# SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

# SEGURIDAD INFORMÁTICA

2.1.0.MF0487_3. Capítulo 1
Parte 1 de 2

Criterios generales comúnmente aceptados sobre auditoría informática

JOSÉ PABLO HERNÁNDEZ

# 1. INTRODUCCIÓN

**Auditor informático:**

**Profesional independiente que evalúe la eficiencia de sus sistemas informáticos y que sea capaz de formular recomendaciones y propuestas de mejora con la finalidad de mantener la integridad y exactitud de los datos y así garantizar un servicio correcto dentro de unos estándares de calidad.**

# 2. CÓDIGO DEONTOLÓGICO DE LA FUNCIÓN DE AUDITORÍA

**La auditoría es el análisis exhaustivo de los sistemas informáticos con la finalidad de detectar, identificar y describir las distintas vulnerabilidades que puedan presentarse.**

**Los auditores deben cumplir una serie de normas éticas y un código deontológico.**

**El código deontológico consiste en una serie de preceptos en los que se determinan los derechos exigibles a ciertos profesionales.**

**ISACA (Information Systems Audit and Control Association), expide el certificado CISA (Certified Information Systems Auditor) .**

# 2.1. NORMAS PROFESIONALES DE LA ISACA

**Normas de Auditoría de Sistemas de Información:**

**1. El auditor de los sistemas de información debe ser independiente del ente auditado, tanto en actitud como en apariencia.**

**2. Para que la auditoría se desarrolle de un modo objetivo, la función de auditoría debe ser independiente del área que se pretende auditar.**

**3. El auditor debe cumplir con los preceptos del Código de Ética Profesional de la ISACA. Nota: El Código de Ética Profesional de la ISACA está formado por una serie de directivas de actuación profesional y personal que deben seguir todos los miembros que forman parte de la asociación.**

# 2.1. NORMAS PROFESIONALES DE LA ISACA

**Normas de Auditoría de Sistemas de Información:**

**4. El auditor debe tener los suficientes conocimientos técnicos y destrezas para desempeñar correctamente las funciones de auditoría encomendadas.**

**5. El auditor de sistemas de información debe reciclar continuamente sus conocimientos para mantener en un nivel adecuado su competencia técnica.**

**6. Las auditorías de sistemas de información deben ser planificadas y supervisadas con suficiente rigor para mantener la seguridad de que se cumplen los objetivos de auditoría establecidos y las normas estipuladas.**

# 2.1. NORMAS PROFESIONALES DE LA ISACA

**Normas de Auditoría de Sistemas de Información:**

**7. En el proceso de auditoría, el auditor debe respaldarse necesariamente con evidencias que confirmen sus hallazgos, resultados y conclusiones.**

**8. Las tareas de auditoría deben llevarse a cabo son sumo cuidado profesional, cumpliendo las normativas de auditoría aplicables.**

**9. Durante la realización del informe, el auditor debe expresar con claridad los objetivos de la auditoría, su duración (de fecha a fecha) y las tareas realizadas en todo el proceso.**

**10. En el mismo informe, el auditor también deberá mencionar las observaciones necesarias para una mejor comprensión y las conclusiones obtenidas con las distintas tareas realizadas.**

# 2.2. CÓDIGO DE ÉTICA DE LA ISACA

- Apoyar la implementación y el cumplimiento de los estándares, procedimientos, normas y controles de los sistemas de información y de la tecnología de la empresa.
- Ejecutar las tareas con objetividad, diligencia y rigor profesional, siguiendo los estándares marcados en la profesión.
- Actuar en interés de las partes interesadas (empleadores, clientes, público en general, etc.) de un modo diligente, leal y honesto, sin contribuir en actividades ilícitas o incorrectas que puedan desacreditar la profesión o a la asociación.
- Mantener la confidencialidad de la información que se obtenga en el desarrollo de la auditoría, salvo que sea exigida por una autoridad legal. La información no se podrá utilizar en beneficio propio ni cederla a terceros inapropiados.
- Mantener la aptitud y capacidad en los campos relacionados con la auditoría y los sistemas de información mediante la realización de actividades que permitan actualizar y mejorar las habilidades, competencias y conocimientos necesarios.
- Informar a las partes involucradas de los resultados obtenidos en el proceso de auditoría.
- Apoyar la educación profesional de las partes interesadas (gerencia, clientes, etc.) para una mejor comprensión de las tareas de auditoría, de la gestión de los sistemas de información y de la tecnología de la organización.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de beneficio del auditado**

