

A U D I T O R Í A I N T E R N A



LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA



Criticidad de hallazgos y rating de informes de Auditoría Interna

El INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la Auditoría Interna como función clave del buen gobierno. En España cuenta con más de 3.500 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

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



AUDITORÍA
INTERNA



OBSERVATORIO
SECTORIAL



PRÁCTICAS DE BUEN
GOBIERNO



BUENAS PRÁCTICAS
EN GESTIÓN DE RIESGOS

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

ENCUENTRA TODOS LOS DOCUMENTOS DE LA FÁBRICA EN www.auditoresinternos.es



Criticidad de hallazgos y rating de informes de Auditoría Interna

Mayo 2026

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:

Carmen Hernández Del Castillo, CIA, CRMA. IBERDROLA

Estefanía Arribas Arroyo, COSO CI, COSO ERM, TEAI. GLOBALVIA

Joana Berenguer García, CIA. SANITAS

Lucía González Fernández, COSO CI. CAIXABANK

Patricia López León. REDEIA

Cristina López Navarro, CFS, CEFA. BANKINTER

Roberto Martins González, CIA, COSO CI, COSO ERM, TEAI, ECA, PMP.
ABANCA

Silke Morá Teichman. DELOITTE

María Ortiz Ginestal. BANCO COOPERATIVO ESPAÑOL

Gonzalo Rodríguez Abad, COSO CI, CFS-EU. BANCO SABADELL

Jessica Solorzano Morera, CPA, COSO CI, COSO ERM. BANCO NACIONAL
DE COSTA RICA

Laura Sousa Mazzei. BBVA

La creciente complejidad del entorno regulatorio, operativo y tecnológico exige a las funciones de Auditoría Interna disponer de metodologías homogéneas, objetivas y trazables para evaluar la relevancia de los hallazgos y comunicar de forma clara y consistente las conclusiones de sus trabajos. En este contexto, este documento de la FÁBRICA DE PENSAMIENTO propone un marco metodológico práctico para determinar la criticidad de los hallazgos de auditoría y establecer sistemas de calificación o rating de los informes, alineados con las Normas Globales de Auditoría Interna™ (NGAI).

A lo largo del documento se desarrollan los principios clave para la identificación, evaluación y priorización de los hallazgos, combinando criterios cuantitativos, cualitativos y de probabilidad de ocurrencia, y se plantean diferentes escalas y enfoques de categorización adaptables a la naturaleza y madurez de cada organización. De igual forma, se abordan los distintos modelos para la calificación de las conclusiones de los trabajos de auditoría (automáticos, basados en juicio profesional y modelos mixtos), destacando su contribución a una comunicación más clara, comparable y orientada a la toma de decisiones por parte del Consejo y de la Alta Dirección.

El documento subraya también la importancia de la alineación metodológica en entornos de grupo, así como en trabajos realizados en esquemas de *co-sourcing* u *outsourcing*, y analiza el papel emergente de la Inteligencia Artificial como herramienta de apoyo para reforzar la consistencia, eficiencia y capacidad predictiva de Auditoría Interna, siempre como complemento, y no como sustituto, del juicio profesional. En conjunto, esta guía contribuye a fortalecer la calidad, la objetividad y el impacto estratégico de Auditoría Interna como función clave del Buen Gobierno.



Índice

RESUMEN EJECUTIVO	6
INTRODUCCIÓN	7
Exposición de motivos	7
Objetivos	8
CRITICIDAD DE LOS HALLAZGOS	10
Importancia de los hallazgos: definición de los atributos/componentes	10
Metodología para la categorización y priorización de los hallazgos	11
Criterios para la evaluación y priorización de los hallazgos	12
Categorización de los hallazgos: escalas de criticidad	17
Reevaluación de la criticidad	19
RATING DE INFORMES: CALIFICACIONES DE LAS CONCLUSIONES DE LOS TRABAJOS DE AUDITORÍA	20
Escala de rating	20
Cálculo del rating	21
COMUNICACIÓN Y REPORTE DE LOS INFORMES DE AUDITORÍA	24
Coordinación y consolidación con empresas del Grupo	24
Coordinación en proyectos de co-sourcing y/o outsourcing	25
ALINEACIÓN DE METODOLOGÍAS – VISIÓN INTEGRAL	25
USO DE LA INTELIGENCIA ARTIFICIAL	27
CONCLUSIONES	28
ANEXOS	29
BIBLIOGRAFÍA / REFERENCIAS	35



Resumen ejecutivo

Resulta esencial contar con metodologías para evaluar de forma consistente la relevancia de los hallazgos y comunicar claramente las conclusiones al finalizar los trabajos.

Auditoría Interna tiene entre sus principales objetivos proporcionar al Consejo y la Alta Dirección de las organizaciones aseguramiento independiente y objetivo sobre sus procesos de gobierno, gestión de riesgos y control.

Para ello, resulta esencial contar con metodologías estructuradas que permitan evaluar de forma consistente la relevancia de los hallazgos detectados durante los trabajos y comunicar de manera clara las principales conclusiones obtenidas a la finalización de los mismos.

En este documento se propone un marco metodológico orientado a objetivar estos dos elementos clave dentro de los trabajos de auditoría: la determinación de la criticidad de los hallazgos y la calificación o rating de los informes. Todo ello con el fin de reforzar la objetividad, coherencia y trazabilidad en la evaluación de los riesgos identificados, así como mejorar la calidad y claridad en las comunicaciones realizadas a la finalización de los trabajos de Auditoría Interna.

Esto es relevante con carácter general, pero adquiere especial importancia en aquellas organizaciones con múltiples entidades o con modelos de colaboración entre equipos internos y externos, donde resulta esencial contar con una adecuada alineación metodológica para asegurar la consistencia y comparabilidad en las comunicaciones derivadas de los trabajos.

Los hallazgos identificados al observarse diferencias entre los criterios establecidos (lo que debería ser) y la condición observada (lo que es) se analizan considerando una serie de

componentes fundamentales. De cara a su priorización, se propone una metodología que combina criterios cuantitativos y cualitativos, así como la probabilidad de ocurrencia de los riesgos identificados. Los criterios cuantitativos permiten estimar el impacto potencial en términos económicos u operativos y los cualitativos permiten considerar otros aspectos como los relacionados con el cumplimiento normativo, la madurez del entorno de control o el impacto reputacional y estratégico.

De esta forma, mediante la combinación del impacto y la probabilidad se pueden clasificar los hallazgos en distintos niveles de criticidad, lo que no solo facilita la priorización y el seguimiento de las acciones correctivas, sino que también mejora la asignación de recursos, aporta mayor visibilidad sobre los riesgos más relevantes y permite una toma de decisiones más coherente y focalizada.

Dado que, además de evaluar individualmente los hallazgos, Auditoría Interna emite una comunicación final sobre los trabajos, el establecimiento de escalas o ratings de valoración de informes facilita expresar de forma clara y estructurada la opinión del auditor sobre los procesos de gobierno, gestión de riesgos y control revisados.

Se plantea que el rating de los informes pueda obtenerse mediante modelos basados en la criticidad de los hallazgos, así como mediante el uso del juicio profesional o a través de un modelo mixto, que combina el uso de ambos enfoques.

El documento también menciona el papel creciente de la Inteligencia Artificial, como herra-



mienta de apoyo para facilitar la evaluación consistente de los hallazgos, automatizar el cálculo de ratings e, incluso, ayudar a identificar ciertos patrones o riesgos emergentes. No obstante, se plantea su uso de forma complementaria y que, en ningún caso, sustituye el juicio profesional del auditor.

En resumen, implantar un marco metodológico homogéneo para la evaluación de hallazgos y la calificación de los informes refuerza la calidad, objetividad y coherencia del trabajo de Auditoría Interna, incrementando así su capacidad para contribuir a que las organizaciones creen, protejan y sostengan su valor.



Introducción

1. EXPOSICIÓN DE MOTIVOS

El propósito principal de Auditoría Interna, tal y como se recoge en el Dominio I de las *Normas Globales de Auditoría Interna* (en lo sucesivo NGAI), es proporcionar al Consejo y a la Alta Dirección aseguramiento, asesoramiento, prospectivas y previsiones de manera independiente, objetiva y basada en riesgos, es decir, de manera imparcial y libre de sesgo.

Durante la realización de las auditorías, todas aquellas diferencias entre los criterios de evaluación y la condición¹ deberán ser comunicadas como hallazgos de auditoría siempre que supongan que la organización esté expuesta a un riesgo significativo².

Dado que un hallazgo implica un fallo en los controles o un riesgo no gestionado adecuadamente, es necesario que la organización afronte su remediación mediante el corres-

pondiente plan de acción orientado a mitigar las debilidades identificadas.

Tal y como establecen las NGAI³, se debe **evaluar cada potencial hallazgo del trabajo para determinar su importancia**, para lo cual, **asignar una calificación de criticidad a cada hallazgo se constituye como una herramienta eficaz**. Asimismo, se establece que, para determinar la importancia del riesgo, los auditores internos deben considerar su probabilidad de ocurrencia y el impacto que podría tener sobre los procesos de gobierno, gestión de riesgos y control de la organización.

Si bien no existe una escala de criticidad universal y estandarizada que se pueda aplicar de forma idéntica a todas las organizaciones, la asignación de criticidad, además de reflejar el potencial efecto de las incidencias detecta-

Las NGAI establecen que se debe evaluar cada potencial hallazgo del trabajo para determinar su importancia; por lo que la asignación de una calificación de criticidad a cada hallazgo se constituye como una herramienta eficaz.

1. La norma 14.2 *Análisis y potenciales hallazgos del trabajo* define la condición como el estado existente de la actividad bajo revisión.

2. Norma 14.3 *Evaluación de los hallazgos*.

3. Norma 14.3 *Evaluación de los hallazgos*.

El uso de modelos de objetivación en Auditoría Interna permite reforzar la objetividad, la coherencia y la trazabilidad en la valoración de los hallazgos y en la determinación de las conclusiones de los trabajos.

das, ayudará a la priorización de los planes de acción, ya que los hallazgos con una criticidad más alta requerirán una atención más inmediata y medidas correctoras más contundentes. Además, el grado de criticidad de los hallazgos podrá tener implicaciones sobre su proceso de seguimiento y/o comunicación, en función de la metodología definida en cada organización.

