

# Seguridad y Auditoría Informática

Herramientas y Etapas de la Auditoría Informática

# Objetivos

- Identificar cada una de las herramientas utilizadas en el proceso de Auditoría
- Describir brevemente las etapas del proceso de Auditoría para una Aplicación Informática

# Herramientas en Auditoría de una Aplicación | Entrevistas

- Se debe realizar a quienes más aporten al propósito pretendido.
- Se requiere conocer lo suficiente sobre la aplicación para conducirla y obtener la mayor cantidad de información evitando preguntas cerradas.
- Debe coordinarse con antelación suficiente, especificando los temas a tratar, duración aproximada y solicitando la información o documentación necesaria.
- Los supervisores de los entrevistados deben estar informados de las actuaciones y serán ellos quienes comuniquen al entrevistado de la necesidad de la auditoría.
- El auditor tomará las anotaciones correspondientes y las revisará con el interlocutor para asegurarse que sus aportes estén reflejados completamente.

# Herramientas en Auditoría de una Aplicación | Encuestas

- Se utilizan para determinar el alcance y objetivos de la auditoría y para medir el nivel de satisfacción de los usuarios.
- Aplican la mayoría de los requisitos enunciados para las entrevistas.
- Consiste en preparar un cuestionario que pueda ser respondido rápidamente a base de marcar entre las respuestas posibles.
- Conviene que todas las respuestas tengan espacio para “observaciones” para capturar los comentarios del encuestado.
- Debe identificarse la organización a la que pertenece el encuestado. La identificación personal no es obligatoria, pero permite enriquecer asuntos de interés en los que se quiera profundizar.

# Herramientas en Auditoría de una Aplicación | **Observación del Trabajo de los Usuarios**

- Se observa cómo los usuarios ejecutan las transacciones más significativas por su volumen o riesgo. Esto ayuda a identificar irregularidades e ineficiencias.
- Debe aprovecharse esta oportunidad para probar también la efectividad de los controles de las transacciones, solicitando la simulación de situaciones previsibles de error.

# Herramientas en Auditoría de una Aplicación | **Pruebas de Conformidad**

- Orientadas a comprobar que determinados procedimientos, normas o controles internos se cumplen o funcionan de acuerdo con lo previsto y esperado, según lo documentado.
- La comprobación debe llevar a la evidencia a través de los resultados producidos: registros, documentos, etc. y/o observación directa del funcionamiento de un control ante pruebas específicas de comportamiento.
- Se deben elaborar informes de excepción cuando existe evidencia de incumplimiento.
- Los testimonios de incumplimiento aislados no implican evidencia, pero cuando son obtenidos de varias personas pueden derivar en posibles recomendaciones, ahorrando esfuerzos en obtener evidencias documentadas.

# Herramientas en Auditoría de una Aplicación | **Pruebas Sustantivas o de Validación**

- Buscan detectar la presencia o ausencia de errores o irregularidades en procesos, actividades, transacciones o controles internos integrados en ellos.
- Se buscan irregularidades diversas que pueden afectar a las transacciones.
- Múltiples recursos pueden ser utilizados, muchos de ellos se apoyan en la utilización de herramientas informáticas.
- Otros recursos clásicos utilizados para la detección de errores o sus indicios son de ejecución manual. Normalmente se aplican sobre muestras, estadísticas y no estadísticas.

# Herramientas en Auditoría de una Aplicación | **Uso de Equipos Informáticos**

- Existen en el mercado infinidad de productos de software concebidos para facilitar la tarea del auditor, aunque se pueden obtener resultados similares haciendo uso de herramientas disponibles en la organización como bases de datos.
- Los registros de auditoría de que esté provista la aplicación deben constituir un apoyo importante a la hora de utilizar equipos para detectar situaciones o indicios de posible error.
- También hay que considerar la posibilidad de utilizar la propia aplicación, aplicando juegos de ensayo o transacciones ficticias preparadas por los auditores, para verificar la eficacia de los controles implementados.



# Etapas de la Auditoría de una Aplicación Informática

# Obtención de Información y Documentación sobre la Aplicación (1/2)

- Se necesita tener un conocimiento básico de la aplicación y su entorno, para identificar puntos débiles y riesgos.
- Se inicia el proceso con entrevistas tanto a los usuarios de la aplicación como a los responsables de los Sistemas de Información, hasta poder establecer los objetivos de la auditoría.
- Es necesario tener una guía que establezca pautas y documentos a solicitar, es decir, todo lo que ayude a:
  - Adquirir una primera visión global del sistema
  - Conocer la organización y los procedimientos de los servicios que utilizan la aplicación
  - Describir el entorno en el que se desarrolla la aplicación

# Obtención de Información y Documentación sobre la Aplicación (2/2)

- Entender el entorno de software básico de la aplicación
- Asimilar la arquitectura y características lógicas de la aplicación
- Conocer las condiciones de utilización de la aplicación y los riesgos que se pueden dar
- Conocer las condiciones de seguridad de que dispone la aplicación
- Disponer de información estadística, métricas, indicadores, informes, etc.

# Determinación de los Objetivos y Alcance de la Auditoría

- Las observaciones tras el examen preliminar, la identificación de los puntos débiles y las funciones críticas, deben permitirle al auditor establecer su propuesta de objetivos de la auditoría de la aplicación y un plan detallado del trabajo a realizar
- En la preparación del plan de trabajo trataremos de incluir:
  - La planificación de los trabajos y el tiempo a emplear
  - Las herramientas y métodos
  - El programa de trabajo detallado
  - Pruebas de confirmación, pruebas sobre los datos y los resultados

# Planificación de la Auditoría

- La auditoría de una aplicación informática debe tener una planificación cuidadosa
- No es conveniente que coincida con el momento de la implementación de la aplicación
- No debe tener un retraso excesivo que prolongue el período de exposición a riesgos
- Hay que establecer el ámbito de actuación, priorizando lugares donde estén la mayor cantidad de pruebas a realizar, haya representatividad de usuarios y los costos sean razonables
- El personal de auditoría debe contar con las autorizaciones necesarias para acceder a la aplicación y a las herramientas de usuario

# Trabajo de Campo, Informe e Implementación de Mejoras

- La etapa de realización del trabajo de campo consiste en la ejecución del programa de trabajo establecido
- En la etapa de redacción del informe de auditoría, se reunirán las características del trabajo realizado y sus conclusiones y recomendaciones o propuestas de mejora
- En la etapa de implementación de las mejoras identificadas en la auditoría, la situación óptima a alcanzar es conseguir que la organización auditada asuma las propuestas de actuación para implementar las recomendaciones como objetivos de la organización

# Síntesis

- **Herramientas**

- Entrevistas
- Encuestas
- Observación del Trabajo de los Usuarios
- Pruebas de Conformidad
- Pruebas Sustantivas o de Validación
- Uso de Equipos Informáticos

- **Etapas**

- Obtención de Información y Documentación sobre la Aplicación
- Determinación de los Objetivos y Alcance de la Auditoría
- Planificación de la Auditoría
- Trabajo de Campo, Informe e Implementación de Mejoras

# ¿Preguntas?



¡Muchas Gracias!