T1. CRITERIOS COMUNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

Apartados del BOE

- Código deontológico de la función de auditoría
- Relación de los distintos tipos de auditoría en el marco de los sistemas de información
- Criterios a seguir para la composición del equipo auditor
- Tipos de pruebas a realizar en el marco de auditoría, pruebas sustantivas y pruebas de cumplimiento
- Tipos de muestreo a aplicar durante el proceso de auditoría
- Utilización de herramientas tipo CAAT (Computer Assited Audit Tools)
- Explicación de los requerimientos que deben cumplir los hallazgos de auditoría
- Aplicación de los criterios comunes para categorizar los hallazgos como observaciones o no conformidades
- Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

Certificados de Auditoría

- La regulación de las mejores prácticas de Auditoría en Informática:
  - ISACA → Institute of System Audit and Association
  - IIA → Institute of Internal Auditors

- Institute of System Audit and Association, ISACA
  - Actualmente, los miembros de ISACA –más de **28.000 en todo el mundo**– se caracterizan por su diversidad ya que están presentes en más de **100 países** y cubren una variedad de puestos profesionales relacionados con TI, como son **los Auditores de SI, Consultores, Educadores, Profesionales de Seguridad de SI, Reguladores, Directores Ejecutivos de Información y Auditores Internos**, por mencionar sólo algunos.
  - »En las tres décadas transcurridas desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales de **gobernación, control, seguridad** y **auditoría de información.**
  - » Su certificación **Certified Information Systems Auditor** –Auditor Certificado de Sistemas de Información– **CISA**, es reconocida en forma global y ha sido obtenida por más de 30.000 profesionales.
  - » Su nueva certificación **Certified Information Security Manager** –Gerente Certificado de Seguridad de Información– **CISM**, se concentra exclusivamente en el sector de gerencia de seguridad de la información. Publica un periódico técnico líder en el campo de control de la información, el Information Systems Control Journal –Periódico de Control de Sistemas de Información

- **CISA**
  - La Asociación de Auditoría y Control de Sistemas de Información (ISACA) provee una Certificación en Auditor en Sistemas de Información (CISA), por medio de un examen anual que realiza el Instituto a los candidatos, el cual cubre el conocimiento de actividades requeridas para la función de Auditoría en TI, para lo cual presenta un Manual de Información Técnica para la preparación de los candidatos.
  - La certificación de CISA (Certified Information Systems Auditor) es otorgada por la (ISACA), desde 1978 y es considerada en la actualidad como un reconocimiento de que se cuenta con los conocimientos teóricos y prácticos necesarios para desempeñarse como Auditor de Sistemas siguiendo los estándares y directrices definidos para una mejor preparación.
  - La designación de CISA, se considera hoy en día, una ventaja competitiva y resulta de beneficio no solo para las organizaciones que deben cumplir con requerimientos de certificación profesional de sus colaboradores, sino para las personas que buscan un desarrollo profesional y la obtención de certificaciones que ofrecen oportunidades a nivel internacional.

- **CISM**
  - También ISACA provee la Certificación para la Administración de la Seguridad de la Información del cual intenta garantizar que existan administradores de seguridad de TI que tengan los conocimientos necesarios para reducir el riesgo y proteger a la organización.
  - La certificación CISM está diseñada para dar la certeza de que los individuos certificados tengan los conocimientos para ofrecer una eficaz administración y consultoría de seguridad.
  - Esta orientada a profesionales que administran la seguridad de la información en una organización y tienen el conocimiento y la experiencia para montar, implementar y dirigir una estructura de seguridad para administrar el riesgo con eficacia y tienen la responsabilidad de entender la relación entre las necesidades comerciales y la seguridad de TI.
  - Para obtener esta certificación, los profesionales deben aprobar el examen, adherirse a un código ético y presentar pruebas verificadas de que tienen una experiencia laboral de cinco años en seguridad de la información.
  - Según la ISACA, menciona los principales objetivos de esta certificación como a continuación se mencionan:
    - Desarrollar modelos de riesgos que midan mejor los riesgos de seguridad y los potenciales impactos sobre el negocio.
    - Aumentar la calidad de la gestión ejecutiva de las nuevas amenazas y las ya existentes, a través de la convergencia entre la organización y las medidas de seguridad
    - Impulsar la unificación del enlace entre la seguridad de las organizaciones y los organismos gubernamentales y legislativos, informándoles de las mejores prácticas en seguridad.
    - Continuar definiendo la cualificación, certificación y formación de los Directores de Seguridad -Chief Security Officer (CSO)/Chief Information Security Officer (CISO)- y otros puestos.

