SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

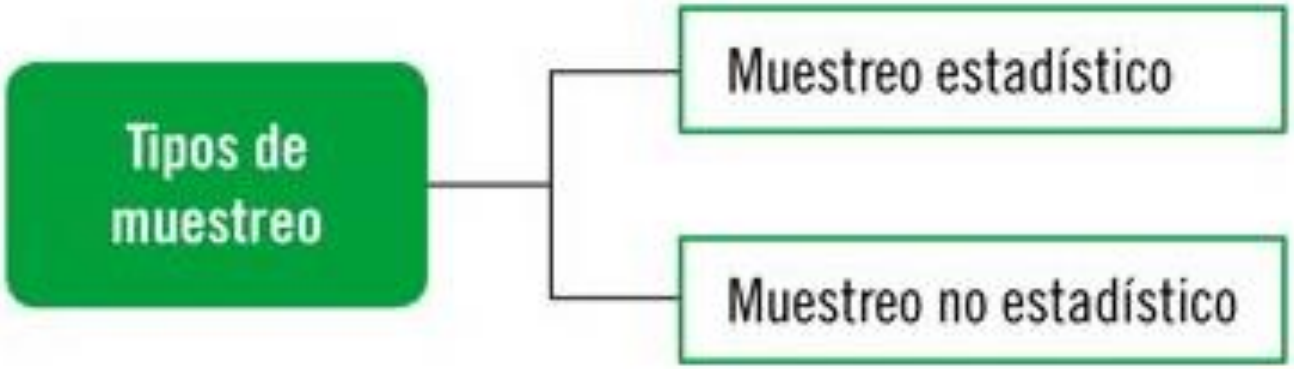
SEGURIDAD INFORMÁTICA

2.1.2.MF0487_3. Capítulo 1
Parte 2 de 2

Criterios generales comúnmente aceptados sobre auditoría informática

JOSÉ PABLO HERNÁNDEZ

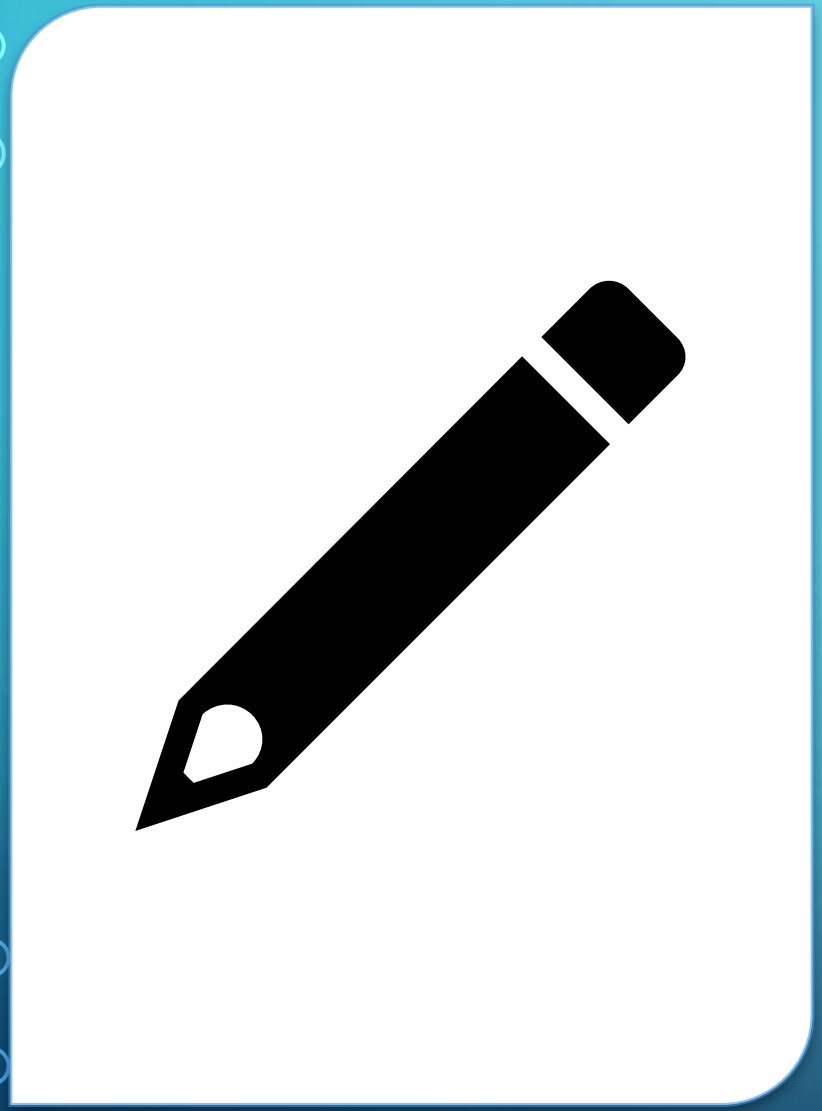
6. TIPOS DE MUESTREO DURANTE EL PROCESO DE AUDITORÍA



6.1. MUESTREO ESTADÍSTICO

Se utilizan técnicas matemáticas.

- **Tamaño de la muestra.**
- **Grados de confianza.**
- **Márgenes de error admitidos.**



Ejemplo

SE OBTIENEN LOS SIGUIENTES DATOS REFERENTES AL TIEMPO DE EJECUCIÓN DE UN PROCESO DE VARIOS EMPLEADOS DE LA ORGANIZACIÓN:

EMPLEADO	1	2	3	4	5
TIEMPO	10 MIN	12 MIN	9 MIN	11 MIN	15 MIN

DE ESTOS DATOS, SE DEDUCE QUE:

EL PROMEDIO DE TIEMPO DE EJECUCIÓN DEL PROCESO ES DE 11,4 MINUTOS, SUMA DE TODOS LOS TIEMPOS DIVIDIDA ENTRE EL NÚMERO DE EMPLEADOS: (10+12+9+11+15)/5.

LAS DESVIACIONES DE LOS DISTINTOS EMPLEADOS SE CALCULAN RESTANDO EL TIEMPO DE CADA EMPLEADO DEL TIEMPO MEDIO OBTENIDO, SIENDO:

EMPLEADO	1	2	3	4	5
TIEMPO	10 MIN	12 MIN	9 MIN	11 MIN	15 MIN
DESVIACIONES	–1,4 MIN	0,6 MIN	–2,4 MIN	–0,4 MIN	3,6 MIN

6.2. MUESTREO NO ESTADÍSTICO

Se basa en el criterio del auditor informático (criterio subjetivo):

- **Técnicas aprendidas en el desarrollo de su profesión.**
- **Conocimientos adquiridos por su experiencia.**

7. HERRAMIENTAS CAAT

CAAT (Computer Assisted Audit Tools): están formadas por un conjunto de herramientas y técnicas cuya función es facilitar al auditor informático el desarrollo de sus tareas.