Todos los hallazgos identificados durante la realización de la auditoría deberán ser considerados en la **conclusión de los trabajos de aseguramiento**⁴, situando la importancia general de los mismos en su conjunto⁵ y la adecuada perspectiva de sus efectos sobre los objetivos revisados.

Dicha conclusión, por lo tanto, sirve para resumir los resultados del trabajo en relación con los objetivos planificados. Al igual que en el caso de la asignación de criticidad en los hallazgos, el uso de una **escala de calificación o rating** para las conclusiones de los trabajos supone una herramienta eficaz de comunicación de los resultados de las auditorías, al contextualizar de manera clara y sencilla la importancia global de las conclusiones alcanzadas.

2. OBJETIVOS

El propósito principal de este documento es proporcionar una **guía metodológica** a los auditores internos, para establecer un **modelo de objetivación** que ayude a determinar:

Por tanto, las comunicaciones de Auditoría Interna⁶ deben incluir tanto la relación de hallazgos identificados –con una criticidad asociada que determine su importancia y priorización–, como una calificación o rating de las principales conclusiones, en relación con los objetivos del trabajo.

En este contexto, el uso de modelos de objetivación en Auditoría Interna permite reforzar la objetividad, la coherencia y la trazabilidad en la valoración de los hallazgos y en la determinación de las conclusiones de los trabajos, facilitando una comunicación clara y consistente de los resultados a los órganos de gobierno y a la Alta Dirección.

Por lo tanto, el uso de **modelos de objetivación** de auditoría sirve como base para **establecer niveles de criticidad de los hallazgos de auditoría y determinar la calificación de las conclusiones de auditoría** de manera objetiva, imparcial y libre de sesgo. La asignación de las criticidades de los hallazgos y calificaciones de las auditorías se basará en la evaluación de la materialidad o importancia relativa de cada auditoría.

- La criticidad de los hallazgos de auditoría.
- Las calificaciones de las conclusiones de los trabajos de auditoría.

4. En adelante, cuando se menciona la conclusión de los trabajos, se hace referencia únicamente a aquellos que corresponden a servicios de aseguramiento realizados por la Función de Auditoría Interna, excluyendo otras actividades como los servicios de asesoramiento o de otro tipo.

5. Norma 14.5 *Conclusiones del trabajo*.

6. Norma 15.1 *Comunicación final del trabajo*.



Las **VENTAJAS** de establecer estos modelos de objetivación de criticidades de hallazgos y de rating de conclusiones son las siguientes:

- Permitir la **priorización de planes de remediación** de manera más eficiente y acorde al riesgo identificado, aumentando la madurez del marco de control de la entidad.
- Optimizar la **trazabilidad** de la evaluación de la criticidad, tanto de los hallazgos como de las conclusiones de auditoría, a través de criterios objetivos y la documentación uniforme de criterios expertos.
- Hacer más **eficiente** la comprensión y homogeneización del reporte a los órganos de gobierno y administración de la organización y/u organismos públicos.
- Asegurar que la criticidad de los hallazgos y el rating de conclusiones de los informes de auditoría asignadas por los distintos equipos de auditoría y filiales son **uniformes y consistentes**, facilitando la comparabilidad y homogeneidad del reporte (*ver punto 5. Alineación de Metodologías - Visión integral*).



En cambio, las posibles **INEFICIENCIAS** que se observan cuando no existen modelos de objetivación de criticidades de hallazgos ni de calificaciones de conclusiones son:

- **Divergencia** en los criterios de valoración de las criticidades de hallazgos entre distintas organizaciones, áreas de control interno dentro de la propia organización e, incluso, entre diferentes equipos de auditoría dentro de la propia Función de Auditoría Interna.
- Rating de conclusiones de auditoría **no uniforme o poco consistente** entre los diferentes equipos de auditoría.
- Prevalencia de criterios exclusivamente cualitativos y/o de juicio experto.
- Ausencia de vínculos de criterios cuantitativos con el concepto de materialidad.



Estas ineficiencias pueden derivar en las siguientes **CONSECUENCIAS**:

- Dificultades a la hora de priorizar planes de remediación para los hallazgos identificados.
- Dificultad para priorizar el reporte acumulado de todos los hallazgos, a los órganos de gobierno.
- Dificultad, por parte de los destinatarios de las recomendaciones, para comprender el nivel de objetividad en la valoración de la criticidad de los hallazgos.
- Criterios poco trazables, en la determinación de la criticidad, para organismos supervisores externos, tales como el Banco Central Europeo (BCE), el Banco de España (BdE), Dirección General de Seguros y Fondos de Pensiones (DGSFP) o la Comisión Nacional del Mercado de Valores (CNMV), entre otros.
- Dificultad para concluir correctamente o de forma objetiva en las comunicaciones finales del trabajo de auditoría.

Con todo ello, se propone contribuir a **mejorar las comunicaciones** al Consejo, a la Alta Dirección o a otros órganos a los que reporte

la Función de Auditoría Interna, de los resultados de los trabajos que ésta lleva a cabo.



Criticidad de los hallazgos

1. IDENTIFICACIÓN Y COMPONENTES DE LOS HALLAZGOS

Los atributos básicos que constituyen el hallazgo son: criterio, condición, causa y efecto (impacto).

Las NGAI definen el **hallazgo** como “las diferencias entre los criterios de evaluación y el estado existente de la actividad bajo revisión, conocido como *condición*”⁷..., debiendo ser comunicada a la Dirección de la entidad auditada. Es decir, un hallazgo surge de la divergencia en el contraste entre los hechos observados (**condición** o “*lo que es*”) y los criterios de auditoría (**criterio** o “*lo que debería ser*”).

Como ejemplos de la diferente casuística de hallazgos pueden citarse, entre otros, la no conformidad con la normativa, o deficiencias que deberán subsanarse para prevenir su incumplimiento; errores en la ejecución de controles; riesgos no gestionados adecuadamente; uso ineficiente de recursos; situaciones de conflicto de interés o vulneración del código ético; situaciones que impliquen asumir un nivel de riesgo superior al deseado por la organización, tal y como se establece en su apetito de riesgo; y/o situaciones que impliquen que la organización se desvíe significativamente en el cumplimiento de los objetivos corporativos establecidos.

Los **atributos básicos** que constituyen el hallazgo son, entonces⁸:

- **Criterio:** norma o parámetro con la que el auditor interno mide la condición. Los criterios constituyen las unidades de medida que permiten la evaluación de la condición. Se identifica con “*lo que debería ser*”.
- **Condición:** constituye la situación existente observada por el auditor interno con respecto a una operación, actividad o transacción. La condición refleja el grado en el que los criterios están siendo logrados o aplicados. Se identifica con “*lo que es*”.
- **Causa:** es la razón o razones fundamentales por las cuales se materializó la condición, es decir, el motivo por el que no se cumplió el criterio. La causa enfatiza la razón de la diferencia entre la condición y el criterio. El análisis de la causa debería alcanzar el nivel de la causa raíz para poder identificar las razones subyacentes, basando la recomendación de auditoría en la misma, ya que, de este modo, se evitaría que la misma tipología de incidencias se repitiera en el futuro.

7. Norma 14.2 *Análisis y potenciales hallazgos del trabajo*

8. Norma 14.2 *Análisis y potenciales hallazgos del trabajo* y Norma 14.3 *Evaluación de los hallazgos*



- **Efecto/Impacto:** es la materialización, resultado o consecuencia real o potencial de la incidencia detectada (divergencia entre la condición y el criterio). Sea real o potencial, debe definirse en la medida de lo posible en términos cuantitativos –tales como moneda, tiempo, unidades de producción o número de transacciones–, lo que ayuda a demostrar la necesidad de la acción correctiva y proporciona evidencia sobre la importancia del hallazgo. Aunque en algunas ocasiones no sea posible la cuantificación del efecto, se debe informar siempre sobre las observaciones importantes.

A partir de los hallazgos identificados, se formularán las **recomendaciones de auditoría** que se consideren necesarias para remediar las divergencias identificadas. La recomendación de auditoría constituye el principal mecanismo mediante el cual Auditoría Interna contribuye a generar y proteger el valor de la organización.

El compromiso efectivo con las recomendaciones se formaliza a través de un **plan de acción**, que será diseñado por el área audita-

da y describe las medidas específicas que la Dirección asumirá para corregir las deficiencias identificadas. El plan de acción es fundamental para asegurar que las recomendaciones se implementen de manera efectiva y oportuna. Es importante establecer recomendaciones y/o planes de acción que aborden la **causa raíz** identificada en cada hallazgo.

Si bien la estructura del plan de acción puede variar según cada organización, el área auditada deberá establecer, al menos, los siguientes **aspectos básicos**:

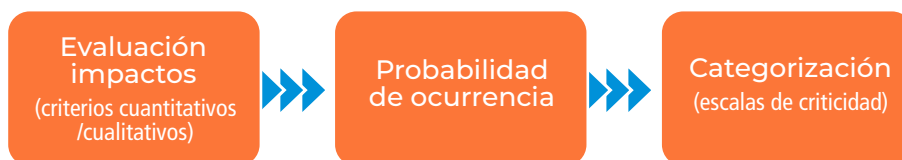
- **Acciones por ejecutar**, detalladas y orientadas a resolver las causas identificadas.
- **Responsables.** En algunas organizaciones puede existir una doble responsabilidad, diferenciando entre el responsable del riesgo (es decir, el área o centro sobre el que recae el riesgo o está directamente afectada por el hallazgo) y el responsable de implementar el plan de acción.
- **Fecha prevista de implantación**, que permita establecer plazos de seguimiento y control.

Los auditores internos deben priorizar los hallazgos con base en la importancia de su efecto, empleando metodologías para su categorización y priorización.

