

CAATs - Computer Assisted Audit Techniques

Seguridad y Auditoría Informática
Maestría en Tecnologías de la Información
FCEQyN - UNaM / FACENa - UNNE



Antes de empezar

Obtener todo el material

Clonar el repositorio con el material necesario para el desarrollo de las actividades prácticas:

Ejecutar (*en la clase*):

```
git clone http://172.16.7.200/rej/auditoria.git
```

Offline:

Descomprimir archivo .zip con el material general.



Obtener las imágenes de docker a usar

Pasos a seguir:

- Abrir el archivo **README.md** de la raíz del repositorio clonado (*que contiene estas instrucciones*)
- Copiar el archivo **daemon.json** según las instrucciones del archivo anterior.
- **Reiniciar** el servicio de docker
- Obtener (**pull**) las imagenes (3) -- puede demorar --





Contexto

CAATs

Son todas las herramientas software que un auditor puede utilizar como parte de su trabajo habitual a fin de procesar datos de potencial utilidad para los objetivos del proyecto de auditoría. Su utilización podría resultar en una mayor cobertura de los objetivos de la auditoría, una mayor consistencia en los análisis a realizar y una reducción de los riesgos relacionados a la actividad.

ISACA plantea lineamientos para su utilización en la **Guía G3**.



Guía G3 - ISACA

Definiciones:

- “CAATs include **many types of tools and techniques**, such as generalised audit software, customised queries or scripts, utility software, software tracing and mapping, and audit expert systems.”
- “CAATs **may produce a large proportion of the audit evidence developed on IS audits [...]**”



Guía G3 - ISACA (cont.)

“

CAATs may be used in performing various audit procedures including:

- *Tests of details of transactions and balances*
- *Analytical review procedures*
- *Compliance tests of IS general controls*
- *Compliance tests of IS application controls*
- *Penetration testing*

”



Fases en el uso de CAATs: Planificación

Evaluación de viabilidad

- Conocimientos
- Disponibilidad de software
- Riesgos
- Aplicabilidad (tiempos - recursos)

Planificación

- Objetivos
- Recursos (datos - sistemas - redes)
- Procedimientos a seguir

Acuerdos

- Tiempos
- Accesos
- Impacto en actividades de la organización

Pruebas

- Integridad
- Usabilidad
- Seguridad

Seguridad

- Integridad de elementos de análisis
- Confidencialidad

Fases en el uso de CAATs: Ejecución

Analizar los elementos a auditar

Obtener las características de cada elemento (datos, software, hardware) a analizar y de los recursos necesarios para la tarea.



Analizar el contexto

Revisar cuestiones relativas a particularidades en la infraestructura o configuración que deban ser consideradas en el proceso.



Determinar el tipo de software a utilizar

- Software general de auditoría
- Software de propósito general
- Desarrollos propios
- Herramientas de monitoreo
- Sistemas expertos de auditoría informática

Fases en el uso de CAATs: Documentación



Fases en el uso de CAATs: Informe

Consideraciones

- El uso de CAATs se va a detallar en el informe a entregar al auditado.
- Las cuestiones que se consideren relevantes sobre el proceso deberán ser incluidas en el cuerpo del informe, o en su defecto en anexos junto a los reportes de las herramientas.



Ejemplos de herramientas y aplicaciones

- Escaneo de servidores (nmap)
- Análisis de sitios web (owasp)
- Análisis estático y dinámico de código (sonarqube)
- Análisis de datos (estadística)
- Detección de patrones ocultos en los datos (minería de datos)

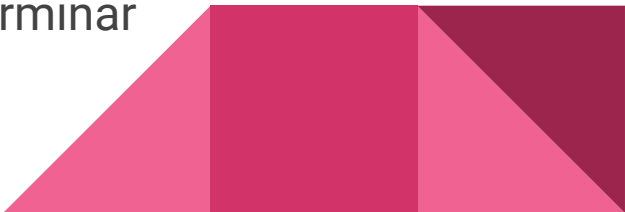
Ejemplos

[1] Análisis estático de código con Sonarqube

Tipo de auditoría:

- Procesos de desarrollo | adquisición de software
- Explotación | mantenimiento

Escenario:

- Ante el desarrollo, la adquisición o cambio de versión de un producto software se realiza una evaluación del mismo en términos de la calidad de su código fuente para determinar si se cumplen los SLAs establecidos.
- 

[2] Análisis de calidad de datos con Python

Tipo de auditoría:

- Datos | base de datos
- Explotación de un sistema software

Escenario:

- Se desea generar una solución de tipo OLAP o implementar procesos de explotación de información para obtener conocimiento a partir de los datos disponibles. Previamente se tiene que evaluar la calidad de los datos.

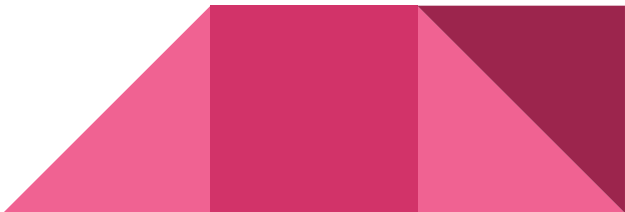


[3] Análisis de una aplicación web con OWASP

Tipo de auditoría:

- Seguridad | comunicaciones
- Explotación de un sistema software

Escenario:

- Se desea analizar la seguridad de una aplicación web de la entidad auditada, incluyendo algunas cuestiones relativas a su seguridad y optimización para el uso por parte de diferentes clientes.
- 

Práctica

Conclusiones

Algunas ideas...

El uso de CAATs es de gran utilidad para un proyecto de auditoría informática, a través de ellas se puede obtener una serie de **evidencias** que darán soporte a **hallazgos** que se incluyan en el informe final de la actividad.

En determinados escenarios y tipos de auditoría, el uso de estas herramientas se vuelve (casi)obligatorio para poder **cubrir el alcance del entorno a auditar**.

Es responsabilidad del auditor conocer las herramientas que **mejor aplican** en cada caso y determinar los **procedimientos** para su uso.



Trabajo práctico

Trabajo práctico

Modalidad: grupal

Plazo de entrega: 15 días

Consigna:

- Seleccionar uno de los ejemplos de casos de uso de CAATs planteados y reproducirlos sobre un escenario similar al planteado en clase.
- Registrar las evidencias recolectadas.

