Comportamiento organizacional

Requisito Temático

Guía de Usuario

The Institute of Internal Auditors

Traducción al Español Auspiciada por:

Instituto de Auditores Internos de España

Contenido

Resumen de los Requisitos Temáticos

Los Requisitos Temáticos son un componente esencial del Marco Internacional para la Práctica Profesional (International Professional Practices Framework®), junto con las Normas Globales de Auditoría Interna (Global Internal Audit Standards™) y las Guías Globales. El Instituto de Auditores Internos requiere que los Requisitos Temáticos sean utilizados de manera conjunta con las Normas Globales de Auditoría Interna, las cuales proporcionan la base autorizada de las prácticas requeridas. Las referencias a las Normas aparecen a lo largo de esta guía como una fuente de información más detallada

Los Requisitos Temáticos formalizan cómo los auditores internos abordan las áreas de riesgo habituales para promover la calidad y la coherencia dentro de la profesión. El Mandato de Auditoría Interna define claramente el alcance y los tipos de servicios prestados por la Función de Auditoría Interna, lo que incluiría la consideración de los Requisitos Temáticos (Norma 6.1 - Mandato de Auditoría Interna). Los Requisitos Temáticos establecen una base y proporcionan criterios relevantes para la realización de los servicios de aseguramiento relacionados con el tema en cuestión contemplado en un Requisito Temático (Norma 13.4 Criterios de evaluación). La conformidad con los Requisitos Temáticos es obligatoria para los servicios de aseguramiento y se recomienda su evaluación en los servicios de asesoramiento. Los Requisitos Temáticos no pretenden abarcar todos los aspectos potenciales que deben tenerse en cuenta al realizar trabajos de aseguramiento, sino más bien proporcionar un conjunto mínimo de requisitos que permitan una evaluación coherente y fiable del tema en cuestión.

Los Requisitos Temáticos se encuentran claramente vinculados al Modelo de las Tres Líneas del IIA y a las Normas Globales de Auditoría Interna. Los procesos de gobierno, gestión de riesgos y de control son los principales componentes de los Requisitos Temáticos que se ajustan a la Norma 9.1 Comprender los procesos de gobierno, gestión de riesgos y control. En referencia al Modelo de las Tres Líneas, el gobierno se vincula al Consejo/Directorio (órgano de gobierno), la gestión de riesgos se vincula a la segunda línea y los controles o procesos de control se vinculan a la primera línea. Mientras que la dirección está representada tanto en la primera como en la segunda línea, la Función de Auditoría Interna se representa en la tercera línea como un proveedor de aseguramiento independiente y objetivo, que informa al Consejo/Directorio (órgano de gobierno) (Principio 8 Supervisión del Consejo)

Aplicabilidad, riesgo y criterio profesional

Los Requisitos Temáticos deben cumplirse cuando las Funciones de Auditoría Interna realicen trabajos de aseguramiento sobre temas para los que exista un Requisito Temático o cuando se identifiquen aspectos del Requisito Temático en otros trabajos de aseguramiento.

Como se describe en las Normas, la evaluación del riesgo es una parte importante de la planificación del Director de Auditoría Interna. Determinar los trabajos de aseguramiento a incluir en el Plan de Auditoría Interna requiere evaluar las estrategias, objetivos y riesgos de la organización al menos anualmente (Norma 9.4 Plan de Auditoría Interna). Al planificar trabajos individuales de aseguramiento, los auditores internos deben evaluar los riesgos relevantes para el trabajo (Norma 13.2 Evaluación de riesgos del trabajo).

Cuando el tema en cuestión de un Requisito Temático se identifica durante el proceso de planificación de auditoría interna basada en riesgos y se incluye en el Plan de Auditoría Interna, entonces los requisitos descritos en el Requisito Temático deben ser utilizados para evaluar el tema en cuestión en los trabajos aplicables. Además, cuando los auditores internos realicen un trabajo (incluido o no en el Plan) y surjan elementos de un Requisito Temático, deberá evaluarse la aplicabilidad del Requisito Temático como parte del trabajo. Por último, si se solicita un trabajo que no estaba originalmente en el Plan e incluye el tema en cuestión, debe evaluarse la aplicabilidad del Requisito Temático en ese trabajo.

El juicio profesional desempeña un papel clave en la aplicación del Requisito Temático. Las evaluaciones de riesgos orientan las decisiones de los Directores de Auditoría Interna sobre los trabajos que deben incluirse en el Plan de Auditoría Interna (Norma 9.4). Además, los auditores internos utilizan el juicio profesional para determinar qué aspectos se cubrirán en cada trabajo (Normas 13.3 Objetivos y alcance del trabajo, 13.4 Criterios de evaluación y 13.6 Programa de trabajo), así como para identificar los recursos necesarios para alcanzar los objetivos del trabajo (Norma 13.5 Recursos del trabajo).

Deberán conservarse evidencias de que se ha evaluado la aplicabilidad de cada uno de los requisitos contemplados en el Requisito Temático, incluida una justificación de la exclusión de cualquier requisito. La conformidad con el Requisito Temático debe documentarse utilizando el juicio profesional de los auditores internos, tal como se describe en la norma 14.6 Documentación de los trabajos.

Aunque el Requisito Temático proporciona una base de procesos de control a considerar, las organizaciones que evalúen el tema de riesgo como muy alto pueden necesitar evaluar aspectos adicionales.

Si un Director de Auditoría Interna determina que la Función de Auditoría Interna no tiene los conocimientos necesarios para llevar a cabo trabajos de auditoría sobre un tema de máxima exigencia, el trabajo podrá contratarse con un proveedor de servicios externo (Normas 3.1 Competencia, 7.2 Cualificaciones del Director de Auditoría Interna, 10.2 Gestión de los recursos humanos). Las Normas se aplican a cualquier persona o función que ofrece servicios de Auditoría Interna, independientemente de que la organización contrate directamente a los auditores internos, a través de un proveedor externo de servicios o mediante una combinación de ambos. El Director de Auditoría Interna mantiene la responsabilidad última de garantizar la conformidad. Además, si el Director de Auditoría Interna determina que los recursos de auditoría interna son insuficientes, el Director de Auditoría Interna debe informar al Consejo/Directorio sobre el impacto de la insuficiencia de recursos y cómo se abordará cualquier déficit de recursos (Norma 8.2 Recursos).

Desempeño, documentación e informes

Al aplicar los Requisitos Temáticos, los auditores internos también deben ajustarse a las Normas, realizando su trabajo de acuerdo con el Dominio V: Desempeño de los Servicios de Auditoría Interna. Las normas del Dominio V describen la planificación de los trabajos (Principio 13 Planificar eficazmente los trabajos), la realización de los trabajos (Principio 14 Ejecución de los trabajos) y la comunicación de los resultados de los trabajos (Principio 15 Comunicar las conclusiones del trabajo y monitorear los planes de acción).

Los Requisitos Temáticos están diseñados para dar soporte a las prácticas de auditoría interna coherentes y de alta calidad. Deben aplicarse junto con las leyes, regulaciones, expectativas de supervisión y otros marcos reconocidos profesionalmente, que pueden imponer requisitos adicionales o más específicos. Es posible que los auditores internos ya hayan desarrollado programas de trabajo y procedimientos de comprobación basados en estas normativas y marcos. Los auditores internos deben conciliar sus pruebas de control previstas sobre el comportamiento organizacional y cualquier prueba fiable proporcionada por otros proveedores de aseguramiento internos y externos (Norma 9.5 Coordinación y Confianza) con el Requisito Temático para asegurar una cobertura adecuada.

La cobertura del Requisito Temático puede documentarse en el Plan de Auditoría Interna o en el programa de trabajo del trabajo de auditoría, según el criterio profesional de los auditores internos. Uno o más trabajos de auditoría interna pueden cubrir los requisitos. Además, puede que no todos los requisitos sean aplicables. Deben conservarse evidencias de que se ha evaluado la aplicabilidad del Requisito Temático, incluida una justificación que explique cualquier exclusión.

Aseguramiento de la Calidad

Las Normas exigen que el Director de Auditoría Interna desarrolle, implemente y mantenga un Programa de Aseguramiento y Mejora de la Calidad que abarque todos los aspectos de la Función de Auditoría Interna (Norma 8.3 Calidad). Los resultados deben comunicarse al Consejo/Directorio y a la Alta Dirección. Las comunicaciones deben informar sobre la conformidad de la Función de Auditoría Interna con las Normas y el logro de los objetivos de desempeño.

La conformidad con los Requisitos Temáticos debe tenerse en cuenta en las actividades de supervisión a nivel del trabajo (Norma 12.3 Supervisar y mejorar el desempeño del trabajo) y se evaluará en las Evaluaciones de Calidad.

Comportamiento Organizacional

Reformular la auditoría de la cultura

> **Nota**
>
> Los Requisitos Temáticos utilizan la terminología general de Auditoría Interna definida en las Normas Globales de Auditoría Interna. Los lectores deben consultar los términos y definiciones contempladas en el glosario de las Normas.

El paso de considerar la auditoría de la cultura como un tema abstracto y vago a una evaluación estructurada y precisa del comportamiento organizacional representa una evolución necesaria y oportuna dentro de la profesión de Auditoría Interna. Aunque se reconoce ampliamente que las deficiencias culturales suelen estar en la base de fallos significativos de control, este ámbito no ha logrado una implantación relevante en las prácticas de Auditoría Interna. Reformular la auditoría de la "cultura" como auditoría del "comportamiento organizacional desalineado con los objetivos de la organización" proporciona una base más clara, estructurada, precisa y auditable. Como ocurre con cualquier riesgo, las organizaciones pueden gestionarlo mediante el diseño de controles adecuados y su aplicación efectiva.

El Requisito Temático sobre Comportamiento Organizacional adopta esta filosofía, estableciendo requisitos mínimos obligatorios para evaluar el comportamiento cuando una evaluación de riesgos determine que se encuentra en el ámbito de revisión. Estos requisitos son totalmente compatibles con el enfoque tradicional de auditoría basada en el riesgo y pueden aplicarse, con una adaptación mínima, a todas las Funciones de Auditoría Interna. Esta Guía de Usuario complementaria proporciona ejemplos prácticos de cómo este enfoque puede integrarse en los trabajos de auditoría estándar, así como orientación sobre la revisión del marco de comportamiento organizacional más amplio o de los componentes individuales. La influencia significativa de esta cuestión en los objetivos de la organización exige una consideración y adopción proactivas.