2. METODOLOGÍA PARA LA CATEGORIZACIÓN Y PRIORIZACIÓN DE LOS HALLAZGOS

Una vez establecidos los hallazgos, los auditores internos deben priorizarlos con base en la importancia de su efecto, empleando las

metodologías para la categorización y priorización de los hallazgos que establezca cada Función de Auditoría Interna.



La adecuada evaluación y priorización de los hallazgos permite no solo dimensionar su re-

levancia, sino también enfocar los recursos de la organización en aquellas debilidades que

Es recomendable que la metodología contenga criterios (cuantitativos y cualitativos); criterios para valorar la probabilidad de ocurrencia; y una escala de valoración.

representan mayor riesgo para el logro de sus objetivos estratégicos y operativos, considerando de forma integrada los distintos impactos relevantes.

Será recomendable que la metodología implementada contenga, al menos, los siguientes aspectos:

- **Criterios** cuantitativos y cualitativos que determinen la **relevancia** de los hallazgos.
- Criterios para valorar la **probabilidad de ocurrencia** de los efectos derivados de los hallazgos.

3. CRITERIOS PARA LA EVALUACIÓN Y PRIORIZACIÓN DE LOS HALLAZGOS

A continuación, se presenta una propuesta de los criterios para evaluar los posibles impactos y establecer así la priorización de los hallazgos.

3.1 CRITERIOS CUANTITATIVOS

Los criterios cuantitativos permiten medir de manera objetiva el efecto de la incidencia identificada. Para ello, se utilizan magnitudes numéricas y estadísticas para determinar la importancia y relevancia de los errores o deficiencias detectadas.

La implementación de una metodología cuantitativa para dimensionar la relevancia de los hallazgos identificados permite realizar una evaluación objetiva, sistemática y homogénea de las debilidades detectadas por Auditoría Interna, reduciendo la subjetividad en la toma de decisiones y ofreciendo las siguientes **VENTAJAS**:

- **Mejora de la toma de decisiones:** aporta información objetiva para la definición de acciones correctivas.

- **Escala** de categorización de los hallazgos, con base en los criterios de importancia y la probabilidad de ocurrencia.

Asimismo, se podrán considerar otros posibles factores asociados, tales como criterios de comunicación en base a la relevancia (es decir, los niveles de escalado de cara a la comunicación de los hallazgos), cambios de la criticidad a lo largo del ciclo de vida de los hallazgos, etc.

- **Transparencia:** mejora la comunicación de los hallazgos y su gravedad ante las partes interesadas, mostrando el impacto real de los hallazgos.

- **Comparabilidad:** permite analizar resultados entre diferentes áreas, períodos o unidades de negocio de manera consistente.

- **Priorización efectiva:** facilita la identificación de áreas críticas que requieren atención inmediata con base en el nivel de riesgo cuantificado.

- **Seguimiento estructurado:** contribuye al monitoreo del grado de avance en la mitigación de riesgos y en la implementación de mejoras.

Para poder estructurar esta metodología, es necesario considerar las siguientes **FASES**:

1. CONOCER EL IMPACTO ASOCIADO A LA DEBILIDAD

La aplicación de métodos cuantitativos para determinar los impactos de las debilida-

des requiere, en primer lugar, realizar una **estimación del impacto** que la debilidad identificada, o los eventos derivados de su materialización, puede generar sobre los procesos de gobierno, gestión de riesgos y control.

Entre los tipos de impactos a considerar se pueden incluir:

- Pérdidas financieras derivadas de fraudes, errores contables, pagos indebidos, malversación de fondos, etc.
- Costes por sanciones regulatorias: el incumplimiento normativo puede dar lugar a multas o penalizaciones impuestas por entidades reguladoras.
- Sanciones por incumplimiento de obligaciones contractuales que puedan resultar en demandas legales, indemnizaciones y los gastos jurídicos asociados.
- Impacto en ingresos futuros: la disminución de la calidad del producto, del servicio al cliente o de la transparencia financiera puede traducirse en pérdida de clientes, disminución de la confianza del mercado o reducción de oportunidades comerciales.
- Aumento de costes operativos: ineficiencias en procesos internos (duplicidad de funciones o planificación deficiente) generan gastos innecesarios, desperdicio de recursos y demoras operativas que afectan al flujo de caja.
- Deterioro de activos y/o pérdida de inventario: deficiencias en el control de inventarios o custodia de los activos pueden derivar en pérdidas físicas, caducidad de productos u obsolescencia.

2. DEFINIR UMBRALES DE CRITICIDAD

Para dimensionar adecuadamente la relevancia del impacto estimado se pueden establecer **umbrales cuantitativos** de referencia que permitan comparar y clasificar dicho impacto de manera objetiva.

La definición de estos umbrales debe considerar variables como el apetito y la tolerancia al riesgo establecida por la organización. Asimismo, se podrían considerar otros factores adicionales tales como la materialidad financiera utilizada por auditores externos u organismos reguladores.

Ejemplos de criterios cuantitativos para el establecimiento de umbrales pueden ser los siguientes:

- Porcentaje de ingresos, activos o patrimonio neto: estableciendo el umbral de error que se considera material.
- Errores en el balance o en la cuenta de resultados: evaluando el impacto de los hallazgos en las cuentas individuales y en el balance en su conjunto, o en las ventas, ingresos brutos, margen u otras variables de la cuenta de resultados.
- Frecuencia de los hallazgos: analizando la repetición de un error para determinar si es un problema sistemático o aislado.
- Efecto en otras magnitudes: el volumen de transacciones afectadas, el número de productos o servicios involucrados, o el número de clientes y/o de empleados en los que impacta.

El impacto estimado se compara con los umbrales calculados con los ejemplos anteriores, lo que permite calificar los hallazgos en los niveles de criticidad establecidos en la organización, o bien ponderarse

Para dimensionar adecuadamente la relevancia del impacto estimado se pueden establecer umbrales cuantitativos de referencia que permitan comparar y clasificar dicho impacto de manera objetiva.

Los criterios cualitativos se emplean cuando no es posible medir de manera objetiva el efecto de la incidencia identificada mediante criterios cuantitativos.

con determinados factores, considerando, por ejemplo, el nivel de riesgo de auditoría o la criticidad del proceso, entre otros.

3. REVISAR Y RECALIBRAR LOS UMBRALES

Con el fin de garantizar la razonabilidad de los umbrales de materialidad definidos, es recomendable realizar un ejercicio periódico de *backtesting*, para determinar si éstos permiten una clasificación adecuada de los hallazgos o si, por el contrario, generan distorsiones en la priorización de riesgos debido a una posible sobrestimación o subestimación de su impacto.

Este proceso de *backtesting*, o proceso de validación, requiere un análisis retrospectivo basado en datos históricos, contrastando el comportamiento de los umbrales frente a eventos reales ocurridos. Esta evaluación permite ajustar su precisión, sensibilidad y capacidad discriminativa, asegurando así que los umbrales sigan alineados con el perfil de riesgo, la tolerancia definida por la organización y las condiciones operativas del entorno.

Aunque el análisis cuantitativo proporciona una base objetiva y estructurada para la evaluación de riesgos, puede ser necesario complementarlo con análisis basados en criterios cualitativos.

3.2 CRITERIOS CUALITATIVOS

Los criterios cualitativos se emplean cuando no es posible medir de manera objetiva el efecto de la incidencia identificada en términos económicos o numéricos, tal y como se hace con los criterios cuantitativos, pero que tienen un impacto significativo en la valoración

de un hallazgo y que consideran factores como el contexto, los riesgos inherentes y los posibles impactos en la organización, más allá del aspecto financiero o económico.

A continuación, se exponen los principales criterios cualitativos clasificados según temáticas comunes, con el fin de facilitar su interpretación y aplicación práctica:

1. MARCO NORMATIVO

Los hallazgos de Auditoría Interna pueden estar relacionados con el incumplimiento de requerimientos relativos a la normativa externa o del marco de gobierno interno de la unidad auditada. La identificación del tipo de normativa vulnerada permite dimensionar la gravedad del hallazgo y su posible impacto reputacional, legal o estratégico.

A continuación, se establecen algunos ejemplos:

- Legal / regulatorio: infracción de leyes, disposiciones de organismos supervisores / reguladores o licencias.
- Política y normativa interna: incumplimiento de políticas, procedimientos, normas, instrucciones técnicas, etc.
- Estándares y marcos de referencia externos: nivel de conformidad con marcos internacionales (por ejemplo: ISO, COSO, IFRS⁹).

2. ENTORNO DE CONTROL

Uno de los aspectos fundamentales para tener en cuenta en la valoración del hallazgo es el análisis de la existencia y/o madurez del entorno de control en la or-

9. ISO: "International Organization for Standardization"; COSO: "Committee of Sponsoring Organizations of the Treadway Commission"; IFRS: "International Financial Reporting Standards".



ganización o en el proceso evaluado. Este análisis permite evaluar los riesgos existentes, teniendo en cuenta si los controles internos están correctamente identificados, diseñados e implantados.

Un factor complementario relevante es el grado de automatización del proceso (automático, manual o semiautomático) ya que esto incide en la evaluación de la eficacia de los controles definidos.

Asimismo, este criterio permite la identificación del origen o causa-raíz del hallazgo, que puede estar relacionado con aspectos como:

- Diseño del proceso: no existen mecanismos de prevención o detección. El control no ha sido identificado.
- Ejecución deficiente: el control existe, pero el diseño no es adecuado o no se aplica correctamente.
- Falta de formación/sensibilización: el personal desconoce el control o su propósito.
- Cultura de control deficiente: el nivel de sensibilización de la organización sobre la importancia del control interno es bajo.

También se podrían utilizar los componentes COSO (entorno de control, evaluación de riesgos, actividades de control, información y comunicación y supervisión) como otra forma de estructurar la evaluación del entorno de control como criterio cualitativo.

3. ALCANCE O EXTENSIÓN DEL HALLAZGO

Un hallazgo puede afectar, conforme a la estructura de cada organización, a múltiples unidades o diversas geografías (áreas, filiales, etc.).

Adicionalmente, el hallazgo puede estar localizado en un área o en un proceso, ser un caso puntual o recurrente, o repetido en el tiempo en distintas auditorías.