7. HERRAMIENTAS CAAT

- Pruebas de controles en aplicaciones.
- Selección y monitorización de transacciones.
- Verificación de datos.
- Análisis de los programas de las aplicaciones.
- Auditoría de los centros de procesamiento de la información.
- Auditoría del desarrollo de aplicaciones.
- Técnicas de muestreo.

El auditor de sistemas de información debe tener un conocimiento profundo de estas herramientas.

7. HERRAMIENTAS CAAT

Estas herramientas constan de una serie de aspectos fundamentales y, entre sus funcionalidades principales, destacan las siguientes:

- **Capacidad de muestreo.**
- **Utilización de algoritmos de búsqueda de patrones de fraude.**
- **Acceso a datos de varios formatos.**
- **Filtrado de datos.**
- **Recurrencia de pruebas.**
- **Relación de información procedente de varios archivos distintos.**
- **Generación de informes y reportes, tanto de texto como con gráficos.**

7. HERRAMIENTAS CAAT

Ventajas de las herramientas CAAT:

- **Se reduce el nivel de riesgo de la auditoría, al ser aplicaciones especializadas que minimizan la probabilidad de error.**
- **Al ser técnicas mecanizadas, añaden independencia a las actividades desarrolladas por el auditor.**
- **Proporcionan mayor coherencia a los resultados de la auditoría.**
- **Facilitan una mayor disponibilidad de la información.**
- **Facilitan y mejoran la identificación de las posibles excepciones.**
- **Añaden posibilidades de detectar, analizar y cuantificar los puntos débiles de los controles internos de los sistemas auditados.**

