

OBSERVATORIO SECTORIAL



LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA



Aplicación del Marco Integrado de Control Interno (COSO) en el Sector Público español

El INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la Auditoría Interna como función clave del buen gobierno. En España cuenta con más de 3.200 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

LA FÁBRICA DE PENSAMIENTO es el laboratorio de ideas del Instituto de Auditores Internos de España sobre gobierno corporativo, gestión de riesgos y Auditoría Interna, donde participan más de 150 socios y profesionales técnicos expertos.



AUDITORÍA INTERNA



BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS



OBSERVATORIO SECTORIAL



PRÁCTICAS DE BUEN GOBIERNO

El laboratorio trabaja con un enfoque práctico en la producción de documentos de buenas prácticas que contribuyan a la mejora del buen gobierno y de los sistemas de gestión de riesgos en organizaciones de habla hispana. Además de desarrollar contenido, fomenta el intercambio de conocimientos entre los socios.



Aplicación del Marco Integrado de Control Interno (COSO) en el Sector Público español

Noviembre 2016

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:

Loreto Alonso Berrio, CIA.

Pablo Lanza Suárez, CISA. IGAE

Gregorio Cuñado Ausín. CORREOS

Francisco Javier Fernández Arévalo, ROAC. ADIF

José María Franco Fernández. CANAL DE ISABEL II

Carlos García Bengoechea, CIA, CGAP, CRMA, CCSA, CISA, CRISC. NACIONES UNIDAS

Juan Antonio Garde Roca. AEAT

Héctor Izquierdo Triana. RENFE

Soledad Llamas Tutor, CIA, CCSA, CRMA. CANAL DE ISABEL II

Carlos López Hernanz. FNMT

Esperanza Mainar Jaime. FNMT

Ana M^a Naveira Naveira. INSPECCIÓN GENERAL. MINHAP

Juan Luis Peñaranda Acera. AENA

Carmen Ruiz Conde. AENA

Celedonio Villamayor Pozo. CONSORCIO DE COMPENSACIÓN DE SEGUROS

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

Depósito Legal: M-30127-2016

ISBN: 978-84-945594-1-9

Diseño y maquetación: desdezero, estudio gráfico

Impresión: IAG, SL

Propiedad del Instituto de Auditores Internos de España. Se permite la reproducción total o parcial y la comunicación pública de la obra, siempre que no sea con finalidades comerciales, y siempre que se reconozca la autoría de la obra original. No se permite la creación de obras derivadas.

Es un orgullo para mí presentar este documento de LA FÁBRICA DE PENSAMIENTO, el primero dirigido al Sector Público español, al que analiza y mejora empleando los principios que forman el *Marco Integrado de Control Interno*, cuya última actualización en 2013 por COSO (Committee of Sponsoring Organization of the Treadway Commission), es referencia mundial en la materia.

La Comisión Treadway sobre Control Interno define el control interno como un proceso, responsabilidad del Consejo de Administración, desarrollado por toda la organización y diseñado con el objeto de proporcionar un grado de seguridad razonable en la cobertura de los riesgos que atentan contra la consecución de los objetivos empresariales.

El Marco COSO permite a cualquier organización aumentar y mantener un sistema de control interno que le ayude a cumplir sus objetivos, y que dote a la organización de capacidad de adaptación a los cambios operativos y de negocio del entorno.

Este documento hace un exhaustivo análisis del Marco en referencia al sector público español, incidiendo en todas las cuestiones relevantes a considerar para que cada organización visualice el grado de madurez de su modelo de control interno y acometa las buenas prácticas que le permitan adquirir los adecuados niveles de excelencia en el ámbito del Gobierno Corporativo, Auditoría Interna y Gestión de Riesgos.

Felicito a los autores de esta guía, todos ellos auditores internos que trabajan o han trabajado gran parte de sus carreras profesionales en el sector público, por compartir generosamente su valiosa experiencia. Están ayudando con ello a los gestores de cualquier organización pública a visualizar el grado de madurez de su modelo de control interno para mejorarlo y conseguir los niveles de excelencia óptimos demandados por la sociedad en el ámbito del Gobierno Corporativo, Auditoría Interna y Gestión de Riesgos.

Ernesto Martínez Gómez, CIA, CRMA

Presidente del Instituto de Auditores Internos de España

Índice

RESUMEN EJECUTIVO	06
TAXONOMÍA DEL SECTOR PÚBLICO: EXTENSIÓN DEL SECTOR PÚBLICO	07
METODOLOGÍA APLICADA	09
ANÁLISIS DE LA MADUREZ DE LOS PRINCIPIOS COSO EN EL SECTOR PÚBLICO	11
Componente 1: Entorno de Control	11
Componente 2: Evaluación de Riesgos	16
Componente 3: Actividad de Control	20
Componente 4: Información y Comunicación	23
Componente 5: Supervisión	26



Resumen Ejecutivo

Este documento también puede ser útil para cualquier organización. Analizando los principios del *Marco Integrado*, comprobará el nivel de madurez de su modelo de control interno

El sistema de **control interno** (conjunto integrado y continuo de operaciones, efectuadas por personas de la propia organización) proporciona una **seguridad razonable** –no absoluta– de que los objetivos serán alcanzados.

Recientemente, el *Committee of Sponsoring Organization of the Treadway Commission* ha publicado el nuevo **Marco Integrado de Control Interno**, más conocido como COSO III. Es una guía para diseñar, implementar y desarrollar, y evaluar la efectividad el control interno. Este nuevo *Marco Integrado* permite a cualquier organización aumentar y mantener –de forma efectiva y eficiente– un sistema de control interno que incrementa la probabilidad de cumplir los objetivos de la organización y de adaptarse a los cambios operativos y de negocio del entorno.

El *Marco Integrado* describe las relaciones entre los objetivos –a qué aspira la entidad–, los componentes –necesarios para alcanzar dichos objetivos– y los principios relevantes –los conceptos fundamentales relacionados con los componentes–.

El Instituto de Auditores Internos de España ha creado una Comisión Técnica, formada por profesionales de diversas organizaciones, entidades y empresas relacionadas con el sector público español, que ha analizado el nuevo *Marco Integrado* en referencia a la actividad pública. La diversa procedencia, dentro de las diferentes áreas del sector público, de los

componentes de la comisión técnica (administración central y autonómica, organismos y entidades, sector público empresarial), enriquece este documento desde múltiples y variadas perspectivas, y con sugerentes matices.

Se ha utilizado el **modelo de madurez** para determinar la medida de progreso y se han establecido diferentes niveles de evolución, cada uno de los cuales puede, a su vez, contar con áreas o actividades como objetivo.

Pero este documento no presenta un modelo rígido de evolución, donde siempre lo mejor para cada organización es estar en el nivel más alto simplemente porque es el más evolucionado. Las características propias de cada organización pública deben flexibilizar la interpretación del grado de madurez. Y los estados que define el documento no siempre son secuenciales.

COSO concibe el Control Interno como un proceso integrado en la gestión, que comprende a todos los agentes de la organización, comenzando por los máximos directivos. Aunque el nuevo modelo va más allá, respeta el ámbito de responsabilidad que desempeñan ya órganos prestigiosos de supervisión interna y externa como el Tribunal de Cuentas, la Intervención General de la Administración del Estado, las Intervenciones Generales (órganos autonómicos de control interno), y las Inspecciones de los servicios, con su corres-



pondiente función fiscalizadora o jurisdiccional.