4. OTROS FACTORES ASOCIADOS A RIESGOS RELEVANTES PARA LAS ORGANIZACIONES

Además de los criterios previamente mencionados, pueden considerarse otros factores cualitativos vinculados a los riesgos identificados en los mapas de riesgos o planes estratégicos de la organización. Estos factores permiten enriquecer la valoración del hallazgo y asignar un nivel de criticidad más alineado con el perfil de riesgo de la organización, lo cual resulta clave para determinar la prioridad de la recomendación correspondiente.

Entre los factores a considerar, se incluyen:

- **Riesgo estratégico o de negocio:** cuando el hallazgo afecta directamente al cumplimiento de los objetivos estratégicos.
- **Riesgo tecnológico o de ciberseguridad:** especialmente relevante en entornos digitales o automatizados.
- **Riesgo ambiental, social y de gobierno (ESG):** vinculado al cumplimiento de compromisos ambientales, sociales y de gobernanza.
- **Riesgo en seguridad y salud ocupacional:** cuando compromete la integridad física o el bienestar del personal de la organización.
- **Riesgo reputacional:** cuando el hallazgo puede afectar negativamente la imagen institucional ante reguladores, usuarios o la opinión pública en general.

Adicionalmente, pueden considerarse otros factores cualitativos vinculados a los riesgos identificados en los mapas de riesgos o planes estratégicos de las organizaciones.

En el Anexo I se incluye un ejemplo de una posible matriz de valoración de impactos, usando los criterios cuantitativos y cualitativos comentados anteriormente.

3.3 PROBABILIDAD DE OCURRENCIA

La probabilidad de ocurrencia hace referencia a la posibilidad de que el riesgo asociado al hallazgo se concrete de manera efectiva.

Como se ha señalado anteriormente, la criticidad de un hallazgo se determina a partir de la combinación entre el impacto potencial que podría generar en caso de materializarse y la probabilidad de ocurrencia del riesgo identificado.

En este contexto, la probabilidad de ocurrencia hace referencia a la posibilidad de que el riesgo asociado al hallazgo se concrete efectivamente. Cabe destacar que, en la mayoría de los casos, esta probabilidad se estima a partir del juicio profesional o criterio experto del auditor interno, sustentado en información histórica, en el análisis del entorno de control y en otros antecedentes relevantes.

Por tanto, suele tratarse de una probabilidad teórica o estimada que, si bien no puede expresarse con total certeza empírica, debe encontrarse debidamente justificada, documentada y aplicada de forma coherente en todo el proceso de auditoría.

En caso de que la organización cuente con modelos de evaluación de riesgos donde se valore la probabilidad de ocurrencia del mismo tipo de hallazgos identificados mediante métodos estadísticos (tales como generación de escenarios u otros), podrá considerarse su utilización siempre y cuando así lo recojan las metodologías de auditoría interna aprobadas.



La elección de una escala de probabilidad adecuada depende, entre otros factores, de la disponibilidad de información, del tipo de auditoría y del grado de madurez del enfoque basado en riesgos de la entidad.

Las escalas de probabilidad pueden tener diferentes números de niveles, desde dos hasta cinco o más categorías (poco habitual), y pueden basarse en descripciones generales de ocurrencia o hacer referencia a porcentajes establecidos de materialización.

El uso de escalas binarias reduce la subjetividad ya que minimiza la ambigüedad al forzar una clasificación clara. Por su parte, las escalas de tres o cuatro niveles permiten una mayor diferenciación, ya que se consideran niveles intermedios de riesgo sin llegar a una complejidad excesiva.

A continuación, se muestran los ejemplos más habituales.

EJEMPLO DE ESCALA BINARIA

NIVEL	CATEGORÍA	DESCRIPCIÓN
1	Probable (Probabilidad Alta) 	El riesgo tiene alta probabilidad de materializarse en el corto o medio plazo.
2	No Probable (Probabilidad Baja) 	La ocurrencia del riesgo es altamente improbable; sólo sería posible en escenarios limitados o excepcionales.

EJEMPLO DE ESCALA DE TRES NIVELES

NIVEL	CATEGORÍA	DESCRIPCIÓN
1	Remoto (Bajo)	La ocurrencia del riesgo es altamente improbable; sólo sería posible en escenarios excepcionales o muy inverosímiles.
2	Posible (Medio)	El riesgo podría materializarse bajo ciertas condiciones específicas o en escenarios limitados.
3	Probable (Alto)	El riesgo tiene alta probabilidad de materializarse en el corto o medio plazo, dadas las condiciones observadas.

EJEMPLO DE ESCALA DE CUATRO NIVELES

NIVEL	CATEGORÍA	DESCRIPCIÓN
1	Remoto (Bajo)	La probabilidad de materialización es menor al 15%.
2	Posible (Medio)	La probabilidad de materialización está entre el 15% y el 50%.
3	Probable (Alto)	La probabilidad de materialización está entre el 50% y el 85%.
4	Altamente Probable (Muy Alto)	La probabilidad de materialización es superior al 85%.

4. CATEGORIZACIÓN DE LOS HALLAZGOS: ESCALAS DE CRITICIDAD

Una vez definidos los criterios cuantitativos, cualitativos y de probabilidad de ocurrencia, se plantea proceder a la **categorización de los hallazgos** identificados durante las auditorías.

Este paso resulta fundamental para **priorizar** la atención de los riesgos detectados y orientar la formulación de recomendaciones proporcionales a la severidad del hallazgo.

4.1 OBJETIVO DE LAS ESCALAS DE CRITICIDAD DE HALLAZGOS

Las **escalas de criticidad** o de valoración, son herramientas metodológicas que permiten **comunicar de forma estructurada y objetiva la gravedad de los hallazgos** identificados. Su uso facilita una evaluación homogénea, estandarizada y comprensible para todos los interlocutores del proceso de auditoría.

La terminología empleada y los criterios específicos de evaluación pueden variar según la naturaleza, el sector o el marco normativo de cada organización.

Es esencial que, independientemente de la escala adoptada, ésta se encuentre claramente definida y sea comprendida por todos los involucrados. Además, debe aplicarse de manera uniforme con el fin de asegurar la objetividad, la trazabilidad y la comparabilidad en la evaluación de los riesgos.

Es importante destacar que la terminología empleada y los criterios específicos de evaluación pueden variar según la naturaleza, el sector o el marco normativo de cada organización. A pesar de esta variabilidad, existen principios comunes que sustentan el diseño de estas escalas, las cuales suelen estructurarse en tres o cuatro niveles jerárquicos.

4.2 ENFOQUES PARA LA CATEGORIZACIÓN

Las escalas para la valoración de los hallazgos pueden basarse en diferentes enfoques de

evaluación del riesgo, entre los que destacan los siguientes:

- **Impacto potencial o real** del hallazgo, ya sea económico, operativo, reputacional u otros, sin considerar inicialmente la probabilidad de ocurrencia.
- **Importancia** del proceso o área afectada, en función de su peso dentro de la estructura operativa o estratégica de la organización.
- **Nivel de debilidad del control interno**, considerando su capacidad para prevenir, detectar o mitigar los riesgos asociados.
- **Prioridad de implantación:** prioriza la urgencia con la que debe corregirse un hallazgo, considerando su impacto, el riesgo asociado y la criticidad del proceso afectado.

A continuación, se presentan ejemplos representativos de posibles escalas a utilizar para clasificar los hallazgos de auditoría.

EJEMPLOS DE ESCALAS APLICABLES




MEDIDA DE EVALUACIÓN	ESCALA DE VALORACIÓN DEL HALLAZGO
Nivel de riesgo / Impacto de la debilidad	Crítico, Alto, Medio, Bajo
Importancia del proceso	Crítico, Alto, Medio, Bajo
Debilidad del control	1, 2, 3, 4
Prioridad de implantación	Alta, Media, Oportunidad de mejora

MEDIDA DE EVALUACIÓN: NIVEL DE RIESGO / IMPACTO

NIVEL DE RIESGO / IMPACTO	DESCRIPCIÓN
<p>Bajo</p>	Deficiencias de naturaleza menor, con un impacto limitado en la situación financiera, los fondos propios o el perfil de riesgo de la entidad.
<p>Medio</p>	Deficiencias que, si no se corrigen, podrían tener un impacto adverso en la entidad, aunque no de forma inmediata o severa. Afectan a la eficacia de los controles internos o a la gestión de riesgos en áreas específicas.
<p>Alto</p>	Deficiencias significativas que suponen una amenaza para la solvencia, la liquidez o la rentabilidad de la entidad. Evidencian fallos importantes en el gobierno, la gestión de riesgos y/o los controles internos.
<p>Crítico</p>	Deficiencias de máxima gravedad que tienen un impacto directo y material en la viabilidad de la entidad o que suponen un incumplimiento grave de la normativa prudencial. Representan una amenaza inminente para la seguridad y solidez de la organización.



MEDIDA DE EVALUACIÓN: PRIORIDAD DE IMPLANTACIÓN

PRIORIDAD DE IMPLANTACIÓN	DESCRIPCIÓN
<p>Alta</p> 	Requiere una acción inmediata y puede llevar a medidas correctoras más severas.
<p>Media</p> 	Requiere un plan de acción correctivo con plazos definidos.
<p>Oportunidad de mejora</p> 	No requiere un plan de acción con plazos asociados.

Es importante resaltar que cada organización define el número de niveles de sus escalas de valoración según sus necesidades, salvo que exista alguna regulación aplicable que determine una escala específica.

En el **Anexo II** se incluye un caso práctico con distintos escenarios e hipótesis para ayudar a aplicar los criterios de definición de la criticidad de los hallazgos considerando lo indicado anteriormente sobre la estimación del impacto y probabilidad de estos.

5. REEVALUACIÓN DE LA CRITICIDAD DE LOS HALLAZGOS

Es conveniente señalar que algunas Funciones de Auditoría Interna contemplan en su metodología la posibilidad de revisar y actualizar el nivel de criticidad de los hallazgos una vez transcurrido un plazo determinado (por ejemplo, un año) o cuando se producen eventos relevantes que así lo aconsejan. Esta práctica permite adaptar la valoración del hallazgo a la evolución del riesgo asociado.