7.1. DOCUMENTACIÓN DE LAS TÉCNICAS DE LAS HERRAMIENTAS CAAT UTILIZADAS

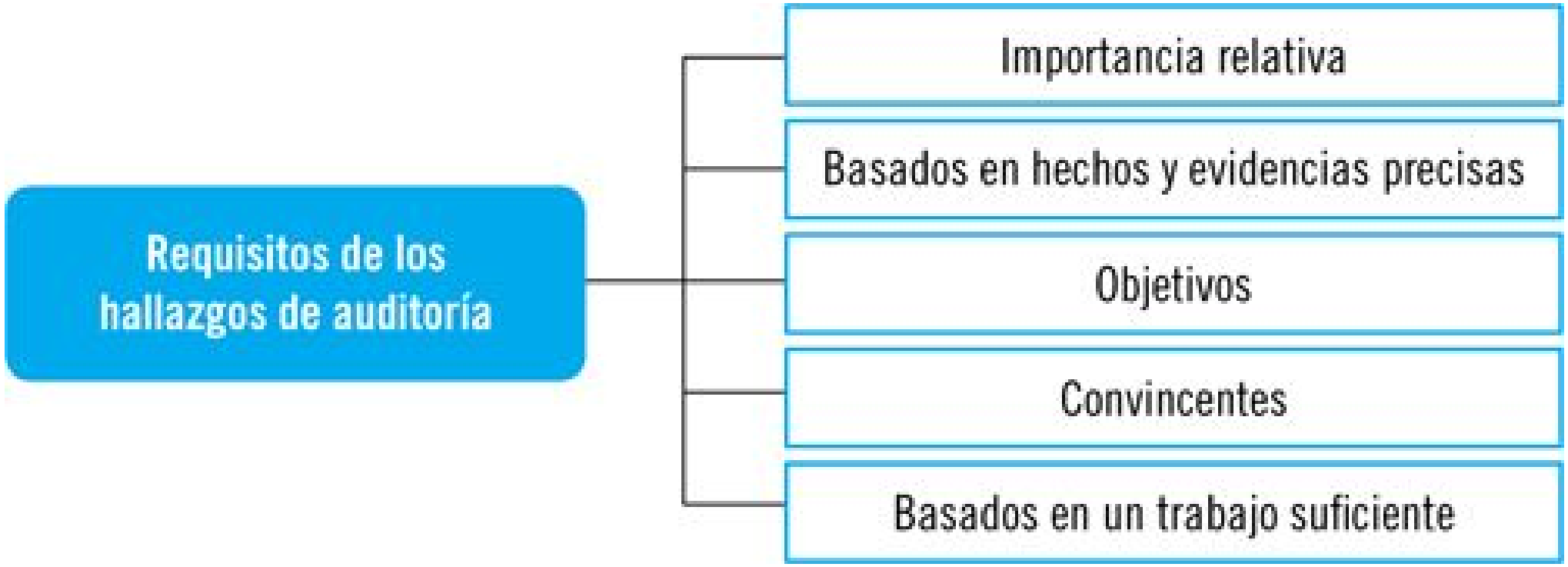
Algunos de los modos de documentación de las técnicas CAAT utilizadas para ayudar y complementar al auditor son:

- **Listado de los programas analizados y utilizados.**
- **Flujogramas.**
- **Informes que justifiquen las muestras obtenidas.**
- **Diseño de los archivos y los registros.**
- **Definición de los campos analizados.**
- **Relación de las instrucciones de operación realizadas.**

8. HALLAZGOS DE AUDITORÍA

Los hallazgos de auditoría son hechos que el auditor ha detectado durante su examen y servirán como base para que el auditor pueda emitir sus conclusiones y recomendaciones para mejorar el funcionamiento del sistema auditado.