Este documento pretende ayudar a cada organización a visualizar el grado de madurez de su modelo. Para ello describimos los **17 principios que forman el Marco Integrado**, con su correspondiente análisis, que va desde el ambiente de control hasta las labores de información, comunicación y supervisión, pasando por las actividades propias del control interno y evaluación de riesgos.

Aunque en principio este documento se dirige al **sector público español**, también puede ser

útil para cualquier **otro tipo de organización**, que puede comprobar, mediante el análisis de los principios del *Marco Integrado*, en qué situación se encuentran y cuáles son sus niveles óptimos.

Estas buenas prácticas en el ámbito del control interno permiten armonizar los planteamientos seguidos en los sectores público y privado en la búsqueda de unos **adecuados niveles de excelencia** en el ámbito del gobierno corporativo, Auditoría Interna y gestión de riesgos.



Taxonomía del Sector Público: Extensión del Sector Público

El Sector Público está formado por la Administración General y todas aquellas organizaciones, controladas directa o indirectamente por ella, que, en general orientan su actividad a la producción de bienes o servicios públicos. Organizaciones agrupadas bajo los epígrafes de Entidades Públicas y Sector Público Empresarial.

Es complejo un ejercicio completo de taxonomía. Debería abordarse desde un enfoque multidimensional que incluyera la forma jurídica, la naturaleza pública, o no, de los bienes y servicios prestados, la significación económica de los precios ofertados... Este análisis excede al objeto de este capítulo, en el que sólo se pretende presentar una idea de a qué

se refiere cuando se utiliza el término Sector Público.

A la vista de esta limitación, se sugieren tres características generales que definen a las entidades del Sector Público, y que pueden utilizarse al clasificar a una entidad particular dentro del mismo:

- Producen bienes o servicios considerados bienes públicos o que responden a políticas públicas.
- Se financian con presupuestos públicos o con precios definidos en el marco de políticas públicas.
- La toma de decisiones está controlada, bajo cualquier fórmula, por la Administración, a la que además rinde cuentas la entidad.

El sector público está formado por la **Administración General y las organizaciones controladas por ella, que orientan su actividad a la producción de bienes o servicios públicos.**

A efectos del control interno, no debe existir distinción entre el Sector Público estatal, de comunidad autónoma, local o, incluso, supranacional.

En esta propuesta de taxonomía, el documento se abstrae del hecho territorial. A efectos del control interno, no debe existir distinción entre el Sector Público estatal, de comunidad autónoma, local o, incluso, supranacional.

Tampoco se pretende una clasificación exhaustiva. Se proponen cuatro grandes apartados: Administración General, Entidades que operan bajo Derecho Público, Sector Público Empresarial y Organismos Reguladores.

Administración General

Administración General es todo cuerpo de gobierno estructurado sobre una autoridad territorial definida. Baza su actividad en competencias propias.

Las Administraciones Generales ejercen potestades administrativas y se financian con cargo a los Presupuestos Generales del Estado (en adelante, financiación presupuestaria).

Toda Administración General es cuentadante (que debe dar cuenta de los fondos que maneja) de una autoridad central política (el poder legislativo, un consejo, una corporación municipal, un gabinete o el jefe del ejecutivo), electa directa o indirectamente por el cuerpo electoral.

INCLUYE: ministerios, departamentos, consejerías, concejalías, etc...

Entidades que operan bajo Derecho Público

Son organizaciones que operan bajo derecho público, creadas por alguna Administración General (a la que están adscritas), para ejecutar programas y proveer bienes o servicios pú-

blicos. Poseen autonomía de gestión respecto a la Administración General de la que dependen y pueden disponer de un órgano superior colegiado de gobierno.

Para el desempeño de su misión, pueden ejercer potestades administrativas.

Se financian fundamentalmente con el presupuesto, aunque puede recibir ingresos vía tasas o precios públicos.

INCLUYE: organismos autónomos, agencias, universidades, hospitales, ICO, INCIBE, Red.es, CSIC, etc...

Sector Público Empresarial

Son entidades dotadas de personalidad jurídica y patrimonio propio, constituidas en el ámbito más alejado del núcleo central del Sector Público, la Administración General. Constituidas con fórmulas de derecho administrativo o directamente como sociedades de capital. Normalmente, están sujetas al derecho privado, aunque adicionalmente dependen en parte de la regulación general del Sector Público y de la normativa específica de aplicación a cada entidad. Los estatutos definen su misión y actividad, y los órganos de gobierno sus objetivos.

Estas entidades tienen sus propios órganos de gobierno, según sea su forma jurídica. No obstante, la titularidad de los derechos que sustentan el poder de decisión es de la Administración General u otras Entidades Públicas. Producen bienes y servicios en el mercado y se financian mayoritariamente vía precios (públicos o de mercado). Pueden colaborar con Agencias o las propias Administraciones en los programas públicos o en la provisión de

bienes y servicios públicos, pero siempre mediante contrato y precio, y un marco temporal limitado.

El Sector Público Empresarial INCLUYE entidades públicas empresariales, como por ejemplo, en el ámbito del Gobierno central: Adif, ADIF-Alta Velocidad, ENAIRE, Fábrica Nacional de Moneda y Timbre, Puertos del Estado (y cada una de las Autoridades Portuarias)...; también incluye empresas públicas: las empresas del Grupo SEPI, y el Grupo de Empresas Patrimonio, Aena, S.A., las sociedades del grupo Renfe Operadora; y engloba a la em-

presa pública a nivel de Comunidad Autónoma: Canal de Isabel II Gestión, S.A. ...

Organismos reguladores

Son los Organismos que regulan o supervisan externamente un determinado sector o actividad económica, en este caso con independencia funcional o una especial autonomía respecto de las Administraciones Generales.

INCLUYE: Banco de España, Comisión Nacional de los Mercados y la Competencia, Comisión Nacional de los Mercados de Valores, etc.

El sector público lo forman la Administración General, Entidades que operan bajo Derecho Público, las Entidades Públicas Empresariales y Organismos Reguladores



Metodología aplicada

El objetivo del *Marco de Control Interno*, publicado por COSO, es "apoyar a la dirección a mejorar el control en la organización" y "proporcionar herramientas para mejorar la capacidad para supervisar el control interno". Un objetivo que se alcanza a través de 5 componentes, desarrollados en 17 principios.



Para el análisis, la Comisión Técnica del Instituto de Auditores Internos de España ha aplicado un modelo de madurez a COSO (2013), tratando de identificar los pasos que una organización del sector público emprende en el camino de definir, implantar y poner en funcionamiento los 17 principios. La metodología pone de manifiesto la interactividad entre los principios.

La descripción de los 5 niveles son:

Nivel 1 · Entorno legal

Aspectos externos que potencian el principio de seguridad desde fuera de la organización. Básicamente, esto se refiere al papel que juegan las leyes, reglamentos y estatutos a la hora de estimular, u obligar, al diseño e implan-

Los objetivos de apoyar a la dirección en la mejora del control de la organización y proporcionar herramientas para mejorar su supervisión se alcanzan a través de 5 niveles desarrollados en 17 principios.

tación de los principios individuales en cada organización del sector público. Queda, por tanto, fuera de la capacidad de actuación de la unidad.