Las definiciones de los siguientes términos clave son necesarias para comprender y aplicar el Requisito Temático. Dada la inmadurez de la cuestión, las organizaciones utilizan estos términos de forma incoherente. Las definiciones proporcionadas deben ayudar a los usuarios a alinear la terminología de sus organizaciones con la terminología proporcionada en el Requisito Temático y en esta Guía de Usuario.

- **Incentivos de comportamiento** - Cualquier elemento que pueda darse para motivar el comportamiento, incluidos incentivos monetarios como aumentos, primas u opciones sobre acciones; o incentivos no monetarios como cumplidos, asignaciones preferentes o días libres.
- **Patrones de conducta** - Patrones de conducta en los que el comportamiento es recurrente o se produce con mayor frecuencia. Los patrones se identifican como "cómo se hacen las cosas" de forma más general, en contraposición a situaciones puntuales.
- **Riesgo de comportamiento** - Riesgo de que el comportamiento sea incoherente con los objetivos de la organización.

- **Indicadores de riesgo de comportamiento** - Información de gestión procesable relativa al comportamiento.
- **Consejo de Administración** - máximo órgano de gobierno de la organización. Consejo/Directorio.
- **Conducta** - Comportamiento en relación con los requisitos regulatorios y las expectativas.
- **Cultura** - Las decisiones que toman los empleados al hacer su trabajo y cómo trabajan con los demás, junto con lo que impulsa esos comportamientos organizacionales. Los impulsores u orientadores incluyen mecanismos formales, como incentivos y objetivos, e informales, como valores y creencias colectivas.
- **Comportamiento organizacional** - Las decisiones observables que toman los empleados al hacer su trabajo y cómo trabajan con los demás. Este comportamiento influye en el desempeño y en la consecución de los objetivos de la organización. En pocas palabras, el comportamiento organizacional es "la forma en la que hacemos las cosas" y se considera un subconjunto de la cultura.
- **Revisiones de desempeño** - Evaluaciones individuales o en grupo sobre la suficiencia del propio trabajo.
- **Parte interesada** – Individuo o colectivo con algún interés directo o indirecto en las actividades y resultados de la organización. Las partes interesadas pueden incluir al Consejo/Directorio, los empleados/colaboradores, clientes, proveedores, accionistas, agencias regulatorias, instituciones financieras, auditores externos, el público en general y otros.
- **Valores** - Principios que guían cómo se espera que se comporten las personas.

Secciones

Los requisitos obligatorios del Requisito Temático sobre Comportamiento Organizacional y las consideraciones no obligatorias de esta Guía de Usuario se dividen en tres secciones:

- **Gobierno** - Objetivos y estrategias de base claramente definidos para el comportamiento organizacional que apoyan los objetivos, políticas y procedimientos de la organización.
- **Gestión de riesgos** - Procesos para identificar, analizar, tratar y supervisar los riesgos relacionados con el comportamiento organizacional, incluido un proceso para elevar los incidentes con prontitud.
- **Controles** - Procesos de control establecidos por la dirección y evaluados periódicamente para mitigar los riesgos relacionados con el comportamiento organizacional.

Además del Requisito Temático y de esta Guía de Usuario, los auditores internos pueden consultar guías profesionales adicionales sobre comportamiento organizacional, tales como las Guías Globales del MIPP (IPPF) y otros recursos específicos de la industria.

Consideraciones

Los auditores internos pueden utilizar las siguientes consideraciones como ayuda para su evaluación de los requisitos contemplados en el Requisito Temático sobre Comportamiento Organizacional. La letra de cada consideración que figura a continuación hace referencia a su requisito correspondiente en el Requisito Temático. Estas consideraciones son ilustrativas, pero no obligatorias. Los auditores internos deben basarse en su juicio profesional para determinar qué incluir en sus evaluaciones.

Las restricciones en los trabajos de auditoría interna del Sector Público debidas a la legislación, la estructura gubernamental o los entornos políticos se reconocen como barreras potenciales para abordar ciertos aspectos de este trabajo. Los auditores internos del Sector Público deben documentar dichas limitaciones del alcance como parte de su proceso de evaluación de riesgos y aplicar su criterio profesional para definir y comunicar claramente el alcance adaptado de su revisión.

Consideraciones sobre el gobierno

Para evaluar cómo podrían aplicarse los procesos de gobierno al comportamiento organizacional, los auditores internos pueden revisar:

A. Funciones y responsabilidades estructuradas para garantizar que el Consejo/Directorio mantenga visibilidad e influencia sobre las dimensiones conductuales de la organización. Las pruebas pueden incluir que:
   - Un Comité de Gobierno:
     - Establece y mantiene una junta o subcomité(s) especializado(s) centrado(s) en el comportamiento organizacional con un mandato claro que vincule la supervisión del comportamiento organizacional con la ejecución estratégica.
     - Realiza revisiones periódicas de los indicadores de riesgo de comportamiento que se alinean con los objetivos empresariales a largo plazo. Los indicadores de riesgo de comportamiento son métricas para establecer si es necesario actuar para garantizar que el comportamiento se mantiene alineado con los objetivos de la organización, los valores relacionados y el propósito de la organización.
     - Incluye objetivos de comportamiento en las evaluaciones del desempeño y la remuneración de los ejecutivos.
   - Los marcos de información del Consejo/Directorio:
     - Proporcionan información sobre los indicadores de riesgo de comportamiento mediante cuadros de mando estructurados (por ejemplo, compromiso del personal, tendencias de los incidentes, satisfacción del cliente, reconocimiento basado en valores).
     - Integran las métricas relacionadas con la cultura en los informes estratégicos de desempeño a nivel del Consejo de Administración.
   - Los mecanismos de retroalimentación (*feedback*) de las partes interesadas, como las encuestas, permiten:

- Que el Consejo/Directorio reciba información directa de empleados, clientes y otras partes interesadas sobre la alineación del comportamiento con los valores y la estrategia.
- Retroalimentación (*feedback*) para ayudar a dar forma a la dirección estratégica y las intervenciones conductuales.

B. La gestión eficaz del comportamiento organizacional se produce a través de una rendición de cuentas claramente definida en toda la organización. El Consejo/Directorio es responsable, en última instancia, de garantizar que la organización promueva y mantenga un comportamiento alineado con sus objetivos organizacionales, lo que incluye establecer expectativas claras de conducta, supervisar los informes sobre riesgos de conducta y cuestionar la gestión cuando se detecte un desajuste. Las pruebas pueden incluir que:

- El Consejo/Directorio:
  - Aprueba el apetito de riesgo de comportamiento y los objetivos culturales clave de la organización.
  - Exige la presentación periódica de informes sobre indicadores de riesgo de comportamiento (por ejemplo, tendencias, patrones de incidentes, temas de denuncia).
  - Hace que la dirección ejecutiva rinda cuentas de los resultados culturales mediante mecanismos como las estructuras de incentivos y el "tono en la cúpula" (*tone at the top*).
  - Se reúne con funciones de segunda y tercera línea sobre asuntos relacionados con la elevación de riesgos de comportamiento, las brechas en la supervisión y la suficiencia de las medidas correctoras.
- Las unidades de negocio y la dirección operativa integran las expectativas de comportamiento en las operaciones diarias, garantizando que las decisiones, las comunicaciones y la dinámica de equipo reflejen los valores declarados de la organización. Esto puede incluir asumir la responsabilidad de:
  - Modelar los comportamientos deseados y mantener un entorno psicológicamente seguro.
  - Implantar controles que influyan en el comportamiento, como rutinas de contratación, incentivos, comunicación y liderazgo.
  - Identificar de forma proactiva y elevar los riesgos de comportamiento a medida que surgen en entornos operativos.
  - Mitigar el riesgo de comportamiento que es consecuencia de un comportamiento desalineado dentro de sus equipos y la necesidad de controles (formales e informales).

- Las funciones de riesgo, cumplimiento, recursos humanos y supervisión relacionadas diseñan y mantienen el marco de riesgo de comportamiento de la organización, que incluye:
  - Funciones y responsabilidades definidas para la supervisión del comportamiento.
  - Vías de elevación de incidentes y procesos de análisis de datos.
  - Cuadros de mando, análisis temáticos y evaluaciones periódicas para ofrecer una visión prospectiva de las condiciones de comportamiento en toda la organización.
  - La capacidad de cuestionar prácticas en las que los incentivos, las comunicaciones o los comportamientos de liderazgo divergen de los objetivos establecidos.
  - Consulta sobre todos los cambios importantes en los controles relacionados con las personas, los marcos de gobierno o las iniciativas de transformación estratégica que puedan influir en la cultura.
  - Revisión de las tendencias emergentes de los informes de incidentes, los resultados de las auditorías y otros mecanismos de aseguramiento que indiquen problemas relacionados con el comportamiento.

c. Proceso de gobierno que garantiza la supervisión del comportamiento, el seguimiento regular, la evaluación y la alineación de los patrones de comportamiento y los objetivos de la organización. El proceso puede incluir:
   - Utilizar un cuadro de mando para proporcionar información clave procedente de fuentes como los resultados de las encuestas de satisfacción e integridad de los empleados, las tasas de abandono y absentismo, el contenido del canal de comunicación abierta, los datos sobre incidentes y las métricas de desempeño e innovación. Entre las características de un cuadro de mando eficaz sobre comportamiento organizacional se incluyen:
     - Definición de valores umbral para identificar oportunidades de mejora del comportamiento.
     - Separación de los datos sobre el comportamiento (como los datos sobre las intervenciones) de los datos sobre los impulsores/orientadores (como la claridad de funciones y responsabilidades) y los datos sobre los resultados (como las quejas de los clientes).
     - Combinación de datos cuantitativos, como los de las encuestas, con datos cualitativos, como los de los grupos de discusión y los canales de comunicación abierta.
   - El Consejo/Directorio entiende cómo podrían abordarse los aspectos actuales del comportamiento organizacional para mejorar la eficacia y el desempeño de la organización. Estos aspectos comprenden cómo:

- Se toman las decisiones, incluida la búsqueda de diferentes perspectivas y retos.
- Los empleados se comunican entre sí, incluso expresando sus preocupaciones y expectativas.
- Los empleados colaboran, incluso entre equipos y a la hora de gestionar conflictos.
- Los empleados responden al fracaso, por ejemplo, aprendiendo de los errores o respondiendo con culpa o negación.
- El comportamiento de liderazgo de los mandos intermedios y superiores influye en las demás categorías de comportamiento (por ejemplo, cómo responden los líderes a los errores y cómo invitan a cuestionar la toma de decisiones).
- La estrategia y el modelo de negocio impulsan u orientan la toma de decisiones, los códigos de conducta y la gestión del rendimiento de los incentivos/desincentivos.

