

# INGENIERIA DE SISTEMAS



Mgs. C.X.M.A

# INTRODUCCIÓN

La auditoría como actividad genérica se define como la **revisión de la gestión** de una organización en un ámbito determinado, con el propósito de verificar y evaluar si esta se ajusta a la normativa o a las políticas establecidas.

Siguiendo esta línea, la auditoría de seguridad de la información se define como la revisión e inspección **independiente** de las medidas de seguridad implantadas para valorar su idoneidad y eficacia al verificar y asegurar su conformidad con las políticas y los procedimientos establecidos y recomendando los cambios necesarios.

Las auditorias de seguridad en función del objetivo se pueden clasificar de la siguiente manera:

- ▶ **De cumplimiento:** tiene como objetivo evaluar la conformidad de los entornos auditados con respecto a una normativa de seguridad de la información establecida. Por ejemplo, el estándar de seguridad ISO 27001, RGPD o de las propias políticas y procedimientos internos de seguridad de la organización.
- ▶ **Técnicas:** auditorías o revisiones de seguridad técnica cuyo alcance está acotado a los sistemas informáticos, o de telecomunicaciones, y son objeto de la revisión.

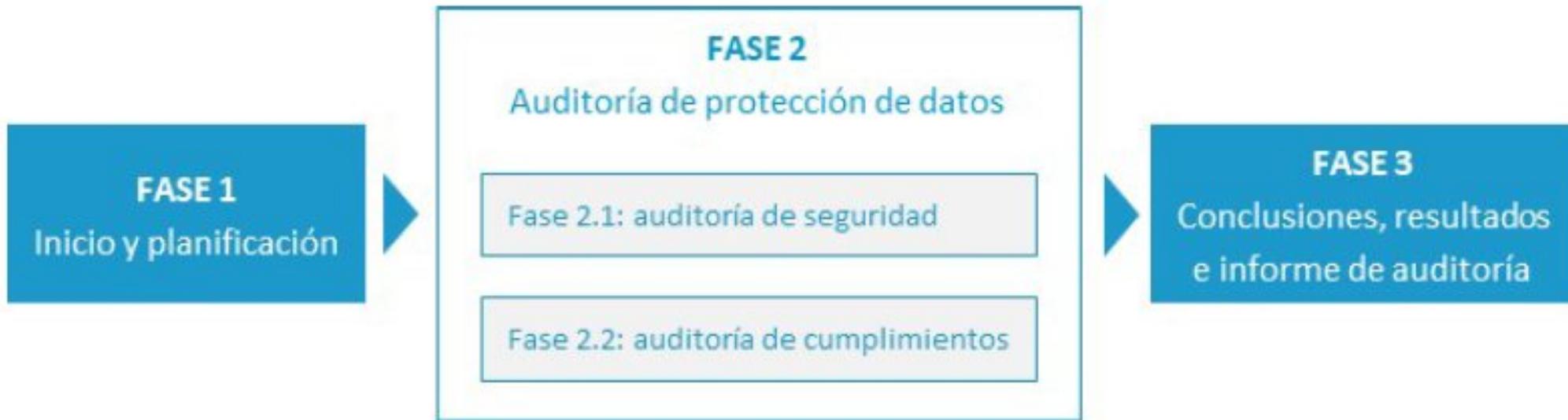
# OBJETIVOS

---

- ▶ Definir y explicar los conceptos relacionados con las auditorías de seguridad de cumplimiento de seguridad de la información.
- ▶ Estudiar las diferentes metodologías de realización de auditorías de seguridad técnicas existentes en la actualidad.
- ▶ Aprender a seleccionar qué metodología de auditoría de seguridad es la más conveniente para la realización de un tipo concreto de auditoría.
- ▶ Obtener el conocimiento necesario para poder realizar los diferentes tipos de auditorías que comprende la seguridad de la información.

- **TIPOS DE AUDITORIAS**
- El proceso habitual para la realización de una auditoría técnica de seguridad será, en primer lugar, un acuerdo con la compañía a auditar para poder llevar a cabo las acciones de intrusión ajustándonos al marco jurídico actual. Para ello, dicha compañía nos tendrá que aprobar estas acciones.
- 
- Una vez se tiene acordada la realización de este tipo de auditorías, se deberán conocer y acordar, a su vez, la modalidad de auditoría que se desea realizar. Podemos distinguir entre las siguientes:

# FASES DE TIPOS DE AUDITORIA



- Caja blanca. Se dispone de acceso y conocimiento de todo acerca del objetivo.
  - Es decir, se tendrán usuarios con permisos administrativos, usuarios de cualquier perfil, mapa de red, etc.
- 
- Caja negra. No se tiene ningún conocimiento del objetivo, únicamente la información que se pueda encontrar públicamente. Se puede considerar como la modalidad más realista en cuanto a un ataque, puesto que normalmente los ciberdelincuentes no tienen conocimiento o acceso interno.
- 
- Caja gris. Se dispone de información limitada. Normalmente es la compañía por auditar la que decide qué información nos provee, usualmente un usuario con permisos restringidos y un acceso a la red como mínimo.