Nivel 2 · Actividades silos

Es un nivel mínimo de definición del principio dentro de la organización, que abarca las normas, estatutos, procedimientos, creación de comisiones o unidades internas; y reflejan la inquietud de la organización por asimilar y poner en marcha internamente el principio de control interno.

Nivel 3 · Actividades integradas en un proceso

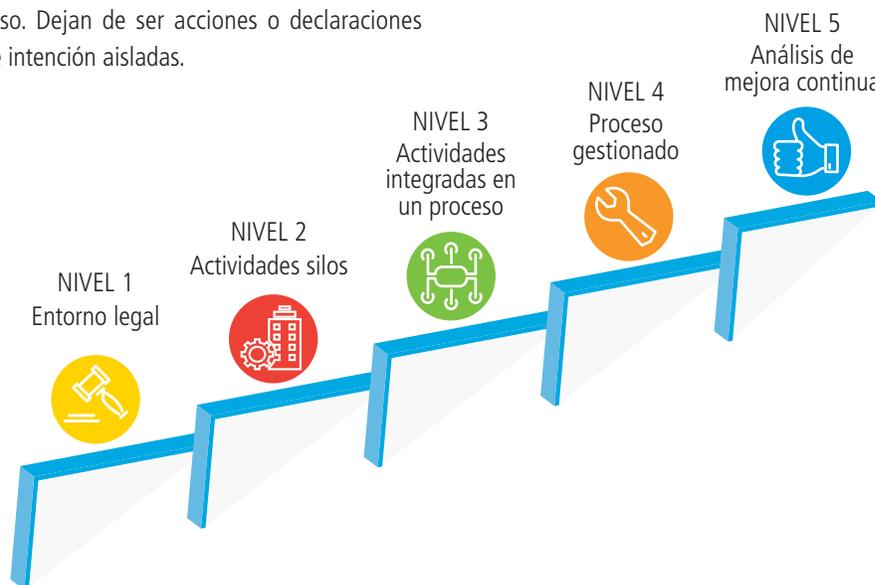
En este nivel, el desarrollo del principio de control interno queda definido como un proceso. Dejan de ser acciones o declaraciones de intención aisladas.

Nivel 4 · Proceso gestionado

El proceso de control ya es, a su vez, objeto de revisiones internas. De esta forma, la organización identifica cambios internos o externos, o el mal funcionamiento del proceso y lo adapta, e incluso sanciona irregularidades.

Nivel 5 · Análisis de mejora continua

El propio proceso de control interno es objeto de un análisis permanente, que permite incorporar las mejores prácticas y su optimización.





Análisis de la madurez de los principios COSO en el Sector Público

En este análisis se parte de la definición de COSO de Control Interno; luego se introduce cada componente; y al final, se aplica cada principio asociado al modelo de madurez.

Según COSO, “el Control Interno es un proceso llevado a cabo por los órganos de gobierno, la dirección y el resto del personal de una organización, diseñado con el objeto de proporcionar un grado de aseguramiento razonable para la consecución de los objetivos relati-

vos a las operaciones, a la información y al cumplimiento.”

El Control Interno es, por tanto, un proceso realizado por personas que se puede adaptar a la estructura de cada organización. El desarrollo de un modelo de madurez (al ser un proceso) no es estático y se puede adaptar a la diversidad del sector público.

Al tratarse de un proceso que implica contemplar la madurez de una organización, el control interno se puede adaptar a la diversidad del sector público.

COMPONENTE 1: ENTORNO DE CONTROL

Según el *Marco Integrado de Control Interno* de COSO, el entorno de control es el “Conjunto de normas, procesos, y estructuras que

constituyen la base sobre la que se desarrolla el control Interno de la organización” y “tiene una influencia muy relevante sobre el resto de los componentes”.



En el entorno de control hay que valorar especialmente el compromiso con la integridad y los valores éticos, y las tareas de formación y comunicación de este compromiso a lo largo y ancho de toda la organización, en todos sus niveles; así como la capacidad de validar su cumplimiento.

El *Estatuto Básico del Empleado Público* establece los principios de conducta de los em-

COSO aconseja identificar responsabilidades y asegurar las competencias para evitar conflictos de interés entre el personal con responsabilidades de control interno.

pleados públicos; sin perjuicio de otras regulaciones específicas sobre Normas de Conducta, tales como la del personal de las Cortes Generales, Asambleas Legislativas, Jueces, Magistrados, Fiscales, Fuerzas Armadas, Fuerzas y Cuerpos de Seguridad, y otra legislación adicional.

No se trata de modificar estos principios, sino de adaptarlos, con sus peculiaridades, en cada caso. COSO recomienda difundir en las or-

ganizaciones el compromiso con los valores éticos para lograr que sea real. Pero también aconseja evitar situaciones de conflicto de intereses entre el personal con responsabilidades de control interno. Para ello, a partir de estructuras organizativas hay que identificar dichas responsabilidades y asegurarse de que las personas implicadas tienen las habilidades y competencias necesarias para desempeñar sus funciones.

Principio 1: La organización demuestra compromiso con la integridad y los valores éticos.

NIVEL 1

- Se refuerza el compromiso con los valores éticos a través de códigos de conducta a nivel estatal y autonómico.
- Se revisan y actualizan los principios de conducta de los empleados públicos (funcionarios, interinos, personal laboral, y eventual).
- Se define un código de buena conducta respecto de los altos cargos.



NIVEL 2

- Se elabora y documenta dentro de la organización un Código de Ética y las normas de conducta que desarrollen los principios establecidos con carácter general y se adapten a las circunstancias concretas del entorno y den respuesta a los conflictos éticos de la organización.
- Se imparte formación sobre los programas éticos.



NIVEL 3

- Se expresa un compromiso formal (escrito) con el Código de Ética de todos los empleados.
- Se comprueba el cumplimiento del código de conducta y la eficacia del mismo. Se adoptan medidas disciplinarias en caso necesario.
- Se incluye el comportamiento ético en la descripción de los puestos de trabajo.
- Se informa a los grupos de interés de su existencia y contenido.
- La formación sobre los programas éticos se imparte a todo el personal, al menos cada 3 años.



NIVEL 4

- Se revisa y actualiza anualmente el Código de Ética.
- Se facilita la participación de los empleados, que pueden elevar preguntas éticas y completar cuestionarios relativos al cumplimiento del Código de Ética.
- Se incorpora en las decisiones disciplinarias a RRHH, legal y cumplimiento.



NIVEL 5

- Se realizan revisiones externas que aseguren un alineamiento con las mejores prácticas.



Principio 2: El órgano de gobierno demuestra independencia de la dirección y supervisa el desempeño del sistema de control interno.

NIVEL 1

- Se manifiesta expresamente con rango de Ley que la responsabilidad sobre el control interno recae sobre los órganos de gobierno*, la dirección y empleados del Sector Público, y no sobre sus órganos de supervisión.



