TEMA 038. AUDITORÍA INFORMÁTICA. CONCEPTO Y CONTENIDOS. ADMINISTRACIÓN, PLANEAMIENTO, ORGANIZACIÓN, INFRAESTRUCTURA TÉCNICA Y PRÁCTICAS OPERATIVAS.

Actualizado a 20/01/2022

TEMA 038. AUDITORÍA INFORMÁTICA. CONCEPTO Y CONTENIDOS. ADMINISTRACIÓN, PLANEAMIENTO, ORGANIZACIÓN, INFRAESTRUCTURA TÉCNICA Y PRÁCTICAS OPERATIVAS.

1. Conceptos y Contenidos

La Auditoría de los Sistemas de Información debe entenderse como una herramienta más que ayudará a las organizaciones a supervisar su sistema de control, a gestionar sus riesgos; su objetivo es contribuir a establecer un clima de confianza en el uso de las tecnologías de la información y de las comunicaciones y a reforzar la gestión de su seguridad y calidad.

Auditoría (Ron Weber): proceso de recoger, agrupar y evaluar evidencias para determinar si un SI:

- salvaguarda los activos
- mantiene la integridad de los datos
- lleva a cabo los fines de la organización
- utiliza eficientemente los recursos

Auditar consiste principalmente en **estudiar los mecanismos de control** que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos.

En la realización de una auditoría informática el auditor puede realizar pruebas sustantivas o de cumplimiento.

Los controles deben ser: simples, revisables, adecuados y rentables

Tipos de controles: según el momento: preventivos – reactivos; por su frecuencia: continuo – esporádico - periódico; por su naturaleza: generales – de aplicación – de proceso o de continuación; otros: detectivos – correctivos; automáticos; compensatorios

Tipos de auditoría: según sujeto: interna – externa; según amplitud: total – parcial; según frecuencia: periódica – ocasional; según contenido: operativas – cumplimiento – forenses – regularidad – de economía, eficacia y eficiencia - de los sistemas de información: de dirección TI – seguridad – desarrollo y mantenimiento – explotación – contratación; otros: control de accesos, bases de datos, técnicas de sistemas, calidad de los productos, seguridad comunicaciones, gestión de la continuidad…

2. Administración

La función de control de la Administración Pública española se desarrolla en tres ámbitos: - **control político** (ejercido por el Parlamento), - **control judicial** (ejercido por los Tribunales de Justicia) y – **control administrativo** (ejercido por órganos administrativos): Tribunal de Cuentas, IAGE, Inspecciones Generales de los servicios, Inspección General del Ministerio de Hacienda y Administraciones Pública y Servicio de Auditoría interna de la Agencia Tributaria, Comisión Sectorial de Administración Electrónica, Dirección General de Gobernanza Pública realiza Informes de Evaluación de la Calidad de los Servicios, Agencia Española de Protección de Datos.

2.1. Normas y recomendaciones

- **NORMAS DEL SECTOR PÚBLICO**
  - Normas de Auditoría del Sector Público de la IGAE.
  - Resolución de 23 de junio de 2003, del Instituto de Contabilidad y Auditoría de Cuentas, por la que se publica la norma técnica de auditoría sobre “la auditoría de cuentas en entornos informatizados”.
  - Serie del Centro Criptográfico Nacional CCN-STIC
- **PROCEDIMIENTO ADMINISTRATIVO**
  - Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las AAPP

  - Real Decreto 4/2010, de 8 de enero, por el que se regula el ENS
  - Real Decreto 3/2010, de 8 de enero, por el que se regula el ENI
  - MAGERIT v3, Metodología de análisis y gestión de riesgos de los sistemas de información
- **PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**
  - Reglamento (UE) 2016/679 General de Protección de Datos
  - Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales
  - DIRECTIVA (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.
  - Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación, y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- **RECOMENDACIONES DE ORGANIZACIONES INTERNACIONALES**
  - COBIT (Control Objectives for Information and Related Technologies) de ISACA (Information Systems Audit and Control Association).
  - ITIL (Information Technology Infrastructure Library) creado por el gobierno del Reino Unido.
  - NIST (Publicaciones Especiales del Instituto Nacional de Estándares y Tecnología de EE.UU.)
  - Instituto SANS (SysAdmin, Audit, Network, Security)
- **NORMAS INTERNACIONALES**
  - ISO/IEC 27002 Código de buenas prácticas para la gestión de la seguridad de la información
  - ISO/IEC 27001 SGSI - sistemas de gestión de la seguridad de la información
  - ISO/IEC 15408 Criterios comunes de evaluación de la seguridad de las TIC
  - ISO/IEC 13335 Gestión de la seguridad de las TIC
  - ISO/IEC 18045 Metodología para la evaluación de la seguridad de los SSII

3. Planeamiento

Como proceso estratégico, el procedimiento de Auditoría se encuadraría en la pirámide documental de la organización:

- **Nivel Estratégico**: Política de Seguridad; Política de Calidad; Manual de Calidad
- **Nivel Táctico**: Plan de Seguridad; Plan de Calidad; Normas de Seguridad y Calidad; Especificaciones, estándares y guías de Seguridad y Calidad
- **Nivel operativo**: Procedimientos de Seguridad y Calidad; Instrucciones Técnicas de Seguridad y Calidad

Políticas: qué y por qué.
Normativas: Reglas generales.
Procedimientos: cómo.
Instrucciones: Detallan técnicamente

4. Organización

En un Departamento de Auditoría Interna separado, dependiente de la alta dirección y que constituye un órgano especializado de control. La AEAT aconseja que debería contar con un 0,5 a 1 % del personal de la organización. O bien en los propios centros informáticos para asegurar el funcionamiento de los sistemas de información.

ISACA – Certificaciones:

- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)

- CGEIT (Certified In the Gobernance of Enterprises IT)
- CRISC (Certified in Risk and Information Systems Control)

ISACA también establece un Código de Ética Profesional para guiar la conducta profesional y personal de los miembros de la asociación y/o portadores de las certificaciones

5. Infraestructura técnica

Existen diferentes técnicas para analizar programas la cuales ayudan al auditor en el trabajo de campo y de las cuales las más importantes se mencionan a continuación: traceo, mapeo, comparación de código y jop accounting software.
Algunas herramientas **CAAT** (Computed Audit Assisted Techniques) son: ACL, Auto Audit, AuditMaster, Delos.

6. Prácticas operativas

El proceso de auditoría consiste en los siguientes pasos:

1. **Planificación de la auditoría**:
2. **Formalización del inicio de actuación**
3. **Ejecución**, examen y evaluación de la información obtenida en la fase previa.
4. **Comunicación** de los resultados mediante informes de auditoría.
    a. Reunión de cierre.
    b. Borrador de informe.
    c. Procedimiento de tramitación con periodo de respuesta para observaciones y alegaciones.
    d. Informe definitivo (se acompaña de anexos).

    La estructura de los informes será:
    - Título, índice, introducción,
    - objetivo y alcance, metodología,
    - resultados de la actuación (criterio, condición, efecto, causa)
    - conclusiones y recomendaciones
5. **Seguimiento** de las recomendaciones y soluciones que deben ser llevadas a cabo en un período de tiempo determinado a contar tras su recepción. No suelen ser directamente ejecutivas (de obligado cumplimiento por parte del auditado). **Impacto de un hallazgo según su materialidad**.