Control 1.2	Prueba 1.1 Prueba 1.2	A-1	RC	3	…	…
Objetivo 2	Riesgo 2	Control 2.1	Prueba 2.1	B-1	PV	6	…	…
Objetivo 3	Riesgo 3	Control 3.1 Control 3.2	Prueba 3.1 Prueba 3.2	C-1	GU	2	…	…
…	…	…	…	…	…	…	…	..

Temas Claves

- *El Programa de Trabajo es la guía operativa del trabajo, organiza y estructura las actividades con base en los riesgos, objetivos y criterios.*
- *Se deriva directamente del Memorándum de Planificación, traduciendo sus lineamientos estratégicos en procedimientos concretos, responsables, cronograma y recursos necesarios.*
- *Es un documento dinámico que debe elaborarse antes de la ejecución del trabajo, actualizarse ante cambios significativos y conservarse como evidencia de una planificación trazable y técnicamente fundamentada.*

Paso N° 8

Formular Planilla de Trazabilidad del Trabajo de Auditoría (Complementaria)

a. Aspectos generales

La Planilla de Trazabilidad del Trabajo de Auditoría es una herramienta estructurada, estandarizada y metodológicamente integrada que permite documentar de forma sencilla y sistemática todas las fases del desarrollo de un trabajo de auditoría, desde la comprensión inicial de la actividad bajo revisión hasta la elaboración del informe borrador. Su diseño incorpora criterios técnicos, normativos y operativos alineados con los *Principios 3, 14 y 15 del Dominio V: Desempeño de los Servicios de Auditoría Interna.*

Esta herramienta tiene como propósito central garantizar la trazabilidad, consistencia y calidad técnica en la ejecución de los trabajos de auditoría, asegurando que cada etapa; planificación, ejecución y comunicación de resultados, esté debidamente desarrollada y supervisada.

Además, la planilla contribuye significativamente al fortalecimiento de la calidad, la transparencia y la mejora continua de la función de auditoría interna, actuando como soporte clave para los procesos de supervisión, revisión de calidad y evaluación del desempeño, así como evidencia objetiva del cumplimiento con las NOGAI.

Para las funciones de auditoría interna que cuenten con sistemas de gestión de procesos de auditoría interna o equivalentes, no es necesario utilizar esta planilla, sin perjuicio que deberían verificar que dichos sistemas tienen incorporada la lógica de la trazabilidad desde el estudio preliminar hasta el seguimiento de la implementación de recomendaciones y/o planes de acción.

a.1. Estructura y componentes

La planilla en formato Excel está compuesta por distintas hojas que reflejan las fases y productos clave del trabajo de auditoría:

- **Levantamiento de Comprensión Inicial:** Define la estructura organizativa de la actividad bajo revisión, los objetivos de procesos y criterios preliminares.
- **Matriz Preliminar de Riesgos y Controles:** Identifica y evalúa riesgos significativos y sus controles asociados.
- **Matriz Preliminar de Riesgos y Controles para Fraudes:** Aborda riesgos específicos de fraude y sus controles mitigantes.
- **Programa de Trabajo:** Operacionaliza los objetivos en pruebas, técnicas y evidencias a recolectar.
- **Identificación, Análisis y Evaluación de Información:** Identifica la información, sistematiza los hallazgos, su validación y análisis de causa raíz.
- **Informe Borrador:** Consolida observaciones, recomendaciones y trabajos institucionales.

b.2. Relación con el Memorándum de Planificación y el Programa de Trabajo

La planilla se vincula directamente con el Memorándum de Planificación, del cual deriva la definición de objetivos, alcance, riesgos y criterios de evaluación, y se proyecta en el Programa de Trabajo, donde se operacionalizan dichos elementos en pruebas, técnicas y evidencias concretas.

Asimismo, facilita la consolidación de observaciones y la formulación de recomendaciones debidamente sustentadas, garantizando la trazabilidad normativa y documental desde la planificación inicial hasta la emisión del informe. Cada observación queda vinculada de forma directa y verificable con una prueba aplicada, un riesgo previamente identificado y un objetivo específico del trabajo de auditoría.

b.3. Relación con las NOGAI

- Alinea el trabajo de auditoría con el cumplimiento efectivo de las *Normas 13.1 a 15.2*, asegurando una planificación, ejecución y comunicación de resultados conforme al enfoque establecido en el *Dominio V: Desempeño de los Servicios de Auditoría Interna*.
- Facilita los procesos de supervisión, revisión de calidad y evaluaciones internas y/o externas, al proporcionar una trazabilidad completa del trabajo realizado.
- Constituye un papel de trabajo integral, coherente y verificable, que respalda la metodología aplicada y la justificación técnica de las decisiones adoptadas durante la auditoría.
- Provee insumos fundamentales para la medición del desempeño del equipo auditor y para las evaluaciones de calidad conforme al *Principio 12: Mejorar la Calidad*.

Sin perjuicio de que la planilla de trazabilidad puede elaborarse utilizando distintos sistemas o herramientas informáticas, en el **Anexo Nº 13** se presenta, en formato Excel, una descripción detallada de las hojas que la componen para su aplicación en trabajos de auditoría interna El archivo Excel de la planilla de trazabilidad es un complemento a esta GGSAI.

En **Anexo N° 14** se presenta un modelo de madurez para planificación del trabajo en funciones de auditoría interna.

VI. Aspectos Relevantes de la Planificación del Trabajo en Funciones de Auditoría Interna Pequeñas

1 Elementos Clave de la Planificación en Funciones de Auditoría Interna Pequeñas

En funciones de auditoría interna pequeñas (de 1 a 3 profesionales considerando el Jefe de Auditoría), la planificación no debe perder rigurosidad, sino que debe adaptarse a los recursos disponibles sin dejar de cumplir con las NOGAI. Esto implica mantener la alineación con principios fundamentales como la objetividad, la independencia y la documentación del proceso, incluso cuando este se lleve a cabo de manera simplificada. El rol del Jefe de Auditoría es especialmente crítico, ya que en la mayoría de los casos asume directamente la responsabilidad de la evaluación de riesgos, la definición del universo de auditoría y la elaboración del Plan Anual de Auditoría.

La evaluación de riesgos debe ser práctica y centrada en lo esencial, utilizando herramientas accesibles como matrices en archivos en formatos Excel, entrevistas con responsables de procesos y análisis de hallazgos previos. Lo importante es que el análisis permita priorizar de forma lógica y documentada los temas a auditar, sin recurrir a metodologías complejas o software costoso que podrían superar la capacidad de la unidad.

Es recomendable contar con un inventario básico y actualizado de procesos críticos, que sirva como base para el universo de auditoría. La selección de temas o áreas debe justificarse en función de su relevancia, exposición al riesgo y objetivos institucionales. Incluso cuando se disponga de poco tiempo o personal, esta selección debe estar respaldada con evidencias que permitan demostrar la cobertura adecuada de los riesgos más relevantes.

En cuanto a la documentación, si bien se admite menor formalidad en funciones pequeñas, siempre debe existir evidencia escrita que respalde el análisis, las decisiones y la trazabilidad del trabajo. Esto puede lograrse mediante archivos simples (en formatos Word, Excel), notas internas, correos electrónicos o plantillas adaptadas. Lo esencial es que la planificación esté documentada de forma clara y accesible, y que se pueda presentar ante revisiones de calidad internas o externas.

Finalmente, es esencial que el Plan Anual de Auditoría sea revisado al menos una vez al año, incorporando de manera formal cualquier ajuste derivado de eventos significativos o cambios en el perfil de riesgos. La flexibilidad en la planificación constituye una práctica recomendable, siempre que las modificaciones queden debidamente registradas, justificadas y autorizadas. En todo caso, la planificación debe ser realista, estar alineada con los objetivos institucionales y contar con una documentación clara y trazable que respalde cada decisión adoptada.

2 Recomendaciones para Funciones de Auditoría Interna Pequeñas

La siguiente tabla presenta un conjunto de actividades clave que toda función de auditoría interna, especialmente aquellas con equipos pequeños o recursos limitados, debe considerar para asegurar una planificación y ejecución alineadas con las NOGAI y el Manual de Evaluaciones de Calidad del IIA.

Cada actividad se acompaña de una recomendación específica, el responsable principal de su implementación, los tipos de evidencia que respaldan su cumplimiento, observaciones prácticas para su aplicación efectiva y la frecuencia sugerida para su ejecución. Este enfoque busca ser práctico, adaptable y centrado en fortalecer la calidad técnica y la trazabilidad de los trabajos de auditoría, incluso en contextos con capacidades operativas acotadas.

Tabla N° 18: Ejemplos de Evidencias de Conformidad, Buenas Prácticas y Recomendaciones para Unidades de Auditoría Interna Pequeñas

Actividad	Recomendación	Responsable	Evidencia de Conformidad	Buenas Prácticas / Observaciones	Frecuencia
Comprender gobierno, riesgos y control	Identificar y priorizar riesgos estratégicos y operacionales	Jefe de Auditoría	Minutas, entrevistas, mapas de procesos, análisis FODA	Coordinar reuniones periódicas con el Jefe de Servicio	Anual
Estrategia de Auditoría Interna	Definir visión, objetivos estratégicos y principios rectores	Jefe de Auditoría	Documento breve validado y actualizado	Desarrollar una estrategia plurianual adaptable a recursos disponibles	Bienal / Trienal
Plan de Auditoría Interna	Formular, revisar y actualizar el plan basado en riesgos	Jefe de Auditoría	Matriz de riesgos, listado priorizado, validación del Jefe de Servicio	Incorporar cambios relevantes en tiempo real y dejar trazabilidad de ajustes	Anual / Según necesidad
Evaluación de calidad interna	Ejecutar autoevaluación estructurada y, si es posible, revisión por pares	Jefe de Auditoría	*Checklist* del IIA, informe de evaluación, evidencia de revisión cruzada	Incluir acciones de mejora continua derivadas de hallazgos	Anual
Documentación de trabajos	Registrar de manera organizada y completa todo el ciclo de auditoría	Jefe de Auditoría	Papeles de trabajo, respaldos digitales, uso de plantillas oficiales	Estandarizar formatos y revisar archivos periódicamente	Continua
Coordinación interna	Intercambiar información con áreas clave (TI, control interno, cumplimiento)	Jefe de Auditoría	Actas, correos, acuerdos o minutas de coordinación	Participar en mesas técnicas y espacios de coordinación institucional	Según necesidad
Rol del Jefe de Auditoría	Liderar, revisar y supervisar todo el proceso de auditoría	Jefe de Auditoría	Plan firmado, informes con observaciones y seguimiento	Registrar intervenciones clave en planificación, ejecución y cierre	Permanente
Objetividad y ética	Asegurar independencia, integridad y cumplimiento del código de ética	Jefe de Auditoría	Declaraciones firmadas, estatuto de auditoría, actas de validación	Mantener evidencia fácilmente accesible para auditorías de calidad	Anual

VII. Bibliografía

1. Marco Internacional para la Práctica Profesional de la Auditoría Interna del Instituto de Auditores Internos Global – IIA.

1.1. Normas Globales de Auditoría Interna (NOGAI)

- **Dominio IV: Gestión de la Función de Auditoría Interna**

Principio 11 Comunicar de manera eficaz

- Norma 11.1 Establecer relaciones y comunicarse con las partes interesadas
- Norma 11.2 Comunicación eficaz
- Norma 11.3 Comunicar los resultados
- Norma 11.4 Errores y omisiones
- Norma 11.5 Comunicar la aceptación de los riesgos

- **Dominio V: Desempeño de los Servicios de Auditoría Interna**

Principio 13: Planificar Efectivamente los Trabajos

- Norma 13.1: Comunicación durante el trabajo
- Norma 13.2: Evaluación de riesgos del trabajo
- Norma 13.3: Objetivos y alcance del trabajo
- Norma 13.4: Criterios de evaluación
- Norma 13.5: Recursos del trabajo
- Norma 13.6: Programa de trabajo

Principio 14: Ejecutar Efectivamente los Trabajos de Auditoría

- Norma 14.1 Recopilación de información para el análisis y evaluación
- Norma 14.2 Análisis y potenciales hallazgos del trabajo
- Norma 14.3 Evaluación de los hallazgos
- Norma 14.4 Recomendaciones y planes de acción
- Norma 14.5 Conclusiones del trabajo.
- Norma 14.6 Documentación de los trabajos

.

Principio 15: Comunicar Resultados del Trabajo de Auditoría

- Norma 15.1 Comunicación final del trabajo
- Norma 15.2 Confirmar la implementación de recomendaciones o planes de acción

1.2. Documentos de referencia del IIA

- Modelo de las Tres Líneas del IIA (2020)
- Guía para Implementar un Plan Estratégico de Auditoría Interna Herramienta de Evaluación de Preparación para la Conformidad (2024)
- Guía para Implementar un Plan Estratégico de Auditoría Interna
- Guía del Dominio III – Modelo de las Tres Líneas
- Manual de Evaluación de Calidad del IIA
- Mapeo Bidireccional IPPF 2017 vs NOGAI 2024
- Guías Prácticas para el Sector Público (IIA)
- Herramienta de Evaluación de Preparación para la Conformidad

2. *Sponsoring Organizations of the Treadway Commission (COSO)*

- COSO 2013: Marco Integrado de Control Interno
- COSO ERM 2017: Marco Integrado de Gestión de Riesgos Empresariales
- COSO Gestión del Riesgo de Fraude

VIII. Anexos

1 Anexo: Comparación de Servicios de Aseguramiento y Asesoramiento según las NOGAI

Las NOGAI emitidas por el Instituto de Auditores Internos (IIA) contienen cambios respecto de la aplicación de los principios y normas *del Dominio V: Desempeño de los Servicios de Auditoría Interna* para los trabajos de aseguramiento y asesoramiento que realizan los auditores internos.

En primer lugar, es relevante considerar que en el glosario de las NOGAI, encontramos las siguientes definiciones:

- Los servicios de aseguramiento corresponden a “servicios a través de los cuales los auditores internos realizan evaluaciones objetivas para proporcionar aseguramiento. Entre los ejemplos de servicios de aseguramiento se encuentran los trabajos de cumplimiento, financieros, de la operativa, de desempeño y de tecnología. Los auditores internos podrán proporcionar aseguramiento limitado o razonable, dependiendo de la naturaleza, el momento o la extensión de los procedimientos ejecutados”.

- Los servicios de asesoramiento corresponden a “servicios a través de los cuales se ofrece asesoramiento a las partes interesadas de la organización sin proporcionar aseguramiento ni asumir responsabilidades de gestión. La naturaleza y alcance de los servicios de asesoramiento están sujetos al acuerdo efectuado con las partes interesadas relevantes. Los ejemplos de estos servicios incluyen el diseño e implementación de nuevas políticas, procesos, sistemas, y productos; servicios forenses; formación (capacitación); y la facilitación de debates sobre riesgos y controles. Los 'servicios de asesoramiento' también se conocen como “servicios de consultoría”.

- La Auditoría Interna corresponde a “un individuo o grupo profesional responsable de proporcionar a una organización servicios de aseguramiento y asesoramiento.”

- La función de auditoría Interna se define como “un servicio independiente y objetivo de aseguramiento y asesoramiento diseñado para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos al aportar un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de gobernanza, gestión de riesgos y control.”

Por su parte, en el *Dominio V* se establece que los servicios de auditoría interna implican proporcionar aseguramiento, asesoramiento o ambos. Y se espera que los auditores internos apliquen y cumplan con las NOGAI al realizar los trabajos, ya sean servicios de aseguramiento o de asesoramiento, excepto cuando se especifique lo contrario en las normas individuales.

También se destaca que los auditores internos podrán iniciar servicios de asesoramiento o realizarlos a solicitud del Jefe de Servicio, de la Alta Dirección o de la Dirección de una actividad dentro de la organización. La naturaleza y alcance de los servicios de asesoramiento pueden estar sujetos a acuerdo con la parte que solicita los servicios.

Al prestar servicios de asesoramiento, se espera que los auditores internos mantengan la objetividad y no asuman responsabilidades de gestión. Por ejemplo, los auditores internos pueden realizar servicios de asesoramiento como trabajos individuales, pero si el Jefe de Auditoría asume responsabilidades más allá de la auditoría interna, entonces se deben implementar salvaguardas apropiadas para mantener la independencia de la función de auditoría interna.

A continuación, se presenta un cuadro que muestra cómo se relacionan los tres principios y las catorce normas individuales del *Dominio V,* con los requisitos que aplican a los Servicios de Aseguramiento y de Asesoramiento. Cuando sea el caso, se describen diferencias relevantes para los Servicios de Asesoramiento.

Estas diferencias están en línea con lo expresado en las consideraciones para implementación de las normas de los *principios 13, 14 y 15* del *Dominio V*, especialmente cuando se menciona que los trabajos de asesoramiento son más flexibles y adaptados al acuerdo con las partes interesadas. No obstante, hay normas donde pese a que no hay excepciones, lo cual es técnicamente cierto en términos normativos, en la práctica la naturaleza del trabajo de asesoramiento sí permite enfoques distintos, y esto se reconoce en las consideraciones para la implementación de las NOGAI.

Tabla N° 1: Relación entre los Principios y Normas Individuales del Dominio V y los Servicios de Aseguramiento y de Asesoramiento

Principio 13: Planificar Eficazmente los Trabajos

Normas Individuales	Requerimientos para Servicios de Auditoría	Requerimientos para Servicios de Asesoramiento
13.1. Comunicación durante el Trabajo	Los auditores internos deben comunicarse eficazmente durante todo el trabajo. Deben comunicar los objetivos, el alcance y oportunidad con la administración.	Aunque la norma no establece excepciones, la comunicación puede ser menos formal y adaptada al tipo de asesoramiento.
13.2. Evaluación de los Riesgos para la Actividad bajo Revisión	Los auditores internos deben desarrollar una comprensión de la actividad bajo revisión para evaluar los riesgos relevantes	Puede no requerirse una evaluación de riesgos formal y documentada, si el acuerdo con las partes interesadas así lo permite, conforme a la naturaleza consultiva del trabajo
13.3. Objetivos y Alcance del Trabajo	Los auditores internos deben establecer y documentar los objetivos y el alcance de cada trabajo.	Se debe considerar si el trabajo tiene como objetivo proporcionar servicios de aseguramiento o asesoramiento porque las expectativas de las partes interesadas y los requisitos de las Normas difieren según el tipo de trabajo. Los objetivos y el alcance de los trabajos de asesoramiento generalmente los establecen conjuntamente los auditores internos y la Dirección de la actividad bajo revisión. Pueden ser más flexibles según el tipo de servicio.
13.4. Criterios de Evaluación	Los auditores internos deben identificar los criterios más relevantes que se utilizarán para evaluar los aspectos de la actividad bajo revisión definidos en los objetivos y alcance del trabajo. Cuando los criterios utilizados por la actividad bajo revisión son inadecuados o inexistentes, los auditores internos pueden recomendar que la administración implemente los criterios identificados por los auditores internos.	En trabajos de asesoramiento, la identificación de criterios de evaluación puede no ser necesaria, dependiendo del acuerdo con las partes interesadas pertinentes. En especial formales si las partes acuerdan enfoques consultivos o exploratorios. La discusión sobre la falta de criterios adecuados en un trabajo de aseguramiento puede llevar a la decisión de brindar servicios de asesoramiento en el área bajo revisión. La ausencia de criterios preexistentes puede ser una oportunidad para formularlos con la Dirección, más que evaluarlos críticamente como en aseguramiento.
13.5. Recursos para el Trabajo	Al planificar un trabajo, los auditores internos deben identificar los tipos y la cantidad de recursos necesarios para lograr el objetivo del trabajo.	Aunque no hay excepción expresa, la planificación y asignación de recursos puede ser proporcionalmente más flexible en asesoramiento.
13.6. Programa de Trabajo	Los auditores internos deben desarrollar y documentar un programa de trabajo para cumplir con los objetivos del trabajo.	El programa de trabajo debería desarrollarse en colaboración con las partes interesadas que solicitaron el servicio de asesoramiento. Y debe ser adaptado a los fines del servicio.

Principio 14: Ejecución del Trabajo

Normas Individuales	Requerimientos para Servicios de Auditoría	Requerimientos para Servicios de Asesoramiento
14.1. Recopilación de Información para el Análisis y Evaluación	Los auditores internos deben recopilar información relevante, confiable y suficiente para realizar los análisis y evaluaciones durante el trabajo.	La norma no menciona ninguna excepción. En asesoramiento, la rigurosidad en la obtención de evidencia puede ajustarse a los objetivos establecidos con las partes interesadas. Puede no requerirse recolección exhaustiva de evidencia si los objetivos se centran en brindar orientación o facilitar decisiones.
14.2. Análisis y Potenciales Hallazgos de Auditoría	Los auditores internos deben analizar información relevante, confiable y suficiente para desarrollar potenciales hallazgos del trabajo.	La recopilación de evidencia para desarrollar hallazgos puede no ser necesaria, dependiendo del acuerdo con las partes interesadas pertinentes. En especial, si la asesoría no incluye una evaluación formal de controles.
14.3. Evaluación de los Hallazgos	Los auditores deben evaluar cada posible hallazgo para determinar su importancia. Deben colaborar con la Dirección para identificar las causas raíz cuando sea posible, determinar los posibles efectos y evaluar la importancia del problema.	La norma no menciona ninguna excepción. Aplicable solo si se identifican hallazgos durante el trabajo de asesoría.
14.4. Recomendaciones y Planes de Acción	Los auditores deben determinar si desarrollarán recomendaciones, solicitarán planes de acción a la Dirección o colaborarán con ella para acordar acciones para resolver las diferencias, mitigar los riesgos, abordar la causa raíz, mejorar o fortalecer la actividad bajo revisión.	La norma no menciona ninguna excepción. En asesoría se puede optar por recomendaciones no vinculantes o sugerencias según el contexto. Puede no requerirse un plan de acción formal, sino acuerdos sobre mejoras recomendadas.
14.5. Conclusiones del Trabajo	Los auditores internos deben elaborar una conclusión del trabajo que resuma los resultados en relación con los objetivos del trabajo y los objetivos de la Dirección. La conclusión debe resumir el juicio profesional de los auditores internos sobre la importancia general de los hallazgos del trabajo consolidados o agregados.	Las conclusiones del trabajo de asesoramiento deberían alinearse con los objetivos y el alcance del trabajo de asesoría acordado.
14.6. Documentación del Trabajo	Los auditores internos deben documentar información y evidencia para respaldar los resultados del Trabajo. Los análisis, evaluaciones y la información de respaldo relevante deben documentarse de manera que un auditor interno informado y prudente, o un auditor con un nivel de información similar, pueda comprenderlos.	La norma no menciona ninguna excepción. Aunque debe mantenerse documentación adecuada, puede ser más resumida, si el servicio de asesoría es informal o exploratorio, conservando siempre la trazabilidad.

Principio 15. Comunicar las Conclusiones del Trabajo y Monitorear los Planes de Acción

Normas Individuales	Requerimientos para Servicios de Auditoría	Requerimientos para Servicios de Asesoramiento
15.1. Comunicación Final del Trabajo	Para cada trabajo, se debe elaborar una comunicación final que incluya los objetivos y alcance del trabajo, las recomendaciones y/o planes de acción si corresponde, y las conclusiones.	La norma no menciona ninguna excepción. En trabajos de asesoría, la comunicación final puede adoptar un formato menos estructurado (memorando, presentación, etc.), según lo acordado.
15.2. Confirmación de la Implementación de los Planes de Acción	Los auditores internos deben confirmar que la Dirección ha implementado las recomendaciones o los planes de acción de la Dirección siguiendo una metodología establecida que incluya; indagar sobre el progreso, evaluaciones de seguimiento y actualizaciones sobre el estado de las acciones.	En asesoría no suele requerirse un seguimiento formal del plan de acción, salvo que se haya pactado expresamente con la Dirección. No aplica la obligatoriedad de verificación metodológica de implementación como en aseguramiento.

2 Anexo: Relación entre Objetivos del Trabajo y Procedimientos de Auditoría

Cada una de las múltiples actividades operativas que se realizan en las organizaciones públicas y privadas presenta retos para los auditores internos a la hora de decidir qué incluir y qué excluir de un programa de auditoría. Lo mismo puede decirse de los objetivos del trabajo y los procedimientos de auditoría necesarios para cumplir con dichos objetivos. Probablemente no existe un compendio de todos los procedimientos de auditoría necesarios para satisfacer todos los objetivos del trabajo.

La selección de procedimientos debe estar siempre alineada con los objetivos de auditoría. Solo así es posible obtener evidencia suficiente, competente y relevante para emitir conclusiones fundadas y recomendaciones útiles para la mejora de la gestión organizacional.

En este contexto se presentan a continuación algunas áreas y temas comunes en las organizaciones y procedimientos de auditoría que podrían aplicarse en ese contexto:

a. Publicidad

La publicidad es generalmente contratada a una agencia especializada. La agencia normalmente factura los gastos en que incurre además de una comisión sobre la base de esos gastos. El mejor aseguramiento del auditor que puede entregar es determinar si los gastos están documentados y son razonables. Un objetivo del trabajo podría ser revisar en terreno los registros de la agencia y los procedimientos operativos. Otros procedimientos operativos, tales como el desarrollo del presupuesto de publicidad, seleccionar los medios de comunicación correctos, o el establecimiento de controles financieros para la agencia están fuera del alcance de la auditoría.

b. Venta de activos

En una auditoría a los controles sobre la venta de activos, los auditores están por lo general tratando de determinar si las ventas en particular se hicieron correctamente según las normas y políticas. Algunos procedimientos de auditoría pueden ser: Realizar revisiones de aprobaciones escritas de las personas responsables de las ventas, toma de muestra para evaluar la conformidad con los procedimientos establecidos, o determinar si las ventas han seguido los procedimientos prescritos que satisfacen los objetivos del trabajo.

a. Cotizaciones de salud del personal

Un objetivo del trabajo puede ser determinar la validez de las deducciones desde la nómina de pago del personal para cotizaciones de salud. Si las cotizaciones de los empleados cubren los costos del seguro es una buena pregunta, pero es irrelevante para el objetivo. Un procedimiento de auditoría adecuado podría ser determinar si las deducciones de la nómina de pago de los empleados cuentan con el soporte adecuado mediante formularios con autorizaciones escritas adecuadas y pertinentes.

b. Dispositivos de alarma

Un auditor interno trata de determinar si los dispositivos están instalados y en funcionamiento. Procedimientos de auditoría que pueden ser interesantes, pero irrelevantes, serían la revisión de los documentos de especificaciones de las alarmas, el examen de las facturas de los dispositivos, o entrevistar al oficial de seguridad de la planta. El único procedimiento que podría ofrecer aseguramiento adecuado de la instalación y operación sería una observación de la existencia de las alarmas y de pruebas reales de su utilidad.

c. Inventarios

Un objetivo del trabajo podría ser determinar si los inventarios significativos se han registrado correctamente. Algunos procedimientos de auditoría podrían ser pertinentes, pero ineficaces, como por ejemplo, la obtención de declaraciones desde la jefatura del servicio, o flujogramar el ciclo de inventario, o entrevistar al personal. Un procedimiento eficaz sería realizar o revisar los inventarios físicos y obtener valoraciones desde expertos.

d. Adquisiciones de terrenos

Un objetivo del trabajo podría ser verificar la propiedad legal de los terrenos considerados para la adquisición. Examinar la escritura existente y los documentos de título sería interesante pero no concluyente, ya que podrían haber sido falsificados. La forma más segura de determinar la propiedad legal es inspeccionar los registros formales en el conservador de bienes raíces u organismo correspondiente.

e. Organizaciones sin fines de lucro

Muchos objetivos del trabajo pueden formularse en una auditoría en una entidad sin fines de lucro. Una auditoría orientada a la administración tratará de determinar si la actividad está haciendo el trabajo para la que fue creada. Por lo tanto, procedimientos de auditoría adecuados serían determinar la misión de la entidad, qué normas se han establecido para medir el desempeño de la misión, y la medida con que las normas se cumplen.

f. Cuentas por pagar

La auditoría se puede realizar para determinar posibles pagos en exceso por cuentas por pagar. Los pagos se efectúan sobre la base de documentos que atestigüen la venta; las órdenes, los recibos y las facturas. Pese a que los pagos parciales se producen a menudo, comparar los registros de cada pago sería oneroso. Un procedimiento adecuado a tal fin es tomar una muestra y comparar las cantidades pagadas con la orden de compra. Trabajar solo con registros de la orden de compra, informe de recepción, o la factura no sería concluyente. Se debería utilizar comparaciones de análisis automatizados.

g. Nóminas de pago al personal

Si un objetivo del trabajo es verificar las distribuciones de costo apropiadas de la nómina de sueldos a las cuentas específicas. Muchos procedimientos de auditoría pueden ser perfectamente válidos en la auditoría a la nómina, pero no guardan relación con el citado objetivo. Por ejemplo, sería irrelevante reconciliar el total de costos de la nómina con los costos de distribución de la nómina, para revisar las tarjetas de tiempo para aprobación de un supervisor, o para comparar el costo de la distribución de la nómina, con las normas de horas laborales. Para el citado objetivo, el procedimiento adecuado sería trazar los costos de distribución de la nómina a las tarjetas de tiempo de trabajo, para determinar si la cuenta o contrato ha sido cargado realmente en la relación con lo que el empleado trabaja, y para verificar que los trabajos realizados correspondían al trabajo planificado.