Esta **reevaluación del riesgo** puede deberse, por ejemplo, a la mitigación parcial del hallazgo (por la implantación parcial de los planes de acción), a cambios en el entorno o a nuevas medidas de control implantadas (como, por ejemplo, la implementación de nuevas tecnologías o nuevos controles que modifican el entorno del riesgo).

Para esta reevaluación, Auditoría Interna analiza las condiciones en las que se identificó el hallazgo, comparándolas con las existentes

en el momento del ejercicio de reevaluación, y suele requerir el juicio de expertos o responsables de auditoría.

Este proceso de reevaluación debe estar debidamente descrito en la metodología de auditoría interna, en cuanto a los criterios y umbrales que activan la reevaluación, y ha de quedar debidamente documentado, de forma que quede evidenciada su trazabilidad y se asegure el cumplimiento de los criterios definidos para determinar la criticidad de los hallazgos.

No obstante, es más habitual adoptar un enfoque más prudente, consistente en mantener la criticidad original del hallazgo y gestionar por separado cualquier cambio en el riesgo o riesgo residual. Esta gestión se hace a través de mecanismos de seguimiento o informes complementarios, sin modificar el registro inicial, con el objetivo de preservar la integridad del dato histórico y facilitar su trazabilidad.



Rating de informes: calificaciones de las conclusiones de los trabajos

Es importante definir una escala de valoración del informe que permita jerarquizar las conclusiones, adaptándola al contexto y metodología de la organización.

Tal y como se establece en las NGAI¹⁰, es importante incluir en la comunicación final de los trabajos de aseguramiento realizados por Auditoría Interna, entre otros aspectos, los hallazgos, su importancia y priorización (tratado anteriormente en este documento), así como la **conclusión** respecto a la eficacia de los procesos de gobierno, gestión de riesgos y control de la actividad revisada. En caso de que no haya formado parte del alcance de la revisión alguno de estos aspectos, se deberá incluir una explicación de las limitaciones al alcance, en su caso.

En este sentido, es importante establecer una **escala de valoración o rating del informe**,

tanto a nivel de objetivos individuales como a nivel global, que permita dimensionar y jerarquizar las conclusiones de la auditoría con respecto a la eficacia de los procesos de gobierno, gestión de riesgos y control, adaptando y personalizando dicha escala al contexto específico de cada organización y desarrollándola en sus metodologías.

La utilización de una escala de valoración o rating, además de dimensionar y jerarquizar las conclusiones de cada auditoría, permite visibilizar y estandarizar los criterios de Auditoría Interna de manera uniforme y consistente para todos sus trabajos.

1. ESCALA Y CRITERIOS DE EVALUACIÓN

Para crear una escala de valoración o rating de las conclusiones de los informes de auditoría, es importante establecer un sistema que permita evaluar y calificar de manera homogénea y objetiva las comunicaciones finales de los trabajos (informes).

En la definición de las distintas escalas, se pueden considerar los siguientes factores:

- Cumplimiento con los objetivos de negocio o estratégicos de la organización o del área auditada.

- Efectividad de los sistemas o procesos de gobierno.
- Capacidad de gestión de riesgos dentro del apetito.
- Efectividad de los sistemas o procesos de control (marco de control).
- Cultura de riesgos.
- Existencia y cumplimiento de políticas, estándares y procedimientos operativos.

10. Normas 14.5 Conclusiones del trabajo y 15.1 Comunicación final del trabajo



- Cumplimiento con requerimientos legales, regulatorios, contables o contractuales.
- Materializaciones del riesgo (incidentes, casos de fraude, etc.).

Cuando se crea una escala de rating de las conclusiones de los informes de auditoría se debe poner atención a la redacción. Es posible que el uso de términos generales, como satisfactorio, efectivo o insatisfactorio, no define suficientemente el significado, por lo que la redacción debe ser clara y adecuada para facilitar su entendimiento, asegurando que todas las áreas implicadas comprenden y

aceptan estos criterios y cómo podrían afectarles, incluida su responsabilidad en relación con el mantenimiento de un entorno de control interno adecuado.

En el estudio del Instituto de Auditores Internos sobre *Escalas de Valoración de Auditoría Interna, análisis comparativo* (marzo, 2025), en el que participaron 22 compañías españolas (90% de ellas del IBEX-35), el 100% de las respuestas indicó que utilizaban escalas de valoración para expresar la opinión de Auditoría Interna, empleando, en la mayoría de los casos (59%), una escala de 4 niveles.

Para asignar un rating a la comunicación final de un trabajo de Auditoría Interna, se puede utilizar un modelo automático, un proceso manual o un modelo mixto.

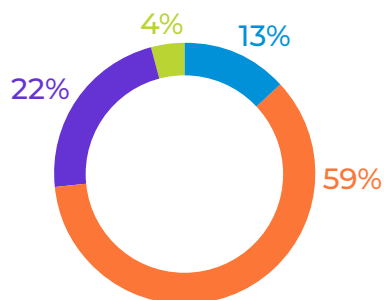
● 3 niveles

● 4 niveles

● 5 niveles

● Otras

Una compañía utiliza 7 niveles en su escala de valoración



Fuente: Instituto de Auditores Internos de España - *Escalas de Valoración de Auditoría Interna, análisis comparativo*. Marzo 2025

En el **Anexo III** se plantean algunos ejemplos como referencia sobre los distintos tipos de escalas de rating.

2. CÁLCULO DEL RATING

A la hora de asignar un rating a la comunicación final de un trabajo de Auditoría Interna realizado, se puede utilizar:

- Un modelo **automático** de rating, lo que ofrece rapidez, consistencia y reducción de sesgos, asegurando además que la calificación parte de una base estructurada y homogénea para todos los trabajos de Auditoría Interna.
- Un proceso **manual**, en base al juicio profesional de los auditores internos, lo cual permite una evaluación más flexible y adaptada a contextos específicos, aunque implica subjetividad.
- Un modelo **mixto**, que combina la objetividad de un sistema puramente cuantitativo con la aplicación del juicio profesional, asegurando de este modo calificaciones con-

Cálculo automático: utiliza parámetros fijados por la organización, considerando el número y criticidad de hallazgos y el nivel de control en el área auditada.

sistentes, comparables y que refleje fielmente el resultado del trabajo.

A continuación, se detallan cada uno de los posibles modelos.

2.1 CÁLCULO AUTOMÁTICO DE RATING

Para el cálculo automático de rating se establecen unos parámetros iniciales con base en los criterios definidos en la organización, teniendo en cuenta aspectos como el número de hallazgos identificados y su criticidad, o el nivel de control establecido en el área auditada.

La automatización del cálculo del rating de un informe permite estandarizar la evaluación de los resultados, mejorar la objetividad y faci-

tar la toma de decisiones. Este sistema se basa en una metodología estructurada que combina criterios cualitativos y cuantitativos, ponderaciones y escalas de puntuación.

EJEMPLO

Los hallazgos tendrán una calificación de impacto con base en su criticidad, considerando tanto los que han surgido en la revisión de referencia, como el resto de los hallazgos de revisiones anteriores pendientes de implantación, que resulten relevantes para el alcance de la auditoría.

Esto significa que, para un hipotético escenario en el que existen 3 tipos de hallazgos (de criticidad alta, media y baja), se otorgará una puntuación, por ejemplo:

TIPOS DE HALLAZGOS POR CRITICIDAD

- Hallazgos de criticidad baja
- Hallazgos de criticidad media
- Hallazgos de criticidad alta

PUNTUACIÓN

- 1 punto
- 4 puntos
- 24 puntos

El rating de la auditoría se determinará mediante la suma de la puntuación de hallazgos aplicables, conforme a la siguiente escala estandarizada de 4 niveles que se presenta a modo de ejemplo:

RATING DE AUDITORÍA

Efectiva
Parcialmente efectiva
Necesita mejoras significativas
Inefectiva

PUNTUACIÓN OBTENIDA

- De 0 a 3 puntos
- De 4 a 23 puntos
- De 24 a 95 puntos
- A partir de 96 puntos

El rating se calculará multiplicando la puntuación de cada hallazgo del siguiente modo:

$$\text{Rating final} = \sum (\text{Puntuación de cada tipo de hallazgo} \times \text{Número de hallazgos})$$

Si una auditoría tiene los siguientes hallazgos:

CRITICIDAD DEL HALLAZGO	Nº DE HALLAZGOS OBTENIDOS	PUNTUACIÓN	TOTAL (Nº HALLAZGOS X PUNTUACIÓN)
■ Hallazgos de criticidad baja	3	1	3
■ Hallazgos de criticidad media	2	4	8
■ Hallazgos de criticidad alta	1	24	24

Puntuación total: 35

Tomando como referencia el ejemplo ilustrado, el cálculo automático del rating otorgaría a la auditoría un rating de *“necesita mejoras significativas”*.

No obstante, el cálculo automático del rating tiene un carácter instrumental y de apoyo. Los resultados obtenidos podrán ser calibrados, en su caso, en base al juicio experto del responsable de la auditoría, debiendo quedar suficientemente documentado el racional de dichos ajustes (ver 2.3 Modelo mixto de rating). En todo caso, la responsabilidad última sobre la determinación del rating del informe corresponde al auditor interno responsable del trabajo.

2.2 JUICIO EXPERTO

La aplicación del **juicio profesional** del auditor interno es un aspecto recogido en las NGAI, que subrayan la importancia del pensamiento crítico y la experiencia del auditor.

El cálculo experto de rating considerando los criterios definidos para cada categoría, permite a los auditores internos considerar factores cualitativos y contextuales que un modelo automático no puede capturar, ajustar las calificaciones en función de circunstancias específicas y cambios en el entorno de control y utilizar, en mayor medida, la experiencia y el juicio experto del auditor interno. Entre los

factores cualitativos que un modelo automático no puede capturar, caben mencionar los siguientes:

- **Agregación de riesgos:** varias observaciones de bajo impacto individual pueden, en conjunto, suponer un riesgo significativo para la entidad.
- **Causa raíz:** si diferentes hallazgos apuntan a una única causa raíz (por ejemplo, una cultura de control deficiente), el riesgo es mayor que la simple suma de sus partes.