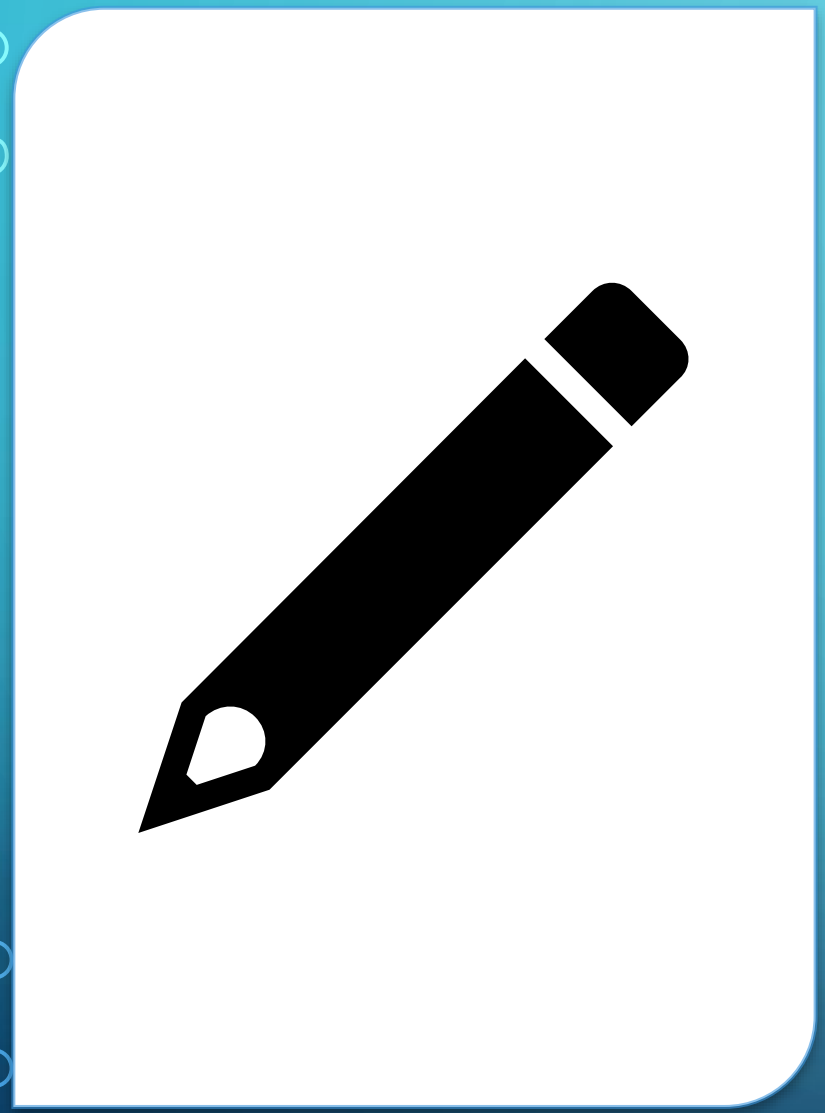
8.1. REQUISITOS BÁSICOS DE LOS HALLAZGOS DE AUDITORÍA



Estos requisitos son subjetivos y están sujetos a interpretaciones.

8.2. PASOS A SEGUIR EN EL DESARROLLO DE HALLAZGOS

- Identificación de la condición o asuntos deficientes o debilidades del sistema de información según los criterios aceptables definidos.
- Identificación de los responsables respecto a las operaciones implicadas en el hallazgo.
- Verificación de la causa o causas de la deficiencia detectada.
- Determinación de si la deficiencia es un caso aislado o una condición generalizada y difundida.
- Determinación de la relevancia y consecuencias de la deficiencia.
- Entrevista con los interesados que puedan estar afectados con el hallazgo para obtener datos adicionales.
- Determinación de las conclusiones de auditoría obtenidas por el análisis de la evidencia a raíz del hallazgo.
- Definición de las acciones correctivas y/o recomendaciones que subsanen la deficiencia detectada.



Ejemplo.

EN PLENO PROCESO DE AUDITORÍA INFORMÁTICA, LAS HERRAMIENTAS DE AUDITORÍA HAN DETECTADO UNA SERIE DE DEBILIDADES QUE PODRÍAN CLASIFICARSE COMO HALLAZGOS. NO OBSTANTE, LA IMPORTANCIA DE ESTAS ES BASTANTE BANAL Y, ADEMÁS, EL TRABAJO REALIZADO PARA DETECTARLAS NO FACILITA SUFICIENTE INFORMACIÓN COMO PARA RESPALDAR LAS POSIBLES CONCLUSIONES QUE PUEDAN OBTENERSE.

¿ESTAS DEBILIDADES PODRÍAN CONSIDERARSE HALLAZGOS?
¿CUMPLEN CON TODOS LOS REQUISITOS?

