***Imagen que contiene Logotipo

Descripción generada automáticamente***

Alejandro Ortega Martínez

Grado en Ingeniería Informática

30/4/2021

Trabajo 4

Auditorias Informáticas

Seguridad Informática

Contenido

[1. Introducción 3](#_Toc70718239)

[1.1. Definición y conceptos 3](#_Toc70718240)

[1.2. Peritaje Informático 4](#_Toc70718241)

[2. Pasos para hacer una auditoría informática 5](#_Toc70718242)

[2.1. Análisis 5](#_Toc70718243)

[2.2. Planificación 5](#_Toc70718244)

[2.3. Determinación de riesgos e incidencias 6](#_Toc70718245)

[2.4 Ejecución 6](#_Toc70718246)

[3. Tipos de auditorías informáticas 7](#_Toc70718247)

[3.1. Auditoría Externa o Perimetral 7](#_Toc70718248)

[3.2. Auditoria WIFI o Auditoria de Seguridad de Red Inalámbrica 8](#_Toc70718249)

[3.3. Auditoría Interna 9](#_Toc70718250)

[3.3. Auditoria de código fuente 11](#_Toc70718251)

[3.4. Auditoria Web 12](#_Toc70718252)

[3.5. Auditoria de dispositivos móviles 13](#_Toc70718253)

[3.6. Ejercicio de Red Team 14](#_Toc70718254)

[3.7. Auditoria de Sistemas de Control DCS y SCADA 15](#_Toc70718255)

[3.8. Auditoria de SCI e infraestructuras criticas 16](#_Toc70718256)

[4.Tipos de Certificados de auditor informático 18](#_Toc70718257)

[4.1. SSCP 18](#_Toc70718258)

[4.2. CRISC 18](#_Toc70718259)

[4.3. CISA 18](#_Toc70718260)

[4.4. CISA.CISM 18](#_Toc70718261)

[4.5. CISSP 19](#_Toc70718262)

[4.6. CompTIA Security+ 19](#_Toc70718263)

[5. Importancia de las auditorias: Alcance de los ataques 19](#_Toc70718264)

[5.1. Solarwind 20](#_Toc70718265)

[5.2. Robo de datos en Adobe 20](#_Toc70718266)

[6. Conclusión 22](#_Toc70718267)

[7. Bibliografía 23](#_Toc70718268)

# 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 (más adelante concretaremos todos los tipos de auditorías):

* **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 prácticas 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 auditorías 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 auditorías alcanzan a elementos tipo servidores web, extranet, proxis, intranet, firewalls, 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.

**Beneficio**

Gracias a este tipo de auditoría informática se dispone de una visión global de los vectores de acceso, las configuraciones erróneas y las vulnerabilidades existentes en el perímetro.

## 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, número 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 último, técnicas de ataques a contraseñas.

**Beneficios**

Gracias a estas auditorias, podemos saber que tan seguras son nuestras redes WLAN.

## 3.3. Auditoría Interna

**Objetivo**

Esta auditoria tiene como objetivo ver cuanta información sensible se puede conseguir de la empresa desde dentro de esta, poniendo a prueba los protocolos de autenticación, servicios de la plataforma que utilice la organización, etc.

En este tipo de auditoria se intenta acceder a todo lo que se pueda desde dentro de la organización (servidores, dispositivos IoT, equipos, impresoras, etc.)

**Como se realiza**

Primero se lleva a cabo una **fase de recogida de información**, en la que se intenta determinar como funciona por completo la red y sus hosts.

Después se llevan a cabo la fase de **enumeración**, de la que salimos con una gran cantidad de información recopilada, con la cual realizaremos un **modelo**.

Tras analizar este modelo, se procederán con **técnicas mas específicas**, como pueden ser análisis de las redes VLAN, intentar ataques Man in The middle, escalado de privilegios, etc.

**Beneficios**

La finalidad de esto es corregir y subsanar estas brechas de seguridad, las cuales podrían ser utilizadas por un atacante interno de la empresa de la misma forma que lo ha hecho el auditor para poder acceder a los distintos segmentos de red y escalar privilegios hasta conseguir su propósito.

## 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 cómo 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 práctica es el desarrollo de keygens, reparación de productos, etc.

**Beneficios**

Entre los beneficios que alberga este tipo de auditorías, están 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 auditorías externas, pero tiene sus matices, 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 barreras de seguridad. Así, intentamos descubrir todas las vulnerabilidades y fallos de seguridad posibles.

El alcance de estas auditorias se limita a la página 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 aplicación. 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 por lo 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 recoge 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 último, 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 ilícitas) 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 sería su nivel de impacto si se produjera un ataque informático, así como su capacidad de detección y respuesta frente a estos.

**Como se realiza**

Este es el tipo de auditoria mas personalizada, ya que depende por completo del tipo de organización que lo contrata, por lo que cada auditoria de red Team es única, dependiendo a lo que se quiera enfocar (por ejemplo, un banco, una empresa, etc).