- El Consejo/Directorio requiere un sistema de aprendizaje continuo que identifique las oportunidades de mejora y las aborde de forma activa y mensurable mediante:
  - La utilización de conocimientos basados en pruebas y en el comportamiento real de los empleados.
  - El enfoque en lo que se sabe que ocurre en la organización en lugar de en lo que se pretende o desea.
  - La evaluación de una combinación de datos cualitativos y cuantitativos, a menudo obtenidos mediante encuestas, canales de opinión o de comunicación abierta, conversaciones confidenciales y grupos de discusión.
  - La aplicación de los conocimientos adquiridos para determinar acciones que refuercen y aborden determinados aspectos del comportamiento organizacional.
  - La incorporación de un plan de acción para combinar intervenciones específicas en áreas críticas (por ejemplo, estrategia de comunicación, formación, desarrollo del liderazgo y debates a nivel de equipo).

D. Se establecen políticas y procedimientos que abordan los protocolos de riesgo conductual, se revisan periódicamente, se comunican eficazmente y se integran en las operaciones empresariales y la toma de decisiones. Las políticas y procedimientos abarcan la ética, los recursos humanos, el cumplimiento, el riesgo, las operaciones y los derechos de decisión para garantizar:

- Las expectativas de comportamiento se articulan formalmente en las políticas pertinentes (como un código de conducta y/o políticas sobre ética, recursos humanos, incentivos y delegación de autoridad). Dichas políticas deben definir los comportamientos aceptables e inaceptables con ejemplos prácticos, alineados con el apetito de riesgo de la organización.

- Las funciones de gestión de riesgos asignan las expectativas de comportamiento a procesos operativos clave -como la contratación, las revisiones del desempeño, la incorporación y la gestión de clientes-, garantizando que se reflejen en las decisiones diarias. Las revisiones de aseguramiento deben comprobar cómo influyen estas expectativas en los comportamientos reales e informar al Consejo/Directorio en consecuencia.
- El Consejo/Directorio busca y recibe aseguramiento de que las políticas de la organización son accesibles y se comunican claramente a través de múltiples canales (por ejemplo, intranet, formación, reuniones generales). La incorporación de casos prácticos y árboles de decisión ayuda a contextualizar las expectativas de comportamiento. Los cuadros de mando pueden hacer un seguimiento de las métricas de comprensión y uso.
- Todas las políticas y procedimientos de comportamiento están sujetos a un ciclo de revisión programado y se actualizan como respuesta ante incidentes, resultados de encuestas o cambios normativos. Las funciones de segunda línea deben mantener un registro de lecciones aprendidas para identificar las lagunas que surjan entre el comportamiento y los objetivos de la organización.
- El Consejo/Directorio recibe periódicamente información actualizada sobre la cobertura, claridad y eficacia de las políticas. La segunda línea debe analizar los incumplimientos, las repercusiones políticas y la adecuación a los comportamientos deseados. La eficacia de la política debe revisarse mediante información cualitativa e indicadores de riesgo de comportamiento.

Consideraciones sobre la gestión de riesgos

Para evaluar cómo se aplican los procesos de gestión de riesgos al comportamiento organizacional, los auditores internos pueden revisar si:

A. Un proceso de gestión de riesgos de comportamiento está claramente definido e incluye características de comportamiento críticas para alcanzar los objetivos de la organización. Las características de la gestión de riesgos podrían incluir:
   - Las funciones y responsabilidades se ajustan a los marcos de riesgo y gobierno de la empresa y las líneas jerárquicas permiten la independencia y la influencia.
   - Autoridad para cuestionar decisiones y elevar las cuestiones de riesgo relacionadas con el comportamiento sin temor a represalias o dilución.
   - Independencia de la gestión operativa con acceso directo a la Alta Dirección y al Consejo/Directorio.
   - Acceso a datos de riesgo de comportamiento procedentes de múltiples fuentes que sean relevantes, oportunos y contrastados entre ellas. Estos datos incluyen tanto formas estructuradas (como resultados de encuestas o infracciones de las políticas) como no estructuradas (por ejemplo, informes de conversaciones o reflexiones de grupos de discusión). Las fuentes de datos incluyen recursos humanos (como datos

sobre bajas, retención y encuestas), denuncias, quejas de clientes y resultados de auditorías.

- Uso de análisis de datos para identificar tendencias, anomalías y riesgos emergentes.
- Uso de cuadros de mando e indicadores de riesgo para informar a la dirección y al Consejo/Directorio.
- Uso de indicadores de riesgo de comportamiento vinculados a los objetivos de la organización.
- Realización o subcontratación de revisiones de la causa raíz de los fallos de conducta y el desalineamiento cultural.
- Familiaridad con los impulsores u orientadores formales e informales del comportamiento (por ejemplo, incentivos, seguridad psicológica y tono de liderazgo).
- La credibilidad y confianza de los altos cargos en los equipos operativos, combinada con la capacidad de influir en la toma de decisiones en tiempo real.
- Participación activa en el diseño y la revisión de los controles relacionados con los recursos humanos (por ejemplo, incentivos, contratación y formación).
- Función de asesoramiento en programas de cambio estratégico e iniciativas de transformación.
- Compromiso con la dirección de la empresa para moldear la cultura a través de la influencia, no sólo de la imposición.
- Recogida y análisis continuos de datos, que pueden incluir:
  - Encuestas sobre el compromiso y el bienestar de los empleados.
  - Datos de reconocimiento y recompensa del comportamiento basado en valores.
  - Informes y quejas de denunciantes.
  - Comentarios de clientes, destacando tanto la satisfacción como la insatisfacción.
  - Evaluaciones del desempeño que reflejen la colaboración, la integridad y la innovación.
- Uso de análisis de datos para identificar vulnerabilidades y detectar tendencias.
- Un proceso claramente definido para elevar rápidamente riesgos y comportamientos que no se ajusten a los objetivos de la organización.
- Supervisión de la determinación y ejecución de planes de acción de gestión para abordar los riesgos y reforzar los comportamientos requeridos.

B. Los procesos de supervisión oportuna del comportamiento organizacional incluyen la comunicación de los resultados a las partes interesadas. Entre los ejemplos de indicadores de riesgo en las categorías de comportamiento, impulsores y resultados y deficiencias notificables se incluyen:

- Toma de decisiones: Falta de cuestionamiento efectivo o inclusión insuficiente de diferentes perspectivas.

- Comunicación: Atención inadecuada a los problemas señalados por los individuos.
- Colaboración: Entornos de trabajo fragmentados en los que los empleados se centran únicamente en su propio trabajo.
- Respuesta a las deficiencias: Culpar y castigar los errores involuntarios.
- Impulsores u orientadores formales: Funciones y responsabilidades poco claras u objetivos contradictorios.
- Impulsores u orientadores informales: Baja seguridad psicológica o dinámica ineficaz entre las tres líneas.
- Datos de desempeño: Quejas excesivas de los clientes o estancamiento de la innovación o la digitalización.
- Datos sobre recursos humanos: Altos niveles de abandono y absentismo y bajos niveles de satisfacción en los resultados de las encuestas.
- Riesgo y datos jurídicos: Elevado número de investigaciones, infracciones de las políticas o alertas y situaciones evitadas por un margen estrecho.

c. Procesos para garantizar que las desviaciones entre los comportamientos esperados y los observados se identifican y comunican a quienes tienen autoridad y capacidad para actuar. Los auditores internos podrán revisar que:

- La comunicación eficaz es oportuna, se basa en pruebas y se apoya en el análisis de los factores subyacentes y las causas raíz.
- El diseño y la eficacia operativa de los esfuerzos de comunicación evitan soluciones superficiales, daños a la reputación o fracasos repetidos.
- La información se recopila y sintetiza a partir de múltiples fuentes, como los comentarios de los empleados, informes de denunciantes, resultados de auditorías y revisiones de incidentes.
- Las técnicas de análisis estructurado -como las revisiones temáticas, los modelos de ciencia del comportamiento y los marcos de causas raíz- van más allá de los síntomas superficiales e identifican los factores subyacentes del desalineamiento [por ejemplo, incentivos poco claros, baja seguridad psicológica o tono en la cúpula (*tone at the top*) ineficaz].
- Las deficiencias no se presentan simplemente como infracciones de la normativa o incidentes aislados, sino como sucesos con causas raíz en el comportamiento que reflejan problemas culturales, sistémicos o de liderazgo.
- Las comunicaciones destacan lo ocurrido y su causa, basándose en datos cuantitativos y cualitativos para soportar las conclusiones.
- La organización separa los patrones de comportamiento, las vulnerabilidades derivadas de los impulsores u orientadores del comportamiento y los resultados de la organización (por ejemplo, el impacto en el desempeño, la confianza de las partes interesadas), lo que permite abordar el comportamiento y sus impulsores u

orientadores. Los resultados se comunican al público adecuado, con el nivel de detalle adecuado:

- Gestores operativos para la corrección inmediata del proceso.
- Liderazgo de alto nivel para la asignación de recursos, mensajes y tono.
- El Consejo/Directorio o los comités pertinentes para la supervisión y las implicaciones estratégicas.

- Las herramientas visuales y narrativas, como los cuadros de mando, los mapas de calor o los resúmenes de casos, explican las conclusiones y respaldan las recomendaciones y/o los planes de acción.
- En las revisiones de los procesos se incluyen las implicaciones para la exposición al riesgo y la resiliencia del entorno de control.
- La comunicación de las brechas se encuentra vinculada a medidas correctoras y se monitorea su cumplimiento.
- Los resultados de las intervenciones se evalúan y comparten, completando así el ciclo de aprendizaje.
- Las comunicaciones se encuentran libres de influencias indebidas y se ajustan a los protocolos de elevación establecidos, preservando la independencia y credibilidad de las evaluaciones.

D. Las diferencias entre los comportamientos esperados y los reales se resuelven de forma estructurada y participativa para garantizar que las medidas correctoras se basan en las opiniones de las partes interesadas, se da seguimiento hasta su finalización y se evalúa su eficacia. Los auditores internos pueden revisar si:

- El proceso de resolución implica de forma significativa a las partes interesadas más cercanas al problema, como directores operativos, recursos humanos, socios empresariales, representantes de los empleados, asesores de cumplimiento y personas o equipos afectados. Sus aportaciones garantizan que las acciones sean:
  - Basadas en el contexto: Sensible a las realidades operativas y a las normas informales que pueden haber contribuido al desfase.
  - Creíbles y aceptadas: Es más probable que se respalden e integren si las acciones son diseñadas por las personas directamente implicadas en ellas.
  - Un reto constructivo: Facilitando una reflexión sincera sobre los comportamientos de liderazgo que contribuyen, los puntos débiles del diseño de control o la dinámica de los grupos.
- Se solicitan las aportaciones de las partes interesadas, se sintetizan y se incorporan a los planes de acción. Los mecanismos de retroalimentación (*feedback*) pueden incluir entrevistas, grupos de discusión, encuestas de diagnóstico y otros métodos.
- Las acciones de resolución se encuentran documentadas, con responsabilidad asignada, plazos y criterios de éxito definidos:
  - Las medidas son proporcionales a la gravedad del problema.

