UNIVERSIDAD PONTIFICIA
ICAI ICADE
COMILLAS
MADRID

Seguridad Informática:

Capítulo 3: Legislación y normativa de seguridad

Titulación: Ingeniero en Informática.
Curso 5º - Cuatrimestral (2005-2006)

Javier Jarauta Sánchez
José María Sierra
Rafael Palacios Hielscher

Legislación y normativa de seguridad

- Identificación de normativa aplicable
- Ley Orgánica de Protección de Datos (LOPD).
- Ley de Servicios para la Sociedad de la Información y del Comercio Electrónico (LSSI-CE).
- Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP)
- Ley de Medidas de Impulso para la Sociedad de la Información (LISI)
- Ley de Firma Electrónica.
- UNE-ISO/IEC 17799 y UNE 71502.
- TCSEC, ITSEC, Common Criteria.
- Otros estándares y normas

Marco Legislativo y Normativo

- Marco legislativo: Definir e identificar las leyes aplicables para la organización que tienen relación con la seguridad de los Sistemas de Información

- Marco normativo: Definir e identificar las normas y estándares de seguridad de la información que aplican en cada caso

Legislación de Seguridad
LOPD

Ley 15/1999 de 13 de diciembre
RD 994/1999 de 11 de junio. Reglamento
RD 1720/2007 de 19 de diciembre. Nuevo reglamento

1. Ley de Protección de Datos - LOPD

- Ley Orgánica 15/1999, de 13 de Diciembre de Protección de Datos de Carácter Personal - **LOPD**
- Real Decreto 994/1999 de 11 de Junio por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal – **Reglamento de Seguridad**
- Todas las empresas que tengan ficheros con datos personales han de declararlos a la Agencia Española de Protección de Datos (www.agpd.es)
- Existen agencias en Comunidades Autónomas para ficheros de Titularidad Pública (www.apdcat.net; www.madrid.org/apdcm)

Ley de Protección de Datos - LOPD

- Hay que implantar un documento de seguridad
- Se clasifican en tres Niveles:
  - **Básico**: Ficheros con información personal
  - **Medio**: Ficheros con datos relativos a la comisión de infracciones administrativas, Hacienda Pública, Servicios financieros, así como los ficheros para la prestación de servicios de información sobre solvencia patrimonial y de crédito
  - **Alto**: Ficheros con datos sobre ideología, religión, creencias, origen racial, salud o vida sexual, así como los datos recabados para fines policiales sin consentimiento del afectado
- Hay que aplicar medidas de seguridad técnicas y organizativas en función del nivel y según establece el reglamento
- Auditorías bienales para ficheros de nivel medio y alto

Ley de Protección de Datos - LOPD

- Nivel básico
  - Creación de un documento de seguridad, de obligado cumplimiento para el personal que tenga acceso a los datos.
  - Adopción de medidas para que el personal conozca las normas de seguridad.
  - Creación de un registro de incidencias
  - Creación de una relación de usuarios (procesos o personas) que tengan acceso al sistema de información
  - Establecer mecanismos de control de acceso
  - Establecer mecanismos de control de soporte

Ley de Protección de Datos - LOPD

- Nivel medio
  - Todas las obligaciones de nivel básico
  - Identificación del responsable de seguridad
  - Control periódico para verificar el cumplimiento en lo dispuesto en el documento de seguridad
  - Definir además las medidas para reutilizar o desechar un soporte
  - Auditoría interna o externa. Al menos cada 2 años.
  - Mecanismo para identificar todo usuario que intente acceder al sistema. Limitar el número de intentos.
  - Normas sobre gestión de los soportes.

Ley de Protección de Datos - LOPD

- Nivel alto
  - Todas las obligaciones de nivel básico y nivel medio.
  - Medidas complementarias sobre:
    - Distribución y gestión de soportes de copias de seguridad
    - Registro de accesos lógicos: logs con usuario, hora, tipo
    - Control y registro de accesos físicos
    - Copias de respaldo y recuperación
  - Comunicaciones cifradas en caso de realizar transmisión de datos

Ley de Protección de Datos - LOPD

- Derechos básicos
  - Derecho de consulta al registro general de protección de datos. El registro es de consulta pública y gratuita.

- Servicios gratuitos que debe ofrecer la empresa
  - Derecho de **acceso**. Consulta gratuita de los datos personales de la persona que los solicite.
  - Derecho de **rectificación**. plazo de 10 días
  - Derecho de **cancelación** (derecho a borrar el dato). plazo de 10 días
  - Derecho de **oposición** (eliminación de datos cuyo tratamiento no requiera consentimiento).

Ley de Protección de Datos - LOPD

- Infracciones leves (multa de 600€ a 60.000€)
  - No solicitar la inscripción del fichero en la AGPD
  - No atender las solicitudes de los interesados
  - Recoger los datos sin informar a los interesados sobre: la existencia del fichero, el uso que se va a dar a los datos, el responsable del fichero, los derechos del interesado.