**Beneficios**

Gracias a este tipo de auditorías, se pueden identificar vectores de ataques críticos, y evaluar nuestra exposición y riesgo, para luego poder prevenir los ataques y asegurar las vulnerabilidades y debilidades.

## 3.7. Auditoria de Sistemas de Control DCS y SCADA

Estos sistemas con sistemas de monitorización y control que se usan en ámbitos industriales, con los cuales se monitorizan los equipos y procesos.

El **sistema SCADA** (Adquisición de Datos y Control de Supervisión) recoge los datos de varios sensores y de los equipos de vigilancia en una fabrica o complejo industrial y los envía a un ordenador central para su procesamiento.

El **sistema DCS** (Sistema de Control Distribuido) es similar al anterior, con la diferencia de que los datos no se envían a un ordenador central donde se controla todo, sino que el control esta distribuido por todo el complejo

**Objetivo**

Con esta auditoria conseguimos evaluar el estado de los sistemas de control anteriormente mencionados. Por ejemplo, podríamos evaluar in sistema de transmisión y distribución eléctrica, distribución de gas y petróleo, etc.

**Como se realiza**

Primero se realiza una **fase de reconocimiento** del sistema, donde se estudian características como su funcionamiento o configuración.

Después se **identifican las posibles vulnerabilidades** y vectores de ataque, por las cuales se podría acceder al sistema.

Por ultimola **fase de explotación** solo se realizará por petición explicita del cliente, debido a que los sistemas con los que se esta trabajando son críticos, y un paso en falso podría tener graves consecuencias.

**Beneficios**

Este tipo de auditoria tiene como beneficio el comprobar la seguridad critica de nuestra fabrica, ya que estos sistemas sean vulnerables puede acarrar consecuencias devastadoras.

## 3.8. Auditoria de SCI e infraestructuras criticas

**Objetivo**

Entendemos por **infraestructuras criticas** aquellas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales, es decir, los servicios necesarios para el mantenimiento de las funciones sociales básicas y el correcto funcionamiento de las infraestructuras estratégicas.

Dado que son sistemas indispensables, es necesario auditarlos para prevenir posibles ataques informáticos.

**Como se realiza**

Primero se realiza una **fase de recolección** donde, como es habitual, se obtiene toda la información posible de los sistemas y de su red.

Posteriormente viene la **fase de detección de vulnerabilidades**, que es semejante a la detección de vulnerabilidades de las anteriores auditorias.

Por último, al igual que las auditorias de los sistemas de control, la **fase de explotación** solo se realizará con permiso explicito del cliente, puesto que estamos trabajando sobre infraestructuras críticas.

**Beneficios**

Estas auditorias proporcionan información veraz y fiable del estado de seguridad de los sistemas de control industrial, para posteriormente poder implantar medidas de protección y crear planes de contingencia y continuidad.

Nota: Toda la información, así como las imágenes, han sido tomadas de (HackBySecurity, s.f.) y las correspondientes subpáginas.

# 4.Tipos de Certificados de auditor informático

En este apartado veremos los principales certificados necesarios para ser auditor informático (kyocera, s.f.).

## 4.1. SSCP

**System Security Certified Practitioner**. Es una certificación ofrecida por el ISC (Consorcio Internacional de Certificación de Sistemas de Información de Seguridad) y certifica la capacidad del profesional que la posee para administrar e implementar la infraestructura de la empresa, y alinearla con las políticas de seguridad que permiten garantizar la confidencialidad de los datos.

## 4.2. CRISC

**Certified in Risk and Information System Control.** Es una certificación en sistemas informáticos gestionada por la Information System Audit and Control Association (ISACA). Los profesionales que la obtienen pueden identificar evaluar y preparar respuestas a diferentes riesgos de seguridad.

## 4.3. CISA

**Certified Information Systems Auditor.** Esta certificación en seguridad informática está destinada a quienes realizan auditorías, controles y evaluaciones de los sistemas de TI y también es gestionada por ISACA.

## 4.4. CISA.CISM

**Certified Information Security Manager.** Quienes obtienen esta certificación, además de ser competentes en temas de seguridad, demuestran ser capaces de relacionar la auditoria con el objetivo de la empresa, y son capaces de desarrollar un plan de contingencia.

## 4.5. CISSP

**Certified Information System Security Professional.** En este caso, se trata de una certificación en seguridad informática ofrecida por ISC. Es una certificación ideal para quienes ya tienen conocimientos amplios, tanto técnicos como de gestión, así como experiencia. Es una certificación orientada a diseñar sus propios programas de seguridad.

## 4.6. CompTIA Security+

Se trata de una certificación en seguridad informática confiable a nivel global que cubre los principios esenciales para la seguridad de la red y la gestión de riesgos. Quien posee esta certificación constata sus conocimientos para proteger y asegurar una red contra hackers.