- En caso necesario, las acciones se dirigen a los impulsores u orientadores formales (por ejemplo, políticas, incentivos) e informales (por ejemplo, seguridad psicológica, dinámica de equipo).
- Cuando intervienen varias funciones (por ejemplo, recursos humanos para la formación, gestión de riesgos para los controles), se encuentran garantizadas la coordinación y la claridad en la ejecución transversal y en la rendición de cuentas.

- Se realiza un seguimiento del progreso hasta su finalización, garantizando que los compromisos adquiridos se cumplen y se mantienen. Esto incluye:
  - Mantener un registro de problemas/acciones de comportamiento o un mecanismo equivalente.
  - Realizar comprobaciones periódicas con los responsables de las acciones para verificar su estado.
  - Elevar a los foros de gobierno apropiados los retrasos, las ejecuciones parciales o las resistencias identificadas.
- Se evalúa la eficacia de la resolución para cerrar la brecha y reducir el riesgo de comportamiento. Esto puede implicar:
  - Reevaluación de los indicadores de riesgo de comportamiento tras la implementación.
  - Recopilación del feedback de las partes interesadas sobre los cambios observados.
  - Comprobación de los cambios de comportamiento mediante técnicas de observación, encuestas o auditoría.
  - Ajuste de las acciones o incorporación de refuerzos cuando los resultados sigan siendo débiles o ambiguos.

Consideraciones sobre el proceso de control

Para evaluar cómo se aplican los procesos de control para mitigar el riesgo de que los comportamientos organizacionales no estén alineados con los objetivos de la organización, los auditores internos pueden revisar:

A. Revisiones del riesgo de comportamiento para comprender el riesgo derivado del comportamiento organizacional actual (es decir, las posibles consecuencias no deseadas de cómo se hacen las cosas). Ejemplos de este tipo de revisiones son las evaluaciones de los proyectos una vez finalizados, análisis de las causas raíz y revisiones en detalle de las operaciones puestas en práctica.

B. Procesos estructurados de retroalimentación (*feedback*) para comprender qué mecanismos utiliza la dirección para comunicar las expectativas de comportamiento (por ejemplo, reuniones generales, correos electrónicos y reuniones entre las personas y sus supervisores) y la eficacia del tono de la dirección en el comportamiento dentro de

una organización. Esto puede hacerse evaluando los procesos que captan y analizan las percepciones y la comprensión por parte de los empleados de los mensajes del Consejo/Directorio y de la Alta Dirección. Los auditores internos pueden ayudar a las organizaciones a perfeccionar continuamente sus estrategias de comunicación y ayudar a garantizar que el tono en la cúpula (*tone at the top*) se conozca de forma eficaz en todos los niveles mediante la revisión de controles clave como:

- Encuestas periódicas, entrevistas y debates en grupos de discusión con los empleados, para indagar sobre la claridad, coherencia e impacto de las comunicaciones sobre liderazgo y obtener datos cuantitativos y cualitativos sobre la recepción y comprensión de los mensajes en los distintos niveles de la organización.
- Canales abiertos para comentarios anónimos, que permitan a los empleados compartir sus opiniones sinceras sin temor a represalias. Estos canales deben facilitarse a través de plataformas digitales que permitan comentarios y sugerencias en tiempo real. Los datos derivados de estos canales deben analizarse para comprobar si el tono en la cúpula (*tone at the top*) es bien entendido por los empleados de todos los niveles.
- Recogida de información de las reuniones de la Alta Dirección a través de encuestas, entrevistas, grupos de discusión, actas y canales anónimos para garantizar que la Alta Dirección es consciente de las comunicaciones ineficaces, los malentendidos o las áreas que necesitan mejorar. La Alta Dirección demuestra que valora la opinión de los empleados, respondiendo activamente a sus comentarios y actuando en consecuencia. Cuando esto no ocurre, los empleados pueden sentirse menos favorables a dar su opinión porque creen que las cosas no van a cambiar.
- Los comentarios sobre el desempeño de los altos directivos se integran en sus evaluaciones de desempeño para supervisar continuamente la recepción de las directrices de liderazgo. Esto refuerza la importancia de los mensajes de liderazgo y garantiza que se reflejen en las operaciones cotidianas.

c. Para la pronta identificación y mitigación de riesgos y para establecer un entorno psicológicamente seguro en el que los empleados se sientan cómodos informando de problemas sin temor a represalias, se fomenta elevar las situaciones identificadas a las estancias oportunas dentro de una organización. Los auditores internos pueden revisar los controles clave para ayudar a mejorar la gestión eficaz del riesgo, tales como:

- Mecanismos de retroalimentación (*feedback*) fáciles de usar, incluidas opciones de denuncia directa y anónima, líneas directas internas y externas para fraudes o denuncias, encuestas, buzones de sugerencias y plataformas digitales para permitir la denuncia confidencial y captar problemas que las personas puedan dudar en denunciar abiertamente.
- Procesos bien definidos y fáciles de entender para notificar problemas, con múltiples canales internos y externos directos y anónimos, y esfuerzos para promover la concienciación entre los empleados. Las características de los canales de información deben incluir:

- Garantías de confidencialidad, protegiendo la identidad de las personas que denuncian las incidencias.
- Políticas estrictas de no represalias que se comunican con claridad y se mantienen sistemáticamente para proteger a las personas que denuncian las incidencias.
- Comunicación a las personas que no denuncian los problemas de forma anónima, independientemente del motivo o el resultado.
- Resúmenes periódicos a nivel de toda la organización de las incidencias reportadas en el pasado y sus resultados, con el fin de demostrar que éstas se comunican y se gestionan, así como para garantizar la transparencia respecto a las medidas adoptadas para dar respuesta a las observaciones.

- Comunicación periódica por parte de la dirección en la que se haga hincapié en la importancia de la comunicación abierta y del reporte de incidencias y se demuestre cómo la propia dirección modela ese comportamiento.
- Sesiones periódicas de formación en las que se haga hincapié en la importancia de la seguridad psicológica, se anime a las personas a reportar incidencias y se les oriente sobre cómo elevarlas adecuadamente. La formación (capacitación) debe repetirse periódicamente para reforzar los comportamientos deseados a lo largo del tiempo.
- Reconocimientos informales, como agradecimiento verbal o por escrito y reconocimiento público, para las personas que reporten incidencias.
- Revisiones periódicas del proceso de elevación de incidencias para garantizar su eficacia y eficiencia, incluida la solicitud de comentarios de los empleados para identificar y abordar con prontitud los obstáculos al proceso de denuncia.
- Comunicación sobre la resolución de las observaciones.

D. Los programas de incentivos-desincentivos se alinean con los comportamientos deseados y los objetivos organizacionales y se comunican. Los auditores internos pueden revisar controles como:

- Los incentivos -tanto monetarios (por ejemplo, primas, ascensos) como no monetarios (por ejemplo, reconocimiento, oportunidades de desarrollo)- están alineados con los objetivos de la organización y vinculados a la demostración de los comportamientos deseados.
- Los criterios equilibrados para la evaluación del desempeño incorporan cómo se logran los objetivos (por ejemplo, colaboración, integridad y centrarse en el cliente), así como métricas de logro más tradicionales (como los objetivos financieros).
- Los criterios de incentivación y los umbrales de desincentivación están claramente definidos, se aplican de forma coherente y se encuentran sujetos a revisión por parte de la dirección o de recursos humanos para evitar sesgos y resultados no deseados.
- Los grupos interfuncionales validan la coherencia y equidad de las decisiones sobre incentivos en todas las unidades de negocio.

- Las consecuencias de la mala conducta y las infracciones culturales incluyen desincentivos claros y proporcionados (por ejemplo, reducciones de primas y bloqueos de ascensos), con acciones explicadas y documentadas para garantizar la transparencia.
- Los programas de reconocimiento no monetario destacan a los empleados que modelan los valores culturales, como la toma de decisiones éticas y la seguridad psicológica.
- Los efectos de los programas de incentivos se evalúan sistemáticamente a través de *feedback* de los empleados y los parámetros de comportamiento para perfeccionar o reajustar los mecanismos de recompensa. Los programas de incentivos deben evaluarse y ajustarse para garantizar que:
    - Los objetivos no son ni demasiado particulares ni demasiado generales.
    - Los objetivos son alcanzables.
    - Los objetivos a corto plazo no socavan los resultados a largo plazo.
    - Se articulan niveles aceptables de asunción de riesgos.
    - Se aplican salvaguardas para garantizar un comportamiento ético mientras se alcanzan los objetivos (por ejemplo, los líderes como modelos de comportamiento ético, haciendo que el coste de hacer trampas sea mucho mayor que el beneficio, y una fuerte supervisión).
    - Los objetivos se adaptan a las capacidades y circunstancias individuales, preservando al mismo tiempo la equidad.
    - Los objetivos de equipo no se contradicen con los objetivos individuales.
    - Se evalúa la motivación intrínseca, y la dirección reconoce que algunos objetivos pueden cercenar la motivación intrínseca.
    - Se tienen en cuenta los objetivos últimos de la organización y se evalúa la idoneidad del tipo de objetivo (por ejemplo, desempeño o aprendizaje).
- La organización integra el refuerzo positivo y las acciones correctivas para facilitar un comportamiento organizacional proactivo que se ajuste a sus objetivos y a los requisitos regulatorios. Los controles clave deben incluir:
    - Evaluar periódicamente la eficacia de los programas de comunicación y formación para garantizar que los empleados comprendan la importancia de notificar las incidencias y las consecuencias del incumplimiento y se sientan animados a hacerlo.
    - Los sistemas de seguimiento y reporte supervisan el cumplimiento e identifican posibles incidencias de falta de notificación.
    - Las medidas disciplinarias se aplican de forma coherente y justa y no son ni tan duras que desalienten las denuncias, ni tan indulgentes que no logren disuadir los comportamientos poco éticos.

- Los mecanismos de retroalimentación (*feedback*) que permiten a los empleados reportar incidencias de forma anónima se revisan periódicamente para garantizar que son eficaces y fomentan las denuncias honestas.