NIVEL 2

- Se recoge su responsabilidad en la supervisión del Control Interno en los estatutos o normas de funcionamiento de los órganos de gobierno de la organización.
- Se manifiesta la independencia de los órganos de gobierno respecto a la dirección ejecutiva en las normas internas de la organización.



NIVEL 3

- Se concretan en los estatutos los criterios para garantizar su independencia frente a la dirección; se evitan conflictos de interés y se exige capacitación para las funciones de gobierno. Por ejemplo: permanencia en el cargo, cualificaciones de sus miembros, conflictos de interés, composición, etc.
- Se integran, en la medida de lo posible, miembros independientes
- Se dispone de órganos de control, comisiones de control o Comisión de Auditoría con una unidad de Auditoría Interna independientes, como apoyo en el ejercicio de su responsabilidad.



NIVEL 4

- Se revisan periódicamente los criterios de independencia y se evalúa su cumplimiento.
- Se tienen en cuenta cambios en los entornos externos e internos.
- Se mantiene una comunicación fluida con los órganos de control (IGAE, inspección general o/y unidad de Auditoría interna).



NIVEL 5

- Se realiza una validación externa.
- Se alinea con las mejores prácticas.
- Satisfacción de los grupos de interés por el gobierno corporativo.



* Dependiendo de la tipología y unidad del sector público, el órgano de gobierno puede ser el Consejo de Ministros, los Ministros y sus homólogos en las CCAA, los Consejos de Gobierno, los Consejeros, los Plenos de los Ayuntamientos, los Consejos Rectores, Consejos de Administración, etc.

Principio 3: La dirección establece, con la supervisión del órgano de gobierno, las estructuras, líneas de reporte y niveles de autoridad y responsabilidad apropiados para lograr los objetivos.

NIVEL 1

- Existe una definición de la estructura organizativa de la Administración General o entidad, bajo criterios de gestión financiera, eficacia y eficiencia, evitando duplicidades en las funciones, contemplando una adecuada segregación de funciones y asegurando la supervisión.



NIVEL 2

- Se desarrollan dentro de la organización manuales organizativos que favorezcan la toma de decisiones y supervisión eficiente y oportuna.
- Se incluyen líneas de responsabilidad información y comunicación interna y externa.
- Se delega la responsabilidad en base a capacidades demostradas.



NIVEL 3

- Se evitan situaciones de vacío de responsabilidad o información a través de órganos transversales que permiten que se comparta la información y que toda la organización reaccione para la consecución de los objetivos y la toma de decisiones. En ocasiones estos órganos tienen carácter ejecutivo (comités de cumplimiento, cobros, calidad...).
- Se integra la estructura a los procesos y a las políticas internas.
- Se utiliza la informática como elemento para definir la estructura.
- No se aceptan riesgos inapropiados en la estructura (por ejemplo, se gestionan los riesgos sobre la externalización de servicios).



NIVEL 4

- Se revisa periódicamente la estructura, de acuerdo con los cambios en los entornos externos e internos, y ajustes de la estrategia, políticas, etc.
- Se identifican ineficiencias en la estructura, problemas de comunicación o ejecución de políticas.



NIVEL 5

- Hay un proceso de evaluación y mejora continua.
- Posibilidad de validación externa.
- Alineamiento con las mejores prácticas.



Principio 4: La organización demuestra compromiso con la estrategia para atraer, desarrollar y retener a profesionales competentes.

NIVEL 1

- Se actualizan los procedimientos regulados para la cobertura de puestos o captación de recursos en base a 4 criterios:
 1. Análisis de las necesidades del puesto, viabilidad y continuidad.
 2. Conformidad entre las necesidades y características del candidato.
 3. Aceptación de solicitudes en base a principios de igualdad y no discriminación.
 4. Selección a través de tribunales independientes.
- Mecanismos de promoción interna dentro del grupo. Pruebas para el paso de un grupo a otro.
Se mantienen los 4 criterios anteriores.



NIVEL 2

- Se realiza dentro de la organización un análisis de necesidades de recursos, que incluye la renovación y amortización de puestos.
- Se desarrollan en la organización procedimientos de selección que respeten y desarrollen los mecanismos de promoción interna.
- El procedimiento de promoción interna incluye publicación, y publicidad del puesto y los requerimientos.
- Se elabora un Plan de Formación.



NIVEL 3

- Se planifican, en base a la estrategia y con criterios de eficacia y eficiencia, las necesidades de recursos y su cobertura. Se tienen en cuenta empleos públicos, puestos de libre disposición, asesores y empleados laborales.
- Se identifican unidades o colectivos que potencian y ponen en valor el *expertise* y la formación recibida en tareas, funciones y responsabilidades.
- Se mantienen las carreras profesionales alineadas con las evaluaciones de desempeño.
- Los puestos de libre disposición o selección externa cumplen con los requisitos de capacitación, profesionalidad y experiencia.



NIVEL 4

- Se revisan, evalúan y actualizan las coberturas de puestos; se analizan desviaciones y cambios en la estrategia y gestión de riesgos.
- En consecuencia, se adapta el plan de formación, y carreras profesionales.
- Se establecen créditos de formación para los empleados del sector público.
- Se pone en marcha un Plan de Gestión del Conocimiento.



NIVEL 5

- Se obtiene una evaluación externa sobre los procedimientos de selección, promoción y evaluación de desempeño.



Principio 5: La organización evalúa el rendimiento y define la responsabilidad de las personas en relación con el control interno. Aplica la responsabilidad por la rendición de cuentas.

NIVEL 1

- Se recoge en la norma el deber de que los máximos responsables de la organización rindan cuentas sobre el cumplimiento de objetivos al Parlamento y a la ciudadanía (ley de Transparencia).
- Se legisla sobre la evaluación del desempeño y sobre la necesidad de que los objetivos individuales estén alineados con los objetivos de la organización.



NIVEL 2

- Se detallan en manuales o instrucciones las responsabilidades de los diferentes niveles de dirección en relación con el cumplimiento de los objetivos; se detallan también los sistemas de detección de desviaciones y las medidas correctoras. Por ejemplo: bajos niveles de calidad, desviación sobre objetivos, presupuesto, norma de conducta...)
- Se definen evaluaciones de desempeño adecuadas a la actividad sobre objetivos de la organización o del departamento o unidad, como base para fijar la retribución variable.
- Se aplican criterios de medición de cumplimiento de objetivos y control interno a terceros contratados.



NIVEL 3

- Las evaluaciones del desempeño miden objetivos individuales de empleados públicos con responsabilidad en el funcionamiento de los equipos, alineados con la estrategia y habilidades individuales, y son descendentes. Se acuerdan planes de acción con el evaluado.
- Se incorporan otros mecanismos de recompensa: medallas por servicios prestados, mayor visibilidad y reconocimiento en la organización, etc...
- Se evita la presión excesiva en el personal, lo que puede provocar comportamientos indeseados y conflictos entre los objetivos de los distintos grupos de interés.



NIVEL 4

- Se revisan los criterios de evaluación de desempeño periódicamente, para mantener su contribución a un cumplimiento equilibrado de objetivos y del código de conducta.



NIVEL 5

- Se desarrollan las mejores prácticas en incentivos, medición y evaluación de empleados.



