***Imagen que contiene Logotipo

Descripción generada automáticamente***

Alejandro Ortega Martínez

Grado en Ingeniería Informática

21/4/2021

Trabajo 4

Auditorias Informaticas

Seguridad Informatica

Contenido

[1. Introducción 2](#_Toc68681142)

[1.1. ¿Qué es FOCA? 2](#_Toc68681143)

[1.2. Técnicas 3](#_Toc68681144)

[2. Instalación de FOCA 4](#_Toc68681145)

[3. ¿Qué son los Metadatos? 5](#_Toc68681146)

[3.1 Metadatos en la Informática 6](#_Toc68681147)

[3.1.1. Como ver los metadatos de forma manual 7](#_Toc68681148)

[4. Análisis con FOCA: DNS Spoofing 8](#_Toc68681149)

[5. Análisis con FOCA: Metadatos de un documento 9](#_Toc68681150)

[5.1. Análisis de Metadatos de una imagen 10](#_Toc68681151)

[5.2. Análisis de metadatos de un documento Word 12](#_Toc68681152)

[5.3. Análisis de un dominio Web (marca.com) 14](#_Toc68681153)

[5.3.1. Configuración de Motor de Busqueda personalizado 14](#_Toc68681154)

[5.3.2. Busqueda de los metadatos 15](#_Toc68681155)

[5.3.3. Análisis de los metadatos 18](#_Toc68681156)

[5.4. Análisis de un dominio Web (ubu.es) 20](#_Toc68681157)

[6. Casos que tienen que ver con los metadatos: Tony Blair y el informe Chilcot 24](#_Toc68681158)

[7. Buenas practicas para evitar problemas con los metadatos 25](#_Toc68681159)

[8. Conclusiones 26](#_Toc68681160)

[9. Bibliografía 27](#_Toc68681161)

# Introducción

## 1.1. Definición y conceptos

Podemos definir lo que es una auditoria (Wikipedia, s.f.) como la **acción de verificar que un determinado hecho o circunstancia ocurra de acuerdo a lo planeado**.

Si entramos en el ámbito de la informática, una **auditoría informática** es (Wikipedia, s.f.) un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos ya que esta lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas.

Es decir, podríamos entender como una auditoría informática como un proceso por el cual unos expertos comprueban, de forma sistemática, que los sistemas informáticos dentro de una organización funcionan como deberían. Tras esta comprobación, se **identifican errores**, como **necesidades**, **falsedades**, **errores de implementación**, **fallos de seguridad**, etc. los cuales se recogen en un informe y se entregan a la organización auditada, para que esta pueda paliarlos.

A grandes rasgos podemos encontrar **dos tipos de auditorías**, clasificadas según quien las realiza (mas adelante concretaremos todos los tipos de auditorias):

* **Auditoría Interna:** Es aquella que se hace desde dentro de la empresa; sin contratar a personas ajenas, en el cual los empleados realizan esta auditoría trabajan ya sea para la empresa que fueron contratados o simplemente algún afiliado a esta.
* **Auditoría Externa:** Es aquella en la cual la empresa contrata a personal externo para que haga la auditoría en su empresa.

Por otra parte, podemos agrupar los objetivos de una auditoria informática en 3:

* El **análisis de la eficiencia** de los Sistemas Informáticos.
* La verificación del **cumplimiento de la Normativa**.
* La revisión de la **eficaz gestión de los recursos informáticos.**

## 1.2. Peritaje Informático

Según la Universidad Nacional de Rosario (FCEIA, s.f.) Se conoce como peritaje informático a los estudios e investigaciones orientados a la obtención de una prueba informática de aplicación en un asunto judicial para que sirva a un juez para decidir sobre la culpabilidad o inocencia de una de las partes.

La pericia, por ser un medio probatorio, tiene sus normas, previstas en los códigos procesales, respecto a la designación, tiempos y forma de presentación.