Si un objetivo del trabajo es examinar los pagos a receptores no autorizados, el procedimiento de auditoría más adecuado sería comprobar en terreno la distribución de los cheques de pago. La revisión de las autorizaciones para poner nuevos empleados en la nómina, el cálculo de los pagos de la nómina, o la revisión de las autorizaciones de horas trabajadas son interesantes pero no relevantes.

Un objetivo del trabajo en una auditoría de nómina (personal) puede ser asegurarse de que los empleados o funcionarios no están tomando más tiempo de vacaciones que las que les corresponde. Los procedimientos de auditoría más eficaces serían la observación física o el formulario de registros de vacaciones que muestre que los empleados estuvieron ausentes debido a las vacaciones. A continuación, el auditor interno sería capaz de rastrear esas ausencias a través de los registros de deducciones a los feriados pendientes o acumulados registrados.

Si el tema a probar es si las personas en la nómina de un departamento en particular trabajan realmente allí. La revisión de tarjetas de tiempo o registro de ingreso, la observación de las transferencias de pago, o discutir el asunto con los departamentos de supervisión no sería concluyente, pero una visita por sorpresa al departamento si lo sería.

Para averiguar si las personas son empleados reales, el procedimiento adecuado sería hacer referencias cruzadas del registro de ingreso de la nómina de las personas a los registros y reportes oficiales del departamento personal.

La comparación del personal actual del departamento con los estándares de la industria podría llevar a evaluar el rendimiento o desempeño del departamento. Las comparaciones, no aportarían ninguna información sobre la identificación de falsos empleados o la evaluación de los controles internos o el cumplimiento de las leyes y reglamentos.

h. Precios

Para determinar si los precios aplicados a los productos de una entidad varían de forma inadecuada entre los distintos clientes, un procedimiento posible sería determinar que todos los precios se establecen con objetividad y son respetados en su aplicación. El análisis de costos sería ineficaz en este caso.

i. Producción

Un objetivo del trabajo podría ser evaluar la eficacia y la eficiencia del proceso de producción. Un procedimiento adecuado sería comparar los costos reales con los costos estándares.

j. Compras

Un objetivo del trabajo podría ser determinar si una entidad compra materias primas en exceso. Determinar si se establecen normas de calidad, cantidad y fuentes de materias primas, no aborda el tema del exceso de materias primas. Lo que podría arrojar una luz sobre el tema sería determinar si el presupuesto de producción, las órdenes de trabajo, los niveles estándar de inventario, y el lote económico de compras, están claros y aprobados y se utilizan para determinar las cantidades a ser adquiridas. El análisis del superávit de la cuenta de ventas podría ayudar.

Si un del trabajo es determinar si la compra se autorizó, los procedimientos de auditoría deben incluir la verificación que la documentación de los agentes de compra contiene aprobaciones firmadas por las personas responsables. La revisión de otros documentos, tales como la recepción de notas y facturas de proveedores, sería irrelevante.

k. Calidad

En caso de que un auditor esté tratando de saber la razón que causan las excesivas tasas de rechazo que se están experimentado, el procedimiento de auditoría que podría servir sería evaluar qué tan bien el departamento de ventas está comunicando los productos retornados al departamento de producción. Observar hacia el volumen de ventas o la calificación crediticia de los clientes sería totalmente irrelevante. Por otra parte, el análisis de las cuentas de desperdicios y acumulaciones podría ayudar.

Un objetivo del trabajo razonable consiste en evaluar la propiedad de las normas de control de calidad. Un procedimiento relevante sería examinar la idoneidad y precisión de los datos que la administración utiliza para documentar el desarrollo de las normas. Determinar si las normas se están cumpliendo en su totalidad es irrelevante para el objetivo dado. Esto sería otra parte de otro trabajo y otro objetivo.

Cada actividad bajo revisión representa un conjunto de desafíos para la auditoría al momento de definir qué incluir y qué excluir en un programa, así como los objetivos específicos y los procedimientos que permitan cumplirlos adecuadamente. No existe un catálogo universal de procedimientos aplicables a todos los contextos, por lo que el juicio profesional del auditor resulta esencial para determinar la pertinencia, suficiencia y eficacia de cada acción de auditoría en función de los objetivos trazados.

3 Anexo: Aspectos Fundamentales sobre Procedimientos de Auditoría

a. Determinación de procedimientos durante la planificación

Durante la fase de planificación del trabajo, una vez definidos los objetivos, el alcance, y obtenida una comprensión integral de la actividad bajo revisión, los auditores internos deben identificar y evaluar los riesgos, así como los controles clave asociados. En este contexto, es fundamental evaluar la adecuación del diseño de los controles, con el fin de determinar si, en caso de operar eficazmente, mitigarán los riesgos que podrían afectar el logro de los objetivos.

Completada esta evaluación, deben definirse los procedimientos específicos para probar la efectividad y eficiencia operativa de los controles, los cuales se incluirán en el memorándum de planificación y en el programa de trabajo. Esta actividad también comprende la asignación de recursos. La ejecución de los procedimientos se lleva a cabo durante la fase de ejecución o desarrollo del trabajo de auditoría.

a.1. Evaluación de la adecuación del diseño de control

Esta evaluación puede realizarse durante la planificación o en fases posteriores, dependiendo de la naturaleza del trabajo. Su objetivo es verificar si los controles clave están diseñados para reducir eficazmente los riesgos a niveles aceptables.

Los factores a considerar incluyen:

- Nivel aceptable de riesgo según la tolerancia definida en la entidad.
- Pertinencia y suficiencia de los controles clave.
- Existencia de controles compensatorios.
- Adecuación del diseño del proceso.
- Identificación de brechas y causas raíz.

Los procedimientos utilizados pueden incluir (la lista no es taxativa):

- Indagación: entrevistas, encuestas o cuestionarios al personal.
- Observación: supervisión directa de la ejecución de los controles.
- Inspección: revisión de documentos y registros.
- Recorridos (*walkthroughs*): trazabilidad de procesos para entender el diseño de los controles.

a.2. Documentación de la evaluación

Las conclusiones deben documentarse y discutirse con la administración. La matriz preliminar de riesgos y controles es una herramienta útil para este fin. Las posibles conclusiones pueden incluir:

- Diseño adecuado de los controles.
- Diseño adecuado de los controles con brechas aceptables.
- Diseño inadecuado de los controles con exposición significativa al riesgo.

a.3. Evaluación de la efectividad operativa de los controles

Consiste en desarrollar y ejecutar pruebas que permitan obtener evidencia suficiente y apropiada sobre:

- Oportunidad de la aplicación de los controles.
- Forma y consistencia de la aplicación de los controles.
- Responsable de la ejecución de los controles.

a.3. Selección de controles a evaluar

Es recomendable considerar:

- Controles de nivel superior (monitoreo).
- Controles compensatorios.
- Resultados de la evaluación del diseño.
- Momento operativo del control.
- Cambios recientes en los procesos.

a.4. Naturaleza de las pruebas de auditoría

Las técnicas de prueba, en orden creciente de evidencia proporcionada, son:

- Indagación.
- Observación.
- Inspección.
- Verificación documental.
- Rastreo.
- Re-ejecución del control.

a.5. Alcance y oportunidad o momento de las pruebas

El alcance puede ser parcial (muestreo) o total, según:

- Frecuencia de ejecución del control.
- Confiabilidad de la evidencia.
- Existencia de controles indirectos.

La oportunidad de la prueba depende del periodo cubierto, tipo de control y naturaleza del trabajo.

a.6. Evaluación de la eficiencia del control

La eficiencia se analiza considerando:

- Relación costo-beneficio del control.
- Uso óptimo de recursos.
- Posibles ineficiencias o redundancias.
- Comparaciones mediante benchmarking.
- Identificación de sobre control.
- Los procedimientos incluyen indagación, observación, inspección y análisis de datos.

b. Clasificación por tipo de procedimientos: sustantivos - cumplimiento

b.1. Procedimientos sustantivos

Los procedimientos sustantivos son técnicas aplicadas por los auditores internos con el objetivo de obtener evidencia suficiente y apropiada sobre la validez, exactitud e integridad de las transacciones, saldos u otra información relevante. Estos procedimientos permiten sustentar las conclusiones del auditor respecto de los hallazgos identificados durante un trabajo de aseguramiento o asesoría.

Los procedimientos analíticos permiten identificar áreas que requieren un análisis más profundo o la aplicación de pruebas adicionales. No obstante, debido a su carácter indirecto, estos procedimientos conllevan un mayor riesgo de pasar por alto errores materiales en comparación con las pruebas de detalle. Por ello, su uso debe ser complementado con otras técnicas cuando sea necesario.

Los procedimientos sustantivos se clasifican en dos grandes categorías: procedimientos sustantivos de detalle y procedimientos analíticos sustantivos.

b.1.1. Procedimientos sustantivos de detalle

Consisten en pruebas aplicadas directamente sobre partidas específicas, transacciones individuales o saldos contables, con el fin de verificar su validez documental, exactitud aritmética o correspondencia con hechos y registros reales. Estos procedimientos permiten obtener evidencia directa y concreta sobre las áreas seleccionadas.

Entre los procedimientos sustantivos de detalle más comunes se encuentran:

- **Circularización a terceros**: Confirmación directa con partes externas (proveedores, clientes, bancos, etc.) sobre saldos o condiciones de operaciones registradas.
- **Observación física de activos**: Verificación in situ de la existencia, estado y condiciones de bienes tangibles.
- **Análisis detallado de cuentas**: Revisión y descomposición de saldos contables para evaluar su razonabilidad.
- **Inspección de documentos**: Examen de facturas, contratos, comprobantes y otros soportes que respaldan las operaciones.
- **Reejecución de cálculos**: Verificación independiente de operaciones matemáticas, totales o prorrateos registrados.
- **Pruebas de flujo de transacciones**: Seguimiento de operaciones desde su origen hasta su registro contable para validar su trazabilidad y conformidad con los procesos establecidos.

Estos procedimientos son especialmente efectivos cuando se desea confirmar aspectos específicos o detectar errores materiales en cuentas o áreas de riesgo identificado.

b.1.2. Procedimientos analíticos sustantivos

Los procedimientos analíticos sustantivos implican la evaluación de la información financiera o de gestión mediante el análisis de relaciones entre datos y la comparación con expectativas razonables desarrolladas por el auditor. Su objetivo es identificar inconsistencias, desviaciones significativas o patrones inusuales que puedan sugerir errores, omisiones o irregularidades.

Una premisa básica de estos procedimientos es que las relaciones entre cifras contables, operativas o financieras tienden a mantenerse relativamente estables a lo largo del tiempo, a menos que existan cambios significativos en el entorno o en las operaciones de la entidad.

Entre los procedimientos analíticos más utilizados se destacan:

- **Análisis de estados financieros en valores relativos**: Consiste en expresar cada partida como porcentaje de un total relevante (por ejemplo, ventas o activos totales) para facilitar comparaciones.
- **Análisis de razones o indicadores financieros**: Involucra el cálculo y evaluación de indicadores como liquidez, endeudamiento, rentabilidad, rotación, entre otros.
- **Análisis de tendencias**: Examina la evolución de datos a través del tiempo para identificar cambios anormales o desviaciones significativas.
- **Análisis de información orientada al futuro**: Compara cifras reales con presupuestos, metas o pronósticos aprobados, para detectar desviaciones relevantes.
- **Benchmarking externo**: Contrasta el desempeño de la entidad con organizaciones comparables del mismo sector.
- **Benchmarking interno**: Compara el rendimiento entre diferentes unidades organizacionales dentro de la misma entidad.

b.2. Procedimientos de cumplimiento

Tienen como propósito comprobar los riesgos internos y externos y la efectividad de los sistemas de control. También son denominadas Procedimientos de Control, ya que se utilizan para identificar los riesgos incluidos en las transacciones, como las características o atributos que indican la efectividad o desviación de ellos.

Están diseñados para obtener seguridad razonable de que se cumplen los procedimientos establecidos de control interno contable y no contable. También sirven para detectar desviaciones respecto a los procedimientos de control y para decidir si el grado de tales desviaciones son significativas respecto a lo que se espera de que existan controles adecuados.

En general se utilizan cuando hay evidencias escritas de aplicaciones de control, como por ejemplo, iniciales de las personas autorizadas para aprobar documentación original como facturas, recibos, contratos, notas de contabilidad, etc.

Se aplican para indicar si el procedimiento de control se está ejecutando y pruebas de que la información sujeta al sistema de control es correcta.

En su formulación se guían generalmente por el procedimiento de control que se quiere comprobar. Requieren la realización de pruebas de detalle; que se refieren a la inspección de documentos y pruebas de observación e indagación.

La aplicación de procedimientos de cumplimiento se puede hacer sobre fundamentos subjetivos o estadísticos. El muestreo estadístico constituye un medio práctico para expresar en términos cuantitativos el juicio del auditor respecto a la razonabilidad y para determinar la magnitud de las comprobaciones y evaluar el resultado sobre esta base.

b.3. De doble propósito

Los procedimientos de cumplimiento y sustantivos se relacionan estrechamente. En la práctica, los procedimientos de auditoría entregan con frecuencia evidencia del cumplimiento del control, así como la certeza requerida para propósitos sustantivos.

El control no solo necesita del diseño y realización de ciertos procedimientos y actividades, sino que estos se lleven a cabo en forma apropiada e independientemente. Los procedimientos de cumplimiento, por consiguiente, resuelven aspectos tales como; comprobar si se llevan a cabo los mecanismos de control necesarios, la forma o manera como se desarrollan y por quién están siendo ejecutados.

Un sistema de control bien diseñado y funcionando, así como de una adecuada administración del riesgo, permite al auditor interno programar la ejecución de procedimientos sustantivos reducidos en la confianza de esas aplicaciones al considerar que existen menos probabilidades de errores e irregularidades en los estados financieros.

Se pueden utilizar procedimientos de cumplimiento para la evaluación de riesgos y comprobación de la efectividad del sistema de control interno, si con el hecho de lograr adecuada evaluación de esos dos objetivos se podría reducir los costos del alcance en la aplicación de los procedimientos sustantivos.

En general, un auditor planea utilizar una muestra de doble propósito cuando ha determinado que hay un riesgo aceptablemente bajo de que el porcentaje de las desviaciones de cumplimiento en el universo excede el porcentaje tolerable.

c. Procedimientos manuales y asistidos por computadora

c.1. Procedimientos de auditoría manuales

Los auditores internos usan una gran variedad de métodos para obtener evidencia para respaldar sus conclusiones. La decisión de qué método utilizar depende de varios factores, entre estos están:

- El objetivo de la prueba de auditoría: Por ejemplo, para probar la existencia de un activo el auditor interno debe examinar físicamente el activo.
- El riesgo subyacente: Un control que mitiga un riesgo crítico amerita más aseguramiento y requiere métodos que generen evidencia de auditoría más relevante.

- Los recursos requeridos por el método: La auditoría interna debe respetar la relación costo efectividad. En general los métodos que permiten obtener evidencia más fuerte requieren más tiempo y recursos.

Algunos de los procedimientos o métodos usados frecuentemente por los auditores internos son:

c.1.1. Consulta

Es una técnica en la que se realizan preguntas a personal relacionado directamente con el trabajo de auditoría o bien a terceros para obtener sus respuestas orales o escritas. La consulta permite obtener evidencia indirecta, que rara vez es persuasiva por sí sola. En especial, esto es así, cuando la consulta se dirige al personal del área auditada y el auditor interno no puede confiar en que este personal proporcione respuestas imparciales u objetivas. Los tipos de consultas más comunes incluyen cuestionarios, entrevistas y checklist.

- **Cuestionarios:** Es una técnica utilizable en todas las áreas y niveles que permite obtener evidencias no solo sobre los datos sino sobre el ambiente de control existente en la entidad. Consiste en la formulación de una serie de preguntas programadas, que luego son valorizadas por el auditor con el fin de llegar a una conclusión fundada sobre un objetivo del trabajo determinado previamente.

  Los cuestionarios pueden contener preguntas cerradas (respuestas: sí/no) o abiertas (contestadas con narrativa). Deben estar elaborados de manera que una respuesta no signifique una falencia en el control.

- **Entrevistas:** La entrevista es uno de los medios más comunes para la obtención de datos desde el área auditada. Las más usuales en el proceso de auditoría interna son la entrevista de inicio para obtener el conocimiento necesario que permita facilitar la planificación del trabajo; y la entrevista de cierre que tiene por objeto exponer las conclusiones del trabajo a los interesados y recibir los comentarios y aclaraciones que fueran necesarias. Las entrevistas tienen tres etapas: Primera etapa, la planificación (conocer los propósitos de la entrevista, la determinación de las personas a entrevistar, la preparación de fechas, horarios y duración de la entrevista). La segunda etapa corresponde al desarrollo de la entrevista, en el cual se debe crear un clima cómodo y mantener el foco en la obtención de datos. La tercera etapa corresponde al análisis de la información obtenida, en la cual el auditor evaluará si obtuvo la información deseada, validará la información (contra otras fuentes de evidencia). También puede solicitarse al entrevistado que confirme en forma verbal o escrita sus declaraciones

- **Cuestionarios de control interno (c*hecklist*):** Son cuestionarios que son usados durante las entrevistas y que generalmente son contestados en forma oral durante el proceso de la entrevista. Cumplen una función similar a la de los cuestionarios, en cuanto a sistematizar el trabajo y permiten obtener conclusiones de un modo práctico y eficiente. También sirven como una ayudamemoria durante el desarrollo del trabajo del auditor interno.

c.1.2. Observación

Consiste en observar a las personas, los procedimientos y los procesos en el área auditada. Por lo general, la observación se considera más persuasiva que la consulta en el sentido que el auditor interno obtiene evidencia directa. Por ejemplo, la observación personal directa de un funcionario que aplica o no aplica una actividad de control, generalmente proporciona más aseguramiento que la simple consulta a ese funcionario sobre la aplicación del control evaluado. La observación puede estar también dirigida a la obtención de determinada evidencia de auditoría.

La observación está dirigida a conseguir evidencia documental o física. Puede tomar distintas formas, tales como: i) examen físico (el auditor interno recuenta o realiza una identificación exacta del bien, verifica la legítima propiedad y calidad del mismo) que se orienta a probar la existencia de los bienes, y ii) inspección (se aplica sobre la documentación, el auditor relaciona la existencia física del bien con la documentación respaldatoria existente).

La observación debe documentarse y la calidad de ella depende de la experiencia y capacitación del auditor interno, la observación ocurre generalmente durante la investigación preliminar y los flujos de trabajo y también puede ocurrir cuando se hacen las preguntas para evaluar algún proceso o situación en particular.

En general la observación es preliminar a la utilización de otras técnicas tales como: la confirmación, el análisis o la investigación.

La observación puede detectar exposiciones a riesgos y controles, recursos que no se están utilizando, violaciones a la seguridad, riesgos ambientales y de seguridad.

Una limitación importante de la observación es que proporciona evidencia en un momento determinado. El auditor interno no puede concluir que lo observado es representativo de lo que sucede siempre, ya que las personas suelen cambiar si saben que están siendo observadas.

c.1.3. Inspección

Consiste en estudiar documentos y registros y en examinar físicamente los recursos tangibles. La inspección de documentos y registros proporciona evidencia directa de su contenido. El examen físico de los recursos tangibles (un equipo) proporciona al auditor interno conocimiento personal directo de la existencia y condición física de los recursos. No obstante los auditores internos deben reconocer y considerar su nivel de competencia. En este procedimiento, al igual que en el de observación, la información resultante forma parte de la experiencia directa del auditor interno, por lo que es altamente confiable. La inspección es un procedimiento de limitada utilidad, ya que la experiencia o destrezas de un auditor puede no ser suficiente para producir información confiable. Este procedimiento tiende a probar la existencia en un momento dado.

c.1.4. Revisión de comprobantes

Consiste en rastrear la información hacia atrás desde un documento o registro, hacia un documento o registro preparado anteriormente o hacia un recurso tangible. La revisión de comprobantes se realiza específicamente para probar la validez de la información documentada o registrada. Cuando se trata de auditorías financieras, la revisión de comprobantes se usa para probar su valorización sobre los montos registrados. La revisión de comprobantes indica la verificación de las cantidades registradas al examinar los documentos de respaldo, desde los documentos finales hasta los originales. El objetivo de trabajar hacia atrás es proporcionar información de que las cantidades registradas reflejan transacciones válidas. La revisión de comprobantes soporta la existencia o afirmación de ocurrencias. La revisión de comprobantes es irrelevante a la afirmación de integridad. Que algunas transacciones se encuentren registradas, no prueba que todas las transacciones fueran registradas oportunamente.

c.1.5. Rastreo

Consiste en rastrear la información hacia adelante desde un documento, registro o recurso tangible hacia un documento o registro preparado posteriormente. El rastreo se realiza específicamente para probar la integridad de la información documentada o registrada. En el contexto de las auditorías financieras el rastreo se usa para probar subvaloraciones en los montos registrados o para comprobar la recepción y pagos de cuentas por cobrar y pagar respectivamente. La Dirección de este procedimiento es la opuesta a la de revisión de comprobantes y el objetivo del trabajo al realizar este procedimiento es soportar la afirmación de integridad.

c.1.6. Reejecución

Consiste en volver a realizar las actividades de control u otros procedimientos que ya fueron realizados por los responsables operativos. La reejecución de una actividad de control proporciona evidencia de auditoría directa relacionada con la eficacia operativa, también proporciona evidencia directa de si los cálculos del auditado son correctos. La formulación independiente de una estimación contable, como la reserva para deudas incobrables y la comparación de esta con la estimación del auditor proporciona evidencia directa respecto de la razonabilidad de la estimación del auditado. La reejecución o recálculo es una forma confiable de reunir información, pero es limitada. Un cálculo hecho directamente por el auditor interno proporciona información fuerte y no sesgada en cuanto a la exactitud. Una limitación del recálculo es que no proporciona información acerca de la confiabilidad de la entrada. Por ejemplo el recalcular el ingreso de intereses puede ser poco útil, si es probable que se cobren las cuentas por cobrar que lo respaldan.

c.1.7. Confirmación

Consiste en la obtención de verificación directa por escrito de la exactitud de la información proveniente de terceros independientes. La evidencia obtenida a través de la confirmación, generalmente se considera muy confiable, porque llega al auditor interno directamente desde fuentes independientes. La confirmación es un proceso de corroboración y comparación, por ejemplo: El saldo registrado en la cuenta contable Banco a través de un certificado emitido por la Institución Financiera.

Los dos tipos de solicitudes de confirmación más comunes son: La confirmación positiva, que solicita que los destinatarios respondan independientemente de si creen o no que la información suministrada por la entidad auditada es correcta o no, y la confirmación negativa, es donde se solicita que los destinatarios responsan solo cuando creen que la información suministrada es incorrecta. Una confirmación positiva puede solicitar que el destinatario proporcione la información de interés (confirmación en blanco) o puede incluir la información de interés y solicita que el destinatario indique su acuerdo o desacuerdo respecto de la información proporcionada.

c.1.8. Investigación

Es una búsqueda sistemática de hechos ocultos cuando existen ilícitos o condiciones sospechosas. La investigación debe distinguirse de los análisis y comprobaciones, procedimientos que son aplicables a la información que no es (o que aún no es) sospechosa. La indagación es un tipo de investigación específicamente relacionadas con eventuales ilícitos. Los auditores internos deben ser cautos en estos asuntos. Una indagación realizada en forma incorrecta puede tener desafortunados efectos legales y delictivos, que puedan incluir perjuicios para una entidad, debido a que entra en juego la violación de los derechos de los funcionarios o personal involucrados.

c.1.9. Evaluación

Es una valoración o estimación de trabajo, por ejemplo la formación de un juicio. Esta conclusión es una determinación de la adecuación, la eficiencia y eficacia del tema en cuestión. La evaluación está basada en un juicio profesional que afecta a todos los aspectos del trabajo y se utiliza principalmente en labores de asesoramiento o asesoría que desempeña el auditor al interior de una entidad.

Las evaluaciones típicas consideran: los riesgos de no revisar una actividad versus los costos de realizarla; la necesidad de procedimientos detallados o si basta con un simple recorrido; si los resultados de una muestra son suficientes para los fines de auditoría, de acuerdo a la evaluación de riesgos de la actividad revisada.

La evaluación es un paso más allá de analizar y verificar. Es la culminación de la responsabilidad del auditor interno cuando realiza trabajo de asesoramiento, ya que da sentido a los hechos encontrados a luz de los estándares y objetivos del trabajo, considerando además, un plazo prudente de realización y entrega de informes oportunos y completos.

c.2. Técnicas de auditoría asistidas por computadora (TAAC)

Para ejercer el debido cuidado profesional, de acuerdo con las NOGAI, el auditor interno debe considerar el uso de herramientas asistidas por computadoras y otras técnicas de análisis de datos.

Las técnicas asistidas por computador se definen como toda técnica de auditoría automatizada, como software general de auditoría, software utilitario, datos de prueba, análisis de traza y mapeo, y sistemas expertos de auditoría.

c.2.1. Software general de auditoría (GAS)

Un programa o una serie de programas diseñados para realizar ciertas funciones automatizadas. Estas funciones incluyen la lectura de archivos de computador, la selección de datos, la manipulación y la clasificación de datos, el resumen de datos, la realización de cálculos, la selección de muestras y la impresión de informes y cartas en un formato especificado por el auditor interno. Esta técnica abarca el software adquirido o escrito con fines de auditoría y el software integrado en sistemas de producción.

Hay que destacar el software general de auditoría (GAS por sus siglas en inglés), ya que este tipo de software se ha desarrollado y actualmente es relativamente fácil de usar; incluso para los auditores internos que tienen escasa capacitación relacionada con TI (Tecnología de Información). Combina una interfaz fácil de usar con una funcionalidad de auditoría sólida y permite a los auditores internos extraer datos del área auditada, que están almacenados electrónicamente y realizar diversas operaciones con los datos. Dichas operaciones incluyen:

- Examinar los archivos y registros para verificar su validez, integridad y exactitud.
- Volver a calcular valores registrados u otros que sean de interés para la auditoría.
- Seleccionar e imprimir muestras y calcular los resultados de estas.
- Comparar información de archivos separados.
- Resumir datos, restablecer su secuencia y volver a aplicar formato a los datos.
- Crear tablas dinámicas para análisis multidimensional.
- Buscar posibles fraudes utilizando el análisis de la Ley de Benford.
- Preparar e imprimir informes o reportes específicos.
- Generar automáticamente un registro histórico de los análisis de datos realizados.

Existen diversos Software Generales de Auditoría, entre ellos están: Lenguaje de Comandos de Auditoría (ACL) y el de Extracción y Análisis de Datos Interactivos (IDEA), EASYTRIEVE, SAS. También puede utilizarse ACCESS y EXCEL de MSOffice.

c.2.2. Software utilitario

Programas de computadores proporcionados por un fabricante de hardware o por un proveedor de software y utilizados en la ejecución del sistema[3]. Esta técnica se puede utilizar para examinar la actividad de procesamiento, los programas de prueba, las actividades del sistema y los procedimientos operativos; para evaluar la actividad de los archivos de datos y para analizar los datos contables del trabajo.

[3] ACL, IDEA, EASYTRIEVE, SAS, ACCESS y EXCEL son productos o marcas comerciales registradas y de propiedad de sus respectivos dueños.

c.2.3. Datos de prueba

Transacciones simuladas que se pueden utilizar para probar la lógica de procesamiento, los cálculos y los controles programados en las aplicaciones informáticas. Se pueden probar programas individuales o un sistema completo. Esta técnica incluye instalaciones integradas de pruebas (ITF en inglés) y evaluaciones de sistemas con caso base (BCSE, en inglés)

c.2.4. Análisis de traza y mapeo

Herramientas especializadas que se pueden utilizar para analizar el fluido de los datos a través de la lógica de procesamiento del software de aplicación y para documentar la lógica, los recorridos, las condiciones de control y las secuencias de procesamiento. Se pueden analizar las instrucciones de control de trabajo o lenguaje de comando y el lenguaje de programación. Esta técnica incluye el mapeo de programas/sistemas, la traza, vistas instantáneas, simulaciones paralelas y comparaciones de códigos.

c.2.5. Sistemas expertos de auditoría

Sistemas expertos o de respaldo de decisiones que se pueden utilizar para ayudar a los auditores interno en el proceso de toma de decisiones mediante la automatización del conocimiento de expertos en el campo. Esta técnica incluye análisis de riesgos automatizado, software de sistemas y paquetes de software de objetivos de control.

