AUDITORÍA Y CERTIFICACIÓN DE SISTEMAS INFORMÁTICOS

1. Normalización, evaluación, certificación y acreditación. Marco legal
   1.1. Ley 21/1991 de Industria y Reglamentos de desarrollo.
   1.2. La normalización, la evaluación, la certificación y la acreditación. Definiciones y conceptos.
   1.3. Normalización internacional (ISO, IEC, UIT), regional (CEN, CENELEC y ETSI) y española (UNE).
   1.4. Ámbitos de normalización de las T.I. ISO/IEC JTC 1, UIT-T, ETSI. Comités técnicos de normalización. El comité CTN 320.
   1.5. Normas de iure y de facto. Ejemplos de normas de facto.
2. La auditoría y la consultoría informática.
   2.1. La auditoría. Utilidad y obligatoriedad. Auditoría y control. Objetivos de control. Tipos de auditoría. Auditoría y consultoría. El auditor. Perfil. Independencia. Ética. ISACA. COBIT de ISACA.
   2.2. Modelos de gobierno IT y seguridad desde el punto de vista del auditor. COBIT. Otros estándares, guías y certificaciones de auditoría de sistemas (CISA, CISM). Posible ejercicio con preguntas reales (CISM).
   2.3. Planificación, organización y seguimiento de una auditoría. Metodología. Estándares. Fuentes. Técnicas. Herramientas. El trabajo en equipo. Gestión del proyecto. Tipos de pruebas. Entrevistas. Alcance de evidencias. Papeles de trabajo (físicos y electrónicos).
   2.4. Elaboración del informe de auditoría. Estructura. Contenido. Uso de métricas. Revisión. Discusión. Presentación.
3. La normalización de los SGSI (ISMS). Familia 27xxx. Estudio de las normas UNE-ISO/IEC 27000, 27001, 27002.
   3.1. Normas ISO/IEC de gestión de la seguridad. Familia 27000. Normas certificables.
   3.2. Familia 27000. Normas certificables. Norma UNE-ISO/IEC 27002:2015.
   3.3. Estándares de ciberseguridad. NIST. ISO 27032. Directiva europea de ciberseguridad (NIS).
4. Auditoría de sistemas distribuidos y redes. Auditoría de ciberseguridad.
   4.1. Auditoría de infraestructuras y de instalaciones. Planes de contingencia. Continuidad del Negocio. Gestión de Crisis.
   4.2. Auditoría de sistemas distribuidos y redes: datos, soportes, bases de datos, sistemas operativos, redes (LAN, WAN, WiFi).
   4.3. Auditoría de la calidad de los sistemas informáticos y del software. Del nivel de servicio. Seguridad en el ciclo de vida del desarrollo.
   4.4. Auditoría de terceras partes.
   4.5. Peritajes. Auditoría de respuesta a incidentes de ciberseguridad. Ciberejercicios.
5. Auditoría de ficheros y sistemas sujetos a cumplimiento legal.
   5.1. La auditoría relacionada con los datos personales. Reglamento (UE) 2016/679 (GDPR). Transción desde las derogadas Ley Orgánica 15/1999 de protección de datos personales y R. D. 1920/2007. Agencia española de protección de datos.
   5.2. Auditoría relacionada con el Esquema Nacional de Seguridad. Guías del CCN.

5.3. La auditoría de medios de pago. PCI-DSS.
5.4. Peritaje informático.
5.5. Auditoría de estados financieros.

6. Certificación de sistemas y productos de T.I. Reconocimiento de certificados
   6.1. Criterios de evaluación: TCSEC, ITSEC, Norma ISO/IEC 15408 (Common Criteria).
   6.2. Metodologías de evaluación: ITSEM, Norma ISO/IEC 18045
   6.3. La regulación legal de la evaluación y la certificación en España. Orden PRE. 2740/2007. Esquema nacional de evaluación y certificación.
   6.4. Laboratorios de Evaluación e Institución de acreditación y certificación. El CCN/CNI
   6.5. Criterios y metodologías de evaluación.
   6.6. Reconocimiento mutuo de certificados. Requisitos del reconocimiento.

Mayo 2019