- Institute of Internal Auditors, IIA
  - El Institute of Internal Auditors (IIA) –organización profesional con sede en Estados Unidos, con más de 70.000 miembros en todo el mundo y 60 años de existencia– anualmente organiza su Conferencia Internacional, la que habitualmente congrega a más de un millar de auditores de todos los continentes
  - El IIA es reconocido mundialmente como una autoridad, pues es el principal educador y el líder en la certificación, la investigación y la guía tecnológica en la profesión de la audítoría interna.
  - El desarrollo de los Estándares de la Práctica Profesional de Auditoría Interna, así como las **Certificaciones de Auditor Interno (CIA**), de **Auto evaluación de Control (CCSA)** y de **Auditor Interno Gubernamental (CGAP),** y su participación en el diseño del **Enfoque COSO** son sólo algunos de los hitos que han transformado al IIA en la entidad internacional señera en la profesión.

Código deontológico

- Un código deontológico es un **documento** que recoge un conjunto más o menos amplio de criterios, apoyados en la deontología con normas y valores que formulan y asumen quienes llevan a cabo correctamente una **actividad profesional**.
- Los códigos deontológicos se ocupan de los **aspectos éticos** del **ejercicio de la profesión** que regulan.

- El código ético de ISACA:
  - https://www.isaca.org/About-ISACA/History/Espanol/Documents/ISACA-Code-of-Ethics-Spanish.pdf

Tipos de auditoría de SEGURIDAD TI

1. Test de Intrusión
   - Se centra en evaluar la seguridad de los sistemas de protección perimetral de una empresa así como los diferentes sistemas que están accesibles desde Internet intentando penetrar en ellos y de esta forma alcanzar zonas de la red de una empresa como puede ser la red interna o la DMZ.
2. Auditoría de DMZ
   - El objetivo es evaluar la seguridad de la zona desmilitarizada (red donde una empresa sitúa los servidores que desea hacer accesibles desde Internet) y cómo la inseguridad en la DMZ puede llegar a repercutir en la seguridad de la red interna de la empresa.
3. Auditoría de Red Interna
   - Su objetivo es evaluar la seguridad de la red interna de una empresa ante la posibilidad de recibir ataques por parte de un hacker que haya conseguido alcanzar la intranet o ataques provenientes del personal interno a la empresa.

4. Auditoría de Aplicación
   - Servicio que analiza de forma específica las aplicaciones, incluidas en su sitio web de forma independiente y exhaustiva.
5. Auditoría Técnica
   - En estas auditorías se llevan a cabo revisiones técnicas exhaustivas de los sistemas, convirtiendo este análisis en un estudio integral y profundo a todos los niveles de los SI.
6. Auditoría de Seguridad Física
   - Se apoya tanto en el estándar TIA-942:2005 e ISO 27002 como en la regulación legal vigente y consiste en una revisión de las instalaciones de los CPDs vista desde el punto de vista de infraestructura integral.
7. Auditoría de VPNs
   - Está diseñada para cualquier empresa que quiera detectar las deficiencias de seguridad que puedan estar implicando sus accesos remotos para la seguridad de su red.
8. Auditoría Avanzada de FW
   - Evalúa de forma exhaustiva la respuesta del firewall frente a posibles ataques tanto desde el exterior como desde el interior, mediante la utilización de las mismas técnicas empleadas por los hackers.

9. Auditoría de Redes WiFi
   - Emplear en redes la tecnología inalámbrica la oportunidad de hacerlo con el menor riesgo posible.
10. Test de DoS
11. Test de Ingeniería Social
12. Análisis Forense
13. Y mas ….

Normas, Técnicas y procedimientos de Auditoría informática

- El desarrollo de una auditoría se basa en la aplicación de normas, técnicas y procedimientos de auditoría.
- Es fundamental mencionar que para el auditor en informática conocer los productos de software que han sido creados para apoyar su función aparte de los componentes de la propia computadora resulta esencial, esto por razones económicas y para facilitar el manejo de la información.
- El auditor desempeña sus labores mediante la aplicación de una serie de conocimientos especializados que vienen a formar el cuerpo técnico de su actividad.

- El auditor adquiere responsabilidades, no solamente con la persona que directamente contratan sus servicios, sino con un número de personas desconocidas para él que van a utilizar el resultado de su trabajo como base para tomar decisiones.