Estas definiciones indican que los auditores internos pueden utilizar las TAAC para probar directamente:

- Los controles integrados en los sistemas de información computarizados.
- Los datos incluidos en los archivos de computador.

Se debe tener en cuenta que mediante la prueba directa de los datos incluidos en archivos de computadora, los auditores internos obtienen evidencia indirecta respecto de la eficacia de los controles en la aplicación que procesó los datos.

4 Anexo: Conceptos Generales sobre Apetito de Riesgo y Tolerancia al Riesgo

Según el glosario de las NOGAI, el Apetito de riesgo corresponde a "*Los tipos y la cantidad de riesgo que la organización está dispuesta a aceptar al perseguir sus estrategias y objetivos.*" Es decir, representa el nivel de riesgo que una entidad asume para alcanzar sus objetivos estratégicos, operacionales, financieros y de cumplimiento.

Refleja el nivel de aceptación institucional frente a eventos adversos, considerando su impacto potencial y probabilidad de ocurrencia, y establece el umbral a partir del cual un riesgo se considera inaceptable y requiere una respuesta inmediata, el fortalecimiento de controles u otra acción mitigante.

Por su parte la Tolerancia al Riesgo está definida como las "*Variaciones aceptables en el desempeño con relación al logro de los objetivos*."

Estos conceptos funcionan como referencia clave para:

- La evaluación de la severidad del riesgo o riesgo inherente (combinación de probabilidad e impacto).
- La valoración de la efectividad de los controles mitigantes.
- El cálculo de la exposición al riesgo o riesgo residual.

El auditor interno debe comprender la filosofía de gestión de riesgos utilizada para establecer el apetito y tolerancia al riesgo en la organización, en especial si existe una metodología establecida para determina ambos elementos, y si estos se comunican de manera efectiva por el Jefe de Servicio y los responsables de las áreas operativas.

Lo óptimo es que la organización cuente con una metodología establecida para definir el apetito y la tolerancia al riesgo, ya que las políticas y procedimientos de gestión de riesgos ayudan a garantizar que esta tarea se realice de manera eficaz.

En este contexto, es importante que la función de auditoría interna no asuma responsabilidades de gestión relacionadas con riesgos, tales como es el establecimiento del apetito de riesgo, la tolerancia o la aceptación de responsabilidad general por la gestión de riesgos en nombre de la organización.

Para efecto de esta Guía, el apetito de riesgo se materializa en la escala de clasificación de la exposición al riesgo residual, en la cual se definen los niveles "Menor", "Media", "Mayor" y "No Aceptable", según el siguiente umbral:

Escala del Nivel de Exposición al Riesgo (Ver Anexo N° 5: Tabla Nº 8)

INDICADOR DE EXPOSICIÓN AL RIESGO	ÍNDICE DE EXPOSICIÓN AL RIESGO	NIVEL DE EXPOSICIÓN AL RIESGO	RELACIÓN CON EL APETITO DE RIESGO
NIVEL SEVERIDAD DEL RIESGO **———————** **NIVEL EFECTIVIDAD DEL CONTROL**	**8,0 – 25,0**	**NO ACEPTABLE (Na)**	Excede el apetito de riesgo. Requiere intervención inmediata
	4,0 – 7,99	**MAYOR (Ma)**	Al límite del apetito de riesgo. Requiere atención prioritaria
	3,0 – 3,99	**MEDIA (Md)**	Dentro del apetito de riesgo. Requiere monitoreo periódico
	0,2 - 2,99	**MENOR (Me)**	Bien gestionado. Dentro del apetito de riesgo

Ejemplo aplicado del Apetito de Riesgo

Contexto:

Una función de auditoría interna realiza un trabajo al proceso de asignación y pago de subsidios a poblaciones vulnerables. Uno de los riesgos críticos identificados es:

"*Demoras significativas en el pago de subsidios que pueden afectar gravemente la subsistencia de beneficiarios vulnerables, generando impacto social negativo y cuestionamientos institucionales*."

1. Evaluación de la Severidad del Riesgo (riesgo inherente):

- **Probabilidad:** 4 (Probable)
- **Impacto:** 5 (Catastrófico)
- **Severidad del riesgo (Inherente):** 4 × 5 = 20 → Nivel Extremo

Este riesgo se clasifica como extremo, ya que podría comprometer necesidades básicas de la población objetivo, afectando la misión social de la entidad.

2. Evaluación del control clave:

- **Control existente:** Sistema automatizado de calendarización de pagos, con alertas ante retrasos y seguimiento de carga financiera"
- **Evaluación de efectividad del control:** Regular (2)

(El sistema presenta fallas intermitentes y no cuenta con medidas alternativas de respaldo en casos críticos).

3. Cálculo de la exposición al Riesgo (riesgo residual):

- **Severidad (20) ÷ Efectividad del Control (2) = 10**

4. Comparación con el Apetito y la Tolerancia al Riesgo Institucional:

- **Apetito de riesgo definido para este tipo de riesgo:** Menor → *Solo se aceptan exposiciones residuales de nivel ≤ 2.99*
- **Tolerancia al riesgo (límite máximo aceptable):** Nivel ≤ *3.99* (como excepción, bajo justificación y monitoreo especial)

5. Interpretación según el Apetito de Riesgo (usando el nivel definido en la Tabla N° 8 del Anexo N° 5):

- **Resultado:** Exposición al Riesgo = 10,0
- **Nivel:** No Aceptable
- **Acción requerida:** La exposición al riesgo residual supera el apetito y la tolerancia al riesgo establecida para este proceso por lo tanto, la entidad debe:

  - Reforzar el sistema de alertas con notificaciones en tiempo real y mecanismos de escalamiento automático.
  - Establecer controles de respaldo manual para asegurar los pagos en casos de fallas del sistema.
  - Mejorar la coordinación interinstitucional (p. ej., con Tesorería y áreas operativas) para garantizar la continuidad operativa del proceso.
  - Implementar un monitoreo continuo del cumplimiento de plazos críticos, con reportes periódicos al Jefe de Servicio.

5 Anexo: Tablas Tradicionales de Valuación de Riesgos, Controles, Severidad y Exposición al Riesgo

a. Severidad del Riesgo

- **Probabilidad**

Es la posibilidad de que un riesgo ocurra en un periodo determinado, considerando factores como antecedentes históricos, condiciones actuales, controles existentes y tendencias futuras. Se puede medir en términos cuantitativos o cualitativos y representa qué tan factible es que el riesgo se materialice.

- **Impacto**

Es la magnitud de las consecuencias que tendría la materialización de un riesgo sobre los objetivos de la organización. Puede expresarse en términos cualitativos (por ejemplo, nivel de afectación reputacional, operativa o legal) o cuantitativos (por ejemplo, pérdida financiera estimada). El impacto evalúa qué tan grave sería el efecto del riesgo si llegara a ocurrir.

a.1. Tabla N° 1: Categorías de Probabilidad

Categoría	Valor	Descripción
Casi certeza	**5**	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que este se presente en el año en curso. (90% a 100%).
Probable	**4**	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que este se presente en el año en curso.
Moderado	**3**	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que este se presente en el año en curso.
Improbable	**2**	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que este se presente en el año en curso.
Muy improbable	**1**	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que este se presente en el año en curso.

a.2. Tabla N° 2: Categorías de Impacto (Consecuencias)

Categoría	Valor	Descripción
Catastróficas	**5**	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en el presupuesto y/o comprometen totalmente la imagen pública de la entidad y del Gobierno. Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren en el año en curso.
Mayores	**4**	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la entidad y del Gobierno. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal en el año en curso.
Moderadas	**3**	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la entidad y del Gobierno. Su materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que este se desarrolle parcialmente en forma normal en el año en curso.
Menores	**2**	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la entidad y del Gobierno. Su materialización causaría un bajo daño en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos en el año en curso.
Insignificantes	**1**	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen pública de la entidad y del Gobierno. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afectaría el cumplimiento de los objetivos en el año en curso.

a.3. Tabla N° 3: Nivel de Severidad del Riesgo – Riesgo Inherente

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
Casi Certeza (5)	Catastróficas (5)	EXTREMO (25)
Casi Certeza (5)	Mayores (4)	EXTREMO (20)
Casi Certeza (5)	Moderadas (3)	EXTREMO (15)
Casi Certeza (5)	Menores (2)	ALTO (10)
Casi Certeza (5)	Insignificantes (1)	ALTO (5)
Probable (4)	Catastróficas (5)	EXTREMO (20)
Probable (4)	Mayores (4)	EXTREMO (16)
Probable (4)	Moderadas (3)	ALTO (12)
Probable (4)	Menores (2)	ALTO (8)
Probable (4)	Insignificantes (1)	MODERADO (4)
Moderado (3)	Catastróficas (5)	EXTREMO (15)
Moderado (3)	Mayores (4)	EXTREMO (12)
Moderado (3)	Moderadas (3)	ALTO (9)
Moderado (3)	Menores (2)	MODERADO (6)
Moderado (3)	Insignificantes (1)	BAJO (3)
Improbable (2)	Catastróficas (5)	EXTREMO (10)
Improbable (2)	Mayores (4)	ALTO (8)
Improbable (2)	Moderadas (3)	MODERADO (6)
Improbable (2)	Menores (2)	BAJO (4)
Improbable (2)	Insignificantes (1)	BAJO (2)
Muy improbable (1)	Catastróficas (5)	ALTO (5)
Muy improbable (1)	Mayores (4)	ALTO (4)
Muy improbable (1)	Moderadas (3)	MODERADO (3)
Muy improbable (1)	Menores (2)	BAJO (2)
Muy improbable (1)	Insignificantes (1)	BAJO (1)

En el cuadro anterior se muestra el resultado de la combinación entre las categorías del nivel de impacto del riesgo y las categorías del nivel de probabilidad de ocurrencia del riesgo, es decir, el nivel de severidad.

De ese esquema se puede observar que las categorías de impacto tienen una mayor incidencia en el nivel de severidad asignado, puesto que aunque la probabilidad de ocurrencia sea menor, al tratarse de riesgos con impactos altos, cualquier materialización del riesgo (aunque sea en solo una oportunidad) tendrá una consecuencia significativa en el uso de los recursos y en el cumplimiento de los objetivos del proceso examinado.

Esto explica los casos en que a igual valor, la severidad del riesgo es distinta. A modo de ejemplo se presentan las siguientes relaciones:

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
Muy improbable (1)	Mayores (4)	ALTO (4)
Probable (4)	Insignificantes (1)	MODERADO (4)
Probable (4)	Moderadas (3)	ALTO (12)
Moderado (3)	Mayores (4)	EXTREMO (12)

b. Clasificación de la efectividad del diseño del control clave

b.1. Diseño del control

- **Tabla Nº 4: Oportunidad de la Aplicación del Control (O):**

Clasificación	Descripción
Preventivo (Pv)	Controles claves que actúan antes o al inicio de una actividad.
Correctivo (Cr)	Controles claves que actúan durante el proceso y que permiten corregir las deficiencias.
Detectivo (Dt)	Controles claves que solo actúan una vez que el proceso ha terminado.

- **Tabla Nº 5: Periodicidad en la Aplicación del Control (PD):**

Clasificación	Descripción
Permanente (Pe)	Controles claves aplicados durante todo el proceso, es decir, en cada operación.
Periódico (Pd)	Controles claves aplicados en forma constante solo cuando ha transcurrido un período específico de tiempo.
Ocasional (Oc)	Controles claves que se aplican solo en forma ocasional en un proceso.

- **Tabla Nº 6: Automatización en la Aplicación del Control (A):**

Clasificación	Descripción
100% automatizado (At)	Controles claves incorporados en el proceso, cuya aplicación es completamente informatizada. Están incorporados en los sistemas informatizados.
Semi – automatizado (Sa)	Controles claves incorporados en el proceso, cuya aplicación es parcialmente desarrollada mediante sistemas informatizados.
Manual (Ma)	Controles claves incorporados en el proceso, cuya aplicación no considera uso de sistemas informatizados.

b.2. Tabla Nº 7: Escala de Clasificación de la Idoneidad del Diseño de los Controles

CUMPLIMIENTO CON NORMAS O REQUISITOS DE CONTROL	CARACTERÍSTICAS DISEÑO CONTROL CLAVE/FUNDAMENTAL			CLASIFICACIÓN	VALOR DEL DISEÑO DEL CONTROL
	PERIODICIDAD (PD)	OPORTUNIDAD (O)	AUTOMATIZACIÓN (A)		
CUMPLIMIENTO ADECUADO	PERMANENTE PERMANENTE PERMANENTE	PREVENTIVO PREVENTIVO PREVENTIVO	INFORMATIZADO SEMI INFORMAT MANUAL	OPTIMO	5
CUMPLIMIENTO ADECUADO	PERMANENTE PERMANENTE PERMANENTE	CORRECTIVO CORRECTIVO CORRECTIVO	INFORMATIZADO SEMI INFORMAT MANUAL		
CUMPLIMIENTO ADECUADO	PERMANENTE PERMANENTE PERMANENTE	DETECTIVO DETECTIVO DETECTIVO	INFORMATIZADO SEMI INFORMAT MANUAL	BUENO	4
CUMPLIMIENTO ADECUADO	PERIODICO PERIODICO PERIODICO	PREVENTIVO PREVENTIVO PREVENTIVO	INFORMATIZADO SEMI INFORMAT MANUAL		
CUMPLIMIENTO ADECUADO	PERIODICO PERIODICO PERIODICO	CORRECTIVO CORRECTIVO CORRECTIVO	INFORMATIZADO SEMI INFORMAT MANUAL	MAS QUE REGULAR	3
CUMPLIMIENTO ADECUADO	PERIODICO PERIODICO PERIODICO	DETECTIVO DETECTIVO DETECTIVO	INFORMATIZADO SEMI INFORMAT MANUAL		
CUMPLIMIENTO ADECUADO	OCASIONAL OCASIONAL OCASIONAL	PREVENTIVO PREVENTIVO PREVENTIVO	INFORMATIZADO SEMI INFORMAT MANUAL	REGULAR	2
CUMPLIMIENTO ADECUADO	OCASIONAL OCASIONAL OCASIONAL	CORRECTIVO CORRECTIVO CORRECTIVO	INFORMATIZADO SEMI INFORMAT MANUAL		
CUMPLIMIENTO ADECUADO	OCASIONAL OCASIONAL OCASIONAL	DETECTIVO DETECTIVO DETECTIVO	INFORMATIZADO SEMI INFORMAT MANUAL	DEFICIENTE	1
INSUFICIENTE	NO DETERMINADO	NO DETERMINADO	NO DETERMINADO	INEXISTENTE	1

Para examinar el diseño de un control, en primer lugar, debe expresarse con un breve detalle de las actividades de control realizadas, analizando su nivel de documentación y segregación de funciones (quién autoriza o revisa debe ser distinta a quién ejecuta).

Hay que relevar que el control debe expresarse claramente, señalando qué se hace, cómo se hace, quién lo hace y cuándo lo realiza. Una vez definido, se debe evaluar si el control mitigante asociado a un riesgo tiene un nivel de cumplimiento adecuado respecto de los requisitos de control básicos que en este modelo se han relevado para dar razonable seguridad de cumplimiento de los objetivos y metas. Esto implica realizar un análisis integral de los referidos requisitos (segregación, autorización, formalización, etc.) y determinar si estas se cumplen de para un control examinado en particular.

Producto de este análisis, se puede dar que los referidos requisitos se cumplan satisfactoriamente, es decir, que el control esté sustentado en una estructura básica sólida. Posteriormente, se debe seguir con el análisis del diseño del control, este aspecto es relevante, ya que los riesgos son por naturaleza dinámicos y requieren que los controles tengan una estructura que se oriente a la prevención de la materialización del efecto de los riesgos dinámicos.

Finalmente, se debe clasificar el nivel de efectividad del control examinado, de acuerdo con el esquema presentado, asignándole el valor respectivo según la escala.

En caso de que esto no ocurra, es decir, los requisitos no presentan un cumplimiento suficiente en el control examinado, debe entenderse que su nivel de cumplimiento es insuficiente y corresponde clasificarlo como si se tratara de un control inexistente, con valoración de 1, sin que ya sea necesario evaluar la efectividad en el diseño del control respecto de la ocurrencia del riesgo.

Por consiguiente, debe clasificarse como inexistente, con nivel de eficiencia del control examinado de 1, de acuerdo con la escala contenida en el esquema presentado.

Al describir los controles existentes, se debe señalar al menos: la norma o guía que lo instruye, quién lo realiza, qué actividades desarrolla, cómo las ejecuta y cuándo y cómo se evidencia su cumplimiento (registros documentales o electrónicos en el sistema).

Actividades de control clave comunes

Algunos ejemplos de los distintos tipos de actividades de control clave más comunes que se pueden considerar como claves en los procesos de una entidad son:

- **Aprobar:** Autorización para ejecutar una transacción, otorgada por una persona que tiene facultades para hacerlo.
- **Calcular:** Computar o volver a computar un importe que resulta de otros datos obtenidos en el proceso.
- **Documentar:** Preservar información original o documentar la base lógica de las opiniones emitidas para referencia futura.
- **Examinar:** Verificar la existencia o el surgimiento de un atributo.
- **Comparar:** Comparaciones entre dos atributos diferentes para verificar si coinciden.
- **Controlar:** Verificar para asegurar que una acción se esté realizando.
- **Restringir:** No permitir una acción no aceptable.
- **Segregar:** Separar las responsabilidades incompatibles que pueden crear la posibilidad para una acción no deseada.
- **Supervisar:** Proporcionar instrucciones y supervisión para asegurar que las acciones y las tareas se lleven a cabo tal como se diseñaron.

c. Clasificación del Nivel de Exposición al Riesgo (riesgo residual)

La exposición al riesgo está determinada por la severidad del riesgo dividida por la eficiencia del control asociado a ese riesgo. Estos elementos se obtienen de las relaciones detalladas previamente en este anexo. A continuación, se presenta la escala de nivel de exposición al riesgo que los califica:

Tabla N° 8: Escala del Nivel de Exposición al Riesgo

INDICADOR DE EXPOSICIÓN AL RIESGO	ÍNDICE DE EXPOSICIÓN AL RIESGO	NIVEL DE EXPOSICIÓN AL RIESGO	RELACIÓN CON EL APETITO DE RIESGO
NIVEL SEVERIDAD DEL RIESGO ——— NIVEL EFECTIVIDAD DEL CONTROL	8,0 – 25,0	NO ACEPTABLE (Na)	Excede el apetito de riesgo. Requiere intervención inmediata
	4,0 – 7,99	MAYOR (Ma)	Al límite del apetito de riesgo. Requiere atención prioritaria
	3,0 – 3,99	MEDIA (Md)	Dentro del apetito de riesgo. Requiere monitoreo periódico
	0,2 - 2,99	MENOR (Me)	Bien gestionado. Dentro del apetito de riesgo

Tal como se señaló, la escala previamente presentada, ha sido construida en base a la relación entre el nivel de severidad del riesgo (Bajo, Moderado, Alto. Extremo) y el nivel de efectividad del control asociado a ese riesgo (Deficiente, Regular, Más que regular, Bueno, Óptimo).

Un primer análisis de dicha escala observaría que los niveles de exposición al riesgo Mayor y No Aceptable, pudiesen tener un rango muy extenso de valores; 4,0 a 7,99 y 8,0 a 25 puntos respectivamente, pero al realizar un análisis más riguroso, se debería observar que en realidad los niveles de exposición al riesgo con valores más altos, corresponden a las combinaciones entre los niveles de riesgo más severos y los niveles de eficiencia del control más Bajos, o a las combinaciones entre los riesgos con severidad más altas y con controles que tienen un nivel de efectividad solo de Regular.

Por otra parte, los niveles de exposición al riesgo más bajos están conformados por las combinaciones entre los niveles de riesgos menos severas y los niveles de eficiencia del control más altos, o por las combinaciones entre riesgos con severidades Bajas y controles con niveles de efectividad Deficiente o Regular, o por las combinaciones entre riesgos con severidad altas, pero con controles con nivel de efectividad Óptimo o Bueno.

Por ejemplo, en el Esquema N° 1 se observa que el nivel de exposición al riesgo E1 = 10, (Nivel de exposición al riesgo No Aceptable) está conformado por un nivel de severidad del riesgo, Extremo = 20 y un nivel de efectividad de control, Regular = 2.

En el caso del nivel de exposición E2 = 4 (Nivel de exposición al riesgo Mayor), está conformado por un nivel de severidad del riesgo, Alto = 12 y un nivel de efectividad de control, Más que Regular = 3.

Finalmente, el nivel de exposición E3 = 1 (Nivel de exposición al riesgo Menor), está conformado por un nivel de severidad del riesgo, Alto = 5 y un nivel de efectividad de control, Óptimo = 5.

Esquema N° 1: Mapa de Calor del Nivel de Exposición al Riesgo

NIVEL DEL RIESGO			NIVEL DE LA EFECTIVIDAD DEL CONTROL				
			OPTIMO	BUENO	MAS QUE REGULAR	REGULAR	DEFICIENTE
			5	4	3	2	1
	EXTREMO	25	5	6,25	8,33	12,5	25
		20	4	5	6,67	10 E1	20
		16	3,2	4	5,33	8	16
	ALTO	15	3	3,75	5	7,5	15
		12	2,4	3	4 E2	6	12
		10	2	2,5	3,33	5	10
	MODERADO	9	1,8	2,25	3	4,5	9
		8	1,6	2	2,67	4	8
		6	1,2	1,5	2	3	6
	BAJO	5	1 E3	1,25	1,67	2,5	5
		4	0,8	1	1,33	2	4
		3	0,6	0,75	1	1,5	3
		2	0,4	0,5	0,67	1	2
		1	0,2	0,25	0,33	0,5	1

6 Anexo: Conceptos sobre Dimensiones o Criterios Cualitativos Adicionales en la Evaluación de Riesgos

El nivel de severidad o gravedad de un riesgo, utilizado para determinar su priorización según la literatura especializada, se entiende como una función de todos los criterios que la organización decida emplear en su evaluación. Si bien los criterios más comúnmente utilizados son el impacto y la probabilidad, las organizaciones pueden incorporar otros para enriquecer el análisis, dependiendo del nivel de madurez de su proceso de gestión de procesos. A continuación, se describen algunos que pueden ser aplicados al sector público en mayor o menor medida (la lista no es taxativa):

- Vulnerabilidad.
- Volatilidad.
- Velocidad (que comprende la rapidez de reacción y la rapidez de recuperación).
- Interdependencia.
- Correlación.
- Persistencia.
- Impacto en el Valor Público.

• Vulnerabilidad

La vulnerabilidad es una medida de cuán susceptible es una organización a un riesgo determinado. Esto depende del nivel de preparación, agilidad y adaptabilidad de la organización. Dada esta descripción, es claro que existe una relación estrecha entre vulnerabilidad e impacto, debido a que, a mayor vulnerabilidad, mayor será el impacto probable. Este análisis resulta útil para comprender el riesgo e identificar una respuesta adecuada.

• Volatilidad

En algunos casos, la probabilidad de que un riesgo se active varía según la volatilidad de la situación. Cuando las condiciones fluctúan, es más difícil predecir la probabilidad de un evento determinado. Es probable que un riesgo de este tipo tenga una mayor prioridad para la gestión del riesgo debido a su mayor imprevisibilidad.

• Velocidad

Algunos análisis incluyen el criterio de velocidad del riesgo (o rapidez de aparición). Esta es una medida del tiempo de advertencia previa y de preparación que puede tener una organización entre la ocurrencia del evento y su impacto. Puede dividirse en rapidez de reacción y rapidez de recuperación. El tiempo entre la ocurrencia del evento y su impacto en la organización a veces se conoce como proximidad.

• Interdependencia

Es importante no considerar los riesgos de manera aislada, sino también en combinación. La materialización de dos o más riesgos puede afectar a la organización de forma distinta a la suma de sus impactos individuales y puede depender de si los eventos ocurren de manera simultánea o consecutiva.

Por ejemplo, las centrales nucleares en Japón están preparadas para terremotos y tsunamis. Sin embargo, la concurrencia de ambos eventos puede permitir que una ola supere las defensas ya debilitadas por los temblores. Otro ejemplo: los controles financieros rutinarios suelen exigir la segregación de funciones clave para evitar que un empleado ordene bienes para uso personal. Sin embargo, si dos o más individuos deciden coludirse para cometer dicho fraude, es mucho más difícil de detectar. Las causas de los eventos de riesgo interdependientes no están relacionadas entre sí.

- **Correlación**

La correlación es similar a la interdependencia y se refiere a la conexión entre dos o más riesgos. En este caso, en lugar de una dependencia mutua de riesgos que desencadena nuevos riesgos potenciales, varía el impacto o la probabilidad de los riesgos. Por ejemplo, las debilidades en una economía nacional pueden generar riesgos cambiarios y aumentar los costos de bienes y servicios comercializados internacionalmente. Estos costos pueden aumentar la necesidad de endeudamiento. Los factores económicos subyacentes que provocan fluctuaciones en los tipos de cambio también pueden estar asociados con tasas de interés más altas y mayores dificultades para acceder al crédito. A diferencia de la interdependencia, las causas de los riesgos correlacionados sí están relacionadas.

Las interacciones entre eventos de riesgo (tanto interdependencias como correlaciones) pueden representarse en una cuadrícula, con cada riesgo encabezando todas las filas y columnas. Cuando dos riesgos se cruzan en la cuadrícula, existe el potencial de un riesgo aún mayor. Por ejemplo, una expansión o recesión económica probablemente desencadene, incremente o coincida con una amplia gama de otros eventos de riesgo relacionados con los costos de endeudamiento, los precios de materias primas y la demanda de bienes y servicios.

- **Persistencia**

Es la capacidad de un riesgo de mantenerse vigente, reaparecer o resistir los esfuerzos de mitigación en el tiempo. Refleja la tendencia del riesgo a prolongarse estructuralmente dentro de la organización, independientemente de los controles implementados, y sugiere la existencia de condiciones subyacentes (culturales, operativas o sistémicas) que favorecen su continuidad o reaparición.

Este criterio permite evaluar no solo la duración del riesgo, sino también la resiliencia negativa del mismo: su capacidad de adaptarse o mutar frente a intervenciones, haciendo que su eliminación definitiva sea compleja. Un riesgo con alta persistencia puede parecer controlado temporalmente, pero volver a manifestarse debido a debilidades estructurales no resueltas.

- **Impacto en el Valor Público (variable específica para el sector público)**

En el contexto del sector público, además de las variables tradicionales de impacto y probabilidad y las cualitativas adicionales, es posible incorporar un criterio específico que se refiere al impacto del riesgo en el valor público. Este corresponde al grado en que un riesgo puede afectar la creación, protección o sostenimiento del valor público que generan las instituciones estatales a través de sus políticas, programas y servicios.

La incorporación del impacto en el valor público en la evaluación del riesgo permite priorizar aquellos eventos que no solo amenazan la gestión interna, sino también el valor que la entidad pública entrega a la sociedad, fortaleciendo la alineación con las NOGAI y los principios de gobernanza, integridad y sostenibilidad del Estado.

El impacto en el valor público puede manifestarse en diversas dimensiones:

- **Confianza ciudadana:** Pérdida o deterioro de la percepción de integridad, transparencia y legitimidad institucional.
- **Cumplimiento del mandato público:** Riesgos que impidan el logro de los objetivos estratégicos, metas de política pública o compromisos internacionales.
- **Eficiencia y eficacia del gasto público:** Riesgos que generen uso ineficiente, duplicación o desviación de recursos fiscales.
- **Equidad y bienestar social:** Riesgos que afecten la entrega oportuna, inclusiva y de calidad de servicios públicos esenciales.
- **Sostenibilidad institucional:** Riesgos que afecten la continuidad, capacidad técnica o resiliencia de la organización pública.