Ejemplo. Solución.

LAS DEBILIDADES DETECTADAS NO PUEDEN CONSIDERARSE HALLAZGOS AL NO CUMPLIR CON LOS REQUISITOS BÁSICOS QUE LES DEN GARANTÍA Y CONFIABILIDAD.

POR UN LADO, SE INCUMPLE EL REQUISITO DE IMPORTANCIA RELATIVA, AL NO SER LAS DEBILIDADES DETECTADAS LO SUFICIENTEMENTE RELEVANTES COMO PARA SER COMUNICADAS A LOS RESPONSABLES.

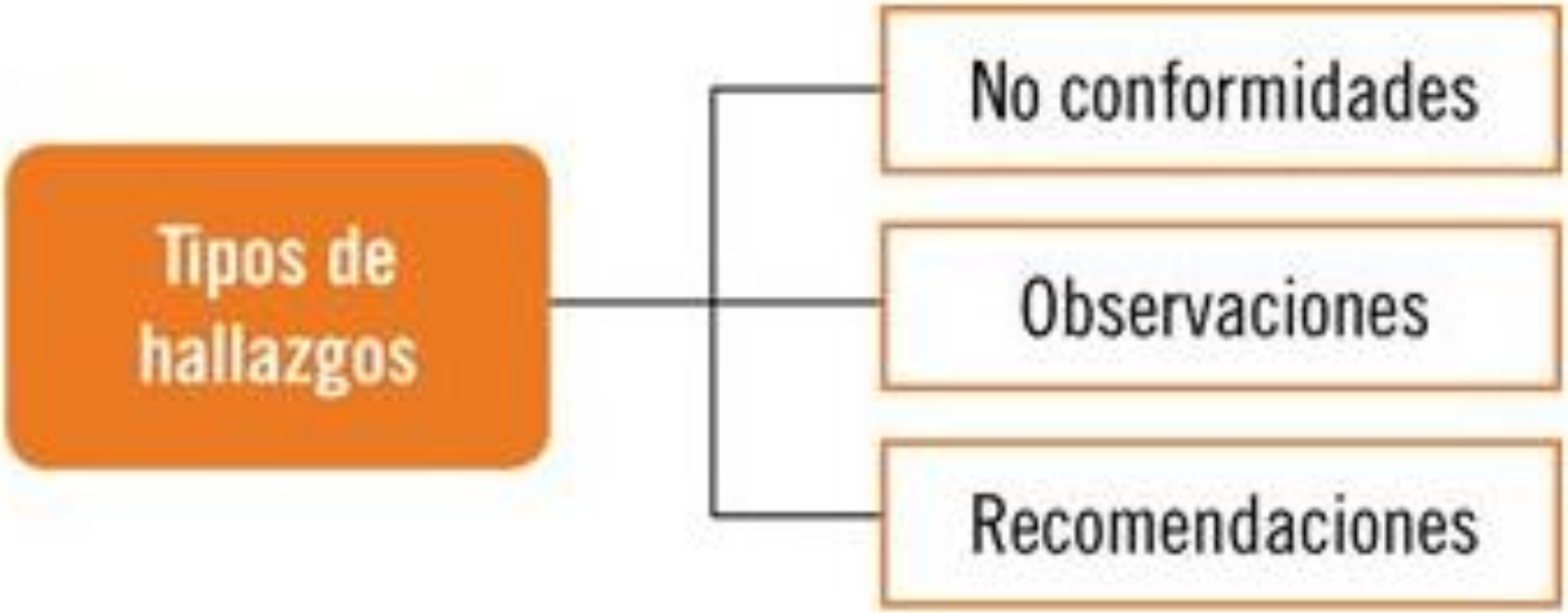
POR EL OTRO LADO, TAMBIÉN SE INCUMPLE EL REQUISITO DE ESTAR BASADAS EN UN TRABAJO SUFICIENTE, AL NO HABER PODIDO OBTENER SUFICIENTE INFORMACIÓN COMO PARA RESPALDAR LOS HALLAZGOS Y DARLES FIABILIDAD.

9. APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES

Los hallazgos son una serie de hechos que han sido detectados con el análisis y la evaluación de los documentos, procesos, actividades, entrevistas, etc., de todas las partes que integran el sistema de información auditado.