# 2. Pasos para hacer una auditoría informática

Por lo general, las auditorías informáticas siempre se realizan de la misma manera, aunque cada empresa realizadora puede tener sus matices o metodologías. Sin embargo, por lo general y a grandes rasgos, todos siguen los siguiente cuatro pasos (Juliá, s.f.):

1. **Análisis**
2. **Planificación**
3. **Determinación de riesgos e incidencias**
4. **Ejecución**

## 2.1. Análisis

Cada empresa tiene diferentes objetivos cuando encargan auditorías informáticas. Puede que tengan una buena red de equipos, y en cuanto a su funcionamiento no les produce ningún problema, pero si tienen problemas en cuanto a la seguridad informática. Por tanto, lo primero que hay que hacer es **determinar los objetivos que se tienen**, y, aunque pueda pasar desapercibido, **hacer un inventario** de todos los aspectos que conciernen a los sistemas y usos informáticos de la empresa. En esta parte juegan un importante papel los empleados, puesto que serán ellos quien ayudarán a elaborar este inventario.

## 2.2. Planificación

Una vez tenemos los objetivos claros, y tenemos el inventario conformado (tanto de los equipos, como de su uso habitual dentro de la empresa), planificaremos nuestras auditorías a través de **herramientas de análisis.** Cómo vamos a evaluar cada uno de los puntos que hemos analizado y de acuerdo con que criterios. Por ejemplo, podemos estar haciendo una auditoria para saber si los equipos informáticos de una determinada empresa están preparados para ofrecer un determinado servicio web a tiempo real. El resultado de nuestra auditoria sería si están preparados o no, y por qué.

## 2.3. Determinación de riesgos e incidencias

El mantenimiento preventivo y predictivo es clave. No se trata de analizar ahora cuantas incidencias o problemas se están produciendo en este momento, sino los **posibles riesgos que existan de que se produzca un problema en el futuro**.

La empresa debe prever estos problemas mediante unas practicas de mantenimiento efectivas, sobre todo en cuanto a **seguridad informática**.

## 2.4 Ejecución

Por último, se toman **medidas para solventar tanto los problemas que hemos detectado que están ocurriendo, como los que hemos detectado que pueden ocurrir**. A partir de ahí, lo normal es elaborar un presupuesto con los puntos que habría que corregir para que se cumplan los objetivos de la empresa.

# 3. Tipos de auditorías informáticas

Antes hemos diferenciado entre auditorias internas o externas, según si el personal que realizaba la auditoria era propio de la empresa auditada, o era contratado para ese fin.

Sin embargo, podemos realizar una mayor clasificación en función del objetivo de la auditoría. Esta información ha sido extraída de HackBySecurity (HackBySecurity, s.f.), empresa experta en auditorias informáticas, basándonos en las auditorías que ellos llevan a cabo.

## 3.1. Auditoría Externa o Perimetral

**Que es**

La auditoría informática externa o perimetral, consiste en realizar un examen sistemático para estudiar el **nivel de seguridad de los elementos que se encuentran públicos por parte de la empresa.**  Para ello, el auditor estudia el estado de seguridad del perímetro de la organización analizando las posibles entradas desde el exterior hacia la DMZ y zonas internas como si de un atacante se tratase.

Este tipo de auditorias alcancan a elementos tipo servidores web, extranet, proxis, intranet, firewals, etc. Es decir, todo lo que este expuesto en el perímetro de la organización y a lo que se pueda acceder desde fuera.

**Como se realiza**

Este tipo de auditoria tiene **dos fases de recolección de información:** footprinting y Fingerprinting. Con ellas se recolecta información de internet para analizar la estructura de la red objetivo.

Una vez se han realizado estas fases, disponemos de mucha información para proceder **a su análisis.** En esta información se pueden **encontrar vulnerabilidades**. Una vez detectadas, se **identifican los posibles vectores de acceso**, y se planifican los **métodos de ataque con mayor viabilidad y efectividad**.

En resumen, se debe disponer de la **certeza de que el sistema es vulnerable**, para que, una vez tengamos el exploit o payload, podamos lanzar el código que nos permita el control sobre el sistema.

## 3.2. Auditoria WIFI o Auditoria de Seguridad de Red Inalámbrica

**Objetivo**

Su objetivo es determinar el nivel de seguridad y confidencialidad que proporcionan las configuraciones de dicha red. Una de las cosas que se suelen encontrar es que se suelen implementar redes de invitados en las empresas, y no se tiene en cuenta todo el impacto que puede tener si un empleado no técnico utiliza esta red para su labor. También pueden encontrarse cifrados no óptimos o configuraciones erróneas.

**Como se realiza**

Primero se realiza una **fase de reconocimiento del entorno y descubrimiento de la infraestructura**. También se visualizan los tipos de cifrados, el número de puntos de acceso de la red, los canales por los que emiten, numero de clientes conectados, etc.