E. El proceso de gestión de incidencias de la organización identifica los comportamientos que no se ajustan a los objetivos de la organización y los eleva cuando es necesario para crear un plan de acción de gestión que mitigue el riesgo de malos resultados. Los auditores internos pueden revisar los controles clave de las intervenciones eficaces para el cambio de comportamiento, tales como:

- Enfoques basados en la evidencia: El plan de acción incorpora enfoques basados en pruebas para cambiar el comportamiento, fundamentados en la ciencia del comportamiento, los modelos conductuales y la gestión del cambio. Si el enfoque no se basa explícitamente en un modelo específico de cambio de comportamiento, debe combinar estrategias de intervención para:
  - Comunicación: Sensibilizar constantemente a los empleados y a la dirección sobre la necesidad de un cambio de comportamiento y de adoptar y apoyar la transformación.
  - Formación y desarrollo de los empleados: Invertir en programas de formación adaptados a las distintas funciones y dotar a los empleados de las habilidades y comportamientos necesarios mediante talleres, aprendizaje electrónico y oportunidades de desarrollo continuo. Esto incluye aprender y ser capaz de aplicar eficazmente las nuevas habilidades y comportamientos necesarios para lograr los cambios deseados por la organización.
  - Desarrollo de la gestión: Los directivos de todos los niveles se plantean cómo propiciar y demostrar cambios de comportamiento en situaciones cotidianas. Esto puede incluir que la dirección ajuste su propio comportamiento para ayudar al personal a sentirse más cómodo aplicando nuevos comportamientos, que solicite directamente a los empleados que apliquen nuevos comportamientos y que fomente el aprendizaje y solicite formación sobre las habilidades y comportamientos que aún son necesarios. Los programas de liderazgo y el *coaching* pueden perfeccionar las aptitudes y la confianza.
- Refuerzos constantes en situaciones cotidianas: Las personas necesitan apoyo, estímulo y recordatorios periódicos para desarrollar nuevos comportamientos e integrarlos en sus rutinas de trabajo diarias.
- Refuerzo congruente: Un plan de intervención debe alinearse con los mensajes de liderazgo, los procesos, los sistemas, la formación y los mecanismos informales de retroalimentación (*feedback*) para reforzar el cambio deseado. Esta alineación elimina la incertidumbre y la confusión, garantizando que los empleados comprendan los cambios de comportamiento deseados, cómo adoptarlos y su importancia.
- Centrarse en los impulsores u orientadores de los comportamientos: Un cambio de comportamiento sostenible requiere abordar los factores subyacentes (véase

Gestión de Riesgos, C) de los comportamientos en lugar de sólo los propios comportamientos.

- Medición: Medir el progreso y la eficacia de las intervenciones ayuda a determinar si se está logrando el impacto deseado y si se necesitan ajustes. Las actualizaciones periódicas actúan como refuerzo positivo y proporcionan a las partes interesadas información sobre los progresos realizados. Un enfoque de medición eficaz combina métodos cualitativos y cuantitativos, como encuestas y entrevistas, y proporciona una comprensión global de los avances.

F. Los programas de formación destinados a influir en el comportamiento están explícitamente vinculados a expectativas de comportamiento definidas o a declaraciones de propensión al riesgo. Algunos ejemplos de temas de formación son la ética, el cumplimiento, el liderazgo, la inclusión, la concienciación sobre riesgos y la toma de decisiones. Los auditores internos pueden revisar que los programas de formación:

- Reflejen las conductas y actitudes deseadas e incluyan objetivos de aprendizaje claros y documentados.
- Se basen en pruebas de comportamiento o en el aprendizaje de incidentes (por ejemplo, resultados de auditorías, análisis de causas raíz y mecanismos de retroalimentación (*feedback*).
- Se imparten a todos los grupos de roles relevantes, con módulos adaptados a la Alta Dirección, los responsables directos y el personal.
- Son obligatorios cuando proceda (por ejemplo, procesos de alto riesgo, responsabilidades reguladas y funciones de control).
- Se actualizan periódicamente y su contenido se revisa al menos una vez al año, para garantizar su pertinencia y eficacia.
- Diseñado para:
  - Incorporar escenarios del mundo real o estudios de casos para hacer tangibles las expectativas de comportamiento.
  - Utilizar técnicas que involucren a los alumnos (por ejemplo, narración de historias y preguntas reflexivas).
  - Implicar activamente a los altos directivos para que indiquen el tono en la cúpula (*tone at the top*) y animen a los empleados a adoptar cambios de comportamiento.
- Incluir controles de impacto y aseguramiento que:
  - Monitoreen la finalización de la formación obligatoria e informen de las excepciones.
  - Midan el impacto del comportamiento y la retención mediante encuestas informales, pruebas sencillas o evaluaciones basadas en la observación.
  - Capten las perspectivas de los participantes y la eficacia de la formación mediante procesos estructurados de retroalimentación (*feedback*).

- Garanticen que el contenido de la formación esté alineado con los marcos de riesgo y los requisitos de control e incluya procesos formales de revisión y aprobación.

G. Los procesos de contratación se ajustan a las expectativas de comportamiento organizacional e incorporan competencias de comportamiento. Los auditores internos podrán revisar elementos de control tales como:

- Herramientas que permitan evaluar la alineación de los candidatos con los valores de la organización, incluidas guías de entrevista estructuradas y preguntas basadas en escenarios.
- Entrevistas de comportamiento y *feedback* de los compañeros para evaluar rasgos como la empatía, el juicio ético y la responsabilidad.
- Los anuncios de contratación y la marca del empleador reflejan las aspiraciones culturales de la organización para atraer a candidatos culturalmente afines.
- Los mecanismos de retroalimentación (*feedback*) permiten evaluar la integración cultural de las personas recién contratadas, de modo que los desajustes puedan abordarse en una fase temprana.
- La documentación (por ejemplo, marcos de puntuación y registros de entrevistas) demuestra que se aplican criterios coherentes de contratación para la toma de decisiones.
- Recursos Humanos y la Alta Dirección revisan los patrones de contratación en busca de riesgos, como favoritismo, parcialidad o incumplimiento de las normas de conducta.
- Las políticas de contratación y promoción se revisan periódicamente para comprobar su coherencia con los valores de la organización y su eficacia en la práctica.

Apéndice A. Ejemplos de aplicación práctica

Los siguientes ejemplos describen escenarios en los que el Requisito Temático sobre Comportamiento Organizacional sería aplicable.

Ejemplo 1: Revisión independiente del marco de comportamiento de la organización

La Función de Auditoría Interna inició una revisión independiente del marco general de una organización para evaluar su diseño y eficacia operativa en la gestión del riesgo de comportamiento. El alcance de este trabajo abarcaba las estructuras de gobierno, las actividades de gestión de riesgos y los controles de comportamiento que sustentan la alineación en toda la organización.

Los auditores internos evaluaron si las responsabilidades de supervisión del comportamiento estaban claramente definidas y libres de conflictos de intereses. El equipo revisó el reglamento del Consejo/Directorio y verificó que éste había recibido informes periódicos sobre indicadores de riesgo de comportamiento, tales como los resultados de encuestas y las tendencias en la disposición de los empleados a expresar sus inquietudes. La revisión incluyó tanto la evaluación de si las políticas relacionadas con la cultura, como aquellas que rigen la denuncia de irregularidades y la conducta ética, se actualizaban y aplicaban sistemáticamente.

Los auditores internos también evaluaron los elementos de gestión de riesgos, empezando por el marco de gestión de riesgos de comportamiento mantenido por la segunda línea, centrándose en si identificaba los principales factores de riesgo de comportamiento (como una baja seguridad psicológica o unos objetivos de desempeño desalineados). La evaluación hizo hincapié en la forma en que la organización seguía y abordaba la desviación entre los comportamientos esperados y los observados, y en si las anomalías en el comportamiento se elevaban y abordaban sistemáticamente.

Se examinó el entorno de control para determinar si los procesos formales respaldaban las expectativas de comportamiento. Los auditores internos evaluaron los protocolos de contratación para la evaluación basada en valores, si el contenido de la incorporación se ajustaba a las normas de la cultura de la organización y en qué medida se revisaban los incentivos (monetarios y no monetarios) para evitar consecuencias no deseadas. También se probaron los programas de formación, los canales de opinión y de comunicación abierta, los mensajes de liderazgo y los análisis de datos utilizados para detectar problemas de comportamiento.

Este trabajo proporcionó una visión global de cómo se gestiona el riesgo de comportamiento a nivel organizacional y constituyó la base para recomendar mejoras en la infraestructura conductual de la organización.

Ejemplo 2: Revisión temática de las prácticas de incentivos

Este trabajo de auditoría se centró en evaluar cómo influyen en el comportamiento los marcos de incentivos de la organización y si se ajustan a la finalidad, los valores y las expectativas regulatorias de la organización. La Función de Auditoría Interna seleccionó este tema debido a la creciente preocupación por el riesgo de mala conducta y a la aparición de pruebas de comportamientos basados en la presión en las unidades de negocio.

La revisión comenzó evaluando los acuerdos de gobierno para diseñar y aprobar las estructuras de incentivos. La Función de Auditoría Interna evaluó si los responsables de aplicar las decisiones de gobierno, como los comités de recursos humanos o de retribuciones, supervisaban formalmente el diseño de los incentivos y si su trabajo era objeto de una revisión independiente por parte de las funciones de riesgos, cumplimiento o auditoría.

Se aplicó una perspectiva de gestión de riesgos para comprender si el desarrollo de estructuras de incentivos incluía una consideración de sus implicaciones conductuales. Los auditores internos exploraron si la organización había probado escenarios o había analizado riesgos de comportamiento en relación con sus estructuras de incentivos. También examinaron si se realizaba un seguimiento de los indicadores clave de comportamiento, como las puntuaciones de colaboración y si se utilizaban para evaluar los resultados.

Las pruebas de control abarcaron una serie de mecanismos diseñados para moldear los comportamientos relacionados con la recompensa. Entre ellos se incluyen los cuadros de mando integral que incorporan criterios de rendimiento que miden los logros y cómo se han conseguido, la aplicación de cláusulas de "malus" (una penalización o reducción de la retribución) y/o disposiciones de recuperación, y la existencia de procesos de retroalimentación (*feedback*) de 360 grados. Los auditores internos también examinaron la formación impartida a los superiores jerárquicos en materia de retroalimentación (*feedback*) conductual y estudiaron los programas de reconocimiento no monetario que recompensaban la conducta basada en valores.