Las tareas del auditor deben estar enfocadas a maximizar el beneficio de sus clientes sin anteponer sus intereses personales.

En caso de hacer prevalecer sus intereses antes de los clientes, se considerará una conducta no ética.

Además, el auditor también deberá evitar recomendar actuaciones que no sean necesarias o que impliquen algún tipo de riesgo sin justificación para el auditado.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de calidad**

El auditor debe ejercer sus tareas dentro de unos estándares de calidad de modo que, en caso de no disponer de medios adecuados para realizar sus actividades convenientemente, deberá negarse a realizarlas hasta que no se garantice un mínimo de condiciones técnicas.

Si el auditor, en el momento de elaborar el informe, considera que no tiene conocimientos técnicos suficientes, deberá remitirlo a otro técnico más cualificado para mejor calidad de la auditoría.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de capacidad**

El auditor informático debe estar plenamente capacitado para el ejercicio de su profesión y, para ello, debe actualizar sus conocimientos de forma periódica mediante actividades de formación continua.

Para conocer sus necesidades de formación, el auditor deberá ser consciente en todo momento de sus aptitudes y capacidades, conociendo también sus puntos débiles con el fin de cometer menos errores en el ejercicio de sus tareas.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de cautela**

Las recomendaciones del auditor siempre deben estar basadas en sus conocimientos y experiencias, manteniendo al auditado siempre informado de la evolución de las tecnologías de la información y de las actuaciones que se deben llevar a cabo.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de comportamiento profesional**

En el momento de realizar las tareas de su profesión, el auditor siempre deberá tener en cuenta las normas tanto explícitas como implícitas, teniendo sumo cuidado en la exposición de sus opiniones.

Además, debe tener seguridad en sus actuaciones y en la exposición de sus conocimientos técnicos, trasmitiendo una imagen de precisión y exactitud a sus auditados.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de concentración en el trabajo**

En momentos de alto volumen de trabajo, el auditor deberá evitar que el exceso de trabajo dificulte su capacidad de concentración y precisión en sus tareas.

Por ello, deberá realizar previsiones de posibles acumulaciones de trabajo y evaluar las consecuencias de no llevar a cabo sus tareas con la precisión y profesionalidad requerida para mantener unos estándares de calidad en la auditoría.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de confianza**

El auditor deberá dar siempre sensación de confianza al auditado mediante la transparencia en sus actuaciones. Esta confianza entre auditor y auditado se confirmará resolviendo las posibles dudas que puedan surgir en ambas partes y utilizando un lenguaje llano que mejore la comprensión y comunicación de las tareas realizadas.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de criterio propio**

El auditor deberá actuar siempre con criterio propio e independencia, sin permitir que su criterio dependa de otros profesionales.

En caso de haber diferencia de criterios, el auditor deberá reflejarlo en el informe, justificando y motivando con claridad su criterio.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de economía**

El auditor deberá delimitar específicamente el alcance y los límites de la auditoría, evitando retrasos innecesarios que puedan llevar a costes extra y protegiendo siempre los derechos económicos de los auditados.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de fortalecimiento y respeto de la profesión**

Los auditores deberán cuidar y proteger el valor de su profesión, manteniendo unos precios acordes con su preparación.