  - La auditoría no es una actividad meramente mecánica, que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo son de carácter indudable.

  - La auditoría requiere el ejercicio de un juicio profesional, sólido maduro, para juzgar los procedimientos que deben seguirse y estimar los resultados obtenidos

- **NORMAS**
  - Las normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña ya la información que rinde como resultado de este trabajo.
  - Las normas de auditoría se clasifican en:
    - Normas personales.
    - Normas de ejecución del trabajo.
    - Normas de información.

- Normas personales
  - son cualidades que el auditor debe tener para ejercer sin dolo una auditoría, basados en un sus conocimientos profesionales así como en un entrenamiento técnico, que le permita ser imparcial a la hora de dar sus sugerencias.
- Normas de ejecución del trabajo
  - son la planificación de los métodos y procedimientos, tanto como papeles de trabajo a aplicar dentro de la auditoría.
- Normas de información
  - son el resultado que el auditor debe entregar a los interesados para que se den cuenta de su trabajo, también es conocido como informe o dictamen.

- **TÉCNICAS**
  - Se define a las técnicas de auditoría como "los métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que fundamente sus opiniones y conclusiones, su empleo se basa en su criterio o juicio, según las circunstancias".
  - Al aplicar su conocimiento y experiencia el auditor, podrá conocer los datos de la empresa u organización a ser auditada, que pudieran necesitar una mayor atención.
  - Las técnicas procedimientos están estrechamente relacionados, si las técnicas no son elegidas adecuadamente, la auditoría no alcanzará las normas aceptadas de ejecución, por lo cual las técnicas así como los procedimientos de auditoría tienen una gran importancia para el auditor.
  - Según el IMCP en su libro *Normas y procedimientos de auditoría* las técnicas se clasifican generalmente con base en la acción que se va a efectuar, estas acciones pueden ser oculares, verbales, por escrito, por revisión del contenido de documentos y por examen físico.

- Siguiendo esta clasificación las técnicas de auditoría se agrupan específicamente de la siguiente manera:
  - Estudio General
  - Análisis
  - Inspección
  - Confirmación
  - Investigación
  - Declaración
  - Certificación
  - Observación
  - Cálculo

- **PROCEDIMIENTOS**
  - Al conjunto de técnicas de investigación aplicables a un grupo de hechos o circunstancias que nos sirven para fundamentar la opinión del auditor dentro de una auditoría, se les dan el nombre de procedimientos de auditoría en informática.
  - La combinación de dos o más procedimientos, derivan en programas de auditoría, y al conjunto de programas de auditoría se le denomina plan de auditoría, el cual servirá al auditor para llevar una estrategia y organización de la propia auditoría.
  - El auditor no puede obtener el conocimiento que necesita para sustentar su opinión en una sola prueba, es necesario examinar los hechos, mediante varias técnicas de aplicación simultánea.
  - En General los procedimientos de auditoría permiten:
    - Obtener conocimientos del control interno.
    - Analizar loas características del control interno.
    - Verificar los resultados de control interno.
    - Fundamentar conclusiones de la auditoría.
  - Por esta razón el auditor deberá aplicar su experiencia y decidir cuál técnica o procedimiento de auditoría serán los mas indicados par obtener su opinión.

Utilización de herramientas tipo CAAT Computer Assited Audit Tools

- Las técnicas de auditoría asistidas por computadora son de suma importancia para el auditor de TI cuando realiza una auditoría. CAAT (Computer Audit Assisted Techniques) incluyen distintos tipos de herramientas y de técnicas, las que más se utilizan son los software de auditoría generalizado, software utilitario, los datos de prueba y sistemas expertos de auditoría. Las CAAT se pueden utilizar para realizar varios procedimientos de auditoría incluyendo:
  - Prueba de los detalles de operaciones y saldos.
  - Procedimientos de revisión analíticos.
  - Pruebas de cumplimiento de los controles generales de sistemas de información.
  - Pruebas de cumplimiento de los controles de aplicación.

- Ejemplo de herramientas CAAT
  - IDEA
  - ACL
  - Auto Auidit
  - Audicontrol APL (AUDISIS)
  - AUIDITMASTER
  - DELOS

Metodologías

- Control Objectives for Information and related Technology, COBIT
- Information Technology Infraestructure Library, ITIL
- BS 7799 e ISO 17799
- British Standard BS 15000
- Committee of Sponsoring Organizations, COSO
- Metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT
- Sarbanes-Oxley, SOX