Tabla Nº 1: Escala Cualitativa de las Variables Adicionales para Evaluación de Riesgos

Variable	Categoría	Ponderación	Descripción Mejorada
Vulnerabilidad	Baja (1)	A definir	El proceso o población afectada cuenta con mecanismos robustos de defensa, respaldo institucional, protocolos activos y flexibilidad operativa.
	Media (2)		Existen controles o mecanismos, pero son parciales, desactualizados o con limitaciones de cobertura o aplicabilidad.
	Alta (3)		Se evidencia exposición crítica por falta de preparación, dependencia tecnológica o institucional, o ausencia de planes de contingencia efectivos.
Volatilidad	Baja (1)	A definir	El riesgo presenta comportamiento estable y predecible; responde de forma constante ante condiciones similares.
	Media (2)		El riesgo puede variar ante ciertos factores internos o externos, pero sus fluctuaciones son generalmente controlables.
	Alta (3)		El riesgo se manifiesta de manera errática, con alta sensibilidad a variables externas e incapacidad para anticipar sus efectos.
Velocidad	Baja (1)	A definir	El impacto del riesgo es progresivo y permite una ventana de reacción mayor a dos semanas sin consecuencias graves inmediatas.
	Media (2)		El impacto se desarrolla en un plazo intermedio (3 días a 2 semanas), lo que exige respuesta diligente pero no urgente.
	Alta (3)		El riesgo genera efectos severos en menos de 72 horas, exigiendo reacción inmediata y protocolos activados de forma automática.
Interdependencia	Baja (1)	A definir	El riesgo puede gestionarse internamente sin depender de otros procesos, actores o sistemas externos.
	Media (2)		Existen vínculos con algunos procesos o sistemas externos, pero el riesgo puede aislarse en escenarios normales.
	Alta (3)		El riesgo se amplifica o se propaga por conexiones operativas, tecnológicas o institucionales con terceros o áreas críticas.
Persistencia	Baja (1)	A definir	El riesgo ha sido erradicado o controlado de forma sostenible, sin recurrencias tras la implementación de acciones correctivas.
	Media (2)		El riesgo ha sido parcialmente mitigado, pero persisten factores estructurales que favorecen su reaparición bajo ciertas condiciones.
	Alta (3)		El riesgo es crónico, sistémico o cultural; ha reaparecido de forma recurrente a pesar de diversos esfuerzos de control.
Correlación	Baja (1)	A definir	El riesgo ocurre de forma aislada y no está relacionado con otros factores económicos, sociales o políticos relevantes.
	Media (2)		El riesgo está condicionado por algunos factores del entorno, pero su ocurrencia aún depende del contexto interno.
	Alta (3)		La manifestación del riesgo está estrechamente vinculada a variables externas (económicas, políticas, sociales, climáticas), lo que complica su predicción y gestión.
Impacto en Valor Público	Baja (1)	A definir	El riesgo, aunque se materialice, no genera afectación significativa al mandato, reputación ni confianza pública de la institución.
	Media (2)		Puede ocasionar deterioro parcial de la percepción institucional, incumplimientos menores de mandato o afectación limitada de servicios esenciales.
	Alta (3)		Genera una afectación severa al mandato, confianza ciudadana, credibilidad institucional, legitimidad del Estado o la equidad en la provisión de servicios públicos.

d. Método de evaluación ajustada de la Severidad del Riesgo (Riesgo Inherente) y Exposición al Riesgo (Riesgo Residual)

1. Evaluación tradicional de la Severidad del Riesgo

Se calcula como el producto entre la probabilidad y el impacto del evento de riesgo, utilizando una escala de 1 a 5.

Severidad del Riesgo Tradicional = Probabilidad × Impacto

- **Probabilidad:** mide la posibilidad de que el evento ocurra.
- **Impacto:** estima las consecuencias si el evento se materializa.

Este resultado entrega una primera estimación de la severidad del riesgo (bajo, moderado, alto, extremo).

2. Ajuste de la Severidad del Riesgo incorporando variables cualitativas adicionales

Para enriquecer la evaluación del riesgo, en este caso, se utilizarán algunas variables cualitativas (5) que reflejan factores de contexto no considerados en el modelo tradicional:

Variable	Descripción
Vulnerabilidad	Grado de exposición o debilidad ante el riesgo.
Velocidad	Tiempo entre el inicio del evento y su impacto.
Interdependencia	Conexión con otros procesos o entidades.
Correlación	Coincidencia o amplificación de riesgos por factores externos.
Impacto en Valor Público	Grado en que el riesgo afecta el mandato, la legitimidad y confianza ciudadana.

Cada variable se califica en una escala de 1 (baja), 2 (media), 3 (alta) y se pondera en este caso al 20% del total. La suma ponderada da un multiplicador cualitativo (entre 1.0 y 3.0) que ajusta el riesgo inherente tradicional, tal como se observa en la siguiente tabla.

Variable	Valor	Porcentaje Ponderación	Subtotal
Vulnerabilidad	(1 - 3)	20%	V × 0.2
Velocidad	(1 - 3)	20%	VE × 0.2
Interdependencia	(1 - 3)	20%	ID × 0.2
Correlación	(1 - 3)	20%	C × 0.2
Impacto en Valor Público	(1 - 3)	20%	VP × 0.2
		Total 100%	**Suma= Multiplicador Cualitativo**

Severidad del Riesgo Ajustada= Severidad del Riesgo Tradicional × Multiplicador Cualitativo

3. Evaluación de la Exposición al Riesgo

Una vez calculado la Severidad al Riesgo Ajustada, se incorpora la efectividad del control mitigante, usando una escala de 1 (deficiente) a 5 (óptimo). Esto refleja cuánto se reduce el riesgo por los controles mitigantes existentes.

Exposición al Riesgo = Severidad al Riesgo Ajustada ÷ Valor del Control

4. Comparación con el Apetito de Riesgo

El resultado final se clasifica y compara con el umbral institucional definido en la Escala del Apetito de Riesgo, que refleja cuánto riesgo está dispuesta a aceptar la entidad:

Esquema N° 2: Tabla de Exposición al Riesgo y Relación con Apetito de Riesgo

ÍNDICE DE EXPOSICIÓN AL RIESGO	NIVEL DE EXPOSICIÓN AL RIESGO	RELACIÓN CON EL APETITO DE RIESGO
8,0 – 25,0	**NO ACEPTABLE (Na)**	Excede el apetito de riesgo. Requiere intervención inmediata
4,0 – 7,99	**MAYOR (Ma)**	Al límite del apetito de riesgo. Requiere atención prioritaria
3,0 – 3,99	**MEDIA (Md)**	Dentro del apetito de riesgo. Requiere monitoreo periódico
0,2 - 2,99	**MENOR (Me)**	Bien gestionado. Dentro del apetito de riesgo

e. Caso Práctico: Riesgo en la entrega y pago de subsidios a poblaciones vulnerables

Contexto del riesgo identificado

La entidad pública responsable de la protección social entrega subsidios mensuales a hogares en situación de pobreza extrema. Un proceso crítico es la transferencia oportuna de estos subsidios. Una falla puede tener consecuencias graves para los beneficiarios y para la legitimidad institucional.

Riesgo Crítico: *Demoras significativas en el pago de subsidios que pueden afectar gravemente la subsistencia de beneficiarios vulnerables, generando impacto social negativo y cuestionamientos institucionales.*

Este riesgo ha sido identificado en el contexto de una auditoría al proceso de gestión y pago de subsidios sociales a población en situación de vulnerabilidad. Se trata de una actividad prioritaria para la política pública y el mandato institucional.

1. Evaluación Tradicional de la Severidad del Riesgo

Variable	Valor	Justificación
Probabilidad	4 (Probable)	Se ha evidenciado un historial de recurrencia de demoras por causas administrativas y técnicas.
Impacto	5 (Catastrófico)	Afecta directamente la subsistencia de los beneficiarios, genera presión política y daño reputacional significativo.

Probabilidad e Impacto: 4 × 5 = 20 → Nivel Extremo

2. Evaluación de la Efectividad del Control Clave

- **Descripción del Control:** Validación automatizada semanal del padrón de beneficiarios, con revisión manual ante discrepancias.
- **Diseño del Control:** Preventivo, periódico, semi-automatizado
- **Evaluación del Diseño: del Control: Bueno → Valor = 4**

3. Cálculo de la Exposición al Riesgo

- **Severidad del Riesgo ÷ Valor Control Clave Existente: 20 ÷ 4 = 5 → Mayor**

Según Escala: Al límite del apetito de riesgo. Requiere atención prioritaria.

4. Ajuste Severidad y Exposición al Riesgo mediante variables cualitativas adicionales

Análisis y Evaluación de Variables Cualitativas

Variable	Descripción Evaluada	Valor (Escala)	Ponderación	Subtotal
Vulnerabilidad	Beneficiarios sin redes de apoyo ni fuentes alternativas de ingreso	3 (Alta)	0.20	0.60
Velocidad	El efecto negativo es inmediato: en menos de 3 días ya hay impacto social	3 (Alta)	0.20	0.60
Interdependencia	Dependencia de sistemas de otras entidades (registro civil, bancos, etc.)	3 (Alta)	0.20	0.60
Correlación	Riesgo se intensifica con recortes presupuestarios y carga de procesos simultáneos	3 (Alta)	0.20	0.60
Impacto en Valor Público	Afectación del mandato, pérdida de confianza institucional y percepción de abandono estatal	3 (Alto Impacto)	0.20	0.60
			100%	3.0

Multiplicador cualitativo = 3.00

Aplicación:

- Nivel de Severidad al Riesgo Ajustado: 20 x 3.0 = 60
- Nivel de Exposición al Riesgo ajustado: 60 ÷ 4 = 15 → **No Aceptable (Na)**

Interpretación: El riesgo supera el Apetito de Riesgo institucional. Requiere intervención inmediata.

Aunque el cálculo tradicional lo ubica en el nivel "**Mayo**r", las condiciones cualitativas elevan la exposición al riesgo al nivel **"No Aceptable"**, superando el nivel de Apetito de Riesgo institucional.

Medidas sugeridas por auditoría interna para tratar el riesgo no aceptable (priorizadas por velocidad)

Variable Relacionada Directamente	Categoría de Medida en Tiempo	Medidas Propuestas
Velocidad	Inmediatas (0–30 días)	Activar protocolo de emergencia para pagos, mesa de crisis, auditoría inmediata
	Corto Plazo (1–3 meses)	Tableros de monitoreo en tiempo real, rediseño del flujo operativo
	Mediano Plazo (3–6 meses)	Indicadores de persistencia y velocidad
Vulnerabilidad	Corto Plazo (1–3 meses)	Validación automatizada del padrón de beneficiarios
	Estratégicas (6–12 meses)	Política transversal de protección del valor público
Interdependencia	Mediano Plazo (3–6 meses)	Alianzas operativas con bancos y registro civil
	Estratégicas (6–12 meses)	Sistemas interoperables, comité de gobernanza de riesgos
Correlación	Mediano Plazo (3–6 meses)	Comité de riesgos críticos, análisis de contextos simultáneos
	Estratégicas (6–12 meses)	Ajustes al plan estratégico de auditoría
Impacto en Valor Público	Inmediatas (0–30 días)	Comunicación institucional proactiva con beneficiarios
	Estratégicas (6–12 meses)	Actualización del apetito de riesgo institucional

Justificación de la prioridad

- Velocidad Alta = Medidas inmediatas para evitar que el daño se materialice en horas o días.
- El resto de las variables cualitativas complementan la exposición, pero si el efecto es inmediato, la contención también debe serlo.

7 Anexo: Aspectos relevantes de los procesos de gobierno, gestión de riesgos y control en la actividad bajo revisión, que se deben conocer y analizar, previo a la planificación del trabajo

Para evaluar los procesos de gestión de riesgos y control en la actividad bajo revisión es posible utilizar alguno o una combinación de los siguientes enfoques de auditoría:

- Un enfoque[4] para evaluar las estructuras y componentes de gobierno, gestión de riesgos y control en la actividad bajo revisión auditada.
- Un enfoque para la evaluación de un proceso específico (actividad bajo revisión) de Gobierno, o de Gestión de Riesgos, o de Control.
- Un enfoque para realizar una evaluación integral a nivel de entidad, a los procesos de Gobierno, o de Gestión de Riesgos, o de Control, utilizando un marco como referencia.

Cualquiera sea el enfoque que se utilice, se debe obtener información relevante para realizar el trabajo. Entre la información que se puede considerar para los procesos de gobierno, gestión de riesgos y control, se pueden considerar las siguientes:

a. Gobierno

Obtener documentación formal física o digital relacionada con estructuras, mecanismos, sistemas o procesos, etc. que sirva para conocer y analizar en forma detallada y general cómo funciona el gobierno en la actividad bajo revisión, y para determinar posteriormente en la ejecución del trabajo, cuáles son sus debilidades y fortalezas. Para ello, es posible analizar, entre otras, las siguientes materias:

- La estructura, comunicación y funcionamiento organizacional de los órganos de gobernanza de la actividad bajo revisión, especialmente con:

  – Los roles y responsabilidades organizacionales de funcionarios claves.
  – La estrategia/Políticas corporativas institucionales y toma de decisiones estratégicas y operativas.
  – El proceso presupuestario y mejoramiento de la gestión.

- Los mecanismos para fortalecer y aplicar la ética y valores organizacionales en la actividad bajo revisión, especialmente relacionados con:

  – La probidad/anticorrupción.
  – Los procesos de Transparencia.
  – El cumplimiento legal y regulatorio.
  – La cultura organizacional.

- La gestión del desempeño y rendición de cuentas (accountability) de la actividad bajo revisión.
- Monitoreo y vigilancia del control y la gestión de riesgos en la actividad bajo revisión.
- Comunicación de riesgos y controles a las áreas adecuadas dentro de la actividad bajo revisión.
- El gobierno de tecnologías de la información dentro de la actividad bajo revisión.

b. Gestión de riesgos

Obtener documentación formal física o digital relacionada con estructuras, mecanismos, sistemas o procesos, etc. que sirva para conocer y analizar en forma detallada y general cómo funciona la gestión de riesgos en la actividad bajo revisión, y para determinar posteriormente en la ejecución del trabajo, cuáles son sus debilidades y fortalezas. Para ello, es posible analizar, entre otras las siguientes materias:

[4] Ver los enfoques en el Documento Técnico N° 111: Conceptos y elementos claves de la naturaleza del trabajo de auditoría interna: gobierno, gestión de riesgos y control en el Sector Público.

- Documentación del contenido de la Matriz de Riesgos Estratégica de la actividad bajo revisión que se va a evaluar.
- Identificación y análisis de riesgos en la Matriz de Riesgos Estratégica, en base a la criticidad e importancia de los procesos a los cuales se asocian.
- Identificación y análisis de los controles en la Matriz de Riesgos Estratégica, que aseguren completitud, adecuada clasificación y razonabilidad del efecto mitigador del riesgo.
- Diseño y cumplimiento de los roles asociados a la gestión de riesgos que se han asignado en la actividad bajo revisión.
- Levantamiento de procesos de la actividad bajo revisión, y adecuación del nivel de desagregación de estos, en componentes menores (procesos, subprocesos o actividades), para desarrollar la gestión de riesgos.
- Revisiones y análisis de los objetivos de los subprocesos o etapas que se identificaron para la gestión de riesgos en la actividad bajo revisión.
- La estructura y los medios de comunicación y consulta que existen en la actividad bajo revisión, con relación a la oportunidad, contenido de reportes, acceso y participación de usuarios, entre otros.
- Análisis de resultados asociados a los riesgos residuales, que sea consistente con la realidad de la entidad.
- Planes de tratamiento de riesgos, que permitan dar seguridad de que se gestionan adecuadamente los riesgos relevantes a través de acciones útiles para disminuir o mitigar los riesgos.
- Mecanismos formales de monitoreo y seguimiento de los planes de tratamiento de riesgos.
- Indicadores para medir el grado de implementación de las estrategias y las metas contenidas en el plan de tratamiento, para dar cuenta del logro al cual se asocia el indicador.

c. Control

Obtener documentación formal física o digital relacionada con estructuras, mecanismos, sistemas o procesos, etc. que sirva para conocer y analizar en forma detallada y general cómo funciona el control en la actividad bajo revisión, y para determinar posteriormente en la ejecución del trabajo, cuáles son sus debilidades y fortalezas. Para ello, es posible analizar, entre otras, las siguientes materias:

- Mecanismos y estructuras o procedimientos para documentar, analizar y evaluar el diseño y la ejecución de los controles.
- Documentación sobre los requisitos del diseño de los controles en relación con la severidad de los riesgos.
- Proceso para actualización constante de las normas relacionadas con las operaciones y de los procedimientos de control, para que reflejen los cambios que se produzcan en el entorno.
- Metas y objetivos para asegurar que los controles funciones tal como se pretende en el diseño.
- Mecanismos y roles para dar respuesta apropiada a los riesgos significativos.
- Mecanismos para mantenerse al tanto de nuevos problemas, leyes y regulaciones relacionadas con obligaciones de control que afecten a la actividad bajo revisión.
- Procedimientos para identificar, evaluar y corregir deficiencias de control.
- Mecanismos y procedimientos para medir y supervisar los costos y beneficios que implican los controles.
- Mecanismos para evaluar si los recursos empleados en los procesos de control exceden de los beneficios para la actividad bajo revisión.
- Mecanismos para evaluar si los controles provocan problemas importantes en los procesos de la actividad bajo revisión (por ejemplo, errores, retrasos o duplicación de trabajo).
- Planes de formación sobre controles y procesos de autoevaluación continua al personal de la actividad bajo revisión.
- Procesos para supervisar avances tecnológicos que pueden mejorar la eficiencia y la eficacia del control en la actividad bajo revisión.

8 Anexo: Procesos Genéricos, Principales Riesgos, Controles Esperados

Tabla N° 1: Relación entre Procesos - Riesgos - Controles

Proceso Clave	Principales Riesgos	Controles Básicos Esperados
Tesorería / Caja / Efectivo	Pagos no autorizados, cheques manipulados, cobros no registrados	Conciliaciones diarias, segregación de funciones, validación dual de pagos, auditoría digital y registro de excepciones.
Cuentas por Pagar / Compras	Fraccionamiento de contratos, pagos duplicados, proveedores falsos	Sistema con controles automáticos de duplicado, validación de proveedores, lista de proveedores sancionados, revisión de contratos.
Cuentas por Cobrar / Ventas	Ingresos desviados, créditos vencidos sin seguimiento	Políticas de crédito claras, validación bancaria, bloqueos automáticos ante morosidad, conciliación de cuentas, monitoreo de cartera.
Nómina / Remuneraciones	Empleados fantasmas, horas extras indebidas, pagos indebidos	Cruce con base de RRHH, validación de asistencia, revisión de altas y bajas, verificación de titularidad, auditoría de nóminas.
Inventarios	Sustracción de inventario, manipulación de stock, sobrevaloración	Control físico periódico, conciliaciones contables, seguimiento de rotación, inventarios sorpresa, registros de acceso.
Activos Fijos	Uso indebido de activos, registros sin autorización, obsolescencia sin seguimiento	Geolocalización y control de activos, registro digital, validación por proceso de adquisiciones, mantenimiento preventivo, reconciliación de estado físico y contable.
Proyectos / Programas Especiales	Desvío de fondos, metas subregistradas, ejecución incompleta	Presupuesto ligado a IA o analítica, indicadores trazables, hitos de ejecución, auditoría del gasto por hito, informes de avance a *stakeholders*.
Contrataciones / Licitaciones	Adjudicación directa injustificada, manipulación de criterios, colusión	Registro electrónico de proceso de licitación inviolable, trazabilidad digital de criterios de adjudicación, auditoría independiente, lista de proveedores bloqueados.
TI / Ciberseguridad	Accesos indebidos, cuentas activas no autorizadas, fuga de datos	Autenticación *multifactor*, monitoreo contínuo, cifrado de datos sensibles, alertas con IA, revisión de logs de acceso, pruebas de vulnerabilidad.
Procesos con IA / Automatización	Decisiones sin control humano, sesgo algorítmico, falta de auditoría del modelo	Logs de decisiones automatizadas, validación de algoritmos, revisión ética de IA, validación humana de decisiones críticas, métricas de sesgo y equidad.
Gestión de Activos	Pérdida de activos, subutilización, obsolescencia no gestionada	Registro centralizado de activos, mantenimiento preventivo programado, revisión de depreciaciones, auditoría de liquidación de activos.
Cadena de Suministro	Interrupciones críticas, fraude en proveedores, riesgos ESG no gestionados	Evaluación de proveedores con criterios ESG, cláusulas contractuales de continuidad, segmentación y clasificación de proveedores, auditoría de contratos clave.
Gestión de Inventarios	Desajustes de inventario, deterioro, pérdidas no detectadas	Sistema WMS (*Warehouse Management System*), rotación *FIFO/LIFO*, inventarios periódicos, reconciliaciones físico-contables, alertas por pérdida.
Adquisiciones y Compras	Corrupción, compras innecesarias, falta de análisis de necesidad	Paneles de evaluación trazables, análisis previo de necesidad, licitación transparente, revisión de mercado, auditoría de contratos de adquisición.
Cumplimiento Normativo	Multas, sanciones, daños reputacionales por incumplimiento	Mapas de cumplimiento normativo, seguimiento regulatorio permanente, capacitación continua, auditoría de cumplimiento, reportes a alta Dirección.
Gestión de Terceros	Riesgo reputacional, servicio deficiente, incumplimiento contractual	Definición de *KPIs*, auditorías periódicas de terceros, clasificación y monitoreo de proveedores, controles de reputación y ética.
GRC – Gobernanza, Riesgos y Cumplimiento	Evaluación ineficaz, desalineación estratégica, respuestas tardías	Reuniones periódicas de comité de riesgos, mapas de calor de riesgos, plataforma integrada de riesgos y cumplimiento, informes gerenciales.
Gestión de Capital Humano	Falta de talento crítico, alta rotación, clima laboral negativo	Matrices de competencias, planes de sucesión, encuestas de clima laboral, análisis de rotación, desarrollo de talento interno.

9 Anexo: Conceptos Fundamentales sobre Riesgo de Auditoría

La auditoría interna es una función clave para apoyar la buena gestión en las organizaciones, especialmente en el sector público. Sin embargo, al igual que cualquier actividad compleja que implica análisis, juicio profesional y toma de decisiones, la auditoría interna también está expuesta a riesgos. Estos riesgos pueden afectar la calidad del trabajo, la confianza que genera en sus usuarios y la utilidad real de sus resultados. Comprender qué es el riesgo de auditoría, cómo se manifiesta y cómo se puede controlar, es fundamental para una función de auditoría efectiva, confiable y con valor agregado.

Gestionar el riesgo de auditoría no es solo una cuestión técnica, es una responsabilidad profesional y ética. Una auditoría con alto riesgo de error pierde su capacidad de generar confianza, aportar valor y contribuir a la mejora continua de la entidad. Por ello, los jefes de auditoría deben asegurar que el riesgo de auditoría sea evaluado, comprendido y tratado adecuadamente en cada trabajo, como parte fundamental del compromiso con la calidad y la efectividad.

¿Qué es el riesgo de auditoría?

El riesgo de auditoría es la probabilidad de que un auditor interno no detecte errores significativos, desviaciones, deficiencias de control o irregularidades en el área, proceso o actividad bajo revisión, y como consecuencia, emita una conclusión o informe que no refleje adecuadamente la realidad de la situación revisada. Esto puede llevar a una falsa percepción de seguridad en los procesos de la entidad, generar decisiones equivocadas por parte de los gestores, y afectar la reputación del equipo de auditoría y de la organización.

El riesgo de auditoría puede existir incluso si se siguen los procedimientos establecidos. Sin embargo, una mala planificación, ejecución deficiente o falta de juicio profesional aumentan considerablemente su probabilidad.

Tipos de riesgo de auditoría

El riesgo de auditoría se compone de tres elementos que deben comprenderse para gestionarlo adecuadamente:

- **Riesgo inherente**

Es el riesgo natural de que existan errores o irregularidades significativas en una actividad, proceso o área, antes de considerar si existen controles que los prevengan o detecten. Es decir, está vinculado con la complejidad de la actividad bajo revisión, el nivel de juicio requerido, el volumen de transacciones, los cambios frecuentes o los contextos operativos inestables.

Por ejemplo, en un área que gestiona grandes sumas de dinero o que depende de juicios técnicos complejos (como contrataciones públicas, presupuestos o cumplimiento normativo) presenta un riesgo inherente más alto que un área con operaciones rutinarias y estandarizadas.

- **Riesgo de control**

Corresponde a la posibilidad de que los controles existentes (políticas, procedimientos, sistemas o mecanismos de revisión) no funcionen adecuadamente o no sean suficientes para detectar o corregir errores importantes. Aunque este riesgo depende de la actividad bajo revisión, el auditor interno debe evaluarlo críticamente y considerar si los controles son eficaces y están bien diseñados.

Ejemplo: Si una actividad bajo revisión tiene controles manuales poco documentados y sin supervisión sistemática, el riesgo de control será alto.

- **Riesgo de detección**

Es el riesgo de que los procedimientos de auditoría aplicados no logren identificar errores significativos que sí existen. Este riesgo sí es directamente atribuible al auditor interno y depende de la calidad del enfoque de auditoría, del diseño de las pruebas, de la ejecución del trabajo y del nivel de escepticismo profesional con que se aborde el trabajo.

Por ejemplo, si se aplican procedimientos genéricos, sin adaptarse a los riesgos específicos de la actividad bajo revisión, o si el auditor no profundiza lo suficiente ante hallazgos inusuales, el riesgo de detección será alto.

- **Consecuencias del riesgo de auditoría**

Un riesgo de auditoría mal gestionado puede tener consecuencias graves:

- Emisión de informes incorrectos o incompletos.
- No detectar irregularidades, fraudes o fallas críticas en controles.
- Pérdida de credibilidad del área de auditoría interna.
- Riesgo reputacional para la entidad.
- Uso ineficaz de los recursos del equipo auditor.
- Falsa sensación de seguridad para la alta Dirección y el consejo.
- Oportunidades de mejora no identificadas o no comunicadas.

- **Factores que aumentan el riesgo de auditoría**

Algunos factores frecuentes que aumentan el riesgo de auditoría interna son:

- Planificación insuficiente o genérica de los trabajos.
- Evaluación superficial de los riesgos del área auditada.
- Uso de procedimientos estándar sin adaptación al contexto.
- Falta de conocimiento técnico o experiencia del equipo auditor.
- Limitada supervisión durante la ejecución.
- Comunicación poco clara o tardía de los hallazgos.
- Falta de protocolos para manejar hallazgos sensibles o sospechas de fraude.
- Involucramiento limitado del jefe de auditoría en auditorías críticas.

- **Cómo gestionar y mitigar el riesgo de auditoría**

Un trabajo de auditoría bien diseñado y ejecutado no elimina por completo el riesgo, pero sí puede reducirlo de forma significativa. Para lograrlo, se deben aplicar ciertas prácticas clave:

- Un trabajo de auditoría efectivo comienza con una planificación clara. Esto implica definir objetivos concretos, conocer bien la actividad bajo revisión y ajustar los procedimientos según el nivel de riesgo identificado. La claridad en esta etapa inicial es clave para orientar el trabajo de forma eficiente y con propósito.

- La evaluación de riesgos debe estar bien fundamentada. Identificar los riesgos más relevantes, estimar su impacto y probabilidad, y determinar la profundidad necesaria del trabajo de auditoría permite enfocar los esfuerzos donde realmente importa. No todos los riesgos tienen el mismo peso estratégico, y entender esto ayuda a tomar decisiones más precisas durante el trabajo.

- Diseñar pruebas eficaces también es esencial. No basta con recopilar testimonios o revisar documentación básica; se necesitan pruebas concretas, suficientes y bien enfocadas que permitan obtener evidencia sólida. Este enfoque evita conclusiones débiles o mal sustentadas.

10 Anexo: Análisis de Datos

El panorama de la auditoría interna ha experimentado una rápida transformación impulsada por los avances en tecnologías como la inteligencia artificial (IA) y el aprendizaje automático *(machine learning*). Superar los enfoques descriptivos y diagnósticos básicos en el análisis de datos es fundamental para gestionar el creciente volumen y la complejidad de la información presente en las organizaciones. Dichas tecnologías permiten la detección y gestión proactiva de riesgos, elevando significativamente el valor que áreas como auditoría interna y la propia administración pueden aportar.

a. Tecnologías avanzadas para la gestión

La incorporación de Inteligencia Artificial (IA) y aprendizaje automático ha abierto la puerta a procedimientos de monitoreo y evaluación en tiempo real de las operaciones en las organizaciones. Estas tecnologías permiten identificar anomalías, predecir fallos operativos y anticiparse a riesgos emergentes mediante el análisis continuo de datos. Así, la administración puede responder con medidas preventivas antes de que las amenazas se materialicen, optimizando la resiliencia de los procesos críticos empresariales.

El potencial de estas herramientas va más allá de la simple automatización; su capacidad de aprender patrones y adaptar los modelos predictivos permite integrar de manera oportuna la inteligencia generada en los procesos de negocio, haciendo viable el escaneo sistemático de cambios externos, como fluctuaciones regulatorias, geopolíticas o de mercado, que puedan representar amenazas incipientes.

b. Auditoría interna y aseguramiento continuo

La integración de análisis avanzados y monitoreo continuo ha revolucionado el rol de la auditoría interna. Hoy es posible implementar auditorías continuas en tiempo real que no solo entregan aseguramiento, sino que también generan información relevante y oportuna para las autoridades. Esto brinda tranquilidad al Jefe de Servicio y permite orientar los esfuerzos de mejora continua. La detección anticipada de fallos, respaldada por la IA, facilita la intervención temprana y la optimización de los controles internos, posicionando a la auditoría interna como un socio estratégico en la organización.

c. Desafíos de los datos estructurados y no estructurados

Una diferencia fundamental en el análisis de datos avanzado reside en la naturaleza de las fuentes de información. Los datos estructurados, como transacciones o registros de empleados están organizados en campos comunes y son fácilmente analizables mediante técnicas tradicionales. Sin embargo, una porción considerable del valor de la información reside en datos no estructurados, tales como correos electrónicos, grabaciones de llamadas o publicaciones en redes sociales.