Deberán evitar establecer precios demasiado reducidos para no caer en términos de competencia desleal y evitar confrontaciones con otros auditores, promoviendo en todo momento el respeto entre ellos.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de integridad moral**

Los auditores deberán desempeñar sus tareas con una actitud honesta, leal y diligente, evitando siempre participar en actividades que puedan perjudicar a terceras personas o al auditado.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de legalidad**

El auditor deberá promover la preservación de la legalidad a sus auditados, no consintiendo la eliminación de dispositivos de seguridad y ni de datos relevantes para la elaboración de la auditoría.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de precisión**

La actuación del auditor debe realizarse siempre con precisión, no emitiendo conclusiones ni informes hasta no estar completamente convencido de su correcta elaboración.

En el momento de la exposición de las conclusiones, el auditor actuará con carácter crítico e indicando con claridad cómo se ha llevado a cabo el análisis de los datos y los motivos que han llevado a sus conclusiones.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de responsabilidad**

El auditor debe asumir la responsabilidad de sus actuaciones, juicios y consejos y estará obligado a hacerse cargo de los posibles daños y perjuicios que haya podido causar alguna de sus actuaciones.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de secreto profesional**

El auditor deberá mantener siempre la confidencialidad de los datos de los auditados, manteniendo siempre una relación de confianza entre ellos.

En ningún momento podrá difundir datos obtenidos en la realización de sus tareas a terceras personas.

# 2.3. CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA

**Principio de veracidad**

El auditor, en el ejercicio de su profesión, deberá asegurar en todo momento la veracidad de sus manifestaciones y opiniones, sin incumplir el secreto profesional y el respeto al auditado.

# 3. RELACIÓN DE LOS DISTINTOS TIPOS DE AUDITORÍA

**La auditoría en sí es una actividad que consiste en emitir un juicio y opinión profesional sobre el objeto o la materia analizada, indicando si se están cumpliendo los requisitos que procedan en cada temática.**

**Esta opinión deberá fundamentarse en una serie de procedimientos que justifiquen y sirvan de soporte al análisis realizado.**