# 5. Importancia de las auditorias: Alcance de los ataques

En este punto veremos ejemplo de ataques sufridos por grandes compañías, para **comprobar la importancia de las auditorias informáticas**, y lo que estas pueden llegar a evitar, gracias a conseguir mejorar la seguridad.

Se relacionarán, diferentes tipos de ataques con las auditorias vistas anteriormente, para ver a cuáles se podría haber recurrido para evitar el problema, realizando un ejercicio de opinión, y demostración de comprensión de las auditorias.

## 5.1. Solarwind

A principios de 2020, unos hacker consiguieron entrar en la empresa estadounidense SolarWind, y añadieron código malicioso en uno de sus productos, llamado Orion, el cual usaban muchas compañías para gestionar sus redes. Según SolarWind, hasta 33.000 empresas hacen uso de este software.

En una de las actualizaciones que solarWind envió a sus clientes, estaba este código embebido. Los clientes, sin sospechar en absoluto, instalaron la actualización, creyendo que únicamente corregiría fallos o añadiría nuevas funcionalidades. Sin embargo, este código malicioso consiguió crear backdoors en todas las empresas atacadas (más de 18.000), haciéndolas vulnerables a robos masivos de información.

(Business Insider, 2020)

**Auditorias que podrían haberlo evitado**

En este caso, bajo mi punto de vista, se podría haber realizado una auditoria de código fuente, para ver que la actualización funcionaba como debería, y no tenía ningún tipo de código malicioso dentro.

Compañías como esta, de las que depende una gran cantidad de empresas, deberían hacer auditorias informáticas muy a menudo, sobre todo si se dedican a la distribución de productos software como es el caso, y sería recomendable que, aunque no sea contratando auditorías externas, se realizara una pequeña auditoria de código a cada actualización que se secara.

## 5.2. Robo de datos en Adobe

En 2013, un grupo de hacker consiguió entrar en las bases de datos de la compañía Adobe, robando la información de más de 2.9 millones de clientes. Esta información comprendía desde nombres de usuarios y contraseñas, hasta información de sus tarjetas de crédito.

Además, también se robó múltiples códigos fuente de productos adobe, por lo que no solo la compañía comprometió datos de sus clientes, sino que también perdió productos propios. (Poeter, s.f.)

**Auditorias que podrían haberlo evitado**

Una auditoria muy practica hubiera sido un ejercicio de Red Team, para ver hasta qué punto los sistemas de Adobe eran seguros. De todas formas, para que una auditoria de estas sea útil, el equipo auditor tiene que ser “mejor hacker” que el cibercriminal.

Otro tipo de auditoria que hubiera sido útil seria la externa o perimetral, a ver hasta qué punto era factible entrar a la empresa.

# 6. Conclusión

A lo largo de este trabajo he indagado en las auditorias informáticas, entendiendo bien que son, como se realizan, y los tipos que hay.

Después de tener estos conceptos claros, he entrado un poco por encima a ver los tipos de certificaciones que hay en este ámbito, ya que, por lo que he investigado, muchas empresas no te piden solo tener un título, sino también una certificación que te avale.

Por último, he intentado poner los conocimientos adquiridos a lo largo de la realización del trabajo en práctica, estudiando dos casos de ataques informáticos a empresas, e intentando relacionarlos con que tipo de auditorías podría haberlos mitigado de haberse realizado, y por qué.

En resumen, me ha parecido bastante interesante el realizar este trabajo, ya que es un tema que en un principio me parecía curioso, pero al ver toda la variedad de auditorias que hay, y lo interesantes que me han resultado, me ha despertado mucho mas la curiosidad sobre este tema, incluso llegando a plantearme el orientar mi carrera a este ámbito (a ser posible en auditorias Red Team).

# 7. Bibliografía

Business Insider. (2020). *businessinsider*. Obtenido de https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

FCEIA. (s.f.). Obtenido de https://www.fceia.unr.edu.ar/asist/intro-aa-t.pdf

HackBySecurity. (s.f.). *HackBySecurity*. Obtenido de https://www.hackbysecurity.com/servicios-empresas/auditoria-informatica

Juliá, S. (s.f.). *gadae*. Obtenido de https://www.gadae.com/blog/guia-para-hacer-una-auditoria-informatica-en-tu-empresa/

kyocera. (s.f.). *kyocera*. Obtenido de https://www.kyoceradocumentsolutions.es/es/smarter-workspaces/business-challenges/paperless/certificacion-seguridad-informatica.html

Poeter, D. (s.f.). *pcmag*. Obtenido de https://www.pcmag.com/news/adobe-hacked-data-for-millions-of-customers-stolen

Wikipedia. (s.f.). *Wikipedia*. Obtenido de https://es.wikipedia.org/wiki/Auditor%C3%ADa

Wikipedia. (s.f.). *Wikipedia*. Obtenido de https://es.wikipedia.org/wiki/Auditor%C3%ADa\_inform%C3%A1tica