Para explotar estos datos, es imprescindible convertirlos a un formato estructurado. Ello requiere la estandarización y la organización de los datos mediante técnicas avanzadas, etapa previa indispensable para descubrir patrones y relaciones significativas. Este proceso implica:

- Selección cuidadosa de datos relevantes para reducir el volumen procesado.
- Limpieza para eliminar información irrelevante y convertir los datos a formatos estándar.
- Transferencia a plataformas de almacenamiento adecuadas.
- Aplicación de técnicas analíticas para identificar tendencias y correlaciones.
- Importancia de la integridad y calidad de la información

La eficacia del análisis de datos avanzado está en función directa de la calidad de la información utilizada. La presencia de duplicados, errores o inconsistencias puede comprometer los resultados, subrayando la necesidad de mantener una estricta limpieza de datos. Solamente a partir de datos íntegros y confiables la inteligencia artificial y el aprendizaje automático pueden desplegar efectivamente su potencial para agregar valor a la gestión de riesgos.

d. Tipos de análisis de datos

Existen cuatro tipos principales de análisis de datos en los cuales las técnicas de IA pueden contribuir al trabajo de auditoría interna, especialmente en los de tipo predictivo y prescriptivo:

Tabla 1: Tipos de Análisis de Datos

Tipo de Análisis	Pregunta que responde	Propósito	Descripción
Descriptivo	¿Qué ocurrió?	Resumir y presentar los datos existentes para entender el comportamiento pasado.	Informar sobre eventos y desempeño, generalmente agregando y resumiendo datos mediante técnicas como promedios y comparaciones entre periodos.
Diagnóstico	¿Por qué pasó?	Identificar causas raíz y relaciones detrás de los datos observados.	Interpretar eventos y desempeño identificando tendencias subyacentes y causas y efectos.
Predictivo	¿Qué podría pasar?	Anticipar resultados futuros usando patrones históricos y modelos estadísticos o de machine learning.	Utilizar tendencias y modelos de interdependencias y correlaciones para generar pronósticos sobre eventos y desempeño futuros.
Prescriptivo	¿Qué debemos hacer?	Sugerir acciones óptimas basadas en análisis predictivo para mejorar resultados futuros.	Usar modelos predictivos para identificar acciones que optimicen el desempeño futuro.

d.1. Análisis descriptivo

Tabla N 2: Ejemplos de Análisis Descriptivo

Ejemplo	Aplicación
Informes mensuales de ejecución presupuestaria	Medición del gasto por unidad o programa
Promedio de días de pago a proveedores	Identificación de eficiencia en pagos
Número de hallazgos por tipo de auditoría	Análisis de desempeño de controles
Tasas de cumplimiento de controles internos	Evaluación de madurez de control interno

d.2. Análisis diagnóstico

Tabla N° 3: Ejemplos de Análisis Diagnóstico

Ejemplo	Aplicación
Identificar causas de errores contables repetitivos	Detección de debilidades estructurales
Correlación entre rotación de personal y fallos de control	Análisis de factores humanos en incidentes
Relación entre demoras en compras públicas y falta de planificación	Mejora del ciclo de contratación
Comparación de patrones de fraude y debilidad de controles	Identificación de áreas vulnerables al fraude

d.3. Análisis predictivo

Tabla N° 4: Ejemplos de Análisis Predictivo

Ejemplo	Aplicación
Modelos que predicen incumplimientos normativos	Priorización de auditorías
Riesgo proyectado de ciberataques	Fortalecimiento de cibercontroles
Predicción de atrasos en proyectos públicos	Gestión preventiva de cronogramas
Probabilidad de error material en estados financieros	Enfoque basado en riesgos en auditoría financiera

d.4. Análisis prescriptivo

Tabla N° 5: Ejemplos de Análisis Prescriptivo

Ejemplo	Aplicación
Reasignación automática de recursos	Optimización de procesos críticos
Sugerencias para rediseñar procesos con pérdidas recurrentes	Mejora continua
Planes de control priorizados por impacto previsto	Gestión de riesgos eficiente
Ajustes de políticas de compra	Optimización de adquisiciones sector público

11 Anexo: Conceptos Fundamentales sobre Fraude

a. Elementos contenidos en las Normas Globales de Auditoría Interna relacionados con fraude

De acuerdo con las NOGAI emitidas por el Instituto de Auditores Internos (IIA), especialmente en los requisitos del *Dominio V: Realización de los Servicios de Auditoría*, los auditores internos deben considerar explícitamente el riesgo de fraude como parte de su trabajo de aseguramiento.

Bajo las directrices de las NOGAI, la función de auditoría interna tiene la obligación formal de considerar el riesgo de fraude como parte integral del desarrollo de cada trabajo. Esto no solo mejora la calidad del aseguramiento entregado, sino que refuerza la capacidad de la entidad para gestionar este tipo de riesgos críticos de manera proactiva y efectiva.

Las NOGAI señalan que:

- El riesgo de fraude debe ser considerado de forma sistemática y documentada en cada etapa del trabajo de auditoría, desde la planificación hasta la comunicación de resultados. Esto incluye la identificación de señales de alerta (banderas rojas), deficiencias de control y condiciones que puedan propiciar la ocurrencia de fraudes.

- El auditor interno debe contar con conocimientos suficientes sobre fraude, incluyendo las características comunes, esquemas típicos, métodos empleados y los controles que pueden prevenir o detectar dichas prácticas. No obstante, las NOGAI reconocen que no se requiere el nivel técnico de un investigador especializado en fraude.

- Las normas del *Principio 13 (Dominio V)* destacan que la planificación debe basarse en la evaluación del riesgo, lo cual implica incluir el riesgo de fraude como un componente crítico en la determinación de áreas prioritarias, naturaleza de las pruebas y extensión del trabajo.

Según las NOGAI, el auditor debe ejercer el debido cuidado profesional considerando:

- La complejidad e impacto de los procesos evaluados.
- La probabilidad de errores significativos, fraude o incumplimientos.
- La calidad y suficiencia de los controles existentes.
- El balance costo-beneficio de los procedimientos aplicados.

- El Jefe de Auditoría Interna debe informar periódicamente al Jefe de Servicio, conforme al *Principio 8* de las NOGAI, sobre la actividad de auditoría interna y los temas relevantes que incluyan exposiciones significativas al riesgo de fraude, deficiencias de control o debilidades de gobierno identificadas.

- Las NOGAI también instruyen que el auditor interno debe evaluar la respuesta de la entidad frente al riesgo de fraude, incluyendo las políticas preventivas, la cultura ética, los mecanismos de denuncia, y los procesos de investigación interna, si existiesen.

b. Factores que motivan el fraude - elementos del fraude

Uno de los marcos conceptuales más reconocidos y aplicados para comprender el origen del fraude es el denominado Triángulo del Fraude, propuesto por el criminólogo Donald Cressey y ampliamente difundido por la *Association of Certified Fraud Examiners (ACFE)*. Este modelo identifica tres elementos esenciales que deben coexistir para que una persona común cruce el umbral ético y cometa fraude: Presión (o motivación), Oportunidad y Racionalización.

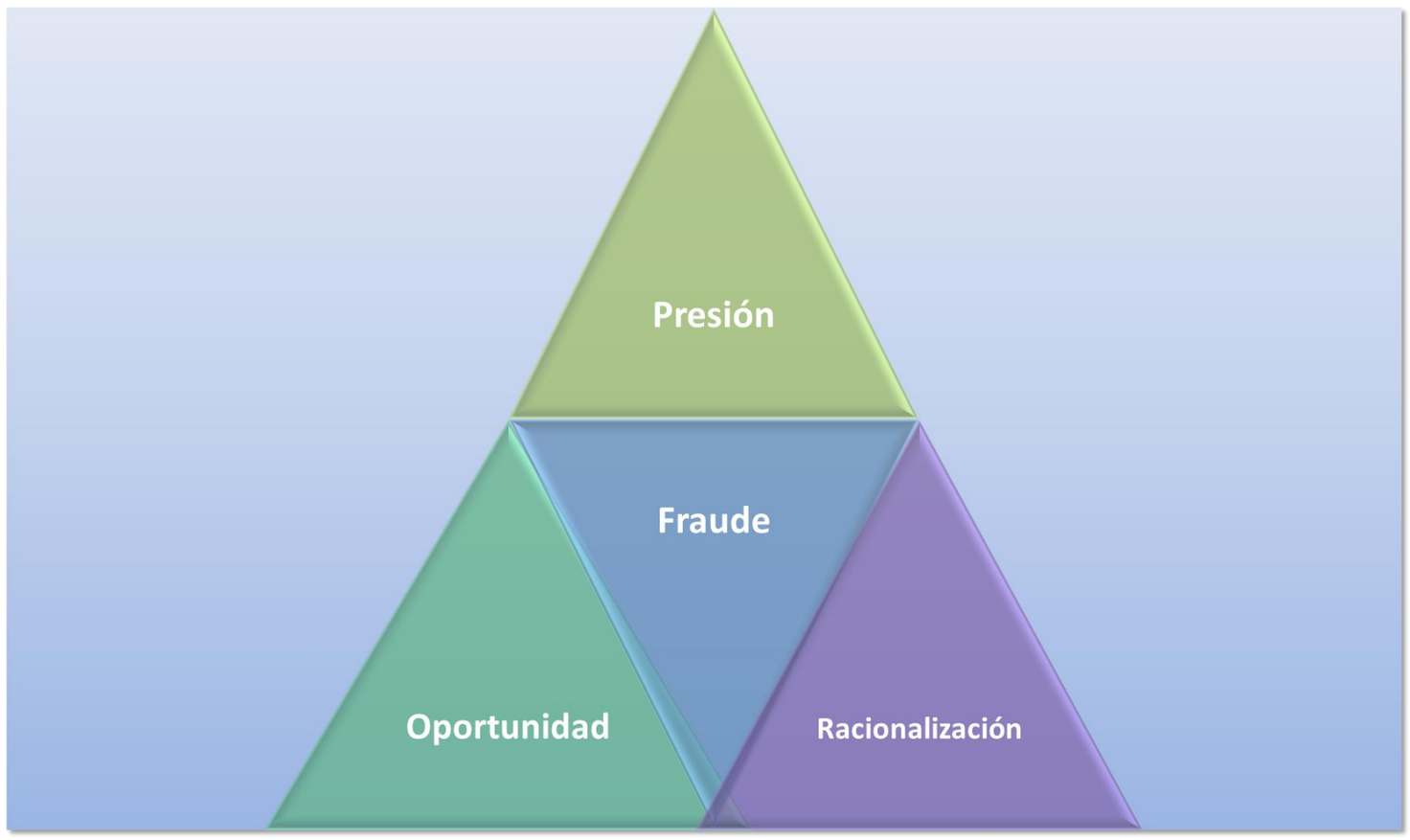
- **Presión**: Es el impulso o motivación que lleva a una persona a considerar el fraude como una opción viable. Por lo general, estas presiones tienen un componente financiero o personal, tales como deudas, dificultades económicas, metas de desempeño difíciles de cumplir, ambición desmedida o adicciones. En el contexto organizacional, pueden manifestarse como presión por alcanzar indicadores exigentes, obtener incentivos monetarios, evitar sanciones por bajo desempeño, entre otros.

- **Oportunidad**: Se refiere a la percepción de que existen debilidades en los controles internos o condiciones organizacionales que permiten llevar a cabo el fraude sin ser detectado. Este elemento está relacionado con la existencia de accesos privilegiados, falencias en la segregación de funciones, ausencia de supervisión y condiciones que permiten actuar sin consecuencias inmediatas. También incluye los casos de colusión entre empleados o entre empleados y proveedores externos, lo cual dificulta la detección del fraude por medios tradicionales.

- **Racionalización**: Corresponde a los mecanismos psicológicos que el individuo utiliza para justificar su conducta impropia y minimizar el conflicto ético o moral. Este componente suele aparecer principalmente antes del primer acto fraudulento. Las personas suelen convencerse de que su accionar está justificado por situaciones como: baja remuneración ("esto no es un robo, es una compensación"), falta de reconocimiento ("es una bonificación que la empresa me debe"), o porque otros también cometen fraudes sin ser sancionados ("si todos lo hacen, ¿por qué yo no?"). Esta racionalización debilita las barreras éticas y facilita la repetición de conductas irregulares.

Estos tres factores interactúan en una dinámica de riesgo que puede materializarse si no existen controles sólidos, una cultura ética fortalecida y mecanismos efectivos de prevención y detección. En el contexto de la auditoría interna y bajo el marco de las NOGAI, es esencial identificar estas condiciones como parte de la evaluación del riesgo de fraude, entendiendo que la mera presencia de uno de los elementos no es suficiente; deben concurrir los tres para que el riesgo se eleve significativamente.

Esquema N° 1: Elementos del Triángulo del Fraude



En la literatura especializada sobre prevención del fraude, se destaca que, de los tres elementos del Triángulo del Fraude, la Oportunidad es el factor sobre el cual las organizaciones tienen mayor capacidad de control e intervención directa. A diferencia de la Presión o la Racionalización, que son factores más difíciles de gestionar desde el entorno organizacional, la Oportunidad puede ser significativamente reducida o eliminada mediante un sistema robusto de control interno.

Esto implica que las organizaciones deben establecer y mantener procedimientos claros, estructuras de control adecuadas y mecanismos de supervisión efectivos que dificulten o impidan la comisión de fraudes. Asimismo, deben contar con herramientas que permitan detectar oportunamente actividades inusuales o sospechosas, incluyendo auditorías periódicas, revisiones cruzadas, segregación de funciones, controles tecnológicos automatizados y canales de denuncia. Minimizar las oportunidades de fraude contribuye no solo a reducir su ocurrencia, sino también a fortalecer la cultura de integridad y transparencia dentro de la entidad.

c. Perfil de la persona que comete fraude

Comprender el perfil típico de quienes cometen fraude es fundamental para que las organizaciones puedan diseñar estrategias de prevención más efectivas. El fraude rara vez es cometido por individuos que encajan con los estereotipos delictivos tradicionales; por el contrario, suele involucrar a personas aparentemente confiables, con historial intachable y que han ganado la confianza de sus superiores y colegas.

Diversos estudios, especialmente los desarrollados por la ACFE, revelan que existen ciertos patrones y características recurrentes entre los defraudadores. Según el informe más reciente de la ACFE, *Report to the Nations: Global Study on Occupational Fraud and Abuse,* el perfil más común del defraudador organizacional incluye:

- Empleados con antigüedad superior a 5 años.
- Suelen ocupar cargos de nivel medio o superior, con acceso privilegiado a información crítica y procesos de aprobación.
- En su mayoría hombres (70%), entre 31 y 45 años.
- Cometen fraudes principalmente en áreas como contabilidad, operaciones, compras y finanzas.
- El 52% actuó en colusión con otros individuos.

Los factores que pueden motivar a una persona a cometer fraude incluyen el deseo de enriquecimiento ilícito, problemas financieros, resentimientos con la entidad, ambición desmedida, sensación de injusticia por su salario o reconocimiento, así como una baja percepción del riesgo de ser descubierto. Además, el entorno organizacional juega un rol clave, particularmente cuando existen oportunidades no controladas y fallas en la supervisión.

Desde el punto de vista psicológico y conductual, los individuos involucrados en fraudes pueden presentar una combinación de las siguientes características:

- Poseen buena educación formal, antecedentes familiares estables y no muestran señales evidentes de problemas personales o adicciones.
- Se muestran altamente comprometidos, trabajan fuera del horario habitual, asisten incluso enfermos y evitan tomar vacaciones.
- Exhiben un estilo de vida que no se condice con su nivel de ingresos, pero justifican sus finanzas con supuestos ingresos de terceros o herencias.
- Evitan la delegación de funciones y concentran el control sobre procesos clave, incluso negándose a ser transferidos o ascendidos.
- Presentan nerviosismo o evasión frente a consultas directas, y suelen dar respuestas innecesariamente extensas o técnicas para desviar la atención.
- Mantienen un alto nivel de visibilidad social en la entidad y tratan de generar simpatía o lealtad con colegas y subordinados.
- Participan activamente en áreas que no les corresponden y mantienen contacto frecuente fuera del horario laboral con proveedores o clientes.
- Piden anticipos, préstamos menores y hacen uso habitual de fondos internos como cajas chicas.
- En ocasiones recurren a ajustes contables o manipulaciones para cuadrar operaciones financieras.
- En escenarios más complejos, pueden actuar en colusión con terceros internos o externos, manipulando a otros para ejecutar actos fraudulentos en su beneficio o como encubridores.

Es importante destacar que la presencia de uno o más de estos factores no significa necesariamente que se esté cometiendo fraude, pero su acumulación o manifestación repetida debería encender alertas. Las unidades de auditoría interna deben considerar estos elementos al diseñar sus evaluaciones de riesgos, establecer sus procedimientos y enfocar sus revisiones en sectores críticos o vulnerables.

El monitoreo continuo, la observación de conductas anómalas y una cultura organizacional orientada a la integridad y a la denuncia responsable son elementos fundamentales para mitigar el riesgo de que estos perfiles se traduzcan en acciones fraudulentas.

d. Conceptos básicos sobre prevención, detección e investigación del fraude

Tal como se ha señalado, el fraude siempre está latente en una entidad, independiente de su estructura, tamaño y complejidad. En consecuencia, es recomendable que el Jefe de Servicio tome la decisión de que se implanten controles para prevenir, disuadir y perseguir situaciones de fraude, con especial énfasis en las acciones preventivas. A continuación se presenta el desarrollo de estos tópicos.

d.1. Prevención de fraudes

En toda entidad es necesario que se elabore un Programa de Prevención de Fraudes, basado en políticas, procesos, entidad y recursos, orientado a prevenir, controlar, detectar y minimizar la probabilidad de ocurrencia del riesgo de fraude. Para iniciar esta etapa es necesario plantearse algunas interrogantes que ayuden a establecer los lineamientos, por ejemplo:

- ¿Dónde puede ocurrir el fraude?
- ¿Qué controles deben existir para prevenir o detectar el fraude?
- ¿Cómo se monitorean estos controles?
- ¿Cómo se comunican los resultados de las actividades de monitoreo?
- ¿Qué hacer cuando se encuentran excepciones o instancias de fraude?

La responsabilidad de la función de auditoría interna es la de asistir en la prevención del fraude por medio del análisis de la eficiencia y eficacia del control interno, acorde con el riesgo potencial en los diferentes segmentos de operación de la entidad.

Dentro de los controles internos que el auditor debe considerar para la prevención de fraudes, se encuentran:

- Segregación de funciones
- Rotación de puestos
- Restricción de acceso a áreas de riesgo
- Incrementar los niveles de seguridad
- Desarrollo de políticas y procedimientos administrativos y contables

El auditor, en el desarrollo natural del proceso de auditoría interna, obtiene el conocimiento de la entidad y su entorno, incluyendo su control interno. Durante la ejecución del programa, el auditor debe considerar si la información obtenida advierte que se encuentran presentes uno o más factores de riesgo de fraude.

Si bien los factores de riesgo de fraude no necesariamente indican su existencia, suelen estar presentes en circunstancias en las que ellos se han producido. Comúnmente se oculta el fraude, lo que puede hacer que sea muy difícil de detectar en una primera instancia, así como también, establecer un orden de importancia de estos factores.

La capacidad de un auditor interno para detectar el fraude dependerá también de factores fuera de su control, principalmente: la habilidad del autor, la jerarquía de los implicados en el fraude, el grado de colusión que conlleva y la frecuencia y amplitud de la manipulación.

En la prevención del fraude, el principal responsable es el Jefe de Servicio, el que debiese implementar medidas que se consideran fundamentales:

- Crear y mantener un clima de honestidad y moral elevada (códigos de conducta conocido por el personal).
- Evaluar riesgos de fraude y tomar la decisión de implementar procedimientos y controles.
- Desarrollar un adecuado proceso de vigilancia.
- Segregar la responsabilidad de los riesgos de fraude identificados.
- Evaluación permanente de nuevos eventos o patrones de fraude que se puedan estar generando.
- Establecimiento de una política de manejo de eventos de fraude.
- Análisis de controles que mitiguen eventos de fraude a nivel procesos.
- Mejora continua del ambiente de control, relacionado con aspectos directos a eventos de fraude.
- Planes proactivos de detección de fraudes.

Dentro esta lista, tiene una gran relevancia el código de conducta, que sirve de guía para el comportamiento de los funcionarios. Entre los puntos que puede incluir están: ética, confidencialidad, conflictos de intereses, propiedad intelectual, acoso sexual, acoso laboral, fraude. Para que el código de conducta resulte eficaz debe ser conocido por todos los empleados, debiendo además estar disponible para su consulta cuando sea necesario.

Algunos estudios señalan que, el fraude es menos frecuente cuando los empleados tienen sentimientos positivos hacia la entidad, no sintiéndose abusados, amenazados o ignorados.

En función de lo mencionado, en la entidad debiesen tener presente algunos factores que van en desmedro de un ambiente de trabajo positivo, y que pueden incrementar el riesgo de fraude, se pueden mencionar: que a la Jefatura del Servicio parezca no importarle recompensar los comportamientos apropiados; reacción negativa y falta de reconocimiento por el desempeño del trabajo; percepción de faltas de equidad en la entidad; baja lealtad a la entidad, falta de sentido de pertenencia, entre otras.

Por otra parte, existen factores que reducen el riesgo de fraude al ayudar a crear un ambiente de trabajo positivo: tales como sistemas de reconocimiento y recompensa alineados con metas y resultados, igualdad de oportunidades de empleo, orientación al trabajo en equipo, políticas de toma de decisiones en forma participada, programas de remuneración administrados profesionalmente, programas de entrenamiento, dando prioridad al desarrollo de carrera en la entidad.

d.1.1. Elementos claves en un programa de prevención

- **Ambiente de control:** El ambiente de control involucra aspectos intangibles como la integridad, la competencia, los valores éticos y principios:

  – Código de ética: Debe involucrar a todos los empleados y señalar pautas de comportamiento.
  – Política antifraude: Debe señalar las acciones que constituyen fraude o corrupción y trazar lineamientos de prevención.
  – Sistema de denuncias: Reportar, administrar, investigar y remediar eventos de fraude y corrupción.
  – Políticas de recursos humanos: Políticas de contratación, selección y promoción de empleados.

- **Evaluación del riesgo**: El proceso de evaluación del riesgo identifica el grado de vulnerabilidad de la compañía frente a potenciales eventos de fraude en sus procesos.

Elementos del proceso de evaluación del riesgo:

– Identificar los esquemas de fraude para cada uno de los procesos.
– Valorar los riesgos (determinar el tipo de impacto, la probabilidad y su consecuencia)
– Monitorear y evaluar la efectividad de los riesgos identificados.

- **Actividades de control:** Una vez se ha evaluado el riesgo, la entidad debe identificar o diseñar las actividades de control para prevenir y detectar los riesgos de fraude y corrupción.

  – En necesario probar la efectividad del diseño y operatividad de cada uno de los controles implementados para mitigar el riesgo al cual está asociado.
  – Los controles y el resultado de su efectividad serán documentados en el sistema para la administración de riesgos.

- **Información y comunicación**: Una comunicación efectiva es clave para asegurar la efectividad del programa antifraude a través de un mensaje claro respecto al trabajo de la compañía frente la prevención del fraude.

- **Plan de comunicación:**

  – Definir los mensajes claves a comunicar.
  – Diseñar la estrategia de comunicación.
  – Definir los medios de comunicación.
  – Elaborar un cronograma.
  – Plan de capacitación: sesiones de capacitación para todos los empleados, que incluyan los elementos del programa antifraude.

- **Monitoreo:** Una vez implementado, el programa antifraude debe ser monitoreado a través de evaluaciones periódicas.

Es importante tener en cuenta durante el proceso de monitoreo:

– La naturaleza y los cambios del mercado.
– Los riesgos asociados al entorno del negocio.
– La competencia y la experiencia de las personas que implementan y ejecutan los controles.
– Los resultados de evaluaciones anteriores.

Esquema N° 2: Elementos Claves en un Programa de Prevención

d.2. Detección de fraudes

Dado que los sistemas de control pueden ser potencialmente evadidos en algún momento, detectar actividades irregulares tan pronto como sea posible es extremadamente importante, así como también la identificación y la eliminación activa de los factores que lo causan y permiten.

Para ello, la detección aplica controles diseñados para alertar al personal apropiado cuando se presentan circunstancias asociadas con actividades fraudulentas. Esto incluye desde auditoría interna hasta canales directos para reportar fraudes de manera anónima.

En el caso del auditor interno se requiere que tenga conocimiento del "negocio," sistemas de control, entorno, motivaciones para cometer fraude, oportunidades para que se cometa fraude, técnicas básicas de detección de fraude.

Además es requisito básico para establecer un sistema de detección de fraude que se tenga la razonable creencia que existe o puede existir fraude en la entidad y la existencia de activos atractivos a ser obtenidos por medios fraudulentos.

Existen apoyos a través de herramientas de detección automática o continua que son capaces de revisar grandes volúmenes de datos, identificando patrones sospechosos en la data, aislando los casos que requieran de una investigación más detallada. Además, existen metodologías y herramientas informáticas que ayudan a los auditores a identificar posibles situaciones de fraude interno, siendo el objetivo primordial el obtener evidencia suficiente para sustentar las situaciones irregulares detectadas y realizar sus recomendaciones.

En forma paralela, el equipo de auditoría interna puede generar indicadores que alerten de la posible existencia de fraude, proveer evidencias ante la existencia de fraude, identificar al culpable, obtener pruebas válidas, utilizar métodos automáticos que ayuden a su identificación, implementar iniciativas, prácticas y promover un cambio cultural para reducir la exposición al riesgo y considerar en su programación lo siguiente:

- Auditorías sorpresivas.
- Capacitación al personal.
- Establecer o revisar una adecuada segregación de funciones en procesos críticos.
- Actuar de manera oportuna, proporcional y firme en caso de ocurra algún fraude, ejecutando soluciones rápidas y adecuadas.
- Seguimiento de las áreas de mayor riesgo sobre las que haya preocupaciones concretas sobre un procedimiento, cuenta o puesto de mando en particular.
- Si la organización tiene antecedentes de fraude y conducta irregular.
- Atención sobre las áreas donde haya mucha rotación de empleados o cambios en la Dirección.
- Revisar si las leyes o regulaciones han cambiado y su aplicación en la entidad.

d.3. Investigación de fraudes

Cuando se descubre información sobre conductas irregulares o fraudes, bien sean potenciales o reales, el Jefe de Servicio debe estar preparado para llevar a cabo una investigación objetiva y exhaustiva. El objetivo de cualquier investigación es recabar hechos que contribuyan a realizar una evaluación creíble de la infracción supuestamente cometida, de modo que el Jefe de Servicio pueda decidir la línea de actuación a seguir.

Un proceso de investigación bien elaborado normalmente incluirá las siguientes características:

- Será supervisado por un grupo independiente sobre los que el Jefe de Servicio no podrá ejercer una presión excesiva ni interferir en sus decisiones.
- Estará dirigido por un responsable que pueda realizar una investigación imparcial, independiente y fundamentada.
- Implicará una colaboración total, no permitiendo que ningún empleado o directivo de la entidad oculte los hechos que dieron lugar a la investigación.

- Protocolos informativos, proporcionando, a los reguladores y, cuando corresponda, al público, la información pertinente sobre las conclusiones de la investigación con total cooperación y transparencia.
- En función de distintos factores, entre otros, la naturaleza del potencial acto ilícito, las partes involucradas y su materialidad, la entidad podrá decidir si usar uno o varios de los pasos mencionados anteriormente. El Jefe de Servicio deberá consultar a las funciones supervisoras pertinentes y también los protocolos internos para determinar cuáles son los mejores pasos a seguir para abordar el caso.

Lo anterior, también implicará establecer protocolos bajo los cuales se realizarán las investigaciones, medidas correctivas, remediación de los daños ocasionados, planes de acción y comunicación, estudio de las causas originales que provocaron las fallas de control (por ejemplo, un órgano regulador), sancionar a aquellos que hayan llevado a cabo acciones inapropiadas así como a aquellos directivos que no hayan sido capaces de prevenir o detectar dichas acciones, comunicar a los empleados que el Jefe de Servicio ha tomado las medidas pertinentes. Este último punto, a pesar de que revelar públicamente un fraude o una conducta irregular puede resultar violento para una entidad, el Jefe de Servicio quizá deba considerar esta posibilidad para así combatir o adelantarse a la publicidad negativa que pueda tener la organización, poniendo de manifiesto su buena fe y contribuyendo a acabar o mitigar el problema.

e. Guía para la Gestión del Riesgo de Fraude (*The Fraud Risk Management-Guide*)

Este marco también es conocido de forma abreviada como *COSO Fraud Risk* y se considera una extensión del Marco COSO de Control Interno de 2013, aplicado específicamente a la gestión del riesgo de fraude.