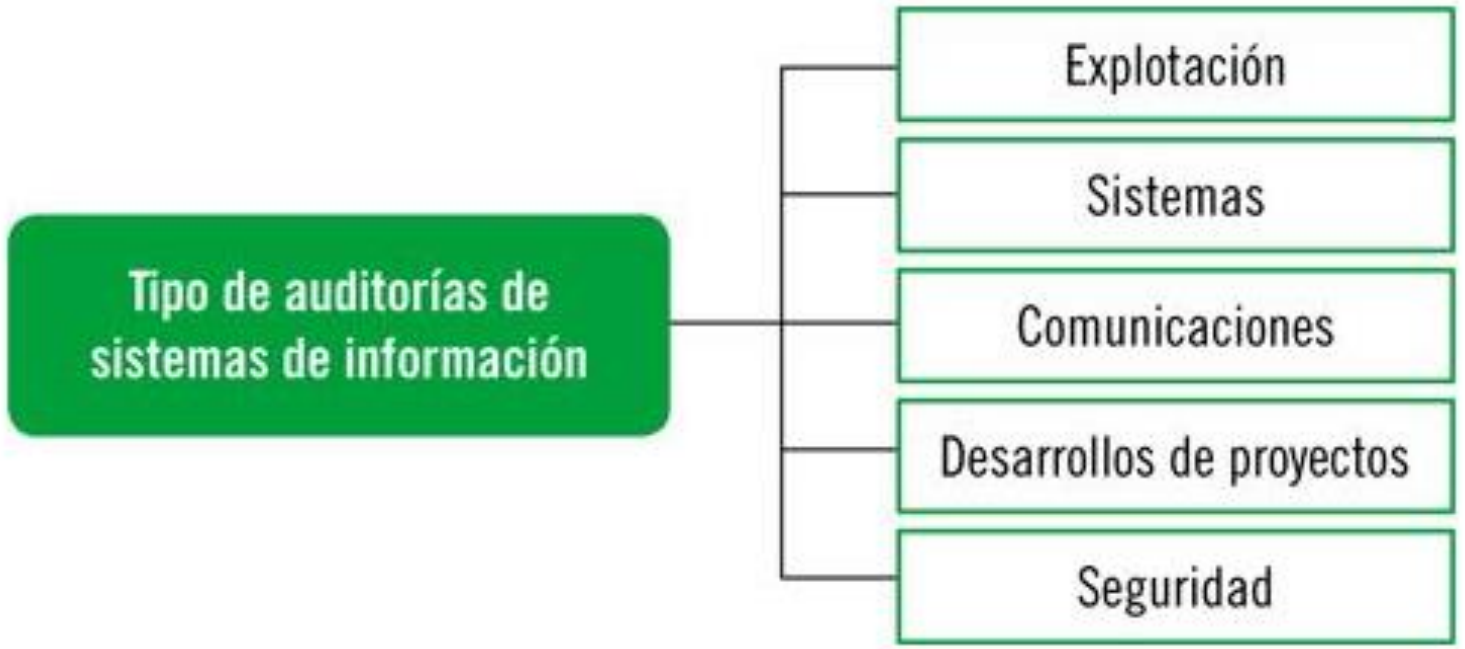
# 3. RELACIÓN DE LOS DISTINTOS TIPOS DE AUDITORÍA

**En la siguiente tabla, se muestran varios tipos de auditoría, atendiendo al tipo de información que se maneja:**

| Clase | Objeto analizado | Finalidad |
|---|---|---|
| Financiera | Cuentas anuales | Verificar la representación de la realidad financiera de la empresa. |
| De gestión | Acciones de los departamentos de la empresa | Comprobar la eficacia y eficiencia de los procesos de la organización. |
| De cumplimiento | Normas establecidas | Comprobar si las operaciones y actuaciones respetan las normas establecidas. |
| Informática | Sistemas informáticos | Comprobar la operatividad y eficiencia de los procesos informáticos según normas establecidas. |

**La variedad de tipologías de auditoría no solo está presente en temáticas generales, sino que dentro de cada una de ellas se pueden distinguir subtipos de auditorías según las áreas específicas.**

# 3.1. TIPOS DE AUDITORÍAS DENTRO DE LOS SISTEMAS DE INFORMACIÓN



# 3.1.1 AUDITORÍA INFORMÁTICA DE EXPLOTACIÓN

**La auditoría informática de explotación se encarga de analizar resultados informáticos de todo tipo: listados impresos, órdenes automatizadas de procesos, etc.**

**El análisis consistirá sobre todo en someter los resultados obtenidos a controles de calidad y en analizar si su distribución posterior (al cliente, a otros empleados, a superiores, etc.) se realiza mediante un proceso adecuado.**

**También se auditan las distintas secciones que componen la informática de explotación y las relaciones existentes entre ellos.**

# 3.1.2 AUDITORÍA INFORMÁTICA DE SISTEMAS

**Sistemas operativos:** se comprueba si están actualizados y, en caso de no estarlo, se averiguan las causas de la desactualización. También se analizan posibles incompatibilidades de software ocasionadas por el sistema operativo.

**Software básico:** se analizan las distintas aplicaciones instaladas para verificar que no agreden ni condicionan al sistema operativo.

**Tunning:** se evalúan las distintas técnicas y medidas de evaluación de los comportamientos del sistema y de los subsistemas.

# 3.1.2 AUDITORÍA INFORMÁTICA DE SISTEMAS

**Optimización de los sistemas y subsistemas:** la auditoría comprobará que las acciones de optimización de sistemas y subsistemas son efectivas y que no se compromete su operatividad.

**Administración de las bases de datos:** el auditor se asegurará del conocimiento de los distintos procedimientos de la base de datos y comprobará la seguridad, la integridad y la consistencia de los datos.

**Investigación y desarrollo:** la auditoría se encargará de mantener la actividad de investigación y desarrollo, impidiendo que por estas se dificulten procesos y tareas fundamentales.