A lo largo del trabajo, los auditores internos trataron de identificar si las prácticas de incentivos podían impulsar involuntariamente conductas indeseables, como la asunción excesiva de riesgos, utilización de atajos o la reticencia a elevar las incidencias. Se formularon recomendaciones para mejorar la transparencia, integrar de forma más coherente los objetivos basados en valores y reforzar las revisiones independientes de los directivos de segunda línea durante su proceso de diseño de incentivos.

Ejemplo 3: Integración en una auditoría tradicional - gestión del ciber-riesgo

En este ejemplo, la Función de Auditoría Interna incorporó consideraciones de riesgo de comportamiento en un trabajo tradicional para evaluar la gestión del ciber-riesgo. Reconociendo que muchos fallos cibernéticos se deben no sólo a problemas técnicos, sino también al comportamiento humano, los auditores internos incorporaron revisiones de comportamiento a lo largo de todo el trabajo.

El trabajo comenzó evaluando hasta qué punto se reconocía el riesgo de comportamiento dentro del gobierno de la ciber-resiliencia. Los auditores internos revisaron la supervisión de la ciber-estrategia por parte del Consejo/Directorio y la Alta Dirección, buscando pruebas de que los órganos supervisaban y debatían sobre la alineación de los comportamientos, tales como el

cumplimiento de prácticas seguras o el modelado de comportamientos seguros por parte de los líderes, con los objetivos de la organización.

En cuanto a la gestión de riesgos, el equipo evaluó si las evaluaciones de ciber-riesgos de la organización tenían en cuenta los factores humanos. Esto incluía evaluar si los datos sobre el comportamiento (por ejemplo, la frecuencia de los fallos en las pruebas de *phishing*, las infracciones de acceso al sistema o los bajos índices de finalización de la formación) se utilizaban para supervisar y elevar el riesgo. El trabajo también investigó si se había determinado la causa raíz de anteriores incidentes de seguridad para identificar posibles impulsores u orientadores del comportamiento, como la falta de claridad en la rendición de cuentas o el tono de la dirección.

Las pruebas de control se centraron en el diseño del comportamiento y en operaciones seguras. Los auditores internos examinaron si en los procesos de contratación de personal para funciones con acceso privilegiado se incluía un control del comportamiento. Se evaluaron las estructuras de incentivos para ver si fomentaban las prácticas seguras online o si, por el contrario, daban prioridad inadvertidamente a los comportamientos de riesgo frente a la seguridad. También se evaluó la formación en ciberseguridad para determinar si era atrayente para los usuarios, si se actualizaba con regularidad y si incluía simulaciones que pusieran a prueba las respuestas conductuales al *phishing* y a la ingeniería social.

Por último, se analizó cómo la dirección reforzaba los comportamientos seguros a través de la comunicación y si los empleados se sentían cómodos informando de ciber-comportamientos inseguros. Se consideró que una cultura de la organización que animara a los empleados a alzar la voz era un factor fundamental para la resiliencia.

La inclusión de aspectos relacionados con el comportamiento en esta ciber-auditoría dio lugar a conocimientos más profundos y recomendaciones útiles, reforzando la capacidad de la organización para gestionar el riesgo en uno de sus ámbitos más críticos.

Apéndice B. Casos prácticos de auditorías específicas

Estudio de caso 1: Departamento de Vivienda (Sector Público)

Los ejemplos de este caso demuestran cómo la Función de Auditoría Interna de una agencia gubernamental aplicaría el Requisito Temático sobre Comportamiento Organizacional para evaluar cómo la agencia cumple su objetivo de proporcionar servicios de vivienda equitativos al público. Los auditores internos deben reconocer que las prioridades de los funcionarios públicos, las sensibilidades políticas, las asignaciones presupuestarias y algunas opciones políticas quedan fuera de su alcance. Sin embargo, la forma en que los altos funcionarios y los directivos interpretan y aplican estas políticas, así como la cultura interna del departamento en cuestión, están muy presentes.

Gobierno

A. Funciones y responsabilidades - El departamento tiene una estructura organizativa clara con separación de responsabilidades entre el diseño de políticas (altos funcionarios) y la entrega de viviendas. Parte del objetivo de la Función de Auditoría Interna para la contratación es determinar si se evitan los conflictos de intereses estructurales: por ejemplo, ¿está separada la responsabilidad del cumplimiento de la política de la supervisión del contratista?
B. Rendición de cuentas - El jefe de la organización y los altos directivos tienen responsabilidades asignadas en relación con los objetivos organizacionales vinculados a los resultados culturales, como la equidad en la asignación de viviendas y el bienestar del personal. La Función de Auditoría Interna evalúa si la rendición de cuentas es visible y aceptada.
C. Supervisión y control - Un "comité de cultura" presidido por un alto directivo revisa trimestralmente las encuestas al personal, los datos sobre denuncias y las quejas de las partes interesadas. Los auditores internos evalúan si estos procesos proporcionan una alerta temprana de comportamientos desalineados.
D. Políticas y procedimientos - Existen códigos de conducta, directrices para la asignación de viviendas y registros de conflictos de intereses debidamente autorizados, que se revisan periódicamente (por ejemplo, como mínimo cada dos años). La Función de Auditoría Interna evalúa si las actualizaciones reflejan las lecciones aprendidas de los escándalos relacionados con la vivienda y de los informes de auditoría pública.

Gestión de Riesgos

A. Marco de riesgo de comportamiento - El departamento identifica los riesgos culturales que pueden afectar a la prestación de los programas de servicios públicos, tales como el favoritismo en la asignación de viviendas, la excesiva burocracia o la reticencia de los empleados a cuestionar las directrices de los funcionarios públicos. La Función de Auditoría Interna garantiza que estos riesgos se registren formalmente en el registro de riesgos, sean examinados por la dirección y se actúe en consecuencia cuando sea necesario.

B. Indicadores y análisis - Los cuadros de mando registran datos de comportamiento, como la rotación de personal, las quejas, el número de reclamaciones informales de inquilinos y del público, y la capacidad de respuesta a las solicitudes de registros públicos o de libertad de información. Los auditores internos evalúan si los indicadores y los análisis son fiables y se debaten dentro de la agencia.

C. Gestión de diferencias - Cuando surgen diferencias (por ejemplo, casos de denuncia de irregularidades que muestran desviaciones de los principios de imparcialidad), se elevan a la Alta Dirección. Los auditores internos verifican si el análisis de las desviaciones da lugar a medidas correctoras.

D. Participación de las partes interesadas en la resolución - Se consulta a las autoridades competentes, asociaciones de vivienda, sindicatos y paneles ciudadanos cuando se detectan problemas culturales (tales como la descortesía del personal de primera línea o el sesgo en la asignación). Los auditores internos verifican que los comentarios de las consultas influyen en los planes de resolución.

Controles

A. Revisiones del riesgo de comportamiento - Las revisiones retrospectivas se realizan tras fallos de los proyectos de vivienda (por ejemplo, retrasos en la construcción de viviendas sociales). Los auditores internos verifican si se evalúan las causas raíz del comportamiento (tales como la escasa colaboración o la cultura de la culpa).

B. Definición del tono: los altos directivos comunican sus expectativas sobre equidad, imparcialidad y calidad del servicio mediante sesiones públicas y vídeos en la intranet. Los auditores internos verifican si se conocen y aplican estas expectativas.

C. Mecanismos de elevación de incidencias - El departamento mantiene una línea directa de denuncia de irregularidades accesible al público y un proceso de reclamación para inquilinos, personal y miembros del público en general. Los auditores internos examinan la puntualidad, la confidencialidad y la evidencia de ausencia de represalias en las denuncias.

D. Incentivos - Las evaluaciones del desempeño hacen hincapié en la colaboración del personal, el compromiso de las partes interesadas y la equidad en las interacciones con los inquilinos. Los auditores internos evalúan si los ascensos y premios refuerzan estos comportamientos.

E. Supervisión del comportamiento: los responsables directos evalúan al personal en función de las normas de comportamiento (integridad, empatía con los inquilinos

vulnerables) durante las revisiones anuales. Los auditores internos determinan si los resultados son coherentes y si se abordan las pautas del mal comportamiento.

F. Formación - Los programas obligatorios cubren los prejuicios inconscientes, la resolución de conflictos y la toma de decisiones éticas en la asignación de viviendas. Los auditores internos comprueban si los índices de finalización son elevados y evalúan los resultados de las encuestas posteriores a la formación.

G. Procesos de remediación - Cuando se detectan vulneraciones culturales (como la manipulación de las listas de espera de vivienda), se realizan análisis de causas raíz y se supervisan los planes de acción. Los auditores internos comprueban si las medidas correctoras son eficaces y sostenibles.

Información clave

Mientras que la dirección de los funcionarios públicos y el diseño de políticas de alto nivel se encuentran fuera del alcance y control de la Función de Auditoría Interna, las estructuras de gobierno, riesgo y control del departamento en torno al comportamiento son auditables. La aplicación de los 15 requisitos del Requisito Temático sobre Comportamiento Organizacional garantiza que los auditores internos puedan evaluar si el comportamiento organizacional influye en la forma en que se prestan los servicios de vivienda, por ejemplo, de manera justa, transparente y alineada con los valores, a pesar del contexto político.

Estudio de caso 2: Pequeña empresa de construcción (Función de Auditoría Interna de tamaño reducido)

La Función de Auditoría Interna de una empresa de construcción de 50 personas se enfrenta a la preocupación de que el Requisito Temático sobre Comportamiento Organizacional se encuentre diseñado para organizaciones grandes y complejas. Sin embargo, se aplican los mismos principios, a escala. Incluso sin un subcomité del Consejo/Directorio, ni sofisticados cuadros de mando, la empresa puede demostrar que cumple los 15 requisitos del Requisito Temático.

Gobierno

A. Funciones y responsabilidades - El alto directivo de la empresa delega formalmente la responsabilidad de los recursos humanos en el director de oficina y la supervisión de los proyectos en los directores de obra. Los auditores internos evalúan si las funciones están claras y se evitan los conflictos (por ejemplo, que ambas funciones aprueben y controlen los gastos de los proveedores).

B. Responsabilidad - Cada director firma declaraciones trimestrales en las que confirma su responsabilidad por el comportamiento del equipo, incluido el cumplimiento de las normas de seguridad y el trato a los proveedores. Los auditores evalúan si estas declaraciones son razonables y están controladas.

C. Supervisión y seguimiento - La dirección se reúne mensualmente para revisar la rotación de personal, las quejas de los clientes y los informes de seguridad de los proyectos. Los

auditores internos verifican si se plantean y se hace un seguimiento de las cuestiones relacionadas con la cultura.

D. Políticas y procedimientos - Los auditores internos verifican que los códigos de conducta escritos, los protocolos de seguridad y las directrices contra el acoso se revisan anualmente y se comunican al personal.