En términos de auditoría, se consideran desviaciones los incumplimientos de los requisitos de acreditación detectados por la observación de los hallazgos detectados en la auditoría.

9. APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES



9. APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES

Un hallazgo se clasificará como **no conformidad** cuando:

- Se trate de fallos generales del sistema.
- Se detecte la ausencia de algún elemento importante para el sistema de información.
- Se detecte un conjunto de varias observaciones que, vistas de un modo aislado, no son importantes, pero que en su detección global pueden desembocar en fallos más relevantes.

9. APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES

Se considerarán **observaciones** aquellos hallazgos en que:

- Se detecten fallos ocasionales, aislados, que no se produzcan con periodicidad.
- Se detecten fallos cuya resolución sea fácil o rápida.
- Se detecten incumplimientos parciales de los requisitos definidos en la auditoría.

9. APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES

Serán **oportunidades de mejora:**

- Las recomendaciones del auditor que, en caso de no aplicarlas, no provoquen debilidades o fallos en el sistema.
- Las recomendaciones que estén basadas en el juicio y la experiencia del auditor.

9. APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES

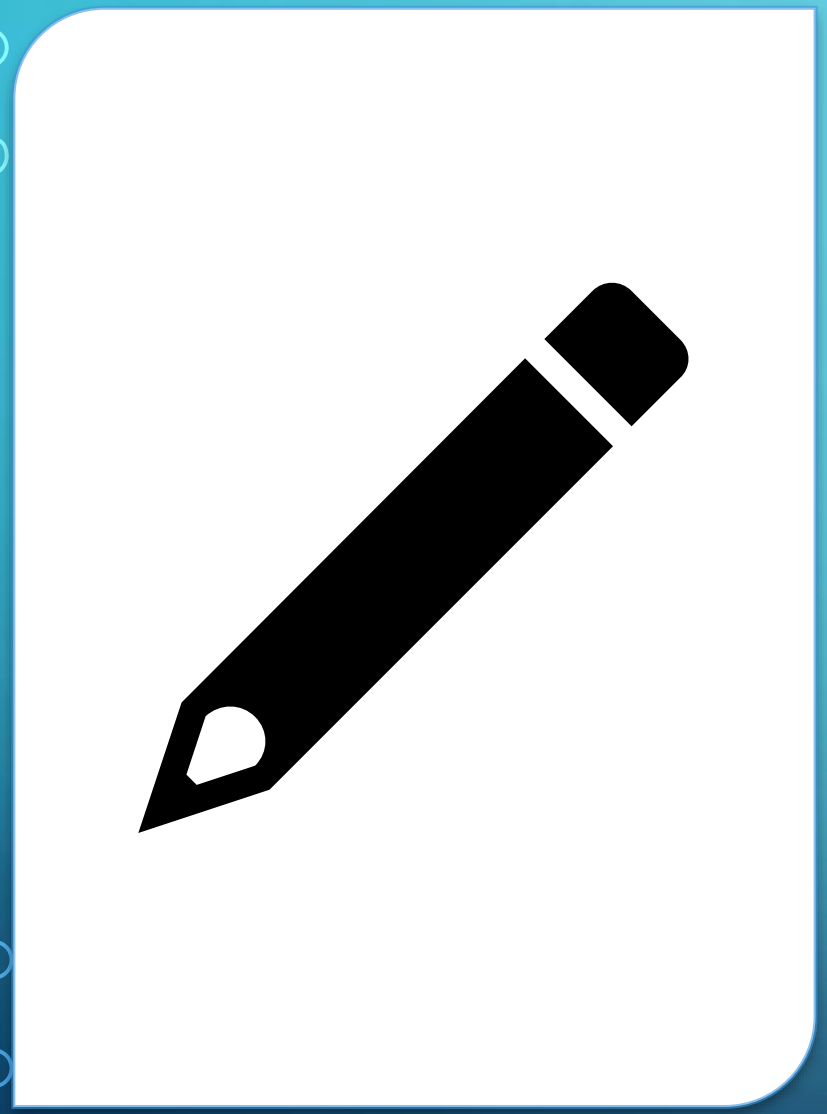
La clasificación de los hallazgos no es un proceso exacto:

ES UN PROCESO SUBJETIVO

Ejemplo.