2.3. MODELO MIXTO DE RATING

Este enfoque combina la objetividad de un sistema cuantitativo con la necesaria aplicación del juicio profesional.

En este modelo se parte de determinar de manera automática una puntuación en base a cada uno de los hallazgos identificados durante la auditoría (en base a algunos de los posibles sistemas comentados en el apartado 2.1 *Cálculo automático de rating* previo). Esta calificación inicial permite partir de una base estructurada y uniforme para todos los trabajos de auditoría.

Una vez obtenido el cálculo base automático, el componente del juicio experto del equipo auditor permitiría confirmar o ajustar los rating automáticos asignados. Este juicio profe-

Proceso manual basado en el juicio profesional: considera los criterios definidos, permitiendo a los auditores internos estimar factores cualitativos y contextuales que un modelo automático no puede capturar.

Modelo mixto: combina la objetividad de un sistema cuantitativo con la necesaria aplicación del juicio profesional.

sional se puede introducir en dos momentos del proceso de cálculo y asignación del rating:

- a) En los niveles más granulares del programa de auditoría, asignando pesos relativos en función de la importancia de cada prueba de auditoría, y asignando una valoración experta para cada prueba. La valoración experta agregada para cada objetivo de la auditoría se contrastará con la calificación automática, de modo que se confirme la misma, o bien se determine la necesidad de su ajuste.
- b) El equipo auditor puede ajustar la calificación final si lo considera necesario, jus-

tificando y documentando dicha necesidad.

Una muestra de un posible ajuste experto sería, por ejemplo, en un trabajo de auditoría donde el cálculo automático de varias observaciones proporciona como resultado una calificación de "Necesita Mejora". Sin embargo, el equipo auditor detecta que todas estas observaciones, aunque afectan a procesos distintos, se deben a la falta de supervisión por parte de una dirección clave. Aplicando el juicio experto, el equipo podría elevar la calificación final a "No Satisfactorio", para reflejar esta debilidad sistémica y de mayor gravedad.



Alineación de metodologías - Visión integral

1. COORDINACIÓN Y CONSOLIDACIÓN CON EMPRESAS DEL GRUPO

La Función de Auditoría Interna debe adoptar una **visión holística** a nivel grupo para identificar y mitigar riesgos que afectan a múltiples entidades, compartir mejores prácticas y garantizar que todas las filiales cumplan con los mismos estándares de control y calidad, fortaleciendo así la eficacia y eficiencia de la Función y contribuyendo a la sostenibilidad de la organización.

Para lograr tal fin, el universo auditable debe cubrir todo el espectro de las actividades de una organización, incluidas las actividades subcontratadas, procesos, sistemas, líneas de negocio y control, así como todas las entidades y sucursales del grupo. Además, para faci-

litar la monitorización de riesgos a niveles consolidados o sub-consolidados, las organizaciones deberían desarrollar marcos de apetito de riesgo para las líneas de negocio y entidades más relevantes, derivados del enfoque desarrollado a nivel de grupo.

Cuando dentro de un grupo existen entidades que cuentan con sus propias funciones de Auditoría Interna, la eficacia de la Función en la organización depende en gran medida de la adecuada coordinación entre las diferentes funciones de Auditoría Interna del Grupo. Una buena práctica consiste en el establecimiento de estándares comunes de Auditoría Interna dentro del grupo.



En este sentido, es posible que cada Función de Auditoría Interna cuente con una metodología propia, si bien es recomendable que existan **estándares y políticas comunes** con el objetivo de asegurar la calidad en los trabajos de las diferentes entidades del grupo y la homogeneidad en la emisión, seguimiento de recomendaciones y rating de los informes de Auditoría Interna de cara a su adecuado reporte a la Comisión de Auditoría y la Alta Dirección del Grupo.

Los criterios principales para la asignación de criticidades de hallazgos y calificaciones de las auditorías (escalas utilizadas, plazos asociados, etc.) deberían ser aplicados de manera

íntegra a todas las sociedades del grupo empresarial, con independencia de su tamaño.

Las diferenciaciones se centrarán en los **umbrales utilizados en función de la importancia relativa de cada sociedad**, de modo que la determinación de las criticidades de los hallazgos, calificaciones de los objetivos analizados y conclusiones tengan en cuenta dicha **importancia relativa**.

La metodología de Auditoría Interna establecerá los criterios para determinar la ponderación de los diversos hallazgos identificados y su criticidad en caso de agregar información de distintas empresas del grupo.

2. COORDINACIÓN EN PROYECTOS DE CO-SOURCING/ OUTSOURCING

Cuando se recurre al *co-sourcing* o al *outsourcing* con un tercero para la realización de ciertos trabajos de auditoría –al igual que ocurre con las empresas filiales dentro de un grupo empresarial– es necesario **homogeneizar** tanto los criterios de criticidad de los hallazgos como los criterios de evaluación de los informes para mantener la calidad y la consis-

tencia de los trabajos, por lo que es fundamental mantener un equilibrio entre confiar en la experiencia del proveedor externo, tomándolo como un **tercero de confianza**¹¹, y asegurar que los informes se encuentren alineados con los criterios y expectativas de la Función de Auditoría Interna.

En grupos de empresas, Auditoría Interna debe adoptar una visión holística a nivel grupo para identificar y mitigar riesgos, compartir mejores prácticas y garantizar que todas las filiales cumplen con los mismos estándares de control y calidad.



Comunicación y reporte de los resultados de Auditoría Interna

La comunicación y el reporte de los resultados de los trabajos de Auditoría Interna a los órganos de gobierno resultan esenciales para

asegurar la transparencia y la mejora continua en la organización.

11. Norma 9.5 *Coordinación y confianza*

La comunicación y el reporte de los resultados de los trabajos de Auditoría Interna a los órganos de gobierno resultan esenciales para asegurar la transparencia y la mejora continua en la organización.

Las NGAI¹² establecen que “Los auditores internos comunican los resultados del trabajo a las partes apropiadas y monitorean el progreso de la Dirección hacia la implementación de las recomendaciones o los planes de acción”.

A la hora de comunicar los resultados del trabajo se podrán incluir: conclusiones de las auditorías, “temas” (entendiéndose estos como patrones o tendencias), y conclusiones a nivel de unidad de negocio o de la organización.

Adaptar el contenido de las comunicaciones a cada órgano de gobierno y sus necesidades específicas resulta crucial para una comunicación efectiva. En este sentido, los principales destinatarios de los resultados de los trabajos de Auditoría Interna son:

- El Consejo o la Comisión de Auditoría.
- La Alta Dirección.
- Las unidades u organizaciones auditadas.
- El supervisor u otros reguladores.

CONSEJOS PARA ELABORAR INFORMES EJECUTIVOS DE AUDITORÍA INTERNA: TENDENCIAS EN COMUNICACIONES EFECTIVAS

El informe ejecutivo de Auditoría Interna es una herramienta fundamental para comunicar los resultados de una auditoría de manera clara y efectiva al Consejo y la Alta Dirección. Este documento debe ser conciso, estructurado y enfocado en los hallazgos más relevantes, proporcionando recomendaciones accionables que contribuyan a la mejora continua de la organización.

Las características que debe tener un informe para que sea efectivo son:

1. **Claridad y concisión:** es esencial que el informe sea claro, conciso y directo. Se re-

comienda evitar el uso de tecnicismos y jerga especializada para asegurar que todos los lectores comprendan el contenido.

2. **Estructura bien definida:**

- Objetivo de la auditoría, alcance y período auditado.
- Conclusión general u opinión de Auditoría Interna.
- Hallazgos clave: es importante resaltar y enfocarse en los hallazgos más relevantes y de mayor impacto para la organización o el área auditada.
- Recomendaciones: deben ser específicas, medibles, alcanzables, relevantes y con planes de acción, responsables y plazos definidos.

3. **Presentación visual:** la utilización de gráficos, tablas y resúmenes facilita la comprensión de la información. Una buena presentación visual puede hacer que el informe sea más atractivo y fácil de entender.

4. **Revisión y retroalimentación (feedback):** antes de finalizar el informe es recomendable revisar el contenido y solicitar opiniones de colegas o superiores para asegurar que el informe sea preciso y completo.

5. **Lenguaje positivo y constructivo:** mantener un tono positivo y constructivo es crucial, destacando no sólo las áreas de mejora, sino también los aspectos positivos encontrados durante la auditoría.

La implementación de estas prácticas en las comunicaciones puede mejorar significativamente la coordinación y el desempeño de Auditoría Interna, asegurando que contribuya de manera efectiva a la mejora continua y la sostenibilidad de la organización.

12. Principio 15: Comunicar las conclusiones del trabajo y monitorear los planes de acción





Uso de la Inteligencia Artificial

La Inteligencia Artificial (en lo sucesivo IA) puede ser una herramienta útil para fortalecer la calidad, consistencia y eficiencia en la determinación de la criticidad de los hallazgos, la asignación de rating de informes e, incluso, en la elaboración de los informes. Su aplicación permite avanzar hacia una auditoría más objetiva, predictiva y eficiente.

En primer lugar, la IA puede ser utilizada para **determinar la criticidad de los hallazgos** de manera más precisa y homogénea. Analizando grandes volúmenes de datos históricos y contextuales, los sistemas inteligentes pueden identificar patrones, correlaciones y anomalías que podrían pasar desapercibidos en una revisión manual. Esto permite asignar niveles de criticidad ajustados al impacto potencial del hallazgo, considerando la importancia relativa de cada entidad del grupo.

Asimismo, también puede contribuir significativamente en la **definición y asignación de rating** para los informes de Auditoría Interna. Mediante algoritmos que aplican criterios predefinidos de forma consistente, se elimina el sesgo humano y se garantiza una evaluación objetiva.