# Tipos de auditorías

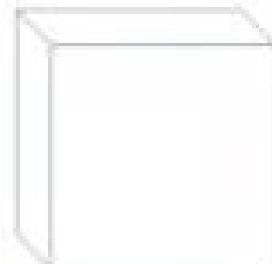
## MODALIDADES

TIPO	CONOCIMIENTOS
WHITE BOX	COMPLETOS
GRAY BOX	LIMITADOS
BLACK BOX	NINGUNO



Black Box Penetration Testing

No Knowledge  
Penetration Test As Attacker  
Most Realistic



White Box Penetration Testing

Full Knowledge  
Penetration Test as a Developer  
Unrealistic



Grey Box Penetration Testing

Some Knowledge  
Penetration Test as Attacker / User  
Semi-realistic

AUDITORÍA  
REDES

AUDITORÍA  
SISTEMAS

AUDITORÍA  
WEB



AUDITORÍA  
CONEXIONES  
INALÁMBRICAS

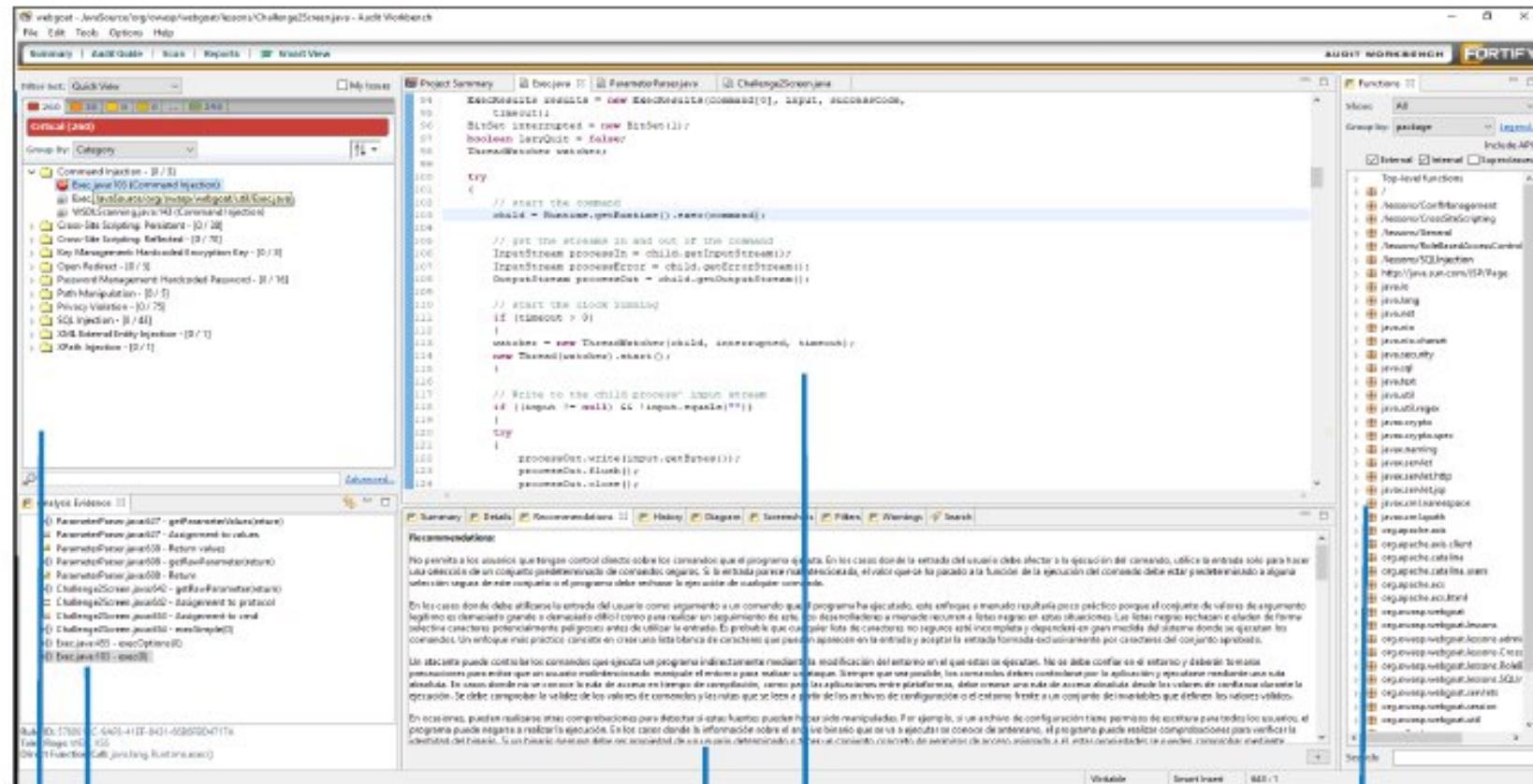
AUDITORÍA  
APLICACIONES

AUDITORÍA  
PERIMETRAL

# EJEMPLOS DE AUDITORIA FINANCIERA



# EJEMPLO DE UNA APLICACIÓN



## Panel de Trazabilidad

## Panel de Hallazgos

## Panel de Código Fuente

Panel de Auditoría

## Panel de Funciones

# EJEMPLO SEGURIDAD DE UN SOFTWARE

- ▶ Las principales causas de la aparición de vulnerabilidades son las siguientes:

- Vulnerabilidades de Componentes**

- ① Mezcla de código

- ✓ Integración de componentes

- ✗ Pruebas de seguridad

- 💡 Falta de conocimiento

- 💡 Guías de codificación

- ✳️ Tolerancia a los defectos

- ✗ Entorno de pruebas

## Erros en el Software

- Complejidad**

- ✗ Debilidades en la Esp. Req.