Gestión de Riesgos

A. Marco de riesgos de comportamiento - La empresa identifica riesgos como la precipitación en el trabajo o la omisión de todos los procedimientos de seguridad requeridos para cumplir los plazos, favoritismo en la asignación de horas extraordinarias y el acoso en las obras. Los auditores internos verifican que estos riesgos estén incluidos en el registro de riesgos.

B. Indicadores y análisis: en lugar de cuadros de mando, la empresa utiliza simples hojas de cálculo para controlar las ausencias, las quejas y los incidentes de seguridad. Los auditores internos evalúan si ponen de relieve ámbitos que deberían revisarse.

C. Gestión de desviaciones - Si las encuestas al personal revelan un desfase entre el "respeto esperado" y la "experiencia real", los directivos deben presentar medidas correctoras en la siguiente reunión. Los auditores internos determinan si las medidas se han implementado y cerrado.

D. Participación de las partes interesadas en la resolución: cuando surgen problemas culturales, se invita a las autoridades competentes, a los representantes de los trabajadores y, a veces, a los clientes clave a que hagan comentarios. Los auditores internos determinan si la respuesta refleja los comentarios recibidos.

Controles

A. Revisiones de riesgos de comportamiento - Después de cualquier fallo del proyecto (como sobrecostes debidos a una colaboración deficiente), el alto directivo organiza una sesión de "lecciones aprendidas". Los auditores internos verifican si se registran las causas culturales (culpa, mala comunicación) y se aplican controles para corregir las acciones en el futuro.

B. Definición del tono - El alto directivo celebra reuniones informativas trimestrales con el personal para reforzar los valores de equidad, calidad y respeto. Los auditores internos recogen las opiniones del personal para comprobar si el tono se percibe.

C. Mecanismos de elevación de incidencias - Al no existir una línea directa formal, se dispone de un buzón de sugerencias cerrado con llave y el acceso directo al alto directivo para canalizar las comunicaciones. Los auditores internos verifican si el personal las utiliza y si existen políticas contra represalias.

D. Incentivos – Los bonus (primas) son modestos, pero están vinculadas al trabajo en equipo y a la opinión de los clientes, no sólo al cumplimiento de los plazos de los proyectos. Los auditores internos revisan si la asignación de incentivos es coherente y razonable.

E. Supervisión del comportamiento - Los supervisores proporcionan comentarios informales sobre la conducta del personal durante las discusiones sobre el desempeño.

Los auditores internos evalúan si la retroalimentación (*feedback*) se aplica de forma coherente en todos los equipos.

F. Formación - Todos los años se imparten talleres breves sobre respeto en el trabajo y seguridad en las obras. Los auditores internos verifican la asistencia y la eficacia mediante entrevistas puntuales.

G. Procesos de remediación - Si se produce acoso o conducta indebida, el directivo (o una autoridad superior si es necesario) investiga, documenta el caso y aplica los resultados. Los auditores internos examinan si las sanciones o medidas correctivas son oportunas y proporcionadas.

Información clave

Incluso sin una segunda línea o un subcomité del Consejo/Directorio, una empresa pequeña puede aplicar los 15 requisitos del Requisito Temático sobre Comportamiento Organizacional mediante mecanismos reducidos: registros sencillos, supervisión directa de la Alta Dirección, revisiones informales y formación proporcionada. Esto demuestra que el Requisito Temático es práctico y pertinente para todas las organizaciones, independientemente de su tamaño.

Apéndice C. Herramienta opcional de documentación

Se espera que los auditores internos ejerzan su juicio profesional para determinar la aplicabilidad de los requisitos, basándose en la evaluación de riesgos y que documenten adecuadamente las exclusiones de determinados requisitos. El Requisito Temático puede documentarse en el Plan de Auditoría Interna o en los papeles de trabajo del proyecto de auditoría interna basándose en el juicio profesional del auditor. Uno o más trabajos de auditoría interna pueden cubrir los requisitos. Además, puede que no todos los requisitos sean aplicables. El formulario imprimible que aparece a continuación ofrece una opción para documentar la conformidad con el Requisito Temático sobre Comportamiento Organizacional, pero su uso no es obligatorio.

Gobierno del Comportamiento Organizacional

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
A. El Consejo/Directorio supervisa y la Alta Dirección estructura las funciones y responsabilidades para evitar consecuencias imprevistas como resultado de un comportamiento organizacional desalineado. Las consecuencias imprevistas incluyen conflictos de intereses o procesos de toma de decisiones poco claros.		
B. El Consejo/Directorio supervisa y la Alta Dirección establece y mantiene la responsabilidad individual y de grupo respecto a las expectativas de comportamiento, garantizando que las funciones y responsabilidades se asumen, se comprenden y se alinean coherentemente con los objetivos de la organización.		

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
C. Existen procesos de gobierno que garantizan la supervisión, evaluación y cuestionamiento periódicos de la adecuación entre las percepciones de comportamiento y los objetivos de la organización, así como la adopción de medidas ante cualquier desajuste.		
D. Se establecen políticas y procedimientos para abordar los riesgos relacionados con el comportamiento, los cuales se revisan periódicamente para asegurar su vigencia y precisión. Estas políticas y procedimientos se comunican eficazmente y se integran en las operaciones y procesos de toma de decisiones de la organización.		

Gestión de riesgos de Comportamiento Organizacional

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
A. La organización ha definido adecuadamente un enfoque para la gestión de los riesgos de comportamiento, incluyendo las características de comportamiento que son críticas para alcanzar los objetivos de la organización.		
B. El seguimiento del comportamiento organizacional es adecuado y oportuno, y los resultados se comunican a las partes interesadas.		
C. Las diferencias entre las expectativas de comportamiento y los comportamientos reales, junto con los análisis de las causas raíz, se comunican de forma eficaz y coherente a las partes interesadas.		

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
D. Las brechas entre las expectativas de comportamiento y las prácticas reales se resuelven con la participación de las partes interesadas. Se hace un seguimiento de las resoluciones hasta su finalización y se miden eficazmente para garantizar que se toman medidas suficientes.		

Controles del Comportamiento Organizacional

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
A. La organización ha diseñado un enfoque para identificar y mitigar patrones de comportamiento dentro de la organización que puedan suponer riesgos para la consecución de sus objetivos. Algunos ejemplos son las revisiones del desempeño y las revisiones del riesgo operacional centradas en el comportamiento.		
B. La organización establece un tono claro y consistente respecto a los comportamientos esperados y comunica estas expectativas a través de canales accesibles y fiables. Se mantienen mecanismos estructurados de retroalimentación para evaluar la comprensión y el apoyo de los empleados y permitir cambios cuando sea necesario.		
C. Se establecen procesos para fomentar la denuncia de comportamientos organizacionales que entren en conflicto con la consecución de los objetivos de la organización. Los procesos incluyen protocolos de protección y resolución.		
D. Los programas de incentivos, incluidas la remuneración y los incentivos no monetarios, se aplican, se comunican y se ajustan a los objetivos de la organización y a los requisitos reglamentarios. También se incluyen los desincentivos y las consecuencias de un comportamiento organizacional inapropiado.		
E. Existe un proceso para gestionar los problemas, que incluye la identificación y corrección de patrones de comportamiento no alineados con los objetivos de la organización y la elevación de problemas cuando sea necesario.		

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
F. Los programas de formación y concienciación diseñados para garantizar la alineación entre el comportamiento organizacional y los objetivos de la organización se imparten de manera periódica y eficaz.		
G. Los procesos de selección e incorporación de personal se encuentran alineados con las expectativas de la organización en cuanto al comportamiento y contemplan competencias conductuales.		

Apéndice D. Mapeo del Marco COSO

El siguiente gráfico relaciona los requisitos de los procesos de gobierno, gestión de riesgos y control del Requisito Temático sobre Comportamiento Organizacional con el *Marco Integrado de Control Interno COSO* (2013) y el *Marco de Gestión de Riesgos Empresariales COSO* (2017). Esta referencia cruzada permite a los auditores internos conciliar sus pruebas basadas en COSO con la cobertura del Requisito Temático sobre Comportamiento Organizacional.

Requisitos de Gobierno

Requisito	Referencia de COSO Control Interno (2013)	Referencia de COSO ERM (2017)
A. El Consejo/Directorio supervisa y la Alta Dirección estructura las funciones y responsabilidades para evitar consecuencias imprevistas como resultado de un comportamiento organizacional desalineado. Las consecuencias imprevistas incluyen conflictos de intereses o procesos de toma de decisiones poco claros.	Entorno de control - Principios 2 (independencia del consejo y supervisión de los canales de escalada), 3 (estructura, autoridad y responsabilidad).	Gobierno y Cultura - Principios 1 (ejerce la supervisión de riesgos por parte del consejo), 2 (establece estructuras operativas).
B. El Consejo/Directorio supervisa y la Alta Dirección establece y mantiene la responsabilidad individual y grupal respecto a las expectativas de comportamiento, garantizando que las funciones y responsabilidades se asumen, se comprenden y se alinean coherentemente con los objetivos de la organización.	Entorno de control - Principios 1 (integridad y valores éticos), 5 (responsabilidad y medidas de desempeño).	Gobierno y Cultura - Principios 4-5 (demuestra compromiso con los valores fundamentales; atrae, desarrolla y retiene a personas capaces).
C. Existen procesos de gobierno que garantizan la supervisión, evaluación y cuestionamiento periódicos de la adecuación entre las percepciones sobre el comportamiento y los objetivos de la organización, así como la adopción de medidas ante cualquier desajuste.	Monitoreo - Principios 16 (evaluaciones continuas/separadas), 17 (evalúa y comunica las deficiencias); Información y Comunicación - Principios 13 (utiliza la información pertinente), 14 (comunica internamente), 15 (comunica externamente, cuando procede).	Gobierno y Cultura - Principio 1 (ejerce la supervisión del riesgo por parte del consejo); Desempeño - Principios 10-14 (identifica el riesgo, evalúa la gravedad, prioriza los riesgos, aplica respuestas al riesgo); Información, Comunicación y Reporte - Principios 18-20 (formación, concienciación y reporte).

Requisito	Referencia de COSO Control Interno (2013)	Referencia de COSO ERM (2017)
D. Se establecen políticas y procedimientos para abordar los riesgos relacionados con el comportamiento, los cuales se revisan periódicamente para asegurar su vigencia y precisión. Estas políticas y procedimientos se comunican eficazmente y se integran en las operaciones de la organización y los procesos de toma de decisiones.	Actividades de control - Principios 10 (selecciona y desarrolla actividades de control), 12 (despliega mediante políticas y procedimientos).	Revisión y Actualización - Principios 15-17 (evalúa el cambio; revisa el desempeño; persigue la mejora).