Gracias al uso de **modelos predictivos**, la IA también puede ayudar a anticipar la identificación de posibles riesgos emergentes, permitiendo a los auditores tomar decisiones más informadas y proactivas.

En la elaboración de **informes ejecutivos**, la IA también aporta valor al facilitar la **identificación de causas raíz**, revelar **tendencias comunes** y sintetizar información relevante para el reporte a los órganos de gobierno. Puede generar borradores preliminares basados en los datos analizados, que luego sean revisados y ajustados por los auditores internos, optimizando así el tiempo y la calidad del proceso.

En todo caso, el uso de las capacidades de la IA no sustituye el juicio profesional del auditor interno, pero sí lo puede complementar, potenciando su capacidad de análisis y asegurando una mayor coherencia en la aplicación de criterios de evaluación y criticidad en toda la organización.

La IA puede ser una herramienta útil para fortalecer la calidad, consistencia y eficiencia en la determinación de la criticidad de los hallazgos, en la asignación del rating y en la elaboración de informes.



Conclusión

Es necesario establecer un marco metodológico robusto y homogéneo para la evaluación de la criticidad de los hallazgos y la calificación de las conclusiones de los informes.

Tal y como se ha puesto de manifiesto a lo largo de este documento, es necesario establecer un **marco metodológico robusto y homogéneo** para la evaluación de la criticidad de los hallazgos y la calificación de las conclusiones de los informes. Su aplicación sistemática permite mejorar la calidad, la objetividad y la trazabilidad de los trabajos de Auditoría Interna, facilitando una comunicación más clara, coherente y eficaz a los órganos de gobierno, la Alta Dirección y otras partes interesadas.

La **estandarización de criterios cuantitativos y cualitativos**, junto con el uso de **escalas de valoración y modelos de cálculo** (manuales o automáticos), puede contribuir a mejorar la priorización de riesgos y una asignación más eficiente de recursos. Esto se traduce en una mayor capacidad para identificar posibles debilidades críticas, proponer acciones correctivas proporcionales y realizar un seguimiento efectivo de su implementación. Además, la incorporación de herramientas como la IA abre nuevas oportunidades para automatizar procesos, reducir sesgos y anticipar posibles riesgos emergentes.

La adopción de una **visión holística** a nivel de grupo, junto con la coordinación entre funciones de Auditoría Interna y proveedores externos, garantiza la consistencia y comparabilidad de los informes, independientemente de la entidad auditada. Esto es especialmente relevante en entornos corporativos complejos, donde la alineación metodológica y la uniformidad de criterios son esenciales para una supervisión eficaz y una toma de decisiones informada.

En definitiva, contar con un marco metodológico para la asignación de criticidades de hallazgos y rating de informes no solo contribuye a mejorar la calidad de los trabajos de Auditoría Interna, sino que también refuerza su impacto estratégico como herramienta de aseguramiento y asesoramiento. Su implementación contribuye a una cultura de control más madura, a una mayor transparencia organizativa y a la sostenibilidad del modelo de gobierno corporativo.





Anexos

ANEXO I – MATRIZ DE VALORACION DE IMPACTOS

A continuación, se muestra una posible matriz de valoración de impacto, considerando 10 categorías de riesgo con 4 posibles niveles de impacto, si bien dependerá de cada organización establecer los criterios cuantitativos, cualitativos y los niveles de impacto que considere relevantes.

CATEGORÍA DE RIESGO	NIVEL DEL IMPACTO			
	BAJO (1)	MEDIO (2)	ALTO (3)	CRÍTICO (4)
Riesgo Financiero o Rentabilidad*	Impacto económico poco significativo; pérdidas no materiales	Impacto económico moderado; pérdidas relevantes pero asumibles	Impacto económico significativo; pérdidas que afectan a resultados anuales	Impacto económico grave; amenaza la viabilidad o continuidad
Afectación a Clientes	Afectación a un número muy reducido de clientes	Afectación a un número moderado de clientes	Afectación a un número significativo de clientes	Afectación masiva a clientes o a segmentos estratégicos
Riesgo Operacional	Problemas menores en procesos internos o sistemas; errores puntuales	Problemas moderados; errores en integridad de información o retrasos	Interrupciones significativas en operaciones clave; degradación de servicios	Fallo crítico en procesos o sistemas estratégicos; imposibilidad de operar
Continuidad del Negocio	Interrupciones menores sin impacto externo	Interrupciones que afectan a servicios críticos durante un período limitado	Interrupciones prolongadas con impacto en clientes y operaciones	Paralización total de operaciones; activación de planes de contingencia y crisis
Riesgo de Personas o Cultura Organizacional	Impacto leve en clima laboral o bienestar	Descontento generalizado, afectación al desempeño	Conflictos laborales, pérdida de talento clave, absentismo elevado	Conflictos graves, crisis organizacional o reputacional
Riesgo de Sostenibilidad	Daños ambientales menores, fácilmente reversibles	Daños ambientales moderados, requieren acciones correctivas	Daños ambientales graves, sanciones regulatorias	Daños ambientales extensos, irreversibles o con repercusión pública
Riesgo Legal y Regulatorio	Incumplimiento sin investigaciones o sanciones legales	Investigaciones o sanciones administrativas leves	Multas relevantes, restricciones operativas	Sanciones penales, pérdida de licencias, intervención de autoridades
Riesgo Reputacional	Impacto interno sin repercusión externa	Cobertura en medios locales, quejas de clientes	Cobertura en medios nacionales, pérdida de confianza de stakeholders	Cobertura en medios internacionales, daño severo a la marca, pérdida de confianza generalizada

* En el apartado de Riesgo Financiero o Rentabilidad, habría la posibilidad de incorporar una referencia cuantitativa que permita clasificar cada nivel en función de la materialidad, considerando su impacto en las cuentas anuales. En este sentido se puede cuantificar tomando como referencia los parámetros utilizados por las cuatro Firmas Globales de Auditoría de cuentas.

CATEGORÍA DE RIESGO	NIVEL DEL IMPACTO			
	BAJO (1)	MEDIO (2)	ALTO (3)	CRÍTICO (4)
Riesgo Tecnológico / Ciberseguridad	Vulnerabilidades menores sin explotación	Incidentes de seguridad limitados, sin fuga de datos sensibles	Acceso no autorizado a información relevante, interrupción de servicios	Brecha de seguridad grave, robo masivo de datos, extorsión o paralización de sistemas críticos
Riesgo de Cumplimiento / Conducta o Ética	Incumplimientos menores de políticas internas	Incumplimientos reiterados, advertencias internas	Sanciones disciplinarias, pérdida de certificaciones	Investigaciones externas, denuncias públicas, daño ético grave

Fuente: https://finance.ec.europa.eu/system/files/2022-09/220701-ceaob-report-materiality-audit_en.pdf

Para determinar el nivel de impacto total, se puede considerar el impacto máximo en cada riesgo, de manera que, si en un determinado riesgo el hallazgo tiene un potencial impacto *Alto*, se considerará como riesgo *Alto*.

ANEXO II- EJEMPLO PRÁCTICO PARA DETERMINAR LA CRITICIDAD DE LOS HALLAZGOS

A continuación, se incluye un ejemplo práctico hipotético para ayudar a determinar la criticidad de los hallazgos.

En este ejemplo, la metodología de Auditoría Interna ha establecido una escala de 3 posibles criticidades: alta, media y baja.

PASO 1. EVALUACIÓN DEL IMPACTO

En primer lugar, se realiza la valoración del **nivel del impacto** con base en las categorías de riesgo establecidas que deberán estar definidas en la metodología aprobada por la Función de Auditoría Interna (por ejemplo, las del **Anexo I**)

En ese ejemplo, una vez realizado el trabajo de auditoría se considera que el hallazgo tiene un potencial impacto ALTO.

PASO 2. PROBABILIDAD

A continuación, se considera la **probabilidad de ocurrencia**.

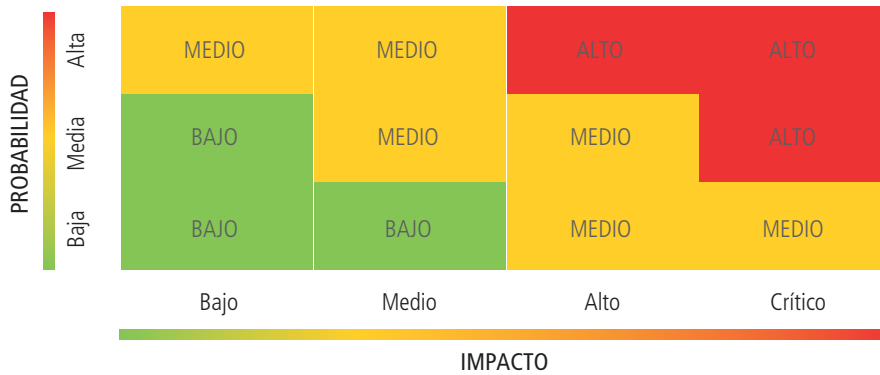
En este ejemplo, la Función de Auditoría Interna ha establecido una escala de ocurrencia de tres niveles:

- Probabilidad baja (o poco probable): la probabilidad de materialización es menor al 30%
- Probabilidad media (o posible): la probabilidad de materialización está entre el 30-70%
- Probabilidad alta (probable): la probabilidad es superior al 70%

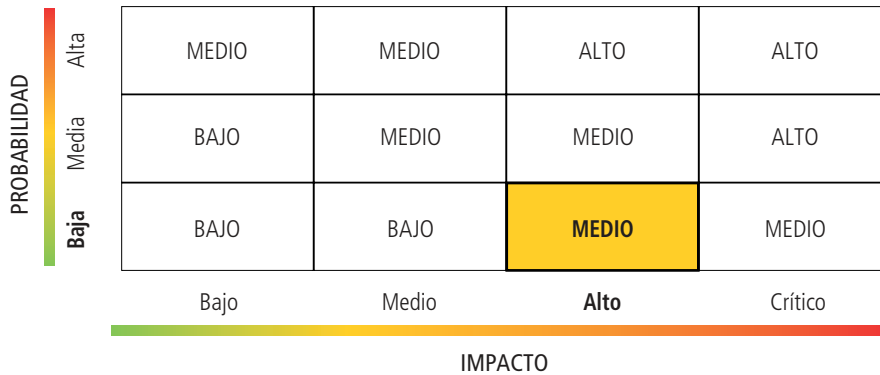
En el ejemplo, se considera que la posibilidad de que el riesgo asociado al hallazgo se concrete efectivamente es BAJA.