El siguiente paso tras la identificación de objetivos es identificar y evaluar los riesgos con un proceso dinámico e interactivo.

COMPONENTE 2: EVALUACIÓN DE RIESGOS

Las organizaciones gestionan los riesgos que amenazan sus objetivos. Por tanto, la definición de unos objetivos claros es el primer paso para evaluar los riesgos. Los objetivos claros de una organización deben abarcar obligaciones, compromisos de cumplimiento presupuestario y de legalidad; objetivos estratégicos, de información, y aquellos que la Dirección determina idóneos para el cumplimiento de su misión y visión.



Una vez que la organización dispone de objetivos claros, el siguiente paso es identificar y evaluar los riesgos con un proceso dinámico e interactivo. El riesgo de fraude debe ser con-

templado con políticas antifraude. También se deben considerar los cambios que, en el entorno interno o externo, afectan a la gestión de riesgos.

Principio 6: La organización define los objetivos con suficiente claridad para identificar y evaluar los riesgos relacionados.

NIVEL 1

- Se establece por ley, y se desarrolla en un reglamento, la obligatoriedad de identificar los objetivos y publicarlos. Se identifican las obligaciones/compromisos de cumplimiento presupuestario, "cumplimiento del principio de legalidad" ⁽¹⁾, objetivos estratégicos.
- Se establecen mecanismos de supervisión de los objetivos.



NIVEL 2

- Se fijan los objetivos (estratégicos, operativos, cumplimiento presupuestario, "cumplimiento del principio de legalidad") de la organización alineados con los objetivos estratégicos del sector público; y se incorporan aquellos que aportan mejoras en la eficiencia y eficiencia ante la misión encomendada. Se valora la carga de trabajos y recursos necesarios.
- Se asigna la responsabilidad en el cumplimiento de objetivos.
- La dirección define los niveles de tolerancia de los objetivos, que señalan las alertas ante los niveles de incumplimiento.
- Los objetivos y niveles de tolerancia son medibles, cuantitativa y cualitativamente.
- Se aprueban, por parte de los órganos de gobierno y la alta dirección, los objetivos anuales o en su caso plurianuales.
- Se miden desviaciones.
- Se informa sobre los objetivos financieros y no financieros a la organización. Se difunden los objetivos en cascada a los niveles inferiores de la organización.



NIVEL 3

- Tanto objetivos como niveles de tolerancia están alineados con la misión, el plan estratégico, y los planes operacionales. Se identifican los riesgos que amenazan el cumplimiento de los objetivos.
- Los objetivos se desglosan en subobjetivos a nivel apropiado.
- El seguimiento de las desviaciones va acompañado de planes de acción, y forma parte de un proceso continuo.
- Se automatiza la información aportada por los indicadores y los controles. Los criterios de medición de objetivos y niveles de tolerancia evitan interpretaciones subjetivas.
- Existen actividades de control para aumentar la probabilidad de alcanzar los objetivos.
- La responsabilidad, a nivel de cumplimiento de objetivos, es asumida por toda la organización.



NIVEL 4

- Se revisan y actualizan los objetivos con la periodicidad necesaria, según los cambios de entorno e internos.
- Se evalúa la comunicación sobre el cumplimiento de los objetivos (financieros, no financieros y de cumplimiento) para asegurar su fiabilidad. Esta evaluación es oportuna (en tiempo) y la llevan a cabo los órganos de control competentes.
- Los órganos de gobierno u organismos delegados tienen acceso libre e independiente a las evaluaciones de fiabilidad de las información sobre el cumplimiento de objetivos.
- Se da publicidad a la sociedad en general sobre el cumplimiento de los objetivos.



NIVEL 5

- La organización tiene formalizado un plan de contingencia que permite identificar, y reaccionar, ante acontecimientos extraordinarios que puedan comprometer la estrategia de la Compañía.
- Posibilidad de validación externa.
- Alineamiento con las mejores prácticas.
- Se analiza la conveniencia de realizar encuestas de satisfacción sobre el procedimiento de medición y seguimiento de objetivos.



1. Los objetivos de cumplimiento de legalidad no deben entenderse como una opción para el incumplimiento, sino como una necesidad de destinar recursos, planificarlos e implantar controles que aseguran su cumplimiento.

Principio 7: La organización identifica los riesgos para lograr los objetivos en todos los niveles, y los analiza para determinar cómo se gestionan.

NIVEL 1

- La responsabilidad de los administradores públicos de considerar y gestionar los riesgos sobre el cumplimiento de los objetivos y sobre los recursos del sector público está recogida en la normativa.



NIVEL 2

- Se identifican riesgos clave y se define el Mapa de Riesgos por importancia.
- Se identifican los controles que mitigan los riesgos y medidas e indicadores de gestión.
- El proceso de identificación y gestión de riesgos se realiza de forma independiente por las diferentes unidades de la organización. No abarca a toda la organización ni a todos los objetivos de la organización.



NIVEL 3

- Se identifican y evalúan los riesgos que amenazan a todos los objetivos. Se evalúan los riesgos al menos una vez al año. Se incluyen en el análisis los riesgos tecnológicos (internos o externalizados) y de fraude.
- La definición de las políticas para la evaluación de los riesgos sobre objetivos y recursos permite definir el "apetito al riesgo" a través del impacto y probabilidad de ocurrencia.
- Los órganos de gobierno u órganos delegados (comisiones) aprueban y supervisan la gestión de riesgos, vigilando su implantación y eficacia, y su aportación a la toma de decisiones.
- Se definen los roles en la gestión de riesgos: evaluador, gestor, y validador de la eficacia de los controles. Se conserva la objetividad e independencia en su función.
- Se implantan planes de continuidad.



NIVEL 4

- El Mapa de Riesgos establecido es acorde con la estrategia de la compañía.
- Existe una efectiva comunicación de la existencia del sistema de gestión de riesgos a todos los niveles.
- Se mitiga o acepta el impacto o probabilidad de ocurrencia de los riesgos críticos o altos que amenazan los objetivos y se realiza un seguimiento de las acciones acordadas.
- Se evalúa el proceso de gestión de riesgos mediante autoevaluación o seguimiento de la eficacia de las acciones correctivas.
- El proceso de gestión de riesgos es evaluado por los órganos de supervisión.



NIVEL 5

- El proceso de gestión de riesgos es validado externamente.



Principio 8: La organización, al evaluar los riesgos para conseguir los objetivos, considera la probabilidad de fraude.

NIVEL 1

- La normativa expresa de forma explícita la responsabilidad de los órganos de gobierno de evaluar el riesgo de que cometan fraude la dirección, el personal y los proveedores de servicios; y de implantar las políticas antifraude efectivas.
- Se fomenta el desarrollo de políticas internas contra el fraude.



NIVEL 2

- La organización identifica los factores de riesgos que incrementan los diferentes tipos de fraude. Por ejemplo: no existen manuales de procedimientos anti fraude o no están actualizados, no se comunican; o no existen normas de conductas de la dirección; la entidad tiene una historia de prácticas cuestionables o de investigaciones con hallazgos de fraude; falta documentación clave; hay fórmulas poco habituales de contratación o transacciones o gastos no autorizados; errores u omisiones continuos en los informes financieros; incentivos; presiones; oportunidades para acceder a los activos...
- Se evalúa cada uno de los riesgos de fraude identificados y se diseñan KRIs.