Requisitos para la gestión de riesgos

Requisito	Referencia de COSO Control Interno (2013)	Referencia de COSO ERM (2017)
A. La organización ha definido adecuadamente un enfoque para la gestión de los riesgos de comportamiento, incluyendo las características de comportamiento que son críticas para alcanzar los objetivos de la organización.	Evaluación de riesgos - Principios 6 (especifica los objetivos adecuados), 7 (identifica y analiza el riesgo), 8 (evalúa el riesgo de fraude), 9 (identifica y analiza los cambios significativos).	Gobierno y Cultura - Principios 3-5 (demuestra compromiso con los valores fundamentales; atrae, desarrolla y retiene a personas capaces); Estrategia y Fijación de objetivos - Principios 6-9 (define el apetito de riesgo, evalúa estrategias alternativas, considera el riesgo en los objetivos).
B. El seguimiento del comportamiento organizacional es adecuado y oportuno, y los resultados se comunican a las partes interesadas.	Información y Comunicación - Principios 13 (utiliza información relevante), 14 (comunica internamente); Monitoreo - Principios 16 (evaluaciones continuas/separadas), 17 (evalúa y comunica deficiencias).	Actuación - Principios 10-14 (identifica el riesgo, evalúa la gravedad, prioriza los riesgos, aplica respuestas al riesgo); Información, Comunicación y Reporte - Principios 18-20 (formación, concienciación y reporte).
C. Las diferencias entre las expectativas de comportamiento y los comportamientos reales, junto con los análisis de las causas raíz, se comunican de forma eficaz y coherente a las partes interesadas.	Información y Comunicación - Principios 14 (comunica internamente), 15 (comunica externamente, cuando proceda).	Información, comunicación y Reporte - Principios 19-20 (comunica información sobre riesgos; informa sobre el riesgo, la cultura y el desempeño).

Requisito	Referencia de COSO Control Interno (2013)	Referencia de COSO ERM (2017)
D. Las brechas entre las expectativas de comportamiento y las prácticas reales se resuelven con las aportaciones de las partes interesadas. Se hace seguimiento de las resoluciones hasta su finalización y se miden eficazmente para garantizar que se toman medidas suficientes.	Actividades de control - Principios 10 (selecciona y desarrolla actividades de control), 12 (despliega mediante políticas y procedimientos); Monitoreo - Principios 16 (evaluaciones continuas/separadas), 17 (evalúa y comunica las deficiencias).	Revisión y Actualización - Principios 15-17 (evalúa el cambio; revisa el desempeño; persigue la mejora).

Requisitos de Control

Requisito	Referencia de COSO Control Interno (2013)	Referencia de COSO ERM (2017)
A. La organización ha diseñado un enfoque para identificar y mitigar patrones de comportamiento dentro de la organización que puedan suponer riesgos para la consecución de sus objetivos. Algunos ejemplos son las revisiones del desempeño y las revisiones del riesgo operacional centradas en el comportamiento.	Evaluación de riesgos - Principios 7 (identifica y analiza el riesgo), 8 (evalúa el riesgo de fraude), 9 (identifica y analiza los cambios significativos); Monitoreo - Principios 16 (evaluaciones continuas/separadas), 17 (evalúa y comunica las deficiencias).	Desempeño - Principios 10-14 (identifica el riesgo, evalúa la gravedad, prioriza los riesgos, implementa respuestas al riesgo); Revisión y Actualización - Principios 15-17 (evalúa el cambio; revisa el desempeño; persigue la mejora).
B. La organización define un tono claro y consistente respecto a los comportamientos esperados y comunica estas expectativas mediante canales accesibles y fiables. Se mantiene mecanismos estructurados de retroalimentación (*feedback*) para evaluar la comprensión y el apoyo de los empleados y permitir cambios cuando sea necesario.	Entorno de control - Principios 1 (integridad y valores éticos), 5 (rendición de cuentas y medidas de desempeño); Información y Comunicación - Principios 13 (utiliza información relevante), 14 (comunica internamente), 15 (comunica externamente, cuando procede).	Gobierno y Cultura - Principios 1 (ejerce la supervisión de riesgos por parte del Consejo), 4 (demuestra su compromiso con los valores fundamentales), 5 (atrae, desarrolla y retiene a personas capaces); Información, Comunicación y Reporte - Principios 18-20 (formación, concienciación y reporte).

Requisito	Referencia de COSO Control Interno (2013)	Referencia de COSO ERM (2017)
C. Se establecen procesos para fomentar el reporte de comportamientos organizacionales que entren en conflicto con la consecución de sus objetivos. Los procesos incluyen protocolos de protección y resolución.	Información y Comunicación - Principio 14 (canales de comunicación interna); Entorno de control - Principio 2 (independencia del consejo y supervisión de los canales de elevación).	Gobierno y Cultura - Principios 1 (ejerce la supervisión de riesgos por parte del consejo), 4 (demuestra su compromiso con los valores fundamentales), 5 (atrae, desarrolla y retiene a personas capaces); Información, Comunicación y Reporte - Principios 19-20 (comunica información sobre riesgos; informa sobre riesgos, cultura y desempeño).
D. Los programas de incentivos, incluidas la remuneración y los incentivos no monetarios, se aplican, se comunican y se ajustan a los objetivos de la organización y a los requisitos regulatorios. También se incluyen los desincentivos y las consecuencias de un comportamiento organizacional inapropiado.	Entorno de control - Principios 1 (integridad y valores éticos), 5 (responsabilidad y medidas de desempeño).	Gobierno y Cultura - Principios 4 (demuestra su compromiso con los valores fundamentales), 5 (atrae, desarrolla y retiene a personas capaces); Desempeño - Principios 10-14 (identifica riesgos, evalúa su gravedad, establece prioridades entre los riesgos, aplica respuestas a los riesgos).
E. Existe un proceso para gestionar los problemas, que incluye la identificación y corrección de patrones de comportamiento no alineados con los objetivos de la organización y la elevación de los problemas cuando sea necesario.	Monitoreo - Principios 16 (evaluaciones continuas/separadas), 17 (evalúa y comunica las deficiencias); Información y Comunicación - Principio 13 (utiliza la información pertinente).	Revisión y Actualización - Principios 15-17 (evalúa el cambio; revisa el desempeño; persigue la mejora); Desempeño - Principios 10-14 (identifica el riesgo, evalúa la gravedad, prioriza los riesgos, implementa respuestas al riesgo).
F. Los programas de formación y concienciación diseñados para garantizar la alineación entre el comportamiento organizacional y los objetivos de la organización se imparten de manera periódica y eficaz.	Entorno de control - Principio 4 (compromiso con la competencia); Información y Comunicación - Principio 13 (utiliza la información relevante).	Gobierno y Cultura - Principio 5 (atrae, desarrolla y retiene a personas capaces); Información, Comunicación y Reporte - Principios 18-20 (formación, concienciación y reporte).

Requisito	Referencia de COSO Control Interno (2013)	Referencia de COSO ERM (2017)
G. Los procesos de selección e incorporación de personal están alineados con las expectativas de la organización en cuanto al comportamiento y contemplan competencias conductuales.	Entorno de control - Principios 1 (integridad y valores éticos), 4 (compromiso con la competencia).	Gobierno y Cultura - Principio 5 (atrae, desarrolla y retiene a personas capaces).

Apéndice E. Actividades de auditoría y aseguramiento relacionadas con el comportamiento

Los auditores internos pueden descubrir que el trabajo que ya están realizando les ayudará a aplicar el Requisito Temático sobre Comportamiento Organizacional. Esta tabla enumera algunas de las auditorías específicas y elementos comunes de auditoría que pueden corresponder a los requisitos y pueden utilizarse para indicar la conformidad, según proceda. Estos ejemplos no deben considerarse auditorías obligatorias, sino que se ofrecen para mostrar cómo las actividades de auditoría más comunes pueden cubrir los Requisitos Temáticos.

Entre los ejemplos de auditorías y actividades de aseguramiento que pueden abordar directa o indirectamente el comportamiento se incluyen:

Área	Auditorías específicas	Elementos de comprobación habituales en las auditorías
Gobierno	• Cultura de riesgo • Gobierno corporativo • Revisión de la eficacia del Consejo/Directorio • Respuesta regulatoria • Compensación de incentivo • Medidas de desempeño • Estrategia y planificación corporativa • Planificación de la transformación • Fusiones y adquisiciones	• Políticas y procedimientos corporativos • Controles de revisión a nivel entidad/dirección • Remediación de asuntos normativos de toda la organización (por ejemplo, plan de mejora del negocio) • Delegación de autoridad
Gestión de Riesgos:	• Función jurídica y de cumplimiento • Marco de gestión de riesgos • Programa de ética y cumplimiento • Asuntos ambientales, sociales y de gobierno • Línea directa para denuncia/revisión de fraudes	• Mantenimiento de registros de riesgos y controles • Autoevaluación de la gestión • Respuesta a fallos de control y a los resultados de auditorías u otros hallazgos

Área	Auditorías específicas	Elementos de comprobación habituales en las auditorías
Controles	• Recursos humanos (incluyendo contratación y retención) • Procesos de venta (por ejemplo, conducta y cumplimiento en las ventas) • Aprovisionamiento (por ejemplo, independencia de proveedores, ocio) • Rama/entidad (por ejemplo, gestión y revisión) • Línea directa para denuncias/revisión de fraudes	• Segregación de funciones • Controles de revisión y seguimiento de la gestión • Riesgos individuales de fraude • Competencias y conciencia del riesgo • Remediación de procesos y controles

Sobre el Instituto de Auditores Internos

El IIA es una asociación profesional internacional que cuenta con más de 265.000 miembros en todo el mundo y ha concedido más de 200.000 certificaciones Certified Internal Auditor® (CIA®) a nivel mundial. Establecido en 1941, The IIA es reconocido en todo el mundo como líder de la profesión de auditoría interna con respecto a las normas, certificaciones, formación, investigación y orientación técnica. Para más información puede visitar: theiia.org.

Descargo de responsabilidad

El IIA publica este documento con fines informativos y educativos. Este material no pretende dar respuestas definitivas a circunstancias individuales específicas y, como tal, sólo pretende servir de guía. El IIA recomienda buscar asesoramiento experto independiente relacionado directamente con cualquier situación específica. El IIA no acepta ninguna responsabilidad por cualquier persona que confíe exclusivamente en este material.

Copyright

Diciembre de 2025

The Institute of
Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101