EN PLENO PROCESO DE AUDITORÍA DEL SISTEMA, EL SOFTWARE INFORMÁTICO HA DETECTADO UN FALLO GENERAL DEL SISTEMA QUE SEÑALA UNA DEBILIDAD GRAVE DEL MISMO. POR OTRA PARTE, TAMBIÉN SE HA DETECTADO UNA DEBILIDAD DE MENOR GRAVEDAD CUYA APARICIÓN ES PURAMENTE OCASIONAL (NO HAY PERIODICIDAD DE LA DEBILIDAD).

CLASIFIQUE AMBOS HALLAZGOS E INDIQUE CUÁL DE LOS DOS DEBERÍA SER RESUELTO PRIORITARIAMENTE.



Ejemplo. Solución.

EL HALLAZGO DETECTADO POR UN FALLO GENERAL Y GRAVE DEL SISTEMA DEBERÍA SER CLASIFICADO COMO NO CONFORMIDAD AL AFECTAR AL CONJUNTO DEL SISTEMA.

SIN EMBARGO, EL HALLAZGO DE LA DEBILIDAD OCASIONAL Y DE POCA GRAVEDAD TIENE QUE CLASIFICARSE COMO OBSERVACIÓN AL NO HABER PERIODICIDAD Y NO AFECTAR AL CONJUNTO GLOBAL DEL SISTEMA EN SÍ.

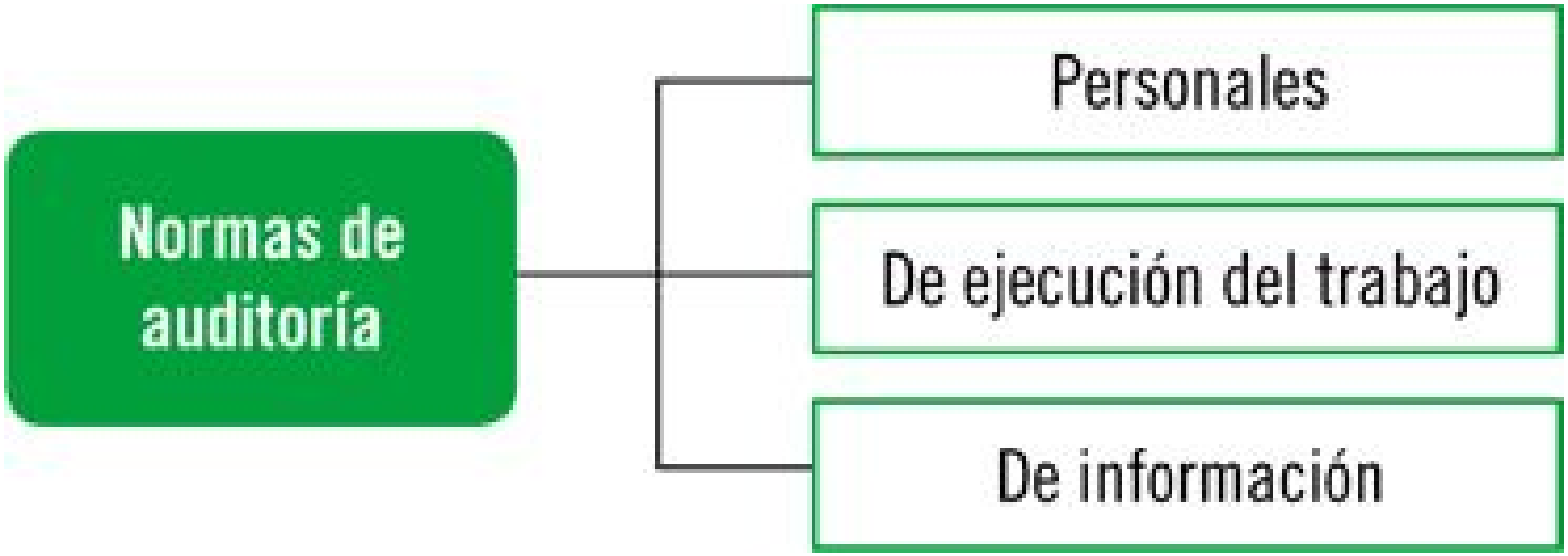
DEBIDO A LA ELEVADA GRAVEDAD, DEBERÍA RESOLVERSE PRIORITARIAMENTE LA NO CONFORMIDAD, PUDIENDO POSPONERSE EL TRATAMIENTO DE LA OBSERVACIÓN HASTA NO SER RESUELTA LA PRIMERA.