Fue publicado originalmente en 2016 y actualizado en 2023 por el Comité de Organizaciones Patrocinadoras de la *Comisión Treadway* (COSO) y la Asociación de Examinadores Certificados en Fraude (ACFE). Es una guía especializada para gestionar el riesgo de fraude dentro de las organizaciones. Esta guía complementa el Marco de Control Interno COSO y se enfoca específicamente en la prevención, detección y respuesta al fraude. Su aplicación es especialmente valiosa para la función de auditoría interna, tanto en el sector privado como público.

Este marco se estructura en cinco principios fundamentales que abordan un aspecto esencial de la gestión antifraude.

Tabla Nº 1: Relación entre Principios de la Guía COSO-ACFE y Componentes del Marco COSO

Resumen de Principios – Guía COSO-ACFE Gestión del Riesgo de Fraude	Componentes Relacionados del Marco COSO 2013	Descripción Detallada
1. Establecer y comunicar un programa de gestión del riesgo de fraude	Ambiente de control	Refleja el compromiso del Jefe de Servicio y la Alta Dirección con una cultura de integridad. Implica definir responsabilidades claras, establecer políticas antifraude, y comunicar expectativas en todos los niveles organizacionales, con un enfoque visible desde el Jefe de Servicio.
2. Realizar evaluaciones de riesgos de fraude para identificar y priorizar exposiciones potenciales	Evaluación de riesgos	Consiste en identificar, evaluar y priorizar los riesgos de fraude que podrían afectar a la entidad, considerando su probabilidad y posible impacto, y evaluando los controles existentes. El proceso debe ser sistemático y adaptarse a los cambios en el entorno.
3. Diseñar e implementar controles preventivos y detectivos para mitigar riesgos de fraude	Actividades de control	Abarca el diseño e implementación de controles proporcionales al nivel de riesgo detectado. Se incluyen controles manuales, automatizados, estructurales y culturales orientados a reducir la posibilidad de ocurrencia o facilitar la detección oportuna.
4. Implementar procesos de denuncia, investigación y acción correctiva ante eventos de fraude	Información y comunicación / Actividades de monitoreo	Implica establecer canales adecuados y seguros para denuncias (por ejemplo, líneas éticas), procedimientos claros de investigación y protocolos para la respuesta disciplinaria, recuperación de activos y mejora de controles.
5. Supervisar y mejorar continuamente el programa de gestión del riesgo de fraude	Monitoreo de actividades	Se enfoca en la evaluación continua del programa antifraude para determinar su efectividad y realizar mejoras. Deben revisarse las métricas, el cumplimiento de políticas y la eficacia de controles, comunicando los resultados a las partes interesadas clave.

Esta estructura no solo facilita la prevención y detección del fraude, sino que potencia la capacidad estratégica de la auditoría interna para proteger y fortalecer a la entidad desde una mirada ética, preventiva y de mejora continua.

En el contexto de la auditoría interna, este marco es especialmente útil en la etapa de planificación, ya que proporciona una metodología clara para identificar riesgos de fraude relevantes y priorizar áreas con mayor exposición. Por ejemplo, al elaborar el mapa de riesgos para definir el plan anual de auditoría, el equipo auditor puede aplicar los cinco principios para detectar procesos críticos como contrataciones, licencias médicas, manejo de efectivo o adquisiciones públicas.

Incorporar este marco de fraude a la planificación del trabajo fortalece el enfoque basado en riesgos, permite integrar dimensiones éticas y de integridad (*Dominio II* de las NOGAI), y promueve trabajos de auditoría que no solo cumplan con los requisitos técnicos, sino que también generen valor en la cultura organizacional.

Además, el marco proporciona ejemplos de buenas prácticas, roles clave, y herramientas como matrices de riesgo y preguntas orientadoras que pueden ser incorporadas directamente en los programas de trabajo del auditor interno.

El marco COSO puede consultarse en: https://www.coso.org/internal-control

El marco COSO Fraude puede consultarse en: https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/fraud-risk-management-guide

f. Esquema general del fraude - Árbol del Fraude de la ACFE

La ACFE ha clasificado el fraude ocupacional en tres grandes categorías, comúnmente representadas en el "Árbol del Fraude", el cual facilita la comprensión estructurada de las formas en que los individuos pueden apropiarse o desviar indebidamente recursos desde una organización.

Estas categorías reflejan los principales esquemas fraudulentos que afectan tanto al sector privado como al sector público, y permiten desarrollar metodologías de evaluación, control e investigación más efectivas:

- **Fraude en estados financieros**

Se refiere a falsificaciones o manipulaciones deliberadas de información financiera o administrativa con el fin de inducir a error a quienes toman decisiones. Este tipo de fraude puede incluir:

- Revelaciones falsas o inexactas en reportes financieros.
- Omisión de información relevante que afecte la interpretación de resultados.
- Alteración de datos contables para mejorar artificialmente la imagen financiera.
- Modificación de estadísticas o indicadores de desempeño institucional.

- **Malversación de bienes (activos)**

Es el tipo más común de fraude y ocurre cuando un funcionario se apropia, desvía o utiliza indebidamente activos públicos. Incluye tanto bienes físicos como recursos financieros o información. Las formas típicas de malversación incluyen:

- Fraude en efectivo: robo antes de contabilizar, depósitos no realizados.
- Facturación falsa o duplicada: pagos a proveedores inexistentes o inflados.
- Manipulación de nómina: horas extras no trabajadas, sueldos a personas inexistentes.
- Uso personal de bienes públicos: vehículos, combustibles, inventarios o equipos.
- Falsificación de documentos de respaldo.

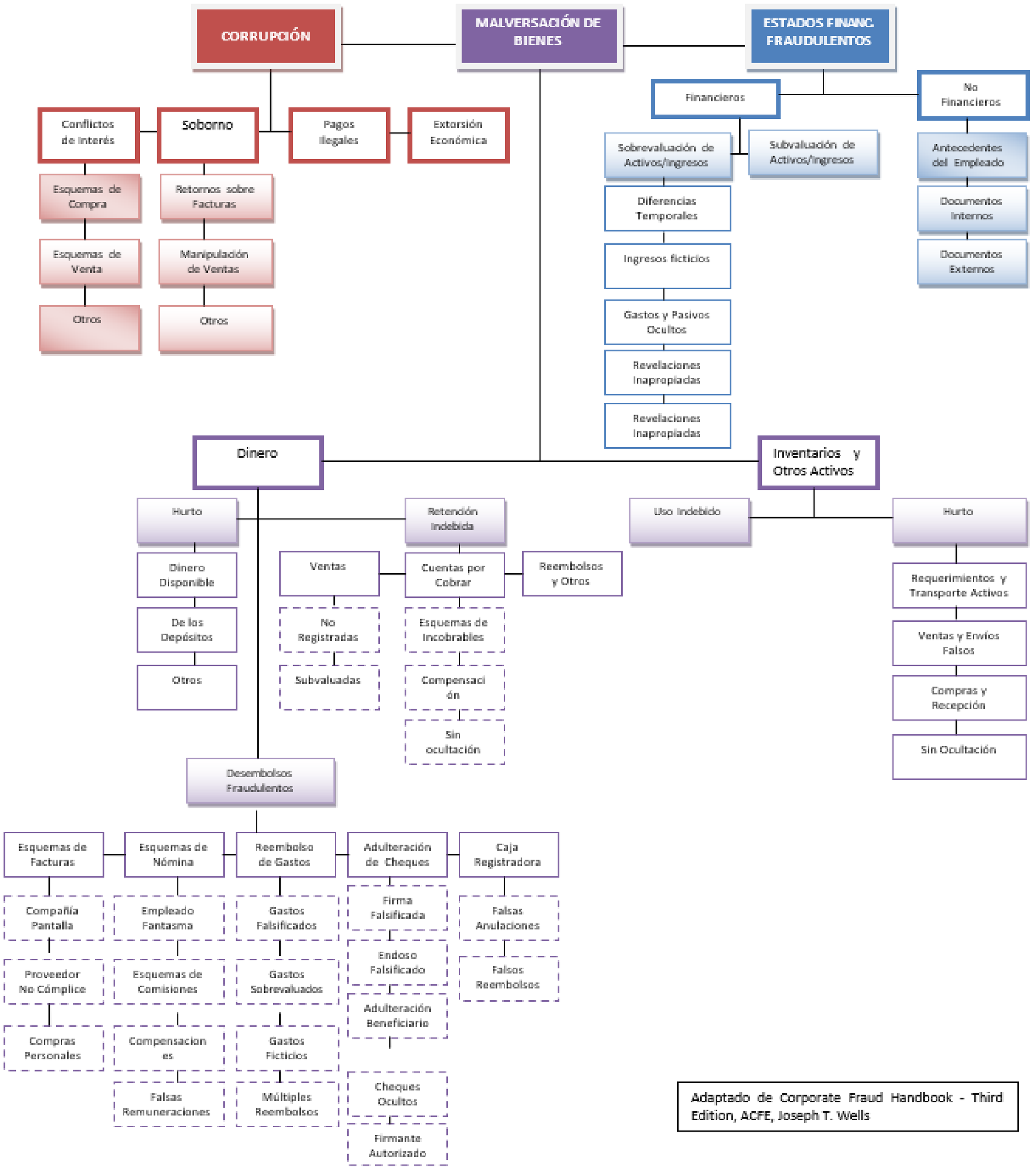
- **Corrupción**

Consiste en el uso indebido de una posición de poder o influencia dentro de la institución para obtener beneficios personales o para terceros, en violación del deber de probidad administrativa. Incluye:

- Cohecho (soborno): recibir o solicitar pagos indebidos a cambio de decisiones favorables.
- Conflictos de interés no declarados ni gestionados.
- Colusión entre funcionarios y proveedores para direccionar adjudicaciones.
- Manipulación de licitaciones o convenios para beneficiar a cercanos.

A continuación, se presenta un esquema del Árbol del Fraude de la ACFE, que ilustra gráficamente la estructura de estos esquemas y sus subtipos. Este diagrama debe ser incorporado en las actividades de capacitación, evaluación de riesgos y diseño de controles preventivos.

Esquema Nº 3: Diagrama del Árbol del Fraude



Adaptado de Corporate Fraud Handbook - Third Edition, ACFE, Joseph T. Wells

g. Banderas Rojas Genéricas por Ciclo de Negocios

g.1 Banderas Rojas Genéricas del Ciclo de Ventas – Cuentas por Cobrar

Las siguientes señales pueden indicar riesgos operativos, financieros o de fraude en el ciclo de ventas y cobranza. Su presencia, especialmente cuando se combinan o repiten, debe alertar al auditor interno sobre la necesidad de investigar causas, validar controles y aplicar procedimientos adicionales:

Estas señales deben ser consideradas como banderas de alerta para evaluar la efectividad del diseño y funcionamiento de los controles clave en el ciclo de ventas. Su identificación requiere análisis combinado de datos, revisión documental, entrevistas y observación directa. Ante la presencia de varias de estas banderas, se sugiere aplicar técnicas ampliadas de auditoría, como análisis de datos, pruebas sustantivas dirigidas o revisión forense selectiva.

g.1.1. Irregularidades en documentación y registros

- Facturas, notas de crédito o débito con numeración faltante, no correlativa o duplicada.
- Documentos comerciales emitidos fuera de horario administrativo habitual.
- Registros de ventas sin respaldo documental o contratos formales.
- Ventas anuladas sin refacturación o justificación adecuada.
- Documentación con descripciones vagas, genéricas o abreviadas.

g.1.2. Comportamientos atípicos en clientes

- Clientes nuevos sin historial financiero, verificación de antecedentes o aprobación crediticia documentada.
- Clientes con datos duplicados o inconsistentes (nombre, RUT, Dirección, cuenta bancaria).
- Mismo cliente con distintos códigos en el sistema, sin justificación.
- Clientes con límites de crédito otorgados por encima de parámetros establecidos, sin autorización formal.
- Cuentas por cobrar con saldos vencidos significativamente antiguos o no gestionados.

g.1.3. Variaciones inusuales en indicadores financieros y operativos

- Aumento repentino e injustificado en volumen de ventas, especialmente hacia el cierre del ejercicio.
- Montos de venta superiores a promedios históricos por cliente o canal.
- Variaciones abruptas en listas de precios, descuentos, bonificaciones o condiciones comerciales.
- Emisión masiva de notas de crédito al final del periodo, sin respaldo operacional.
- Variaciones sustanciales en ratios de devolución o ajuste contable, no explicadas.

g.1.4. Gestión y conciliación deficiente

- Recaudaciones no asociadas a facturas o sin aplicación a cuentas específicas.
- Recibos duplicados, no aplicados o pendientes por largos períodos.
- Diferencias relevantes en conciliaciones con clientes, sin resolución o documentación.
- Falta de revisión independiente de las condiciones de venta, crédito y cobro.
- Procesos manuales o discrecionales para la aprobación de descuentos, notas de crédito o anulaciones.

g.1.5. Comportamientos sospechosos vinculados al personal

- Concentración excesiva de transacciones por vendedor, ejecutivo o unidad de negocio.
- Registro de ventas ficticias para inflar comisiones o alcanzar metas de desempeño.
- Otorgamiento de condiciones excepcionales sin autorización o fuera de política institucional.
- Usuarios con privilegios para modificar condiciones de venta, anular facturas o registrar ajustes contables.
- Notoria rotación de responsables en áreas clave de ventas o cuentas por cobrar.

g.1.6. Otras señales estructurales de riesgo

- Ausencia o ineficacia de políticas formales de crédito, cobranza o gestión de precios.
- Uso intensivo de documentos físicos no registrados en sistemas.
- Limitado acceso del área de auditoría o contraloría a los reportes integrales del ciclo de ventas.
- Frecuencia inusual de ajustes en cuentas contables asociadas a ventas, ingresos diferidos o descuentos.
- Presión institucional excesiva por metas comerciales, sin controles compensatorios.

g.2 Banderas Rojas Genéricas del Ciclo de Compras y Cuentas por Pagar

Las siguientes señales de alerta deben ser cuidadosamente consideradas por el auditor interno al evaluar procesos de adquisiciones y pagos. Muchas de ellas son indicios de posibles irregularidades, fraudes, colusión o simplemente fallos de control, y su aparición, especialmente de forma repetida o sin explicación razonable, puede justificar la aplicación de procedimientos adicionales o pruebas forenses.

Estas señales no deben considerarse de forma aislada. Su utilidad radica en el análisis combinado, especialmente cuando surgen en contextos de presión presupuestaria, baja supervisión o estructuras poco automatizadas. El auditor debe mantenerse alerta, aplicar un enfoque basado en riesgos y, cuando corresponda, escalar la revisión a un nivel forense.

g.2.1. Anomalías en compras por proveedor o comprador

- Concentración excesiva de compras en uno o pocos proveedores, sin justificación técnica ni económica.
- Compras reiteradas por el mismo comprador por encima de los promedios históricos.
- Montos acumulados por proveedor o comprador que no guardan relación con el comportamiento operativo habitual.
- Proveedores con montos individuales bajos, pero que en conjunto representan cifras relevantes.
- Aumento desproporcionado en la frecuencia de pedidos a proveedores específicos.

g.2.2. Documentación inconsistente o incompleta

- Facturas no vinculadas con órdenes de compra ni con informes de recepción.
- Órdenes de pago emitidas sin respaldo suficiente o sin facturas asociadas.
- Documentos comerciales duplicados, anulados o emitidos fuera de horarios normales.
- Ruptura de correlatividad en la numeración de órdenes de compra, guías de recepción y órdenes de pago.
- Diferencias sistemáticas entre montos consignados en órdenes de compra, facturas y pagos.

g.2.3. Variaciones inusuales en condiciones comerciales

- Bonificaciones superiores a los porcentajes históricos sin soporte contractual.
- Aumentos abruptos en los plazos de pago otorgados o en los precios unitarios.
- Cambios constantes en proveedores o condiciones justo antes de cierres presupuestarios o auditorías.
- Uso frecuente de la justificación de “urgencia” para evadir procesos de compras regulares.

g.2.4. Indicios de manipulación o colusión

- Pagos a nombre de terceros distintos del proveedor registrado.
- Órdenes de compra fraccionadas para evitar niveles de aprobación o concursos.
- Existencia de proveedores ficticios o sin movimientos reales.
- Facturas de múltiples proveedores con el mismo diseño gráfico, formato, errores tipográficos o pie de imprenta.
- Proveedores con datos duplicados o compartidos (RUT, cuenta bancaria, Dirección) con otros proveedores o empleados.
- Cheques modificados en beneficiario o montos y cobrados por personas ajenas al proveedor.

g.2.5. Indicadores de controles débiles o fallidos

- Proveedores sin cancelación formal de comprobantes (sin timbre, firma o sello de pagado).
- Ausencia de validación independiente de la existencia y calidad de los bienes o servicios recibidos.
- Reiteración de compras sin registro documental de evaluación de proveedores.
- Diferencias no explicadas en conciliaciones contables entre cuentas por pagar y auxiliares.
- Recepción parcial o sin respaldo de bienes que luego se pagan como completos.
- Códigos duplicados para un mismo proveedor en el sistema de información.

g.2.6. Señales asociadas a comportamiento interno indebido

- Compradores que solicitan adquisiciones reiteradas a proveedores con quienes tienen vínculos personales, sin declarar conflicto de interés.
- Acuerdos informales entre funcionarios y proveedores para beneficiar condiciones particulares.
- Alteración deliberada de montos en cheques o transferencias electrónicas.
- Cambios frecuentes de proveedor justo antes de auditorías o cuando se implementan controles más estrictos.
- Proveedores seleccionados que no cumplen criterios mínimos pero son favorecidos sin fundamento técnico o legal.

g.3 Banderas Rojas Genéricas del Ciclo de Inventarios

Los inventarios representan uno de los activos más vulnerables a errores, pérdidas y fraudes, por lo que los auditores deben estar atentos a señales que sugieran fallos en el control interno, registros inadecuados o posibles actos dolosos.

Estas banderas deben ser abordadas mediante procedimientos que combinen revisión documental, análisis de datos, entrevistas y pruebas físicas de verificación. Su aparición puede requerir la aplicación de técnicas de auditoría asistida por computador, ampliación del muestreo o incluso derivación a auditoría forense si se observan indicios de fraude.

A continuación se describen indicadores o banderas rojas que requieren atención especial durante la revisión de este ciclo:

g.3.1. Anomalías en registros y ajustes

- Ajustes de inventario frecuentes por responsables o áreas específicas sin respaldo físico o técnico.
- Compensación sistemática de ajustes negativos con positivos, dificultando el rastreo de pérdidas reales.
- Ítems con valores negativos en existencias o costos, indicando errores de registro o manipulación.
- Variaciones de costo unitario de un mismo ítem superiores a un umbral razonable (ej. 20%) entre períodos o locaciones.
- Códigos de productos duplicados o modificados sin trazabilidad.

g.3.2. Inconsistencias en movimientos y trazabilidad

- Movimientos de inventario duplicados, sin correspondencia en los sistemas o sin soporte documental.
- Ítems con entradas o salidas sin guía de recepción, parte de salida o remito.
- Registro de devoluciones frecuentes o por grandes volúmenes, sin evidencia de recepción efectiva.
- Ingresos y egresos sin control de calidad o sin validación técnica.

g.3.3. Vulnerabilidades de sistemas y accesos

- Sistemas de inventario que permiten modificaciones sin registro de usuario o sin niveles de autorización diferenciados.
- Acceso múltiple y no restringido al módulo de inventarios en el ERP o sistema de gestión.
- Falta de segregación de funciones entre quienes registran movimientos y quienes los autorizan o supervisan.

g.3.4. Ineficiencias y riesgos financieros

- Inventarios inmovilizados por períodos prolongados, sin rotación ni planificación de uso o disposición.
- Existencias obsoletas o con fecha de vencimiento próxima (por ejemplo, menor a 90 días), sin plan de consumo o disposición.
- Antigüedad excesiva de mercaderías en tránsito o en consignación sin reconciliación.
- Aumento de los costos de almacenamiento, deterioro o pérdida por falta de rotación.
- Falta de conciliación entre inventario físico y contable en cierres mensuales o anuales.

g.3.5. Prácticas inusuales o riesgosas en la gestión operativa

- Depósito de ítems en ubicaciones no registradas, inusuales o de difícil acceso (techos, pasillos, oficinas).
- Modificación frecuente e injustificada de los niveles mínimos y máximos de stock.
- Falta de controles sobre herramientas, equipos menores o bienes asignados a reparación o préstamo interno.
- Compras reiteradas de ítems con existencia suficiente, sin justificación operativa.
- Alta rotación de ítems sin relación con los niveles de producción o demanda.

g.3.6. Indicios de posibles fraudes o pérdidas no reportadas

- Mermas o pérdidas recurrentes por tipo de inventario, proveedor o ubicación física, sin análisis de causa raíz.
- Omisión de bienes costosos en los conteos físicos o existencia de ítems no registrados.
- Costos de almacenamiento que superan el valor del inventario inmovilizado.
- Manipulación de inventarios para ocultar faltantes o sobrevaluación en reportes de gestión.
- Resultados de auditorías físicas o conteos cíclicos que presentan diferencias recurrentes no investigadas.

g.4 Banderas Rojas Genéricas del Ciclo de Remuneraciones o Nómina

El proceso de nómina está particularmente expuesto a errores, omisiones y fraudes, especialmente en entornos donde hay alta rotación de personal, escasa segregación de funciones, procesos manuales o limitada verificación cruzada.

Estas señales deben analizarse de forma integral, contrastando la información de los sistemas de recursos humanos, finanzas, control de asistencia y pagos bancarios. Las técnicas recomendadas incluyen análisis de datos, revisión documental cruzada, entrevistas selectivas, pruebas de validación con terceros (como bancos o entidades previsionales) y verificación física en unidades operativas.

A continuación, se enumeran señales de alerta que los auditores internos deben tener en cuenta durante la revisión de remuneraciones, anticipos, beneficios y egresos relacionados con el personal:

g.4.1. Inconsistencias en identificación y registros

- Registros de empleados con números de cédula duplicados, inconsistentes o incorrectos.
- Datos compartidos entre empleados distintos (nombre, RUT, Dirección o cuenta bancaria).
- Existencia de más de un número de legajo para el mismo empleado sin justificación administrativa.

- Altas registradas de empleados que ya habían sido dados de baja o cuyos contratos habían expirado.

g.4.2. Pagos y movimientos irregulares

- Emisión de pagos por conceptos no vinculados a remuneraciones sin respaldo contractual ni normativo (por ejemplo: bonos extraordinarios, ayudas económicas, "gastos operacionales" sin política formal).
- Pagos a cuentas bancarias que no pertenecen al titular del contrato o que están a nombre de terceros.
- Sueldos duplicados, pagos a “empleados fantasmas” o registros activos de personal inexistente.
- Variaciones abruptas y no justificadas del sueldo base de un mismo trabajador sin respaldo normativo.
- Liquidaciones finales de monto elevado sin documentación de respaldo, cálculo o aprobación formal.

g.4.3. Manipulación de horas y anticipos

- Ranking inusual de horas extras por empleado, área o jefe directo; especialmente en unidades con funciones fijas o carga laboral previsible.
- Registro de horas extra sin verificación independiente ni soporte de tareas efectivamente realizadas.
- Anticipos frecuentes solicitados por los mismos empleados, o porcentajes de adelanto elevados respecto a la remuneración mensual.
- Pagos reiterados por trabajos fuera de horario sin evidencia de necesidad operativa ni autorización formal.

g.4.4. Debilidades en el control del ciclo de vida del empleado

- Alta rotación de personal en ciertas áreas sin análisis de causa o sin seguimiento del proceso de salida.
- Ingreso masivo de contrataciones sin evaluación o estudio de necesidades operativas.
- Inexistencia de validación cruzada entre recursos humanos, contabilidad y finanzas para verificar la consistencia de nómina.
- Cambios contractuales o promociones sin resolución ni documentación de soporte.

g.4.5. Otras señales de riesgo operacional o fraude

- Sueldos asignados a cargos vacantes o sin movimiento operativo durante el período.
- Pagos por funciones incompatibles con el contrato registrado o la categoría funcional.
- Falta de segregación de funciones entre quienes elaboran la nómina, quienes autorizan pagos y quienes realizan transferencias.
- Uso de "fondos rotatorios" o recursos extrapresupuestarios para cubrir conceptos de remuneraciones o beneficios laborales.
- Existencia de pagos recurrentes fuera del calendario normal de nómina sin documentación de urgencia o legalidad.

g.5 Banderas Rojas Genéricas del Ciclo de Tesorería

El ciclo de tesorería concentra una alta exposición a riesgos financieros, errores operativos y fraudes, tanto internos como externos. Su monitoreo requiere especial atención por parte del auditor interno, ya que involucra flujos monetarios directos, instrumentos bancarios y operaciones de alto impacto institucional.

Estas banderas deben evaluarse en conjunto con el diseño y efectividad de los controles existentes en la unidad de tesorería. La auditoría debe aplicar técnicas que combinen revisión documental, análisis cruzado de movimientos bancarios, conciliación financiera, entrevistas a responsables y verificación directa en los sistemas. En casos donde estas señales se agrupan o repiten, se recomienda escalar la revisión hacia un enfoque de auditoría forense o análisis transaccional detallado.

A continuación, se presentan señales de alerta que deben ser consideradas durante auditorías sobre esta función:

g.5.1. Inconsistencias en documentos y operaciones bancarias

- Emisión de cheques sin respaldo en órdenes de pago debidamente autorizadas.
- Cheques duplicados, anulados y no reemitidos sin justificación formal.
- Débitos bancarios que no se relacionan con cheques emitidos ni transferencias autorizadas.
- Créditos bancarios (depósitos) sin trazabilidad con liquidaciones de ingresos de tesorería o sin conciliación con los sistemas internos.
- Transferencias electrónicas con datos inconsistentes (beneficiarios, cuentas, conceptos).
- Ruptura en la correlatividad de los cheques emitidos o documentos de pago.

g.5.2. Controles débiles o inexistentes

- Conciliaciones bancarias sin revisión independiente o no realizadas periódicamente.
- Inexistencia de revisión formal sobre la cobranza de instrumentos financieros (bonos, intereses, dividendos, cupones).
- Falta de validación externa sobre documentos respaldatorios (ej.: facturas en fotocopia sin sello de copia fiel o sin validación de autenticidad).
- Múltiples operaciones en efectivo sin control cruzado con reportes auxiliares.
- Rendiciones de fondos de caja chica sin evidencia de control por parte de una unidad distinta a la ejecutora.
- Inexistencia de un sistema de control cruzado para egresos menores y pagos urgentes.

g.5.3. Comportamientos operativos irregulares

- Ranking inusual de operaciones en efectivo por proveedor o por funcionario responsable.
- Solicitudes de pago de último momento, especialmente fuera de los circuitos administrativos regulares.
- Arreglos particulares con entidades bancarias para operaciones inusuales (prórrogas, sobregiros, refinanciamientos no registrados).
- Falta de consistencia entre los montos operados con bancos y los saldos reales de las cuentas.

g.5.4. Omisiones en trazabilidad o verificación de operaciones

- No se revisan cheques devueltos ni se analizan sus endosos, lo que puede ocultar cobros por terceros no autorizados.
- Depósitos directos realizados por clientes que no son reflejados en recibos ni en registros de ingresos institucionales.
- Diferencias de caja recurrentes por funcionario responsable, sin análisis de causa raíz ni seguimiento disciplinario.
- Inexistencia de mecanismos de alerta sobre límites de operación en cuentas bancarias, autorizaciones máximas o uso indebido de cuentas puente.

g.5.5. Señales de posibles conflictos de interés o fraude interno

- Concentración de funciones en una sola persona (registro, autorización y ejecución de pagos).
- Reiteración de errores u omisiones de conciliación en una misma cuenta o por parte de un mismo responsable.
- Omisión sistemática del proceso de control interno sobre pagos a beneficiarios externos o contratos bancarios.
- Falta de documentación respaldatoria en pagos extraordinarios, devoluciones de fondos o transacciones interinstitucionales.

5.6 Banderas Rojas Genéricas Relacionadas con el Personal

El comportamiento del personal puede ser un reflejo temprano de problemas éticos, conflictos de interés, presión financiera o incluso involucramiento en prácticas fraudulentas. Aunque ningún indicador por sí solo es prueba de fraude, la combinación o reiteración de varios signos puede representar una alerta crítica para la auditoría interna, especialmente en contextos con baja supervisión, exceso de confianza o débil control cultural.