NIVEL 3

- Los procedimientos antifraude son claros y conocidos por la organización.
- No se tolera el fraude. Se fija un apetito de riesgo de fraude cero.
- Se investiga o comunica los indicios de fraude a las unidades de investigación de fraude competentes. Se establece un procedimiento de comunicación interna de los indicios de fraude.
- Se informa a los órganos de gobierno del resultado de las investigaciones de fraude y de las investigaciones en curso; siempre que no formen parte ellos mismos de esas investigaciones y sean parte de las propias evaluaciones de riesgos.



NIVEL 4

- Se evalúa la eficacia de las políticas antifraude. Si es necesario, se realizan cambios en las unidades operativas, procesos de negocio y actividades de la organización.
- Se evalúa el procedimiento de gestión de riesgo de fraude (identificación evaluación y planes de acción).
- Se evalúan periódicamente los controles para detectar o prevenir el fraude y se adaptan en función de los resultados, para mejorar su eficacia.



NIVEL 5

- Periódicamente las políticas antifraude se someten a evaluación por expertos independientes.
- Los controles internos se retroalimentan constantemente y se someten a la evaluación periódica de expertos independientes.



Principio 9: La organización identifica y evalúa los cambios que pueden afectar significativamente al sistema de control interno.

NIVEL 1

- La normativa expresa de forma explícita la responsabilidad de los órganos de gobierno dentro del proceso de gestión de riesgos al considerar los cambios externos, internos y legales que afectan a la consecución de los objetivos.



NIVEL 2

- Se identifican escenarios de riesgos como parte del proceso de gestión, para considerar los diferentes cambios externos e internos que puedan afectar a los objetivos.
- Se diseñan procedimientos y se prepara al personal para la gestión del cambio.



NIVEL 3

- Se evalúa el escenario en términos de probabilidad y se define, para los escenarios que sean medibles, un conjunto de métricas significativas usadas de forma sistemática para identificar los cambios (caída del PIB, variaciones en el IVA...).



NIVEL 4

- Se asocian planes de acción y de contingencia a los cambios de escenario en la evaluación de riesgos.
- Se evalúan los riesgos asociados a los cambios producidos, y se actualiza el mapa de riesgos.



NIVEL 5

- La organización está volcada en la mejora continua, mediante la implementación de alertas que permitan identificar los cambios significativos con suficiente antelación.



COMPONENTE 3: ACTIVIDAD DE CONTROL

Según COSO la actividad de control la forman "las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se llevan a cabo las instrucciones de la dirección para mitigar los riesgos que incidan en el cumplimiento de los objetivos".

La actividad legislativa promueve la normalización de los procedimientos, además del control sobre presupuestos, contabilidad, eficacia y eficiencia. Por otro lado, el incremento

En las áreas donde no existe la segregación de funciones, la dirección debe implantar actividades de control alternativas.



de la tecnología ha dado lugar a un plan nacional de seguridad de los Sistemas de Información y un Plan Nacional de Interoperabilidad. La segregación de funciones se enmarca

dentro de las actividades de control. Sin embargo, en aquellas áreas donde no existe, la dirección debe implantar actividades de control alternativas.

Principio 10: La organización define y desarrolla actividades de control que contribuyen a mitigar los riesgos hasta niveles aceptables para el logro de los objetivos.

NIVEL 1

- Se elabora legislación básica de control interno y se implementan las actividades de control para entidades del sector público sobre presupuestos, control presupuestario, contabilidad, eficacia y eficiencia, y normalización de procedimientos.
- Se promueve la comunicación de la legislación a los grupos de interés.



NIVEL 2

- Los gestores analizan los propios indicadores y medidas ligados tanto a la actividad como a los objetivos y acciones de respuesta al riesgo.
- Se implantan controles detectivos sobre el funcionamiento de las operaciones y transacciones en los niveles medio y bajo de la organización, como primera línea de defensa, y se realiza el seguimiento de la actividad.
- Los controles son esporádicos.
- Se implanta a lo largo de la organización un criterio claro de segregación de funciones: autorización, proceso y registro, revisión y contacto directo con los activos.



NIVEL 3

- Se desarrollan actividades de control, destinadas a mitigar los riesgos, a todos los niveles y de forma integrada.
- A nivel entidad se incluyen los procesos de gestión de riesgos, entorno de control, cierres financieros. Y también a nivel transaccional sobre operaciones y acciones o proyectos.
- Se analiza la periodicidad de los controles de acuerdo con los riesgos y se comunican los resultados.
- Se implantan controles preventivos y automatizados, periódicos y regulares. Se aumenta el alcance del control.
- Se ponen en marcha controles sobre fraude y conductas.
- Se validan desde la segunda línea de defensa la eficacia y eficiencia de los controles.



NIVEL 4

- Se realizan autoevaluaciones de la calidad del control desde las unidades.
- Se evalúan la eficacia y eficiencia de los procesos de gestión de riesgos, control interno y gobierno, en respuesta a los riesgos a través de la tercera línea de defensa.
- Auditoría Interna generalmente cumple con las *Normas Internacionales para la Práctica Profesional de la Auditoría Interna*, es independiente y objetiva.
- Auditoría Interna se coordina con la segunda línea de defensa.



NIVEL 5

- Existe anticipación a los nuevos riesgos y se es innovador siendo un referente en actividades de control (*benchmark*).



Principio 11: La organización define y desarrolla actividades de control sobre la tecnología en la entidad para apoyar la consecución de los objetivos.

NIVEL 1

- A nivel legislativo, se cuenta con un plan nacional de seguridad de los Sistemas de Información y con un plan nacional de Interoperabilidad.
- Se elabora legislación básica sobre el uso de la tecnología en la gestión pública.
- Se promueve la comunicación de la legislación a los grupos de interés.



NIVEL 2

- Se informatizan la mayoría de tus procesos.
- Se sigue un sistema de soporte y documentación de los desarrollos tecnológicos implantados y sus desarrollos posteriores.
- Se establecen políticas concretas para regular el acceso lógico a los aplicativos y sobre algunos de sus controles.
- Sobre la gestión de la seguridad en TI, las responsabilidades operacionales están asignadas a un coordinador, si bien son limitadas. Se desarrollan políticas de seguridad, pero los mecanismos no son adecuados. Existe información sobre seguridad, pero sobre todo como iniciativa individual.
- Se usan controles automáticos detectivos sobre operaciones y transacciones en la primera línea de defensa.



NIVEL 3

- Se definen con claridad los controles generales y sobre los aplicativos.
- Se implantan controles informatizados preventivos.
- Se controla la adquisición y el mantenimiento de la tecnología.
- Se crea un Plan de Seguridad de la Información.
- Se realizan pruebas de seguridad estandarizadas. Se emiten informes sobre la seguridad de los Sistemas de Información, coordinados con la seguridad general de la entidad y ligados a los objetivos operacionales.
- Se planifica formación para responder a necesidades y riesgos de seguridad.
- Se valida desde una segunda línea de defensa la eficacia y eficiencia de los controles automáticos y del uso de la tecnología.
- se amplía el uso de la tecnología en la detección de errores, excepciones, irregularidades de fraude y conductas.