Posteriormente se emplean **técnicas de análisis de vulnerabilidades** sobre el router, técnicas de suplantación de identidad, envenenamiento de la red, y, por ultimo, técnicas de ataques a contraseñas.

## 3.3. Auditoria de código fuente

**Objetivo**

Se realiza sobre una aplicación, herramienta o programa, usando ingeniería inversa para detectar la existencia de errores, bugs, backdoors, etc.

La ingeniería inversa es una actividad mediante la que se intenta descubrir como funciona un programa de cuyo código fuente no se dispone, hasta el punto de poder modificar ese código o generar código propio que cumpla las mismas funciones.

**Usos**

Este tipo de auditoria se puede usar, por ejemplo, para ver si un producto infringe alguna patente o, para desarrollar productos que sean compatibles con otros, sin conocer detalles de desarrollo de estos últimos. Una aplicación practica es el desarrollo de keygens, reparación de productos, etc.

**Beneficios**

Entre los beneficios que alberga este tipo de auditorias, estan la comprensión del software, generar alternativas de procesos, detectar posibles cambios que produzcan efectos no deseados, facilitar la reutilización, etc.

## 3.4. Auditoria Web

**Objetivo**

Se engloba dentro de las auditorias externas, pero tiene sus matizes, por lo que se le ha dedicado un apartado diferente.

Su objetivo es conseguir **información** **del estado de seguridad de la aplicación web**, poniendo a prueba el estado de sus bareras de seguridad. Así, intentamos descubrir todas las vulnerabilidades y fallos de seguridad posibles.

El alcance de estas auditorias se limitan a la pagina o aplicación web de la organización, **no evaluándose los servidores que la alojan, servicios expuestos, etc.**

**Como se realiza**

Primero se **recolecta información** donde se pretende descubrir toda la estructura interna de la aplicación, y se revisa el código fuente para detectar posibles fallos que impliquen una fuga de información.

Después, se realizan **dos fases de pruebas de seguridad**. La primera es una **fase pasiva**, donde se observa el funcionamiento de la aplicación y se ponen a prueba todas sus funcionalidades, esto se hace para entender a fondo cómo funciona la aplicacion. La segunda es una **fase de pruebas de seguridad**, donde se ejecutan pruebas propuestas, según los resultados obtenidos en la fase anterior. algunas de estas pruebas pueden ser la SQL Inyection, métodos de cifrado débil, o validación incorrecta de parámetros.

## 3.5. Auditoria de dispositivos móviles

**Objetivo**

Hay que tener en cuenta que los dispositivos móviles, como smartphones o portátiles, tienen una gran cantidad de información personal, y que si se accede a ellos se podría incluso suplantar la identidad del dueño. Es por esto que se debe proteger la información que se almacena en estos.

El objetivo de este tipo de auditorías es la de evaluar el nivel de riesgo en la seguridad de los dispositivos móviles de la organización, los cuales son un medio para que un atacante pueda acceder a esta.

**Como se realiza**

Estas auditorias disponen de una **fase de verificación de rooteo** (Ver si se tienen permisos de administrador) y otra de **recolección de información** en la cual se recoje toda la información posible almacenada en el dispositivo.

Posteriormente se realiza la **fase de escaneo** para comprobar fallos de configuraciones de seguridad, servicios abiertos, etc.

Por ultimo, se realizan las **fases de exploración de vectores de ataque** y la de **análisis de aplicaciones sospechosas** utilizando ingeniería inversa.

**Beneficios**

Este tipo de auditorías nos proporcionan información sobre el estado de seguridad de los dispositivos móviles de la organización.

## 3.6. Ejercicio de Red Team

**Objetivo**

Este ejercicio consiste en la **simulación de un ataque dirigido** o **ATP** (Advanced Persisted Threat) sobre una determinada organización, simulando que somos un atacante real. Por eso, se usan todas las técnicas (tanto licitas como ilicitas) para que pueda ser todo lo cercano a un ataque real, por lo que se necesitara un permiso explicito por la empresa.

Al contrario que en el resto de las auditorias, **el objetivo no es identificar vulnerabilidades**, sino **lograr el acceso a la organización**, comprometer sus principales activos y demostrar cual seria su nivel de impacto si