10. RELACIÓN DE LAS NORMATIVAS Y METODOLOGÍAS

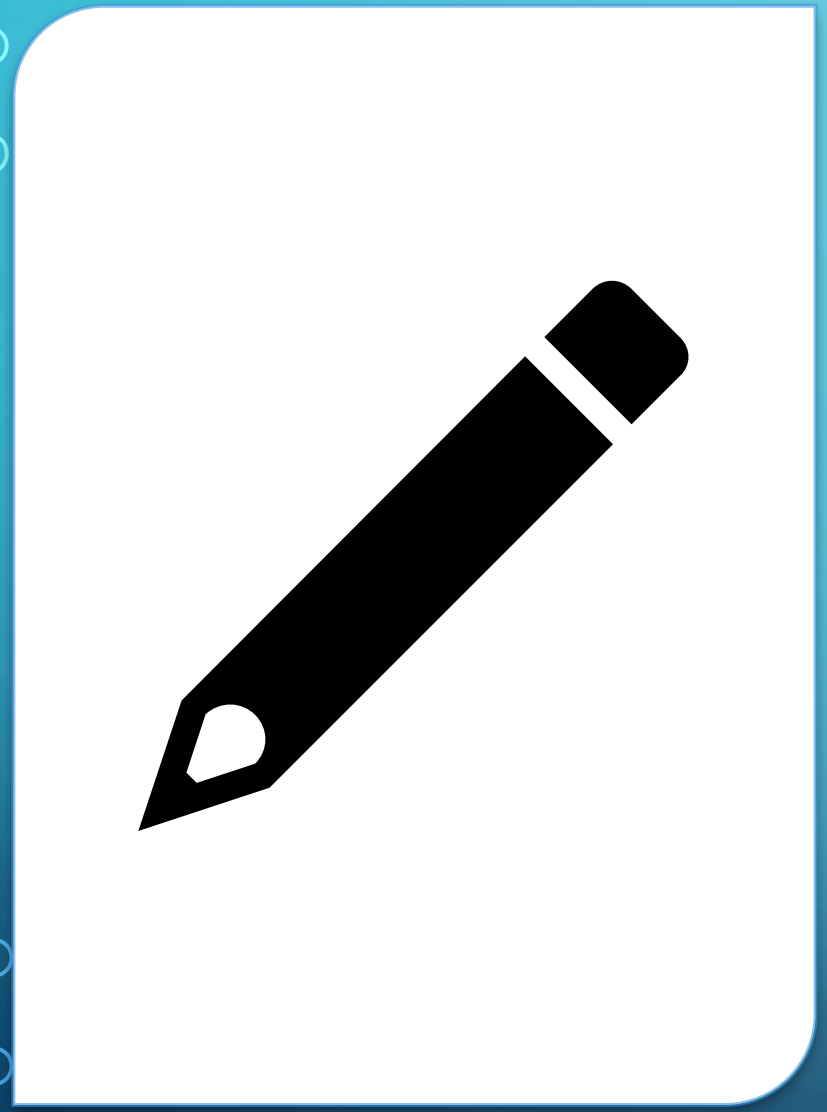
Metodología tradicional: en la que el auditor se encarga sobre todo de revisar los controles del sistema, ayudándose de una lista de control que incluirá varias preguntas pendientes de verificar. La evaluación del sistema consistirá en identificar y verificar una serie de controles establecidos o estandarizados previamente.

Metodología basada en la evaluación de riesgos: en este caso, el auditor no hace un chequeo simple, sino que hace evaluaciones de los riesgos potenciales existentes, bien por la ausencia de controles bien por la deficiencia del sistema. Aquí, el auditor deberá verificar y cuantificar los riesgos para conocer el grado de confiabilidad del sistema, atendiendo a la exactitud y a la integridad de su información.

10.1. NORMATIVAS RELACIONADAS CON LA AUDITORÍA DE SISTEMAS



Ejercicios



2.1.100.1.MF0487_3_EJERCICIOSCAPITULO_1.DOCX