NIVEL 4

- La Dirección asegura el desarrollo y mantenimiento de un plan de infraestructura técnica. Se tiene en cuenta el impacto potencial de la evolución de las tecnologías. Se definen planes de migración para introducir nuevas tecnologías.
- Se aprueba y evalúa el plan de seguridad periódicamente para comprobar su buen funcionamiento.
- Se evalúan los indicadores clave de riesgo; se adapta el plan de seguridad según un proceso de mejora continua.
- Se realizan autoevaluaciones de controles automáticos e infraestructuras tecnológicas.
- La actividad de Auditoría Interna evalúa la exposición al riesgo de los sistemas de información de la organización. (NPPAI 2120.A1)



NIVEL 5

- Las orientaciones del plan de infraestructura técnica están definidas en función de estándares internacionales.
- El plan de infraestructura técnica es susceptible de adaptarse a las modificaciones del entorno. Se aplica un proceso continuo de mejora.



Principio 12: La organización implementa las actividades de control con políticas que establecen las líneas generales del control interno y con procedimientos que concretan dichas políticas.

NIVEL 1

- Se desarrollan normas con los procedimientos legales.
- Se promueve la comunicación de la legislación a los grupos de interés.



NIVEL 2

- Se documentan y formalizan los procedimientos legales.
- Se desarrollan e informatizan los procedimientos adaptados a la organización, objetivos y riesgos (manuales, protocolos, instrucciones).
- Se definen controles para asegurar el cumplimiento de los procedimientos.



NIVEL 3

- Se diseña el mapa de procesos, se identifican los que son clave y se pone a su cargo a personas competentes, con autoridad suficiente.
- Se hace seguimiento de los controles y sus desviaciones.
- Se toman decisiones y se desarrollan planes de acción ante las desviaciones.



NIVEL 4

- Se actualizan los procedimientos y controles de acuerdo a los cambios internos y externos y a los nuevos riesgos.



NIVEL 5

- Se certifican los procedimientos clave de la organización, se innova y se es referente (*Benchmark*).



COMPONENTE 4: INFORMACIÓN Y COMUNICACIÓN

Según el *Marco Integrado*, éste es el "proceso continuo de proporcionar, compartir y obtener la información necesaria". Por tanto solo existe si se interactúa con el resto de los componentes.

La información, sea interna o externa, debe ser relevante y de calidad.

La información debe fluir en todas direcciones, hacia arriba hacia abajo, y en todos los niveles.



Sea interna o externa, la información debe ser relevante y de calidad, fluyendo en todas las direcciones y niveles.

Principio 13: La organización obtiene, genera y utiliza información de calidad relevante para respaldar el funcionamiento del control interno.

NIVEL 1

- Se define en los órganos de gobierno la responsabilidad de mantener un sistema de información (personas, procesos y tecnología) que permita obtener, generar, utilizar y comunicar (interna o externamente) información para rendir cuentas, analizar el desempeño o evaluar el cumplimiento de objetivos. Se entiende como un componente más del control interno. El proceso debe permitir identificar información relevante y de calidad.



NIVEL 2

- Se obtiene la información de forma discontinua a lo largo de los componentes de control interno y su distribución interna o externa es reactiva (por ejemplo: resultado de la evaluación de riesgos, desviaciones sobre los controles críticos o resultados de las evaluaciones continuas o independientes).
- La información se identifica y obtiene de forma esporádica y básicamente sobre requerimientos de la Dirección u órganos de gobierno.
- Los controles sobre la información son, por tanto, esporádicos.



NIVEL 3

- Se identifica la información relevante de los procesos clave de cada componente.
- Generan la información personas autorizadas y fácilmente identificables.
- Se revisa la información, con controles de calidad posteriores, que implican frecuentemente reelaboración y nuevas búsquedas.
- Se consigue consistencia (coherencia) entre distintas fuentes.



NIVEL 4

- Los sistemas de información procesan y transforman datos relevantes en información de utilidad.
- Se mantiene actualizada la información frente a los cambios internos y externos.
- Se revisa la calidad de la información con controles preventivos para minimizar costes de reelaboración.



NIVEL 5

- Se diseña e implanta un proceso general de garantía de calidad de la información. Se tiene en cuenta el mapa de sistemas (PSI) y los objetivos.
- El proceso contempla los atributos de fiabilidad, actualidad, precisión, protección, retención, suficiencia, puntualidad, validez y verificabilidad.



Principio 14: La organización comunica internamente información necesaria para respaldar el funcionamiento del control interno, incluidos los objetivos y las responsabilidades sobre dicho control.

NIVEL 1

- Se define en los órganos de gobierno la responsabilidad de fijar y mantener canales de comunicación internos tanto entre la dirección y el órgano de gobierno, como desde la dirección hacia los empleados.



NIVEL 2

- Existen canales de comunicación interna tanto entre la dirección y el órgano de gobierno, como desde la dirección hacia los empleados. La comunicación interna se efectúa principalmente sobre:
 - Algunas políticas y procedimientos.
 - Objetivos específicos.
 - Importancia, relevancia y ventajas de un sistema de control interno eficaz.
 - Funciones y responsabilidades de la Dirección y del resto de personal relativas al control interno.



NIVEL 3

- Se implantan canales de comunicación transversales que favorecen compartir información para la adecuada toma de decisiones.
- Los canales de comunicación internos abarcan:
 - La misión, visión, y objetivos.
 - Políticas y procedimientos.
 - Importancia y beneficios de los controles internos eficaces.
 - Roles y responsabilidades de los empleados en la operación de los controles.
 - Mecanismos para que todo el personal pueda reportar internamente cualquier desviación, irregularidad o evento que pueda comprometer el funcionamiento del control interno.



NIVEL 4

- Los canales entre dirección y órgano de gobierno, y entre dirección y empleados son monitorizados para detectar problemas de funcionamiento.
- Existen canales de respaldo, o alternativos, por si se produce un corte en los canales habituales.
- Existen canales anónimos para la recepción de denuncias sensibles.
- Se gestiona proactivamente el sistema de denuncias internas en la organización (*whistleblowing*), garantizando la protección del denunciante, y la investigación adecuada de los hechos denunciados.



NIVEL 5

- Se implantan las *best practices* en comunicación y gestión del conocimiento.



Principio 15: La organización se comunica con terceros sobre asuntos que afectan al funcionamiento del control interno.

NIVEL 1

- Se definen las obligaciones de comunicación con todos los grupos de interés de los diferentes participantes tanto del sector público como privado.



NIVEL 2

- Se desarrollan e implementan controles que facilitan la comunicación externa.
- Se incluyen políticas y procedimientos para obtener o recibir información de grupos de interés externos.
- La comunicación se realiza siempre que exista obligación y sea requerida.
- El órgano al que se le requiere contesta de forma aislada.



NIVEL 3

- Se coordina y revisa la fiabilidad de las comunicaciones de acuerdo a su naturaleza. Se evitan comunicados parciales o inexactos.



NIVEL 4

- Existe un sistema de evaluación sobre la información externa, validado por los órganos supervisores internos y externos.



