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, y 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. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Se entiende como Evidencia cualquier información empleada por el auditor para determinar si el proceso que se está auditando cumple con los criterios y objetivos de la auditoría.

La auditoría informática debe cumplir **cinco funciones**:

1. **Velar por la eficacia y eficiencia del sistema informático**, de forma que se alcancen con el menor coste posible los objetivos que le han sido establecidos.
2. **Verificar el cumplimiento de las normas y estándares** vigentes en la organización.
3. **Verificar la calidad** de los sistemas de información y proponer mejoras en los mismos.
4. **Supervisar los mecanismos de control interno** establecidos en los centros de proceso de datos y en la organización en su conjunto para proteger los recursos informáticos humanos y materiales y para mantener la integridad de los datos.
5. **Comprobar e impulsar la seguridad** de los sistemas de información.

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

- Pruebas **sustantivas**: permiten medir el riesgo por deficiencia de los controles existentes o por su ausencia. Se utilizan para determinar si se cumplen los objetivos de salvaguarda de los activos, integridad de los datos, eficacia y eficiencia.
- Pruebas de **cumplimiento**: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

1.1. Controles

El control consiste en un proceso de observación y medida que compara sistemáticamente los objetivos con los resultados y que tiene la capacidad necesaria para regular los sistemas con la intención de que sean alcanzados los objetivos.

El control aporta confianza al garantizar que la información que la organización hace pública reúne unas características determinadas de veracidad y fiabilidad, ofreciendo una imagen fiel de sí misma.

Los controles deberían ser:

- **Simples** (no siempre es posible, en este caso, con la “mínima complejidad necesaria”) y fiables. Ej. Copia de seguridad comprimida, verificar extracción;
- **Revisables** (establecer procedimientos o fechas);
- **Adecuados**, ej. Entrada al sistema con login / password y

- **Rentables** (el coste menor que el beneficio).

Los controles pueden clasificarse atendiendo a diferentes características:

Por el momento en que actúan: preventivos – a priori ; reactivos – a posteriori; concurrente o concomitante (establecido durante la realización del proceso que se observa y mide)

Por su frecuencia: continuo ; periódico o esporádico

Por su naturaleza: **generales** (organizativos y operativos, de desarrollo y mantenimiento, de hardware, de software, de acceso, de procedimiento); de **aplicación** (controles de entrada, de proceso, de salida)

También se pueden clasificar como de **desarrollo** (comprueba que el resultado obtenido concuerda con las especificaciones iniciales), de **proceso** (asegura que la explotación se realiza con las versiones adecuadas de los programas y de los datos) y de **continuación** (determina que se evita la pérdida o corrupción de información, efectuando las salvaguardas y recuperaciones necesarias).

Además, podemos hablar de controles **Detectivos** (reportan errores), ej. Registro de intentos de acceso, análisis de logs; o **Correctivos**: facilitar la vuelta a la normalidad (ej. documentar el proceso de recuperación desde una copia de seguridad).

También existen los controles **automáticos o alarmas** que actúan ante la aparición de acontecimientos que pueden suponer un riesgo para la consecución de los objetivos.

Y por último, el **control compensatorio**: cuando su coste lo haga inabordable, cuando no esté efectivamente implantado o cuando falle su aplicación. Reducen el riesgo ante una debilidad existente

1.2. Tipos de auditoría

- **Según el sujeto que la realiza:** interna (realizada por personal de la propia entidad); externa (realizada por profesionales ajenos a la entidad)
- **Según su amplitud:** total (afecta a toda la organización); parcial
- **Según su frecuencia:** periódica; ocasional
- **Según su contenido o fines**

Otros tipos de clasificaciones:

Auditorías **operativas o de gestión**: evalúan la eficacia en la consecución de objetivos y la eficiencia en los recursos empleados para alcanzarlos.

Auditorías de **cumplimiento**: verificación de los controles internos

Auditorías **forenses**: descubrir fraudes y delitos

Auditoría de **regularidad**: orientada a verificar el cumplimiento de la normativa aplicable.

Auditoría de **economía, eficacia y eficiencia** (o triple E o VFM Value For Money audit): consiste en medir los costes de desarrollo, mantenimiento y operación de un sistema de información, incluyendo equipos y personal

Auditoría de los **sistemas de información**: examen y verificación del correcto funcionamiento y control del sistema informático de la organización. Se considera de tipo operativa:

- **Auditoría de la dirección de tecnologías de la información**: evaluar las áreas de riesgo relativas a cómo se planifican, organizan, coordinan y controlan las actividades propias del órgano con responsabilidad y competencias en TIC.
- Auditoría de la **seguridad**
- Auditoría del **equipamiento informático**: Planificación de la infraestructura tecnológica, Inventario, Mantenimiento HW, Puestos de trabajo, Redes de área local
- Auditoría de los **desarrollos y mantenimiento de los sistemas de información**: Las acciones de verificación comprenderán todo el ciclo de vida del desarrollo de un proyecto, es decir desde que se toma la decisión de realizar un desarrollo hasta la entrega del mismo.
- Auditoría de la **explotación de los sistemas de información**: asegurar la correcta y segura operación de los recursos para el tratamiento de la información.