- ⚠️ Tamaño Excesivo

- ? Cambios de requisitos

- ✳️ Mezcla de Equipos

- ➡️ Cadena de Suministro

- ? Nuevas Funcionalidades

- ⭐ Actualizaciones

# Propiedades de un software seguro

## ▶ Propiedades complementarias

- Fiabilidad.
- Autenticación.
- Trazabilidad.
- Robustez.
- Resiliencia.

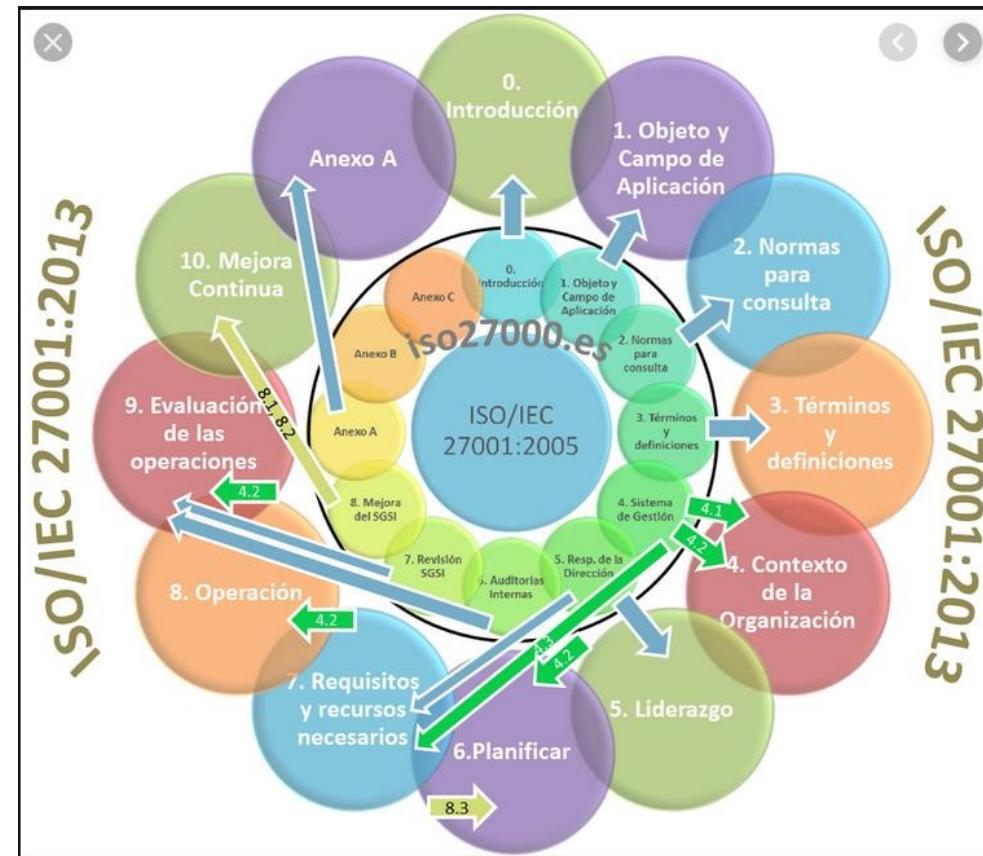


# Estándares de seguridad de la información

- ISO/IEC 27000-series
- ISO/IEC 27001
- ISO/IEC 17799

## Otros estándares relacionados

- COBIT
- ISACA
- ITIL



## **Certificaciones**

- CISM - CISM Certificaciones [4] : Certified Information Security Manager
- CISSP - CISSP Certificaciones [5] : Security Professional Certification
- GIAC - GIAC Certificaciones [6] : Global Information Assurance Certification

## **Certificaciones independientes en seguridad de la información**

- CISA- Certified Information Systems Auditor , ISACA
- CISM- Certified Information Security Manager, ISACA
- Lead Auditor ISO27001- Lead Auditor ISO 27001, BSI
- CISSP - Certified Information Systems Security Professional, ISC2
- SECURITY+, COMPTia - Computing Technology Industry Association
- CEH - Certified Ethical Hacker
- PCI DSS - PCI Data Security Standard

## ISO 27001

---



-Estándar de seguridad que define  
un Sistema de Gestión de  
Seguridad de la Información (SGSI)

-ISO 27002

No aplicable a la automatización y  
control industrial.

---

# **¡PREGUNTAS!**