# 3.1.3 AUDITORÍA INFORMÁTICA DE COMUNICACIONES Y REDES

**La auditoría informática de comunicaciones y redes se encargará de analizar los distintos dispositivos de comunicación que forman parte de las redes de la organización para detectar sus debilidades y proponer medidas que las corrijan.**

**Para ello, los auditores deberán conocer la topología de la red de comunicaciones, en la que se describan con detalle las líneas que forman parte de ella, cómo son y su ubicación para comprobar su nivel de operatividad.**

# 3.1.4 AUDITORÍA DE DESARROLLO DE PROYECTOS

**En la auditoría de desarrollo de proyectos, los auditores informáticos analizan la metodología utilizada para desarrollar los distintos proyectos de la organización, distinguiendo entre cada área de negocio de la empresa.**

**También se analiza el desarrollo de proyectos globales que se extienden al conjunto de la organización, comprobando su correcta ejecución y el mantenimiento de la seguridad a lo largo de todo el proceso.**

# 3.1.5 AUDITORÍA DE SEGURIDAD INFORMÁTICA

**La auditoría de seguridad informática analiza todos los procesos referentes a la seguridad informática, tanto física como lógica.**

**La seguridad física es la protección de los componentes hardware, dispositivos, instalaciones y entornos de los distintos sistemas informáticos.**

**La seguridad lógica, por el contrario, es la protección del software, los procesos y programas del sistema, y su auditoría consistirá en analizar la correcta protección y actualización de estos componentes, además de la protección de los datos que forman parte del sistema.**

# 4. CRITERIOS A SEGUIR PARA LA COMPOSICIÓN DEL EQUIPO AUDITOR

**Antes de empezar la auditoría, el auditor deberá elaborar una planificación en la que se detallen los objetivos y procedimientos que se llevarán a cabo para realizar la auditoría informática.**

**En esta planificación se deberá incluir sobre todo:**

- **Lugar o lugares en los que se realizarán las tareas de auditoría.**
- **Duración de la auditoría.**
- **Fecha límite para la finalización de la auditoría.**
- **Composición del equipo de auditoría.**
- **Áreas que serán auditadas.**

# 4. CRITERIOS A SEGUIR PARA LA COMPOSICIÓN DEL EQUIPO AUDITOR

- Establecimiento y análisis de la política de seguridad.
- Verificación y cumplimiento de los estándares, normas y cualificaciones relacionadas con la auditoría y la seguridad informáticas.
- Organización de la seguridad y clasificación de los recursos.
- Análisis de las inversiones realizadas y futuras de seguridad.
- Análisis de los riesgos de la organización.
- Análisis y control de la seguridad física de la organización.
- Establecimiento de medidas de protección y control de accesos al sistema.
- Evaluación de la seguridad en las comunicaciones y operaciones.
- Evaluación de la seguridad y vulnerabilidades de los sistemas operativos y demás software del sistema.
- Definición del plan de continuidad de la organización.
- Gestión de la seguridad de la organización con el establecimiento de medidas y definición del cuadro integral de mandos.

# 4.1. CARACTERÍSTICAS Y CAPACIDADES DEL EQUIPO AUDITOR

**Se recomienda seleccionar una serie de técnicos especializados que abarquen los conocimientos y capacidades suficientes para desarrollar todas las tareas de un modo global.**

**El número de personas que formen el equipo auditor puede variar según las dimensiones de la organización, de los sistemas y de los equipos, pero, independientemente de la magnitud del equipo, sus miembros deberán estar suficientemente capacitados y deberán tener un alto sentido de la ética y la moralidad.**

**Para seleccionar el equipo adecuado, en un primer lugar hay que pensar en profesionales con suficiente nivel para realizar una correcta coordinación del desarrollo de las tareas de la auditoría, siendo capaz de facilitar la información requerida en todo momento.**