NIVEL 5

- Se utiliza las *best practices* para facilitar la comunicación externa.



COMPONENTE 5: SUPERVISIÓN

Cada uno de los componentes del Control Interno debe ser evaluado para determinar si funciona adecuadamente.

Las evaluaciones pueden ser continuas y/o independientes.

Dentro del Sector Público coexisten diversos órganos de supervisión independiente que cubren la totalidad del sector. Pero, en el ejercicio de su responsabilidad de supervisión del control interno, los órganos de gobierno de-



ben promover una supervisión acorde con la evaluación de riesgos.

Los órganos de gobierno deben promover la supervisión acorde con la evaluación de riesgos

Principio 16: La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema de control interno existen y funcionan.

NIVEL 1



- Todos los organismos o entidades del sector público están incluidos en el ámbito de supervisión de organismos públicos de supervisión que realizarán las evaluaciones independientes de los cinco componentes. Estas evaluaciones (auditorías) se realizan de acuerdo a prácticas profesionales formalizadas y alineadas con las mejores prácticas internacionales.
- Además los organismos del sector público tienen la responsabilidad de comprender el sistema de control interno de los proveedores de servicios externalizados mediante cláusulas en los contratos que permitan la auditoría, o revisar informes y otras auditorías independientes que permitan obtener información de control interno del proveedor.

NIVEL 2



- Se realizan evaluaciones continuas por parte de los responsables directos de las actividades. No están programadas y son básicamente informales. No se comunica el resultado.
- Las evaluaciones independientes son básicamente las realizadas por organismos públicos externos de acuerdo al cumplimiento legal y no se coordinan con las unidades de supervisión / inspección / auditoría interna de la organización.
- Existe una Auditoría Interna que revisa documentos y transacciones y evalúa el cumplimiento de algún procedimiento de forma aislada.

NIVEL 3



- Se implanta el uso de la tecnología para las evaluaciones continuas realizadas por los responsables. Se facilita la objetividad de las evaluaciones continuas y se permite que se revisen eficientemente grandes volúmenes de datos.
- Existe Auditoría Interna con una doble dependencia jerárquica y funcional: del máximo responsable ejecutivo y del órgano de gobierno (consejo, órgano rector...), que aprueba el Plan de Auditoría en base a riesgos.
- Se autoevalúan los cinco componentes mediante cuestionarios o talleres de trabajo. Se determina si están implementados y funcionan.
- Auditoría Interna coordina su actividad con los otros evaluadores independientes externos o internos.

NIVEL 4



- Los superiores de las áreas/direcciones responsables de las evaluaciones continuas demuestran experiencia y desarrollan programas de evaluaciones continuas eficaces y eficientes.
- Se mide la eficacia de las unidades que realizan las evaluaciones independientes internas (métricas sobre cobertura de riesgos, cumplimientos de la planificación, capacitación de sus miembros...).

NIVEL 5



- El alcance de las evaluaciones independientes no se limita al control interno, sino que incluye la gestión de riesgos y gobierno.
- Se certifican/auditan los procesos clave que incluyen la mejora continua en las actividades de supervisión continuada.
- Se revisa externamente la actividad de supervisión y Auditoría Interna (certificaciones de calidad sobre Auditoría Interna).

Principio 17: La organización evalúa y comunica las deficiencias de control interno oportunamente a las partes responsables de aplicar medidas correctivas, incluida la alta dirección y el consejo.

NIVEL 1

- Las normas que regulan el funcionamiento de los órganos de evaluación independientes externos establecen a quién deben distribuirse los resultados de las evaluaciones. Existen criterios respecto a la obligación de establecer un procedimiento de seguimiento de las recomendaciones y los planes de acción.



NIVEL 2

- El resultado de la supervisión realizada a través de evaluaciones continuas no está incluido en la actividad de la unidad, solo se comunica en caso de requerimiento o hallazgo significativo.
- Los resultados de las evaluaciones independientes siempre se comunican al área evaluada.
- Los resultados de las evaluaciones independientes se comunican a los órganos de gobierno siempre y cuando se realicen por órganos externos, pero las de las unidades internas dependen de la propia dirección ejecutiva.



NIVEL 3

- Los resultados de las evaluaciones independientes (auditorías y autoevaluaciones) son comunicados periódicamente a los órganos de gobierno y a los responsables de adoptar las medidas correctoras.



NIVEL 4

- Se elaboran informes periódicos de seguimiento de recomendaciones; se envían a los responsables de las áreas auditadas y a la alta dirección; se automatiza el proceso para agilizar el procedimiento.



NIVEL 5

- Se certifica el procedimiento de seguimiento de recomendaciones.



OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

ENTORNO DE CONTROL: SIETE PREGUNTAS QUE CUALQUIER CONSEJERO DEBE PLANTEARSE

El laboratorio de ideas del Instituto de Auditores Internos analiza en este documento los siete aspectos clave que conforman el entorno de control. Con formato de pregunta y recomendación pretende ayudar a cualquier Consejero en el ejercicio de sus responsabilidades en la evaluación de la fortaleza del entorno de control.

GESTIÓN DEL RIESGO DE FRAUDE: PREVENCIÓN, DETECCIÓN E INVESTIGACIÓN

Aborda los diferentes procesos para una óptima gestión del riesgo de fraude, que pasa por el establecimiento de un programa eficaz de prevención, detección e investigación de fraudes. La publicación define además un enfoque efectivo para la gestión del riesgo de fraude y un análisis profundo sobre las responsabilidades en su prevención, detección e investigación.

COBERTURA DEL RIESGO TECNOLÓGICO: HACIA UNA AUDITORÍA INTERNA DE TI INTEGRADA

Ofrece una visión general del riesgo tecnológico y la exposición del impacto que esta área de procesos de una organización tiene para la planificación y cobertura de Auditoría Interna, entre otros aspectos. También un esquema para integrar Auditoría Interna de TI dentro de la Dirección de Auditoría Interna, o para evaluar el planteamiento actual, si existe la función.

MARCO DE RELACIONES DE AUDITORÍA INTERNA CON OTRAS FUNCIONES DE ASEGURAMIENTO

Es la primera guía en español que clarifica el papel de Auditoría Interna como coordinadora de todas las funciones de aseguramiento. Establece qué funciones de aseguramiento deben darse en una empresa y qué puede y no hacer Auditoría Interna en su papel de coordinación para asegurar que se cumplen y evitar duplicidades.



LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

El *Marco Integrado de Control Interno*, del Committee of Sponsoring Organization of the Treadway Commission, es el modelo de Control Interno de referencia mundial para las organizaciones, ayudándolas a mantener y aumentar un sistema de control que les ayude a cumplir con sus objetivos.

Este documento aplica al sector público español los 17 principios que forman la edición 2013 del *Marco Integrado*, y emplea el modelo de madurez y diferentes niveles de evolución de las organizaciones públicas.

A través del análisis de cada principio que forma el Marco COSO, esta guía da cobertura a todos los ámbitos relativos al control interno de las organizaciones, desde el entorno de control hasta las labores de información, comunicación y supervisión, pasando por las actividades propias del control interno y evaluación de riesgos.