- Auditoría de la **contratación de bienes y servicios TIC**: se verificarán las políticas y los procedimientos de adquisición establecidos por la Organización.
- **Otros tipos de auditorías** de sistemas de información: Control de accesos, Bases de datos, Técnica de sistemas, Calidad de los productos desarrollados, Seguridad en las comunicaciones, Gestión de la continuidad del servicio informático, Acreditación de servicio de confianza.

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), para ejercer este último control nos encontramos con los siguientes órganos especializados:

- **Tribunal de Cuentas** (órgano supremo fiscalizador de las cuentas y de la gestión económica del Estado y del sector público), controla la actividad económica y presupuestaria. Es un órgano externo, de carácter administrativo que también tiene atribuidas funciones de alcance contable, y cuyo destinatario principal es el Parlamento.
- **Intervención General de la Administración del Estado** (IGAE), es un órgano interno de la Administración que examina la gestión del gasto público por parte de los organismos gestores. Desde 1984 debe elaborar anualmente un Plan de Auditorías. Las Normas Técnicas de Auditoría Pública constituyen el núcleo de sus procedimientos de trabajo, clasifican sus actuaciones en dos grandes grupos: - auditorías de regularidad y auditorías operativas. La Ley General Presupuestaria de 47/2003, de 26 de noviembre, refrenda el papel de la IGAE en el control interno, delimitando sus función interventora, de control financiero permanente y de auditoría pública.
- **Inspecciones Generales de los Servicios** especializados en el control interno y en la evaluación de los servicios de cada uno de los Ministerios y de sus organismos públicos dependientes. Su función es supervisar el funcionamiento de los órganos administrativos, lo que incluye el seguimiento de objetivos y el análisis de riesgos y debilidades.
- Otros:
  - Inspección General del Ministerio de Hacienda y Administraciones Pública y Servicio de Auditoría interna de la Agencia Tributaria
  - Comisión Sectorial de Administración Electrónica en materia de administración electrónica
  - Dirección General de Gobernanza Pública realiza Informes de Evaluación de la Calidad de los Servicios
  - La 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
    - 000 – Políticas
    - 100 – Procedimientos
    - 200 – Normas
    - 300 – Instrucciones Técnicas
    - 400 – Guías generales
    - 500 – Entornos Windows

  - 600 – Otros entornos
  - 800 – Desarrollo del ENS
- **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 como estrategia para el proceso de gestión del riesgo (identificar, evaluar, responder, monitorizar y reportar)
- **PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**
  - Reglamento (UE) 2016/79 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), institución americana, dependiente del IT Governance Institute que nació a finales de 1995, es una definición de estándares y conducta profesional para la gestión y control de los Sistemas de Información.
  - ITIL (Information Technology Infrastructure Library) creado por el gobierno del Reino Unido, resume las mejores prácticas de implementación en la gestión de los procesos de Tecnologías de la Información.
  - 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

En el **ciclo de gestión de control la auditoría** tiene la misión de analizar la implementación de los controles y corregir la gestión con la propuesta de mejoras. En este contexto el proceso de la Auditoría se considera como unos de los procesos estratégicos en la organización, tal y como considera cualquier buena práctica (ITIL, CobiT) o estándar de gestión (ISO 9000 Gestión de Calidad). 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: Declaración de intenciones de alto nivel, refleja los objetivos de la organización (**qué y por qué**), deben estar debidamente documentadas y establecer criterios de medición de resultados. Deben ser aprobadas por la alta dirección de la organización, perdurables en el tiempo (mantenerse al margen de la tecnología empleada) y conocidas por toda la organización.
Normativas: **Reglas generales** que desarrollan las políticas de alto nivel, de obligada aplicación para las personas de la organización. Serán definidas por el órgano de dirección responsable de su supervisión. Se ajustarán al despliegue tecnológico, y serán conocidas por los usuarios de los sistemas.
Procedimientos: Señalan el marco de actuación en los distintos campos de las TIC para resolver situaciones concretas (**cómo**). Deben ser desarrollados por la unidad responsable de su implementación y estar ajustados a normas, documentados y con contenidos mínimos ajustados a la materia, deben mantenerse actualizados y han de ser conocidos por los encargados de ejecutarlos y por los usuarios.
Instrucciones: **Detallan técnicamente** la forma precisa de actuar para implementar un procedimiento, señalando los pasos de obligado cumplimiento que deben seguirse. Deben estar documentadas y ser conocidas por los técnicos responsables.

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.
Las funciones desempeñadas por este departamento suelen ser:

- Establecer, mantener y mejorar controles efectivos (evaluando su eficacia y eficiencia).
- Contribuir al establecimiento, mantenimiento y mejora del sistema de gestión de riesgos.
- Velar por el mantenimiento de la seguridad en la organización (sugiriendo mejoras).
- Pueden dedicarse también a cuestiones relativas a la regulación de normas de conducta.
- Pueden ejercer como órgano de asesoría y consultoría al servicio de la dirección.