# 4.1. CARACTERÍSTICAS Y CAPACIDADES DEL EQUIPO AUDITOR

**El equipo debe estar formado por profesionales con conocimientos básicos en cuanto a:**

- **Desarrollo de proyectos informáticos.**
- **Gestión del departamento de sistemas.**
- **Análisis de riesgos en sistemas informáticos.**
- **Sistemas operativos.**
- **Redes locales y telecomunicaciones.**
- **Gestión de bases de datos.**
- **Seguridad física y del entorno.**
- **Planificación informática.**
- **Gestión de la seguridad de los sistemas.**
- **Gestión de problemas, incidencias y cambios en entornos informáticos.**
- **Administración de datos.**
- **Ofimática.**
- **Permisos de acceso y encriptación de datos.**
- **Comercio electrónico.**

# 4.1. CARACTERÍSTICAS Y CAPACIDADES DEL EQUIPO AUDITOR

**Además de los conocimientos básicos anteriores, habría que añadir otros conocimientos más especializados, atendiendo a las características de los sistemas y organizaciones a auditar.**

**Por ejemplo, para auditar empresas cuya actividad principal es el desarrollo del negocio on-line no se requerirá el mismo conocimiento que para empresas cuya actividad se desarrolla enteramente off-line; para las primeras será necesario que los auditores tengan conocimientos más específicos de comercio electrónico, plataformas de pago seguras para Internet, etc.**

# 4.1. CARACTERÍSTICAS Y CAPACIDADES DEL EQUIPO AUDITOR

**Es recomendable contar con colaboradores con características como:**

- **Técnicos en informática.**
- **Conocimientos en administración y finanzas.**
- **Experiencia en informática y análisis de sistemas.**
- **Experiencia y conocimiento en psicología industrial.**
- **Conocimientos específicos de sistemas operativos, bases de datos, redes, etc., según el área que se vaya a auditar.**
- **Conocimientos en análisis de riesgos.**

# 5. TIPOS DE PRUEBAS A REALIZAR EN EL MARCO DE LA AUDITORÍA.

**Pruebas sustantivas:** pruebas que pretenden identificar los errores derivados de la falta de seguridad o confidencialidad de los datos. Evalúan la calidad de los datos y verifican si los controles establecidos por las políticas o procedimientos son eficaces.

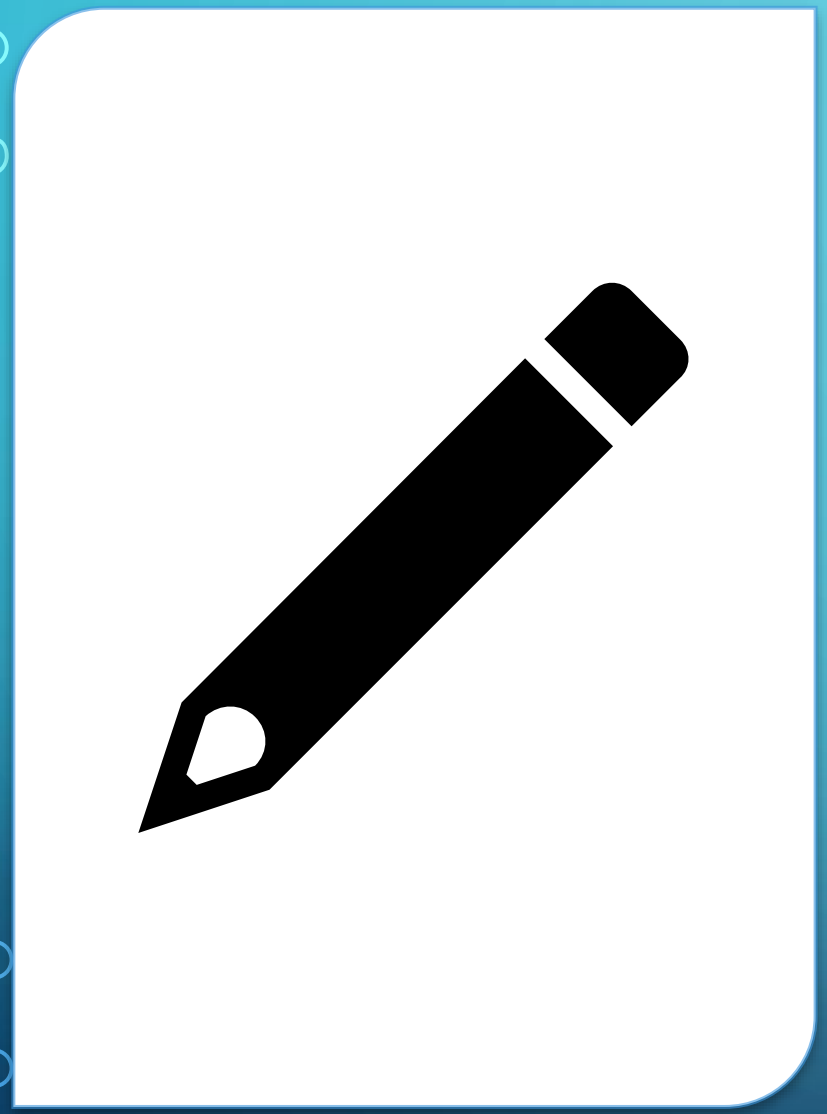
**Pruebas de cumplimiento:** las que permiten determinar si un sistema de control interno y/o procedimiento funciona correctamente y si es acorde con las políticas, normativas y procedimientos definidos por la organización.