Estas señales deben abordarse con una mentalidad profesionalmente escéptica, considerando siempre la confidencialidad, el respeto por la privacidad y la presunción de buena fe. Sin embargo, deben integrarse como parte del análisis de riesgos personales, especialmente en cargos con acceso a activos, datos sensibles o funciones críticas.

El equipo de auditoría puede utilizar herramientas como entrevistas estructuradas, observación directa, análisis cruzado de datos, revisión de conflictos de interés y evaluaciones de cultura organizacional para validar la existencia de estas señales.

A continuación se enumeran situaciones o patrones de conducta observables que deben ser considerados banderas rojas durante la evaluación de riesgos o aplicación de entrevistas y observaciones en terreno:

g.6.1. Indicadores financieros, de estilo de vida o conductas externas

- Exhibición repentina de riqueza no justificada: joyas, vehículos, viajes costosos, gastos ostentosos.
- Realización frecuente de fiestas u otros eventos sociales fuera del alcance de su capacidad económica.
- Grandes cantidades de efectivo sin origen conocido o sin relación con su nivel salarial.
- Adquisición de activos costosos a nombre de terceros o con identidades prestadas.
- Viajes personales recurrentes, especialmente a países sin trazabilidad financiera (paraísos fiscales).
- Uso excesivo de vehículos arrendados, tarjetas prepagadas o medios de pago poco rastreables.
- Inversiones paralelas en negocios intensivos en efectivo (bares, concesionarios, casinos, etc.).
- Actividades bancarias inusuales (retiros frecuentes, depósitos fraccionados, cuentas múltiples).

g.6.2. Comportamiento en el lugar de trabajo

- Cambios bruscos de actitud: irritabilidad, hostilidad o aislamiento social injustificado.
- Conductas evasivas ante preguntas rutinarias o solicitudes del auditor interno.
- Resistencia injustificada a delegar tareas o compartir funciones (especialmente en personal clave).
- Uso personal de recursos de la entidad sin autorización (vehículos, equipos, tarjetas de gasolina).
- Reiterado trabajo en horas fuera del horario habitual, sin justificación objetiva.
- Rechazo persistente a tomar vacaciones o licencias, lo que puede ocultar actividades ilícitas.
- Comportamiento controlador, centralización excesiva de funciones, negativa a compartir información.

g.6.3. Vulnerabilidades personales y sociales

- Problemas económicos severos: deudas personales elevadas, embargos o atrasos crediticios.
- Presión financiera por enfermedad grave de familiar o gastos médicos fuera de cobertura.
- Afición excesiva al juego, consumo de drogas o alcohol.
- Relación cercana o no declarada con proveedores, clientes, o contratistas de la entidad.
- Situaciones personales críticas no gestionadas emocionalmente (divorcios, duelos, separaciones).
- Necesidad de mantener un estatus social que excede las posibilidades reales.

g.6.4. Riesgos éticos y actitudes hacia la entidad

- Frustración crónica con su rol, quejas frecuentes sobre condiciones laborales o remuneración.
- Comentarios recurrentes de desprecio hacia la misión institucional o la Dirección.
- Exhibición de favoritismo excesivo con ciertos subordinados o trato diferenciado sin explicación objetiva.
- Exigencia de lealtad personal por sobre la lealtad institucional o profesional.
- Declaraciones que justifican conductas irregulares como "todos lo hacen" o "la entidad me debe".

g.6.5. Prácticas operativas sospechosas

- Realización de ventas a crédito a familiares o cercanos y posterior registro como incobrables.
- Autorización de adquisiciones innecesarias para obtener beneficios personales o “comisiones”.
- Inclusión de vales o cheques sin fecha o con fecha alterada en caja chica u otros fondos.
- Uso sistemático de bienes de la institución para fines personales o familiares (vehículos, combustible, inmuebles, equipos).
- Interferencia en procesos de selección, contratación o evaluación de desempeño para favorecer cercanos.
- Manipulación de reportes operacionales o financieros para alcanzar metas personales o institucionales.

g.6.6. Uso irregular de Licencias Médicas por el Personal

- Alta frecuencia de licencias en lunes o viernes.
- Licencias médicas recurrentes de corta duración.
- Múltiples licencias emitidas por el mismo médico a distintos funcionarios.
- Evidencia de actividad económica durante el período de licencia médica.
- Presentación de licencias médicas sin seguir el procedimiento de notificación interna.
- Incremento de licencias médicas durante procesos disciplinarios o auditorías.
- Departamentos con tasas de licencias significativamente superiores al promedio institucional.
- Licencias médicas emitidas por médicos fuera de la región de residencia del funcionario.
- Coincidencia de períodos de licencia con vacaciones escolares o festivos largos.

g.7 Banderas Rojas Genéricas de Seguridad, Ciberseguridad y Gestión de Accesos

En la actualidad, los sistemas de información, redes y tecnologías digitales son pilares críticos de operación en cualquier entidad pública o privada. Su vulnerabilidad ante amenazas internas o externas representa un riesgo significativo para la continuidad operativa, integridad de la información, cumplimiento normativo y protección de datos personales.

Estas señales deben ser evaluadas dentro de un marco de gestión integral de riesgos tecnológicos y pueden requerir auditorías especializadas en TI, pruebas de penetración, revisión de políticas, análisis de logs y entrevistas a responsables de sistemas. El auditor interno debe aplicar técnicas de análisis de datos, revisión de roles y pruebas de acceso cruzado para confirmar hallazgos.

Las siguientes banderas rojas pueden indicar debilidades de control, fallos de supervisión o condiciones propicias para incidentes de seguridad o ciberataques:

g.7.1. Gestión de accesos y privilegios

- Cuentas de usuarios sin caducidad asignadas a exfuncionarios, personal externo o temporales.
- Accesos de tipo "Administrador" otorgados sin justificación o sin revisión periódica.
- Usuarios con múltiples roles sin segregación de funciones o sin trazabilidad del cambio de perfil.

- Reasignación de contraseñas sin autorización formal o sin verificación de identidad.
- Inexistencia de controles de bloqueo tras intentos fallidos de acceso al sistema.
- Uso compartido de cuentas de usuario o contraseñas entre funcionarios.
- Cuentas de sistema o de servicio sin monitoreo ni control.

g.7.2. Debilidades en la supervisión de seguridad lógica

- Inexistencia de revisión periódica de logs de acceso, modificaciones de datos o incidentes de seguridad.
- Accesos fuera del horario laboral sin justificación operativa (fines de semana, noches).
- Actividades ejecutadas desde direcciones IP inusuales o no reconocidas.
- Eliminación de logs del sistema o inhabilitación de auditoría del sistema (*event viewer* desactivado).
- Creación de usuarios directamente en bases de datos o sistemas ERP sin pasar por procesos de TI.
- Cambios no documentados en parámetros de seguridad de aplicaciones críticas.

g.7.3. Riesgos en políticas y configuraciones de ciberseguridad

- Ausencia de políticas de seguridad de la información aprobadas y difundidas.
- Antivirus, firewalls o IDS/IPS desactualizados, desactivados o sin monitoreo activo.
- Uso de software no licenciado o descargado sin validación técnica.
- Estaciones de trabajo sin políticas de actualización automática o sin cifrado de disco.
- Múltiples estaciones o servidores con contraseñas por defecto o sin autenticación multifactor.
- No implementación de *backups* periódicos o no verificados en pruebas de restauración.

g.7.4. Falta de controles sobre dispositivos y red

- Acceso libre a puertos *USB*, impresoras o unidades de almacenamiento sin trazabilidad.
- Dispositivos personales conectados a la red interna sin control de acceso (*BYOD* sin política).
- Conexiones remotas habilitadas sin *VPN* o sin controles de *endpoint*.
- Redes *Wi-Fi* internas sin segmentación ni cifrado *WPA2* o superior.
- Dispositivos sin registro en el inventario de activos TI institucional.

g.7.5. Gestión de incidentes y continuidad

- No existencia de plan de respuesta ante incidentes de ciberseguridad.
- Falta de simulacros de recuperación ante desastres o continuidad operativa.
- Incidentes previos sin registro formal, análisis de causa raíz ni acciones correctivas documentadas.
- Fallos de disponibilidad de sistemas críticos sin explicación técnica adecuada.
- Pérdida de datos sensibles sin notificación a los entes reguladores o sin análisis forense.

g.7.6. Conductas de riesgo del personal

- Descarga o ejecución de archivos adjuntos sospechosos en correos institucionales.
- Accesos a sitios web no permitidos desde redes institucionales.
- Uso de mensajería instantánea o plataformas no autorizadas para compartir documentos oficiales.
- Manipulación de información institucional sin cifrado o envío a correos personales.
- Falta de capacitación o sensibilización en temas de ciberseguridad, phishing y gestión de contraseñas.

12 Anexo: Muestreo de Auditoría y Análisis Estadístico

En el trabajo diario de la auditoría interna, rara vez es posible revisar el 100% de los documentos, registros o transacciones de una organización. En su lugar, lo que se hace es trabajar con una muestra representativa que, si está bien seleccionada, permite sacar conclusiones válidas sobre el total de los datos. Esta práctica, conocida como muestreo de auditoría, es uno de los pilares para realizar auditorías eficientes y confiables, y resulta especialmente útil desde la etapa de planificación del trabajo.

El muestreo se aplica sobre todo cuando se necesita revisar grandes volúmenes de transacciones o evidencias documentales, como facturas, contratos o registros contables. En cambio, no es lo más apropiado para otras técnicas como entrevistas, observaciones directas o análisis de tendencias generales, donde la información suele ser más cualitativa o abierta.

Existen dos formas principales de hacer muestreo: el enfoque estadístico y el no estadístico. Ambos son válidos, y la elección entre uno u otro dependerá del tipo de trabajo, del riesgo del área auditada, del nivel de certeza que se necesita, del presupuesto disponible y de cuánto se espera generalizar los resultados

El muestreo estadístico usa herramientas matemáticas para definir con precisión el tamaño de la muestra y el margen de error aceptable. Permite proyectar los hallazgos de manera numérica a toda la población. Es muy útil cuando se requiere objetividad y precisión cuantificable.

El muestreo no estadístico, en cambio, se basa en el juicio profesional del auditor. Aquí, quien audita decide qué elementos incluir en la muestra según su experiencia, el conocimiento del proceso o ciertos criterios como la relevancia del monto o la complejidad de la operación. Es más flexible y menos costoso, pero también requiere mayor cuidado en la interpretación de los resultados.

Dentro de cada enfoque existen varias técnicas. Entre las estadísticas, están el muestreo aleatorio (donde cada elemento tiene la misma posibilidad de ser elegido), el muestreo estratificado (que divide la población en grupos similares para asegurar representación), el sistemático (por ejemplo, seleccionar cada décimo registro), o el llamado “*stop-and-go*”, que permite detener el análisis si no se encuentran errores al inicio.

También se usa el muestreo por atributos, para evaluar si un control está funcionando, o el muestreo por variables, para analizar si los montos de las transacciones están correctos. En casos donde se sospecha la presencia de un error grave aunque poco frecuente, como fraude, se puede aplicar el muestreo de descubrimiento, diseñado para detectar al menos una ocurrencia del problema.

En los métodos no estadísticos, destacan el muestreo dirigido (centrado en los casos de mayor riesgo), el muestreo por bloques (todos los registros de un mismo mes, por ejemplo), o el muestreo por intervalos (como tomar cada veinteavo registro).

Independientemente del método usado, el juicio profesional del auditor es siempre fundamental. Este juicio se aplica para definir la población, establecer el tamaño de muestra, interpretar los errores encontrados, evaluar la suficiencia de la evidencia y, si es necesario, proyectar los resultados al conjunto.

Otro aspecto clave es el riesgo de muestreo, que es el peligro de llegar a conclusiones incorrectas si la muestra no representa bien a la población. Por ejemplo, se puede sobreestimar la efectividad de un control (pensar que funciona cuando no es así) o subestimarla (pensar que falla cuando en realidad sí es efectivo).

En los últimos años, el uso de herramientas de análisis de datos ha mejorado notablemente la capacidad de los auditores para trabajar con grandes volúmenes de información. Gracias al análisis estadístico digital, es posible detectar patrones, identificar transacciones anómalas, dividir la población en subgrupos y seleccionar muestras más relevantes y efectivas. Esto es particularmente útil cuando se manejan datos con las características conocidas como las "*4 V del big data*": gran volumen, alta velocidad, distintos formatos (variedad), y necesidad de asegurar su veracidad.

El uso correcto del muestreo, combinado con herramientas estadísticas y de análisis de datos, no solo optimiza el trabajo del auditor interno, sino que también le permite emitir conclusiones más sólidas y justificadas. Durante la planificación, conviene definir claramente qué se va a auditar, cómo se va a seleccionar la muestra, cuál será el tamaño adecuado y cómo se documentarán las decisiones tomadas. Todo esto permite que la auditoría sea más eficaz, más profesional y alineada con las NOGAI.

La siguiente tabla presenta los elementos técnicos clave que deben considerarse al diseñar, documentar, ejecutar y evaluar un proceso de muestreo en auditoría interna. Cada elemento se describe con base en prácticas recomendadas, alineadas con los principios de escepticismo profesional (N*orma 4.3*), debido cuidado profesional (*Norma 4.2*) y documentación adecuada del trabajo (*Norma 14.6*)

Tabla N° 1: Elementos Clave en la Aplicación del Muestreo

Elemento Técnico	Detalle Recomendado
Definición de población	Asegurar claridad sobre qué universo se va a evaluar (ej.: facturas del año fiscal).
Unidad de muestreo	La menor parte que puede seleccionarse (ej.: número de factura, ítem de inventario).
Tamaño de la muestra	Determinado con base en el riesgo de muestreo y nivel de confianza deseado.
Método de selección	Estadístico o por juicio profesional.
Documentación del diseño	Justificación del método, criterios, cálculos y supuestos.
Ejecución del muestreo	Registro preciso de los elementos seleccionados y pruebas realizadas.
Evaluación de resultados	Identificación de errores y desviaciones; impacto monetario o de control.
Extrapolación a la población	Proyección del efecto estimado al universo completo cuando aplique.
Juicio profesional	Siempre necesario para interpretar los resultados y evaluar su impacto.

A continuación se presenta una tabla explicativa con los tipos de muestreo más relevantes en auditoría interna, organizada por enfoque (estadístico y no estadístico), con sus características clave, ventajas, limitaciones y ejemplos de aplicación práctica:

Tabla N° 2: Tipos de Muestreo más Relevantes en Auditoría Interna

Tipo de Muestreo	Enfoque	Descripción	Ventajas	Limitaciones	Ejemplo de Aplicación
Muestreo Aleatorio Simple	Estadístico	Cada unidad de la población tiene la misma probabilidad de ser seleccionada.	Objetivo, evita sesgos, fácil de justificar ante terceros.	Puede no representar subgrupos importantes de la población.	Seleccionar aleatoriamente 100 facturas de un universo de 5.000.
Muestreo Estratificado	Estadístico	Divide la población en grupos homogéneos (estratos) y se toma muestra proporcional de cada uno.	Mayor representatividad, especialmente en poblaciones heterogéneas.	Requiere conocimiento previo de la composición de la población.	Auditar pagos divididos entre compras menores, intermedias y mayores.
Muestreo Sistemático	Estadístico	Se selecciona cada "n" elemento a partir de un punto de inicio aleatorio.	Sencillo de aplicar con listas ordenadas.	Puede generar sesgo si hay patrones cíclicos en los datos.	Se elige un punto de inicio al azar dentro de los primeros 50 registros y luego se toma cada registro número 50 a partir de ese punto.

Tabla N° 2: Tipos de Muestreo más Relevantes en Auditoría Interna (continúa)

Tipo de Muestreo	Enfoque	Descripción	Ventajas	Limitaciones	Ejemplo de Aplicación
Muestreo Stop-and-Go	Estadístico	Inicia con una muestra reducida. Si se detectan pocos errores, se detiene; si no, se amplía.	Ahorra tiempo si el control es efectivo.	Inapropiado si se espera alta tasa de error.	Evaluar control de autorizaciones si se presume alta conformidad.
Muestreo de Descubrimiento	Estadístico	Diseñado para detectar la presencia de al menos una ocurrencia de un evento raro pero grave (ej.: fraude).	Efectivo para identificar eventos críticos.	Difícil estimar el tamaño de muestra necesario.	Buscar evidencia de pagos duplicados en procesos sensibles.
Muestreo por Unidad Monetaria (MUS)	Estadístico	Asigna mayor probabilidad de selección a elementos con mayor valor monetario.	Enfoca la revisión en transacciones con más impacto.	Subrepresenta elementos de bajo valor donde también puede haber errores.	Evaluar exactitud de saldos contables o pagos de gran cuantía.
Muestreo Dirigido (Judgmental)	No estadístico	El auditor interno selecciona los elementos que considera más relevantes con base en experiencia o riesgo.	Se enfoca en áreas críticas y de alto impacto.	Riesgo de sesgo; no se puede extrapolar estadísticamente.	Elegir contratos mayores a cierto monto o con proveedores críticos.
Muestreo al Azar No Planificado	No estadístico	Selección informal sin una regla definida, usando intuición.	Rápido y simple en auditorías preliminares.	Baja confiabilidad; difícil justificar la representatividad.	Tomar algunas órdenes de compra de un archivador sin seguir patrón definido.
Muestreo por Intervalos (Sistemático No Estadístico)	No estadístico	Selección cada cierto número fijo de elementos, sin fórmula de aleatoriedad formal.	Sencillo de aplicar manualmente.	Puede introducir sesgos si hay periodicidad en los datos.	Auditar cada décimo recibo de caja en una lista impresa.
Muestreo por Bloques	No estadístico	Se selecciona un grupo completo de elementos contiguos (por tiempo, ubicación, etc.).	Útil para análisis preliminares o controles continuos.	Riesgo alto de no representatividad si el bloque seleccionado no refleja el total.	Revisar todas las facturas de un mes específico para evaluar el proceso de cierre contable.

Para mayor detalle, ver guías y metodologías del CAIGG sobre muestreo estadístico para auditores internos.

13 Anexo: Planilla de Trazabilidad del Trabajo de Auditoría Interna

a. HOJA 1: "COMPRENSIÓN INICIAL ACTIVIDAD BAJO REVISIÓN: GOBIERNO - GESTIÓN DE RIESGOS - CONTROLES"

Descripción Estructural y Funcional de la Hoja

Esta hoja cumple la función de documentar de manera sistemática la comprensión inicial del proceso o actividad bajo auditoría, integrando elementos de gobierno, gestión de riesgos y controles. Su diseño permite recolectar información clave para la planificación basada en riesgos, conforme a las *Normas Norma 13.1 Comunicación durante el trabajo, 13.2: Evaluación de riesgos del trabajo y 13.3 Objetivos y alcance del trabajo*.

- Permite construir una línea base del conocimiento del proceso antes de iniciar el trabajo de campo.
- Facilita la identificación y priorización de áreas críticas para el trabajo.
- Proporciona trazabilidad dese la comprensión inicial hasta el programa de trabajo.
- Es una evidencia clave de cumplimiento de los principios y las normas de planificación.

Esta hoja debe ser llenada colaborativamente por el equipo auditor durante la fase inicial del trabajo (comprensión del proceso), apoyándose en entrevistas, revisión documental y análisis.

TIPO DE TRABAJO: Aseguramiento/Asesoramiento
TIPO DE ASEGURAMIENTO: Razonable o Limitado

Bloque 1: Estructura Organizacional

Sección / Columna	Descripción Funcional
Gobierno Corporativo, Gestión de Riesgos y Controles	Categoriza el nivel de análisis del componente revisado. Puede ser Gobierno, Gestión de Riesgos o Control
Componente Principal (Proceso)	Proceso principal a examinar de la actividad bajo revisión (ej. adquisiciones, planificación, tesorería, etc.)
Elemento (Subproceso)	Subproceso o unidad funcional específica dentro del componente
Subelemento (Etapas)	Fase o tarea detallada dentro del subproceso
Objetivo del Componente / Elemento / Subelemento	Explicita el propósito del subproceso o etapa de la actividad a revisar
Tipo de Objetivo	Clasificación del objetivo: estratégico, cumplimiento, de información u operativo

Bloque 2: Criterios de Auditoría

Sección / Columna	Descripción Funcional
Potenciales Criterios de Auditoría Identificados en la Compresión de la Actividad Bajo Revisión	Marcos normativos o documentos internos y/o externos usados como referencia preliminar (ej.: leyes, reglamentos, directrices, etc.)

Bloque 3: Decisiones sobre Criticidad

Sección / Columna	Descripción Funcional
Información Complementaria (si corresponde)	Cualquier dato adicional que enriquezca el análisis (sistemas usados, volumen de transacciones, etc.)
Paso siguiente: Matriz de Riesgos y Controles (Sí/No)	Indica si el componente analizado requiere continuar con análisis de riesgos y controles detallado en la *Matriz de Riesgos y Controles*
Paso siguiente: Análisis y Evaluación de Información (Sí/No)	Indica si el componente analizado debe ser considerado directamente en la fase de análisis y evaluación de la información
Fundamentos	Justificación técnica de por qué se incluye o excluye un componente en determinadas fases posteriores, si así corresponde
REF P/T	Referencia a documentos fuente o trazabilidad (papeles de trabajo)

b. HOJA 2: "MATRIZ PRELIMINAR DE RIESGOS Y CONTROLES - MATRIZ DE PLANIFICACIÓN DE RIESGOS Y CONTROLES"

Descripción Estructural y Funcional de la Hoja

Esta hoja tiene como finalidad identificar, documentar, analizar y evaluar los riesgos y controles asociados a los procesos, subprocesos y actividades identificadas en la fase de comprensión inicial. Es una herramienta esencial para estructurar un enfoque de auditoría basado en riesgos, conforme a los *Principios 13 y 14 del Dominio V de las NOGAI*, especialmente las *Normas 13.2: Evaluación de Riesgos del Trabajo y 14.2: Análisis y Potenciales Hallazgos del Trabajo.*

- Permite priorizar las áreas críticas de la actividad bajo revisión con base en análisis de riesgo.
- Documenta la lógica de evaluación previa a la selección de pruebas de auditoría.
- Apoya la preparación del Programa de Auditoría (*Norma 13.6*) de forma justificada.
- Sirve como evidencia clave de cumplimiento con los requisitos de evaluación de riesgos y controles según las NOGAI y el Manual de Evaluación de Calidad del IIA.

TIPO DE TRABAJO: Aseguramiento/Asesoramiento
TIPO DE ASEGURAMIENTO: Razonable o Limitado

Bloque 1: Estructura Organizacional (Proviene de la Hoja 1: Bloque 1: Estructura Organizacional)

Sección / Columna	Descripción Funcional
Gobierno Corporativo, Gestión de Riesgos y Controles	Categoriza el nivel de análisis del componente revisado. Puede ser gobierno, gestión de riesgos o control
Componente Principal (Proceso)	Proceso principal a examinar de la actividad bajo revisión (Ej.: adquisiciones, planificación, tesorería, etc.)
Elemento (Subproceso)	Subproceso o unidad funcional específica dentro del componente
Subelemento (Etapas)	Fase o tarea detallada dentro del subproceso
Objetivo del Componente / Elemento / Subelemento	Explicita el propósito del subproceso o etapa de la actividad a revisar
Tipo de Objetivo	Clasificación del objetivo: estratégico, cumplimiento, de información u operativo

Bloque 2: Riesgos Críticos

Sección / Columna	Descripción Funcional
Descripción Riesgos Relevantes	Detalle del riesgo que se analizará. Énfasis en la causa y efecto del riesgo.
Probabilidad (Clasificación y Valor)	Grado de ocurrencia estimado del riesgo, según escala
Impacto (Clasificación y Valor)	Gravedad del efecto del riesgo en caso de materialización, según escala
Severidad del Riesgo (Clasificación y Valor)	Resultado combinado según escala de severidad del riesgo

Bloque 3: Evaluación de la Idoneidad del Diseño de los Controles (control principal o complementario)

a. Control Principal

Sección / Columna	Descripción Funcional
Descripción del control mitigante asociado al riesgo	Control implementado para mitigar el riesgo (Quién, Qué, Cómo se ejecuta y Cómo se evidencia)
Cumple Elementos de Control Adecuado	Si/NO. En base a los componentes de un control adecuado definido en la Guía en el Anexo N° 5
Evaluación del Diseño del Control Mitigante	Periodicidad, Oportunidad, Automatización
Periodicidad	Valor según escala
Oportunidad	Valor según escala
Automatización	Valor según escala
Valor	Nivel de efectividad del diseño del control según escala

b. Control Compensatorio

Sección / Columna	Descripción Funcional
Control Compensatorio	SI/NO
Descripción del control mitigante asociado al riesgo	Control implementado para mitigar el riesgo (Quién, Qué, Cómo se ejecuta y Cómo se evidencia)
Cumple Elementos de Control Adecuado	Si/NO. En base a los componentes de un control adecuado definido en la Guía en el Anexo N° 5
Evaluación del Diseño del Control Compensatorio (Si Existe)	Periodicidad, Oportunidad, Automatización
Periodicidad	Valor según escala
Oportunidad	Valor según escala
Automatización	Valor según escala
Valor	Nivel de efectividad del diseño del control según escala

Bloque 4: Priorización para el Programa de Trabajo

Sección / Columna	Descripción Funcional
Valor y Clasificación de la Exposición al Riesgo	Riesgo residual tras aplicar el control a la severidad del riesgo
Nivel Exposición al Riesgo	Clasificación según escala
Valor	Clasificación según escala
Criterio de Priorización para Programa de Auditoría	Severidad, Impacto, Exposición, Combinación, entre otros
Ejemplo: Severidad y Exposición al Riesgo (Control)	Ejemplo para mayor comprensión de la priorización
Programa de Auditoría Asociado	SI/NO
REF P/T	Documentos de respaldo o trazabilidad

c. HOJA 3: "MATRIZ PRELIMINAR DE RIESGOS Y CONTROLES PARA FRAUDES" - MATRIZ DE PLANIFICACIÓN DE RIESGOS Y CONTROLES PARA FRAUDES"

Descripción Estructural y Funcional de la Hoja

La hoja tiene como objetivo identificar, evaluar y documentar los riesgos específicos de fraude en los procesos revisados, así como los controles asociados y su efectividad. Forma parte del cumplimiento de las *Normas 13.2: Evaluación de riesgos del trabajo y de la Norma 4.2: Debido cuidado profesional.*

- Refuerza la aplicación de un enfoque preventivo y proactivo frente al fraude, conforme a las mejores prácticas del IIA.
- Permite a la auditoría interna priorizar la revisión de riesgos críticos de integridad.
- Apoya la planificación de pruebas específicas en el Programa de Trabajo, con base en vulnerabilidades detectadas.
- Esta hoja también puede ser pate de la **HOJA 2: "MATRIZ PRELIMINAR DE RIESGOS Y CONTROLES - MATRIZ DE PLANIFICACIÓN DE RIESGOS Y CONTROLES"**

TIPO DE TRABAJO: Aseguramiento/Asesoramiento
TIPO DE ASEGURAMIENTO: Razonable o Limitado

Bloque 1: Estructura Organizacional (Proviene de la Hoja 1: Bloque 1: Estructura Organizacional)

Sección / Columna	Descripción Funcional
Gobierno Corporativo, Gestión de Riesgos y Controles	Categoriza el nivel de análisis del componente revisado. Puede ser Gobierno, Gestión de Riesgos o Control
Componente Principal (Proceso)	Proceso principal a examinar de la actividad bajo revisión (Ej.: adquisiciones, planificación, tesorería, etc.)
Elemento (Subproceso)	Subproceso o unidad funcional específica dentro del componente
Subelemento (Etapas)	Fase o tarea detallada dentro del subproceso
Objetivo del Componente / Elemento / Subelemento	Explicita el propósito del subproceso o etapa de la actividad a revisar
Tipo de Objetivo	Clasificación del objetivo: estratégico, cumplimiento, de información u operativo

Bloque 2: Riesgos Críticos de Fraude

Sección / Columna	Descripción Funcional
Identificación de Riesgos y/o Esquemas de Fraude	Detalle del riesgo potencial de fraude
Probabilidad (Clasificación y Valor)	Grado de ocurrencia estimado del fraude, según escala
Impacto (Clasificación y Valor)	Gravedad del efecto del fraude en caso de materialización, según escala
Severidad del Riesgo (Clasificación y Valor)	Resultado combinado según escala de severidad del riesgo de fraude
Cargo o Unidad Sujeto al Riesgo de Fraude	Identificar dentro de la organización, el cargo y/o unidades sujetas prioritariamente al riesgo de fraude

Bloque 3: Evaluación de la Idoneidad del Diseño de los Controles (control principal o complementario)

a. Control Principal

Sección / Columna	Descripción Funcional
Descripción del control mitigante asociado al riesgo de fraude	Control implementado para mitigar el riesgo (Quién, Qué, Cómo se ejecuta y Cómo se evidencia)
Cumple Elementos de Control Adecuado	Si/NO. En base a los componentes de un control adecuado definido en la Guía en el Anexo N° 5
Evaluación del Diseño del Control Mitigante	Periodicidad, Oportunidad, Automatización
Periodicidad	Valor según escala
Oportunidad	Valor según escala
Automatización	Valor según escala
Valor	Nivel de efectividad del diseño del control según escala

b. Control Compensatorio

Sección / Columna	Descripción Funcional
Control Compensatorio	SI/NO
Descripción del control mitigante asociado al riesgo de fraude	Control implementado para mitigar el riesgo (Quién, Qué, Cómo se ejecuta y Cómo se evidencia)
Cumple Elementos de Control Adecuado	Si/NO. En base a los componentes de un control adecuado definido en la Guía en el Anexo N° 5
Evaluación del Diseño del Control Compensatorio (si existe)	Periodicidad, Oportunidad, Automatización
Periodicidad	Valor según escala
Oportunidad	Valor según escala
Automatización	Valor según escala
Valor	Nivel de efectividad del diseño del control según escala

Bloque 4: Priorización para el Programa de Trabajo

Sección / Columna	Descripción Funcional
Valor y Clasificación de la Exposición al Riesgo	Riesgo residual tras aplicar el control a la severidad del riesgo
Nivel Exposición al Riesgo	Clasificación según escala
Valor	Clasificación según escala
Criterio de Priorización para Programa de Auditoría	Severidad, Impacto, Exposición, Combinación, entre otros
Ejemplo: Severidad y Exposición al Riesgo (Control)	Ejemplo para mayor comprensión de la priorización
Programa de Auditoría Asociado	SI/NO
REF P/T	Documentos de respaldo o trazabilidad

d. HOJA 4: "PROGRAMA DE TRABAJO"

Descripción Estructural y Funcional de la Hoja

Esta hoja constituye el documento operativo principal del trabajo. Detalla, de forma estructurada, las actividades específicas, procedimientos y pruebas de auditoría, asegurando trazabilidad y control en la ejecución del trabajo.