ISACA – Certificaciones:

- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- CGEIT (Certified In the Governance 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 las cuales ayudan al auditor en el trabajo de campo. Las más importantes se mencionan a continuación:

- **Traceo**: Indica por donde paso el programa cada vez que se ejecuta una instrucción. Imprime o muestra en la pantalla el valor de las variables, en una porción o en todo el programa.
- **Mapeo**: Característica del programa tales como tamaño en bytes, localización en memoria, fecha de última modificación, etc.
- **Comparación de código**: Involucra los códigos fuentes y códigos objetos.
- **Job Accounting Software**. Informe de Contabilidad del Sistema: Utilitario del sistema operativo que provee el medio para acumular y registrar la información necesaria para facturar a los usuarios y evaluar el uso del sistema.

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**: objetivos, alcance, procedimientos. Finaliza en un plan de trabajo o guión de auditoría con:
    a. Punto de control: objetivos de control a supervisar
    b. Directriz de auditoría: tareas a efectuar por punto de control
    c. Identificación de medios humanos y técnicos
    d. Técnica a emplear: entrevista, encuesta, observación, revisión de documentos, pruebas y verificaciones de campo, hallazgos (criterios para documentar los problemas encontrados).
    e. Calendario con los **puntos de control**
2. **Formalización del inicio de actuación** mediante notificación al responsable de la unidad auditada. Trabajo de campo y evidencias (suficientes, relevantes y competentes) y su grado de fiabilidad. Según su naturaleza las podemos clasificar en:
    a. Físicas: obtenidas mediante inspección directa u observación
    b. Documentales: obtenidas a partir de documentos (cartas, informes…)
    c. Testimoniales: obtenidas como resultado de entrevistas, cuestionarios…
    d. Analíticas: obtenidas por medio de comparaciones, cálculos…
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**:
    a. **Bajo** → descripción del hallazgo como vulnerabilidad a la que se expone el sistema.
    b. **Medio** → se refleja en el informe como posible debilidad del sistema de control.
    c. **Alto** → se identifica como una debilidad que debe compensarse o anularse con más controles, o haciendo los existentes más estrictos.

6.1. Guía CCN-STIC 802

La seguridad de los sistemas de información de una organización será **auditada en los siguientes términos, pudiendo incluir la revisión de medidas del RGPD**:

- Que la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
- Que existen procedimientos para resolución de conflictos entre dichos responsables.
- Que se han designado personas para dichos roles a la luz del principio de «separación de funciones».
- Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.

- Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

El **objetivo final** de la auditoría es sustentar la confianza que merece el sistema auditado en materia de seguridad; es decir, calibrar su capacidad para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

Los sistemas de información de categoría **BÁSICA**, o inferior, no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien éste delegue

- El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular y las evidencias que sustentan la valoración anterior.
- Los informes de autoevaluación serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

La auditoría a sistemas de categoría **MEDIA O ALTA**.

- El informe de auditoría dictaminará sobre el grado de cumplimiento del presente real decreto, identificará sus deficiencias y sugerirá las posibles medidas correctoras o complementarias que sean necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen en que se basen las conclusiones formuladas.
- Los informes de auditoría serán analizados por el responsable de seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas

El informe podrá ser favorable o desfavorable. **Si el número de "no conformidades" se pueden planificar e implementar en 1 mes, el informe será favorable con "no conformidades"**, que hay que resolver en ese plazo. Si el informe es **desfavorable**, las "no conformidades" hay que resolverlas en **6 meses.**

Esta auditoría es requerida, de forma **ordinaria**, **cada dos años** para los sistemas de categoría media y alta, según el Anexo I del RD 3/2010, y con carácter **extraordinario**, siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas

Se establece que: "En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas".

Entre la **documentación mínima** a requerir de la auditoría del cumplimiento del ENS está:

- Documentos firmados de conocimiento y aprobación de política de seguridad.
- Organigrama de los servicios o áreas afectadas, con funciones y responsabilidades.
- Identificación de responsables de la información, servicios, seguridad y sistema.
- Descripción detallada del sistema de información (software, hardware, comunicaciones, etc.)
- Categoría del sistema según el Anexo I del ENS, incluyendo criterios y valor de las dimensiones.
- La Política de Seguridad.
- La Política de Firma Electrónica y Certificados (si se emplean estas tecnologías).
- La Normativa de Seguridad.
- Descripción detallada del sistema de gestión de la seguridad y documentación que lo sustancia.
- Informes de la apreciación del riesgo, incluyendo escenarios, análisis y evaluación.
- La Declaración de Aplicabilidad.
- Decisiones adoptadas para tratar los riesgos.
- Relación de las medidas de seguridad implantadas por requisitos legales.
- Relación de registros de actividad en lo relativo a las medidas de seguridad.

- Informes de otras auditorías previas de seguridad incluidos en el alcance.
- Lista de proveedores externos cuyos servicios se ven afectados o entran dentro del alcance.
- Sistemas de métricas con referencia a las guías CCN-STIC 815 y CCN-STIC -824.