# 5.1. RELACIÓN ENTRE LAS PRUEBAS DE CUMPLIMIENTO Y LAS PRUEBAS SUSTANTIVAS

**Existe una correlación directa entre las pruebas de cumplimiento y las pruebas sustantivas necesarias para una correcta auditoría.**

**Si los resultados obtenidos de las pruebas de cumplimiento indican que los controles de sistemas aplicados son correctos y adecuados, son motivo de justificación para utilizar menos pruebas sustantivas.**

**Sin embargo, si los resultados de las pruebas de cumplimiento determinan fallos y debilidades en los controles, las pruebas sustantivas deben ser más detalladas y extensas para comprobar la validez, integridad y exactitud de los datos del sistema.**



# Ejemplo

EN SU ORGANIZACIÓN ESTÁN EN PLENO PROCESO DE PLANIFICACIÓN DE LAS TAREAS DE AUDITORÍA Y NO TIENEN CLARO QUÉ TIPO DE PRUEBAS DEBEN REALIZAR. QUIEREN EVALUAR LA GESTIÓN DE LA ORGANIZACIÓN COMPROBANDO SUS PROCEDIMIENTOS Y CONTROLES INTERNOS PARA DETECTAR SUS POSIBLES DEBILIDADES.

¿QUÉ TIPO DE PRUEBAS DEBERÍAN REALIZAR? SI SE OBTIENEN BUENOS RESULTADOS CON ESTAS PRUEBAS, ¿SERÍA NECESARIO REALIZAR CON PROFUNDIDAD EL OTRO TIPO DE PRUEBAS? ¿POR QUÉ?

# Ejemplo. Solución.

CUANDO EL OBJETO AUDITADO ES LA GESTIÓN DE LA ORGANIZACIÓN Y EL OBJETIVO PRINCIPAL ES COMPROBAR LOS PROCEDIMIENTOS Y CONTROLES INTERNOS DE LA ORGANIZACIÓN, DEBEN REALIZARSE PRUEBAS DE CUMPLIMIENTO.

EN CASO DE OBTENER BUENOS RESULTADOS EN LAS PRUEBAS DE CUMPLIMIENTO, NO SERÁ NECESARIO EJECUTAR EXHAUSTIVAMENTE PRUEBAS SUSTANTIVAS, YA QUE LOS BUENOS RESULTADOS GARANTIZAN QUE LOS SISTEMAS DE CONTROL SE APLICAN CORRECTAMENTE Y ES POCO PROBABLE ENCONTRAR DEBILIDADES IMPORTANTES.