Corresponde principalmente al cumplimiento de la *Norma 13.6: Programa de Trabajo* y es esencial para alinear el trabajo de campo con los objetivos, riesgos y controles previamente identificados.

- Lleva a la práctica los criterios documentados en el memorándum de planificación y en las demás horas de esta planilla.
- Concreta el vínculo entre planificación y ejecución, permitiendo evidenciar el cumplimiento de objetivos con enfoque en riesgos.
- Establece claramente la asignación de tareas y tiempos, optimizando recursos y facilitando el control del desempeño.
- Cumple funciones de control de calidad, ya que puede ser revisado y ajustado en función de los avances del trabajo.

Esta hoja se convierte en parte de los papeles de trabajo, siendo evidencia directa de cumplimiento con los *principios 13 y 14*. Además, su correcta implementación impacta directamente en la medición del desempeño conforme a la *Norma 12.2: Medición del Desempeño*.

TIPO DE TRABAJO: Aseguramiento/Asesoramiento
TIPO DE ASEGURAMIENTO: Razonable o Limitado

Bloque 1: Programa de Trabajo

Sección / Columna	Descripción Funcional
Objetivo General	Declaración del propósito global del trabajo
Alcance del Trabajo	Cobertura y límites definidos de revisión (procesos, periodos, umbrales, etc.)
Nivel de Aseguramiento Planificado por Tema	Distinguir entre Razonable y Limitado para cada objetivo específico de auditoría
Gobierno / Gestión de riesgos / Controles	Categoría principal del componente revisado
Componente - Elemento	Proceso/Área/Etapa/Tarea
Objetivo de la Actividad bajo Revisión	Finalidad operacional o normativa del componente
Riesgos Críticos Asociados al Objetivo	Riesgos priorizados en las fases anteriores
Descripción del control mitigante asociado al riesgo (principal o complementario)	Control implementado para mitigar el riesgo (Quién, Qué, Cómo se ejecuta y Cómo se evidencia)
Objetivos Específicos de Auditoría	Definición de lo que se espera cumplir en el trabajo.
Procedimientos/Pruebas de Auditoría	Actividades y técnicas de auditoría que se utilizarán para cumplir los objetivos de auditoría
Fuentes de Evidencia Esperada	Tipos de documentos, datos o confirmaciones que respaldan el procedimiento de auditoría
Normas o Criterios de Referencia	Base normativa o institucional para evaluar el resultado del procedimiento
Responsable(s)	Supervisor y equipo auditor asignado al procedimiento.
Horas Estimadas	Carga de trabajo prevista para la actividad
Evidencia de Supervisión	Visación de parte del Supervisor
Observaciones	Comentarios o aclaraciones relevantes
Ref. P/T	Documentos de respaldo o trazabilidad

e. HOJA 5: "REGISTRO DE INFORMACIÓN: RECOPILAR, ANALIZAR, EVALUAR Y DOCUMENTAR"

Descripción Estructural y Funcional de la Hoja

Esta hoja está diseñada para sistematizar el proceso de identificación, análisis, evaluación y validación de potenciales hallazgos detectados durante el trabajo de auditoría. Permite transformar las observaciones en resultados sólidos, priorizados y alineados con los objetivos del trabajo. Contribuye al cumplimiento de la *Norma 14.2: Análisis y Potenciales Hallazgos del Trabajo, Norma 14.3: Evaluación de los Hallazgos y a la gestión de calidad del Principio 14.*

- Permite garantizar la trazabilidad entre el programa, el trabajo de campo y el informe borrador/final.
- Asegura la validez y consistencia profesional del juicio auditor, conforme a los principios de objetividad y cuidado profesional *(Principio 4).*
- Facilita el control del seguimiento posterior de recomendaciones y el cierre de hallazgos

Esta hoja es clave para la calidad del trabajo de auditoría. Es necesario que su contenido sea validado internamente antes de su inclusión en el informe borrador/final y cuente con revisión del supervisor del trabajo.

TIPO DE TRABAJO: Aseguramiento/Asesoramiento
TIPO DE ASEGURAMIENTO: Razonable o Limitado

Bloque 1: Antecedentes del Trabajo de Auditoría

Sección / Columna	Descripción Funcional
Objetivo General	Declaración del propósito global del trabajo
Alcance del Trabajo	Cobertura y límites definidos de revisión (procesos, periodos, umbrales, etc.)
Nivel de Criticidad Macro	Definir el Nivel de criticidad en base a la escala y fundamentado en los resultados y conclusiones del trabajo y sus hallazgos en forma agregada

Bloque 2: Estructura Organizacional (Proviene de la Hoja 1: Bloque 1: Estructura Organizacional)

Sección / Columna	Descripción Funcional
Gobierno Corporativo, Gestión de Riesgos y Controles	Categoriza el nivel de análisis del componente revisado. Puede ser Gobierno, Gestión de Riesgos o Control
Componente Principal (Proceso)	Proceso principal a examinar de la actividad bajo revisión (Ej.: adquisiciones, planificación, tesorería, etc.)
Elemento (Subproceso)	Subproceso o unidad funcional específica dentro del componente
Subelemento (Etapas)	Fase o tarea detallada dentro del subproceso
Objetivo del Componente / Elemento / Subelemento	Explicita el propósito del subproceso o etapa de la actividad a revisar
Tipo de Objetivo	Clasificación del objetivo: estratégico, cumplimiento, de información u operativo

Bloque 3: Riesgos Críticos, Objetivos de Auditoria y Hallazgos Potenciales

Sección / Columna	Descripción Funcional
Riesgos Críticos	Riesgos priorizados en las fases anteriores
Objetivos Específicos de Auditoría	Definición de lo que se espera cumplir en el trabajo
Fuente de la Información Recopilada para Análisis y Evaluación del Control (Estudio Preliminar, Trabajo de Campo, etc.)	Identificar si el hallazgo potencial proviene del estudio de la comprensión de la actividad o de la aplicación del programa de auditoria en terreno)
Descripción	Identificar la documentación e información que respalda el hallazgo (evidencia)
Relevante (SI/NO)	Definir si la evidencia de auditoría es (relevante de acuerdo con la definición
Fiable (SI/NO)	Definir si la evidencia de auditoría es fiable de acuerdo con la definición
Suficiente (SI/NO)	Definir si la evidencia de auditoría es suficiente de acuerdo con la definición
N°	Numeración correlativa de los hallazgos (puede ser un código específico y único por hallazgo)
Hallazgos Potenciales Identificados	Describir el o los hechos identificados (hallazgos potenciales identificados que se analizarán para el riesgo crítico. Evidencia competente, fiable y suficiente)

Bloque 4: Análisis de Hallazgos Potenciales

Sección / Columna	Descripción Funcional
Criterio	Norma, política o estándar con el cual comparar los hechos
Condición	Qué ocurrió. Situación real identificada
Inventario de Posibles Causas	Identificación de potenciales causas que podrían generar el problema
Causa(s) Raíz	Origen subyacente de la condición obtenido en base a las posibles causas
Posibles Efectos	Consecuencias del hallazgo (financieras, reputacionales, de control, etc.)
Recomendaciones	Propuestas específicas para corregir o mitigar el hallazgo
Entidad responsable	Unidad o área que debe implementar la acción correctiva
Fecha estimada de cumplimiento	Plazo acordado con el responsable de la actividad bajo revisión
Verificación del Cumplimiento y Fecha de Validación	Campo para seguimiento posterior
Responsable del Seguimiento	Auditor o encargado de confirmar el cierre

Bloque 5: Evaluación de Hallazgos Potenciales

Sección / Columna	Descripción Funcional
Conclusión	Resumir el efecto y la causa del hallazgo, expresando el nivel de desviación respecto a los criterios establecidos
Nivel en que el hallazgo afecta a elemento de la naturaleza (GRC) actividad bajo revisión	Describir el nivel de impacto o consecuencias reales o potenciales del hallazgo en GRC de la actividad bajo revisión
Nivel de Criticidad Micro del Hallazgo	Definir el Nivel de criticidad en base a la escala y fundamentado en la condición y el impacto o consecuencias reales o potenciales del hallazgo

Bloque 6: Priorización de Hallazgos para Informe y Reunión de Cierre

Sección / Columna	Descripción Funcional
Informe Final de Auditoría (SI/NO)	Define si el hallazgo analizado se informará y conversará en la reunión de cierre
Fundamentos	Describe los fundamentos de la decisión de incorporarlo o no en el informe borrador
Ref. P/T	Referencia documental que respalda el hallazgo
Observaciones	Comentarios o aclaraciones relevantes

Bloque 7: Oportunidades de Mejoras Potenciales (Opcional)

Sección / Columna	Descripción Funcional
Condición	**Lo que sucede**. Descripción clara y verificable de cómo está funcionando hoy el proceso, control o recurso (datos cuantitativos y observaciones cualitativas).
Estado	**Lo que podría suceder.** Descripción del resultado esperado o estándar al que se aspira, alineado con metas institucionales o buenas prácticas.
Impulsor	**Que lo podría impulsar.** Qué cambio, tecnología, práctica o decisión permitiría capturar la mejora. Describe la intervención concreta
Beneficio (Esperado)	**Efecto deseado.** Impacto positivo cuantificable y no cuantificable si se captura la oportunidad. Idealmente en términos de economía, eficiencia y/o eficacia
Recomendación de Mejora	Recomendación con foco en el impulsor y si se precisa en el beneficio esperado

Bloque 8: Opinión de Responsables Actividad Operativa/Escalamiento

Sección / Columna	Descripción Funcional
Hallazgo aceptado por los responsables de La actividad bajo revisión (Si/No)	Señar si los responsables de la actividad bajo revisión están de acuerdo o no con el hallazgo
Justificación de los responsables, en caso de no estar de acuerdo	Describir la fundamentación de los responsables en caso de no estar de acuerdo con auditoría interna
Se requiere Escalamiento / A qué nivel	Señalar si es necesario escalar el tema y a qué nivel dentro de la organización
Resolución del Escalamiento	Describir en resultado de solicitud de escalamiento

f. Hoja 6: "INFORME BORRADOR"

Descripción Estructural y Funcional de la Hoja

Esta hoja consolida y presenta los hallazgos de auditoría en un formato de informe preliminar estructurado, permitiendo validar los resultados con la actividad bajo revisión antes de emitir el informe final. Corresponde a la fase de comunicación de resultados y forma parte del cumplimiento de las *Normas 15.1: Comunicación Final del Trabajo* y *15.2: Confirmar la Implementación de Recomendaciones o Planes de Acción*.

- Permite documentar la retroalimentación con la actividad bajo revisión antes de la versión final del informe.
- Consolida hallazgos de forma estandarizada, facilitando la revisión por supervisores o el Jefe de Auditoría
- Garantiza la trazabilidad entre el análisis técnico (hoja anterior de la planilla) y los trabajos institucionales, cerrando el ciclo del trabajo.
- Esta hoja debe ser revisada por el equipo y validada con la unidad auditada mediante una reunión de cierre.
- Su uso fortalece el enfoque de mejora continua, permitiendo evaluar el cumplimiento efectivo de recomendaciones en el seguimiento.

TIPO DE TRABAJO: Aseguramiento/Asesoramiento
TIPO DE ASEGURAMIENTO: Razonable o Limitado

Bloque 1: Antecedentes Generales del Equipo Auditor y del Trabajo

Sección / Columna	Descripción Funcional
Nombre Trabajo de Auditoría	Identificación del trabajo según el plan anual de auditoría
Fecha del Informe	Identificación de la fecha de emisión del informe
Materia	Especificación de la actividad bajo revisión
Alcance	Cobertura y límites del trabajo (áreas, periodos, procesos)
Objetivos del trabajo de auditoría	Describir lo qué se busca evaluar o verificar en la auditoría
Tipo Objetivo	Institucional, Ministerio o Gubernamental, otros
Opinión Criticidad Macro Enfoque N° 1	Opinión Criticidad Macro según escala para Enfoque N° 1
Opinión Criticidad Macro Otros Enfoques	Opinión Criticidad Macro según escala para Enfoques restantes

Bloque 2: Identificación Estratégica del Tema Auditado

Sección / Columna	Descripción Funcional
Proceso/Subproceso/Etapa/Proyecto/Otro	Identificación de los componentes y elementos revisados en la actividad bajo revisión. Proviene de la **HOJA 5: "REGISTRO DE INFORMACIÓN: IDENTIFICAR, ANALIZAR, EVALUAR Y DOCUMENTAR**

Bloque 3: Hallazgos de Auditoría Contenidos en el Informe

Sección / Columna	Descripción Funcional
Naturaleza del Hallazgo	Gobierno/Gestión de Riesgos/Control
Descripción del Hallazgo (Condición)	Descripción en base a criterios respecto del problema detectado
Opinión Criticidad Micro	Clasificación de la criticad según escala
Criterios	Descripción en base a criterios respecto de normas, políticas o marcos incumplidos
Causa(s) Raíz	Descripción en base a criterios respecto del origen subyacente de la condición obtenido en base a las posibles causas
Efecto(s)	Descripción en base a criterios respecto de las consecuencias del hallazgo (financieras, reputacionales, de control, etc.)
¿Se solicita procedimiento sumarial?	Señalar si se solicita un procedimiento sumarial producto de la gravedad de los hallazgos analizados

Bloque 4: Recomendaciones de Auditoría (Asociadas con Hallazgos)

Sección / Columna	Descripción Funcional
Descripción Recomendación	Propuestas específicas para corregir o mitigar el hallazgo. Propuesta para corregir la causa y mitigar los efectos
Plazo Estimado de implementación	Tiempo estimado para implementar la recomendación en opinión de auditoría interna
Responsable	Área o funcionario encargado de implementar la recomendación en opinión de auditoría interna

Bloque 5: Plan de Acción Acordado (Asociadas con Hallazgos)

Sección / Columna	Descripción Funcional
Descripción Compromiso Acordado	Acción o medidas correctivas acordadas
Plazo de Implementación	Plazo acordado con el responsable de la actividad bajo revisión.
Responsable	Área o funcionario encargado de implementar la acción o compromiso
Evidencia y/o Criterios de Cierre	

Bloque 6: Recomendaciones de Auditoría (Asociadas con Oportunidades de Mejora, si es el caso)

Sección / Columna	Descripción Funcional
Descripción Recomendación de Mejora	Descripción de la recomendación con foco en el impulsor y si se precisa en el beneficio esperado
Plazo Estimado de implementación	Tiempo estimado para implementar la opción de mejora, de acuerdo con el responsable de la actividad bajo revisión
Responsable	Área o funcionario encargado de implementar la recomendación, de acuerdo con el responsable de la actividad bajo revisión

Bloque 7: Plan de Acción Acordado (Asociadas con Oportunidades de Mejora, si es el caso)

Sección / Columna	Descripción Funcional
Descripción Compromiso Acordado	Acción acordada para implementar la opción de mejora
Plazo de Implementación	Plazo acordado con el responsable de la actividad bajo revisión
Responsable	Área o funcionario encargado de implementar la opción de mejora

f. Hoja 7: "SEGUIMIENTO DE RECOMENDACIONES Y/O PLANES DE ACCIÓN"

Descripción Estructural y Funcional de la Hoja

Esta hoja consolida y presenta los resultados del trabajo de seguimiento que deben realizar los auditores internos. Corresponde a la fase de seguimiento de la implementación de las recomendaciones o planes de acción y forma parte del cumplimiento de la Norma *15.2: Confirmar la Implementación de Recomendaciones o Planes de Acción*.

- Permite documentar las actividades de seguimiento de la auditoría interna.
- Ayuda a conocer el estado de implementación de las medidas correctivas
- Si es necesario escalar a las autoridades las situaciones identificadas en el seguimiento
- Conocer los resultados del escalamiento
- Su uso fortalece el enfoque de mejora continua, permitiendo evaluar el cumplimiento efectivo de recomendaciones en el seguimiento.

TIPO DE TRABAJO: Aseguramiento/Asesoramiento
TIPO DE ASEGURAMIENTO: Razonable o Limitado

Bloque 1: Antecedentes Generales del Equipo Auditor y del Trabajo

Sección / Columna	Descripción Funcional
Nombre Trabajo de Auditoría / Código	Identificación del trabajo según el plan anual de auditoría
Fecha del Informe	Identificación de la fecha de emisión del informe
Materia	Especificación de la actividad bajo revisión
Alcance	Cobertura y límites del trabajo (áreas, periodos, procesos)
Objetivos del trabajo de auditoría	Describir lo qué se busca evaluar o verificar en la auditoría
Tipo Objetivo	Institucional, Ministerio o Gubernamental, otros
Opinión Criticidad Macro Enfoque N° 1	Opinión Criticidad Macro según escala para Enfoque N° 1
Opinión Criticidad Macro Otros Enfoques	Opinión Criticidad Macro según escala para Enfoques restantes

Bloque 2: Identificación Estratégica del Tema Auditado

Sección / Columna	Descripción Funcional
Proceso/Subproceso/Etapa/Proyecto/Otro	Identificación de los componentes y elementos revisados en la actividad bajo revisión. Proviene de la **HOJA 5: "REGISTRO DE INFORMACIÓN: IDENTIFICAR, ANALIZAR, EVALUAR Y DOCUMENTAR**

Bloque 3: Hallazgos de Auditoría Contenidos en el Informe

Sección / Columna	Descripción Funcional
Naturaleza del Trabajo	Gobierno/Gestión de Riesgos/Control
ID del Hallazgo	Código único que permite rastrear un hallazgo desde su origen hasta su cierre. Debe ser trazable al informe
Descripción del Hallazgo	Explica de manera clara la condición observada. Debe ser fiel al informe
Opinión Micro	Nivel de criticidad del hallazgo (alto, medio, bajo) según escala definida
Recomendación de Auditoría	Propuestas específicas para corregir o mitigar el hallazgo. Propuesta para corregir la causa y mitigar los efectos

Bloque 4: Verificación del Seguimiento de Medidas Correctivas/ Hallazgos

Sección / Columna	Descripción Funcional
Fecha Real de Cierre	Fecha en que la medida fue implementada completamente y verificada por auditoría interna
% Implementación de Medidas Correctivas	% de avance en la implementación de la medida correctiva de acuerdo con el plan de acción acordado.
Estado Actual Medida Correctiva	Abierto / En Proceso / Cerrado / Retrasado / Medida Modificada o Sustituida / No Implementado / Implementación Parcial / Medida Modificada o Sustituida
Estado Actual Hallazgo	Abierto / En proceso de Validación/ Cerrado
Última Fecha de Seguimiento	Fecha del último análisis o validación realizada por auditoría interna
Conclusiones sobre el Nivel de Riesgo Residual	Opinión sobre si el riesgo residual permanece dentro de los niveles de tolerancia al riesgo definido por la entidad.
Comentarios del Responsable	Si corresponde, justificaciones, explicaciones o actualizaciones entregadas por la unidad responsable de implementar la medida
Fecha de Validación Jefe de Auditoría	Si corresponde, fecha en que el Jefe de Auditoría aprueba formalmente el estado de la medida (especialmente el cierre) conforme a la evidencia presentada

Bloque 5: Escalamiento (Cuando Corresponda)

Sección / Columna	Descripción Funcional
A la Alta Dirección	SI/NO
Fecha de Escalamiento	Fecha en que se escaló el caso a la Alta Dirección debido a atrasos, falta de avance o relevancia del riesgo
Resultados del Escalamiento	Acciones, instrucciones o decisiones adoptadas por la Alta Dirección frente al retraso o incumplimiento. Incluye decisión de escalar al Jefe de Servicio.
Al Jefe de Servicio	Fecha en que se elevó formalmente el caso al Jefe de Servicio. Aplica para hallazgos de alta criticidad o riesgos graves
Fecha de Escalamiento	Fecha en que se escaló el caso al Jefe de Servicio
Resultados del Escalamiento	Medidas adoptadas por la autoridad para asegurar la implementación del plan o reasignar responsabilidades. Incluye decisión de aceptar el riesgo por la autoridad

14 Anexo: Modelo de Madurez para la Planificación del Trabajo en Funciones de Auditoría Interna

5 – OPTIMIZADO

- La función de auditoría interna adopta un enfoque sistemático y proactivo, centrado en los riesgos estratégicos, operacionales y emergentes, utilizando análisis avanzados y la experiencia especializada para diseñar planes de trabajo altamente valorados por los responsables de procesos y demás partes interesadas.
- El proceso de planificación impulsa de forma consistente trabajos que generan aseguramiento relevante, conocimientos prácticos y oportunidades concretas de mejora organizacional.
- Se emplean herramientas analíticas desde las etapas iniciales para enfocar el alcance en las áreas de mayor valor agregado, en conformidad con las *Normas 13.1 (Comunicación durante el trabajo) y 13.2 (Evaluación de riesgos del trabajo).*

4 – GESTIONADO

- La auditoría interna mantiene relaciones sólidas y de confianza con los responsables de procesos y partes interesadas clave, lo que le permite anticiparse a riesgos emergentes y adaptar de manera flexible los planes de trabajo. Esta capacidad de respuesta refuerza su posicionamiento como función proactiva y estratégica dentro de la organización.
- Durante la ejecución del trabajo, se establecen puntos de control que permiten ajustar el alcance con base en el cumplimiento de objetivos o la aparición de nuevas prioridades. Si se constata que los objetivos ya se han logrado o no existen beneficios adicionales por continuar, el trabajo se finaliza anticipadamente y los recursos se reasignan eficientemente *(Norma 13.6).*

3 – DEFINIDO

- El plan de auditoría interna se encuentra alineado con la evaluación anual de riesgos y justifica claramente la priorización del trabajo, en línea con las *Normas 9.1 y 13.1.*
- El enfoque del trabajo se centra en los riesgos clave de la actividad bajo revisión, así como en la forma en que la organización gestiona la gobernanza, el control y los riesgos, cumpliendo con lo establecido en la Norma 13.2.
- El alcance, el nivel de esfuerzo y la asignación de recursos reflejan los riesgos específicos del trabajo y permiten que la auditoría interna tenga un impacto relevante y útil para la entidad.

2 – REPETIBLE

- Los trabajos de auditoría interna se planifican utilizando programas estándar o enfoques genéricos, sin adecuarse al contexto o al perfil de riesgos específico de la entidad. La cobertura puede resultar incompleta respecto a los riesgos más críticos.
- Los planes son uniformes para distintas unidades o ubicaciones, con escasa consideración de la naturaleza del proceso, los recursos disponibles o la oportunidad de la intervención. Esto limita la capacidad de la auditoría interna para aplicar adecuadamente los principios establecidos en la Norma 13.2.

1 – INICIAL

- Los trabajos de auditoría interna se ejecutan con escasa planificación previa, sin una estructura formal ni una evaluación adecuada de riesgos.
- Los informes resultantes tienen un bajo impacto, ya que las pruebas realizadas no se orientan a riesgos significativos ni a objetivos claramente definidos, incumpliendo lo requerido por las Normas 13.1 y 13.2.

Tabla N° 1: Evidencias de Conformidad por Nivel de Madurez – Planificación del Trabajo para Funciones de Auditoría Interna

Nivel	Documentos Recomendados	Actividades Clave de Verificación
5 Optimizado	• Programas de trabajo ajustados dinámicamente según riesgos emergentes • Informes de análisis de datos aplicados en la planificación • Registros de retroalimentación positiva del Jefe de Servicio • Minutas de reuniones de redefinición de alcance • Manuales de planificación por tipo de riesgo o sector	• Revisión de planes adaptados en función de resultados preliminares • Entrevistas con auditores líderes y responsables auditados • Evaluación de uso de herramientas analíticas y de BI para definir alcance • Evidencia documental de realineación de recursos
4 Gestionado	• Programas de trabajo con objetivos revisados durante el proceso • Cronogramas con puntos de control y actualización • Justificación formal de ajustes al alcance • Registro de reasignación de recursos con base en riesgo residual	• Observación de cómo se ajusta el plan en función de resultados intermedios • Análisis de impacto de cambios de alcance documentado • Revisión de evidencia de validaciones técnicas internas
3 Definido	• Plan de trabajo vinculado al Plan Anual de Auditoría y evaluación de riesgos • Documentos de planificación con objetivos, alcance, recursos y cronograma • Matriz de riesgos del trabajo alineada al programa de auditoría • Registro de aprobación del plan por el Jefe de Auditoría	• Verificación de que el plan está justificado por el riesgo • Revisión de trazabilidad desde la matriz de riesgos al programa de trabajo • Entrevistas a auditores sobre el proceso de planificación
2 Repetible	• Programas estándar sin modificaciones • Planes genéricos aplicados a diferentes unidades • Listas de verificación comunes sin criterios diferenciadores • Ejemplos de informes con coberturas uniformes y sin análisis de contexto	• Revisión cruzada de informes similares aplicados a contextos distintos • Entrevistas que revelen falta de adaptación del enfoque • Verificación de falta de criterios técnicos en la planificación
1 Inicial	• Ausencia de planes de trabajo documentados • Ejecución de auditorías sin definición clara de objetivos ni alcance • Informes sin vinculación al análisis de riesgo • Planificaciones improvisadas o verbales	• Revisión de documentos incompletos o inexistentes • Entrevistas que evidencien ausencia de metodología • Evaluación de auditorías realizadas sin planificación previa

CAIGG

CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO

Ministerio Secretaría General de la Presidencia

Guías de Gestión y Servicios de Auditoría Interna (GGSAI)

A cerca de las Guías de Gestión y Servicios de Auditoría Interna (GGSAI)

Para fines de promover la realización del trabajo de auditoría interna en el sector público en Chile (según el Domino IV y V de las NOGAI) el Consejo de Auditoría Interna General de Gobierno (CAIGG) desarrolló la siguiente colección de Guías de Gestión y Servicios de Auditoría Interna (GGSAI):

- GGSAI 1 - Plan de Auditoría Interna
- GGSAI 2 - Plan Estratégico de Auditoría Interna
- GGSAI 3 - Planificación del Trabajo de Auditoría Interna
- GGSAI 4 - Ejecución del Trabajo: Recopilación, Análisis y Evaluación de la Información
- GGSAI 5 - Supervisión del Trabajo de Auditoría Interna
- GGSAI 6 - Comunicación en Auditoría Interna y Formulación de Informes sobre Resultados del Trabajo
- GGSAI 7 - Seguimiento de la Implementación de las Recomendaciones o Planes de Acción
- GGSAI 8 - Gestión de la Calidad en la Función de Auditoría Interna

Propiedad intelectual

El contenido de este documento es de propiedad del Consejo de Auditoría Interna General de Gobierno (CAIGG). Se permite la reproducción parcial de este documento únicamente con fines no comerciales, siempre que se cite adecuadamente la fuente, el título completo y la autoría correspondiente.

Área de Estudios del Consejo de Auditoría Interna General de Gobierno