PASO 3. CATEGORIZACIÓN DE LA CRITICIDAD DEL HALLAZGO

La combinación de la valoración del nivel de impacto con la probabilidad de ocurrencia establecería la criticidad del hallazgo. Para ello, se puede utilizar una matriz cualitativa de combinaciones, tal y como se representa a continuación:



Por tanto, en este ejemplo, considerando el nivel de impacto alto y probabilidad baja, la Función de Auditoría Interna podría establecer que el hallazgo tendría una criticidad **MEDIA**.



Otra opción sería asignar valores numéricos a cada uno de los posibles impactos y probabilidades, y construir una matriz cuantitativa en base a los posibles resultados combinados.

De esta forma, se pueden asignar valores a los impactos y a las probabilidades, así como un rango para determinar los niveles de criticidad:

IMPACTO	PUNTUACIÓN	PROBABILIDAD	PUNTUACIÓN	NIVELES DE CRITICIDAD	RANGO
CRÍTICO	4	ALTA (probable)	3	ALTO	8 - 12
ALTO	3	MEDIA (posible)	2	MEDIO	3 - 7
MEDIO	2	BAJA (poco probable)	1	BAJO	1 - 2

El nivel de criticidad se calculará multiplicando la probabilidad por el impacto:

$$\text{Criticidad} = \text{Probabilidad} \times \text{Impacto}$$

PROBABILIDAD	Alta	3 (MEDIO)	6 (MEDIO)	9 (ALTO)	12 (ALTO)
	Media	2 (BAJO)	4 (MEDIO)	6 (MEDIO)	8 (ALTO)
	Baja	1 (BAJO)	2 (BAJO)	3 (MEDIO)	4 (MEDIO)
		Bajo	Medio	Alto	Crítico

IMPACTO

En el ejemplo, con un impacto Alto (3) y una probabilidad Baja (1), la criticidad será de: $3 \times 1 = 3$, lo que se considera, según los rangos previamente definidos, con un nivel de criticidad MEDIA.

Como puede observarse, el resultado dependerá de los valores que se asignen a cada nivel de criticidad que, a su vez, dependerán de varios factores del contexto, tipo de organización, objetivos del área, etc.

Existen múltiples opciones a considerar en función de las características de la organización que pueden dar lugar a distintas matrices de criticidad de hallazgos, por lo que es esencial que los criterios considerados sean cuidadosamente detallados en la metodología correspondiente.

ANEXO III – ESCALA DE RATING

EJEMPLO 1 - TRES ESCALAS

RATING	DEFINICIÓN
SATISFACTORIO	<p>Los hallazgos se consideran de baja criticidad para la organización e impacto limitado. Principales aspectos:</p> <ul style="list-style-type: none"> • Cumplimiento sólido y consistente de las políticas y procedimientos establecidos. • Definición clara y aplicación adecuada de los niveles de autoridad. • Ejecución regular de los controles clave y de las verificaciones necesarias. • Monitoreo efectivo del funcionamiento general y del desempeño operativo. • Identificación únicamente de problemas de bajo riesgo y, en algunos casos, de un número reducido de incidencias de riesgo medio. • Nivel de riesgo global bajo, tanto cualitativa como cuantitativamente.
INFERIOR A SATISFACTORIO	<p>Los hallazgos presentan un nivel de criticidad moderado, ya que algunos de ellos pueden afectar al logro de los objetivos de la organización si no se corrigen en un plazo adecuado. Principales aspectos:</p> <ul style="list-style-type: none"> • Cumplimiento menos que sustancial de las políticas y procedimientos establecidos. • Definición y aplicación de los niveles de autoridad menos que apropiadas. • Realización de la mayoría de los controles clave y verificaciones, aunque con áreas pendientes de mejora. • Monitoreo limitado del funcionamiento general y del desempeño operativo. • Identificación de problemas de riesgo medio y, en algunos casos, de un número reducido de incidencias de riesgo alto. • Nivel de riesgo global superior al deseable, tanto cualitativa como cuantitativamente.
INSATISFACTORIO	<p>Los hallazgos presentan un nivel de criticidad elevado, dado que las deficiencias identificadas comprometen de forma significativa el logro de los objetivos de la organización y requieren actuaciones correctivas urgentes. Principales aspectos::</p> <ul style="list-style-type: none"> • Cumplimiento claramente insuficiente de las políticas y procedimientos establecidos. • Deficiencias relevantes en la definición y aplicación de los niveles de autoridad. • Ejecución incompleta o inefectiva de controles clave y verificaciones fundamentales. • Monitoreo inadecuado del funcionamiento general y del desempeño operativo. • Identificación de múltiples incidencias de riesgo medio y alto. • Nivel de riesgo global inaceptable, tanto desde una perspectiva cualitativa como cuantitativa.

En función del nivel de criticidad se pueden determinar plazos establecidos para llevar a cabo las acciones de seguimiento.

EJEMPLO 2 - CUATRO ESCALAS

RATING	DEFINICIÓN
EFFECTIVO	No se han identificado riesgos significativos y, en su caso, únicamente se han observado aspectos menores. El gobierno corporativo, la gestión de riesgos y la operación de los controles internos se encuentran adecuadamente diseñados, aplicados de manera consistente y funcionan de forma eficaz. En conjunto, estos elementos proporcionan una seguridad razonable de que la organización se encuentra encaminada al logro de sus objetivos.
PARCIALMENTE EFFECTIVO	Se han identificado hallazgos de carácter moderado. Los elementos de gobierno corporativo, las prácticas de gestión de riesgos y los controles internos están adecuadamente diseñados y, en general, bien implementados; sin embargo, se ha detectado uno o un número limitado de aspectos que podrían representar un riesgo moderado para el logro de los objetivos organizacionales. Aun cuando el marco de control es razonablemente sólido, se requiere atención para mitigar estos riesgos.
NECESITA UNA MEJORA SIGNIFICATIVA	Se han identificado uno o varios hallazgos significativos. Los componentes de gobierno corporativo, las prácticas de gestión de riesgos y los controles internos presentan debilidades tanto en su diseño como en su efectividad operativa. Hasta que estas deficiencias sean corregidas, no puede asegurarse razonablemente que la organización esté en disposición de cumplir sus objetivos de forma adecuada. Estas brechas requieren atención prioritaria.
INEFFECTIVO	Se han identificado múltiples hallazgos significativos y/o materiales. Los elementos de gobierno corporativo, las prácticas de gestión de riesgos y los controles internos presentan deficiencias relevantes en su diseño y/o en su efectividad operativa. Debido a la magnitud y naturaleza de estas debilidades, no existe una seguridad razonable sobre la capacidad de la organización para cumplir sus objetivos, que se ve seriamente comprometida hasta que se implementen las correcciones necesarias.

Fuente: Elaboración propia



Bibliografía / Referencias

Normas Globales de Auditoría Interna (IIA, 2024)

<https://auditoresinternos.es/publicaciones/normas-globales-de-auditoria-interna-edicion-2024/>

Global Practice Guide: Communicating Results of Internal Audit Services (IIA, 2025)

<https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/communicating-results-of-internal-audit-services/>

Rating of reports (IIA, 2017)

<https://www.theiia.org/globalassets/site/content/tools/executive/2017/audit-report-rating-approach-audit-rating-tool/audit-rating-tool-audit-report-rating-approach---iia-executive-tool.pdf>

Enterprise Risk Management: Integrating with Strategy and Performance (COSO, 2017)

https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

Internal Control Integrated Framework (COSO, 2013)

https://www.coso.org/_files/ugd/3059fc_1df7d5dd38074

Instituto de Auditores Internos de España

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

ISBN: 979-13-991286-3-5

Maquetación: desdezero, estudio gráfico

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

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

AUDITORÍA INTERNA DE LA CADENA DE SUMINISTRO

El documento ofrece una guía para supervisar la cadena de suministro y el proceso de aprovisionamiento, considerando distintas fases dentro del ciclo de vida del proveedor, desde su selección inicial hasta la desvinculación final, proponiendo un enfoque de revisión basado en riesgos y contemplando actividades de aseguramiento y asesoramiento, facilitando su desarrollo a través de herramientas prácticas para la planificación de auditorías eficaces.

AUDITORÍA INTERNA EN LA EMPRESA FAMILIAR

El documento resalta el papel clave de la función de Auditoría Interna en la empresa familiar para asegurar su continuidad y el buen gobierno. Aborda la cultura organizativa, el marco normativo y los principales retos, ofreciendo herramientas como un autodiagnóstico y un modelo de madurez. Subraya la independencia y adaptación metodológica de Auditoría Interna y recomienda su posicionamiento como aliado estratégico en la consolidación del legado familiar y en la profesionalización de las compañías.

AUDITORÍA INTERNA DEL USO DE METODOLOGÍA DEVOPS

El documento describe el contexto y beneficios del uso de la metodología DevOps y el papel de Auditoría Interna de cara a la supervisión de los procesos de gobierno, gestión de riesgos y control en este ámbito, conforme a lo previsto en los principales marcos de referencia.

AUDITORÍA INTERNA DE LA GESTIÓN OPERATIVA DEL CLOUD

El documento se configura como una guía útil y práctica para que ayude a los auditores internos a afrontar con éxito los retos que se derivan de la adopción de los servicios en la nube, parte importante del proceso de transformación digital de las organizaciones.



LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Este documento plantea una guía práctica para las funciones de Auditoría Interna a la hora de establecer criterios homogéneos y trazables en la evaluación de la criticidad de los hallazgos y la calificación (rating) de los informes de Auditoría Interna, reforzando la calidad, coherencia y utilidad de las comunicaciones al Consejo y la Alta Dirección.