Ley de Protección de Datos - LOPD

- Infracciones graves (multa de 60.000€ a 300.000€)
  - Recoger datos sin recabar el consentimiento expreso de los afectados
  - Crear ficheros de titularidad pública sin tener autorización especial
  - Crear ficheros de titularidad privada con fines distintos al objetivo legítimo de la empresa
  - Mantener los ficheros sin las debidas medidas de seguridad
  - Mantener datos inexactos o no efectuar correcciones/cancelaciones

Ley de Protección de Datos - LOPD

- Infracciones muy graves (multa de 300.000€ a 600.000€)
  - Comunicación o cesión de datos
  - Recogida de datos de forma engañosa o fraudulenta
  - No atender sistemáticamente los derechos de acceso, rectificación, cancelación u oposición

Reglamento medidas seguridad

TIPO DE FICHERO	BASICO	MEDIO	ALTO
Disponer de Documento de Seguridad	SI	SI	SI
Nombrar un Responsable de Seguridad		SI	SI
Funciones y obligaciones del personal	SI	SI	SI
Registro de incidencias	SI	SI	SI
Identificación y autenticación	SI	SI	SI
Sistema de control de acceso lógico	SI	SI	SI
Sistema de control de acceso físico		SI	SI
Gestión de soportes	SI	SI	SI
Copias de respaldo y recuperación	SI	SI	SI
Realizar auditoría bienal		SI	SI
No realizar pruebas con datos reales		SI	SI
Distribución de soportes			SI
Disponer de un registro de accesos			SI
Cifrado de las telecomunicaciones			SI

Legislación de Seguridad LSSI-CE

Ley 34/2002 de 11 de Julio

2. Ley Sociedad Información -LSSI-CE

- Ley 34/2002 de 11 de Julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico – LSSI-CE (www.lssi.es)

- Establece los criterios de servicios en Internet, cuando sean parte de actividad económica.

- Validez y regulación del comercio electrónico

2. Ley Sociedad Información -LSSI-CE

- Servicios por Internet
  - Mostrar en la web: Nombre, NIF, dirección, correo electrónico
  - Datos de inscripción registral incluyendo nombre del dominio
  - Mostrar precios de los productos y servicios,
  - Contratación y tramitación on-line
  - Autenticación mediante certificados y establecer canales seguros SSL
- Sobre la publicidad por Internet
  - Prohibición de los spam (email no solicitado)
  - Posibilidad de borrarse de las listas de correo informativo
- Sobre los prestadores de servicios ISP, Hosting
  - Colaborar con los organos públicos para resolucion de incidencias: almacenamiento de logs y eventos para rastreo
  - Informar a los clientes sobre medidas de seguridad a aplicar
  - No son responsables de contenidos ilícitos si no los elaboran,
  - Sí son responsables si los conocen y no los retiran o no los comunican.
- Sobre titulares de páginas personales
  - Solo sujetas a la ley si tienen publicidad por la que perciban ingresos
  - Identificar claramente la publicidad y la identidad: nombre, tfno, fax, eMail, NIF

Legislación de Seguridad LAECSP

Ley 11/2007 de 22 de junio

3. Ley de Acceso a Servicios Públicos -LAECSP

- Orientada a los derechos de los ciudadanos y obligaciones de las AAPP
- Ejes fundamentales: Interoperabilidad,accesibilidad y seguridad
- Obligación de poner TODOS los trámites administrativos antes del 31 de Diciembre de 2009
- Servicio www.060.es de atención al ciudadano centralizando todos los servicios. Catálogo de servicios
- Existe un Plan Estratégico y un Plan de Actuación con medidas en adaptación de procedimientos, infraestrcuturas y acciones horizontales (p.e. Seguridad)

3. Ley de Acceso a Servicios Públicos -LAECSP

- Acceso de los ciudadanos a una “Sede Electrónica”
- Transmisión de datos entre Administraciones Públicas, para que el ciudadano no aporte datos que ya disponen.
- Identificación y autenticación de ciudadanos y AAPP mediante certificados digitales (DNIe)
- Establecimiento de registros electrónicos 24x7 para la entrega y recepción de solicitudes y escritos
- Notificación por medios electrónicos con firma digital
- Consideración de copias auténticas de documentos electrónicos firmados, que pueden obtener los ciudadanos
- Archivo electrónico de los documentos con servicios de confidencialidad, integridad, autenticidad y conservación
- Gestión electrónica de los procedimientos administrativos: iniciación, instrucción, terminación.

Legislación de Seguridad
LISI
Ley 56/2007 de 28 de diciembre

4. Ley Impulso Sociedad de la Información LISI

- Medidas orientadas a impulsar la Sociedad de la Información en el sector privado
- Tres líneas fundamentales
  - Facturación electrónica
  - Contratación electrónica
  - Interlocución entre clientes, partners y proveedores

4. Ley Impulso Sociedad de la Información LISI

- Facturación electrónica.
  - Uso de medios electrónicos en los procesos de contratación.
- Obligación de disponer de un medio de interlocución telemática
  - Prestación de servicios al público de especial transcendencia económica.
- Ofertas públicas de contratación electrónica entre empresas.
- Utilización de caracteres de las lenguas oficiales de España en ".es".
- Extensión de servicios de banda ancha.
- Mejora de los niveles de seguridad y confianza en Internet.
- Requerimientos de información para fines estadísticos y de análisis.
- Acceso de las personas con discapacidad a las TIC.
- Transferencia tecnológica a la sociedad.
- Cesión de contenidos para su puesta a disposición de la sociedad.
- Regulación del juego.

Legislación de Seguridad
Firma Electrónica
Ley 59/2003 de 19 de diciembre

5. Ley de firma electrónica

- Ley 59/2003 de 19 de Diciembre, de firma electrónica
- Equipara la firma electrónica a la firma física, estableciendo su validez legal
- Regula a los Prestadores de Servicios de Certificación (PSC – Autoridades de Certificación)
- Regula los certificados reconocidos
- Regula los dispositivos seguros de creación de firmas
- Existe directiva europea 1999/93/EC (iniciativas eEurope)
- Se introduce el DNI electrónico (DNIe)
- RD 1553/2005 de 23 Diciembre que regula la expedición
- Portal www.dnielectronico.es

Normativa de Seguridad

Buenas Prácticas UNE-ISO 17799

UNE/ISO 17799 analiza las siguientes 10 áreas de seguridad:

- **Políticas de Seguridad.**
- **Organización de la Seguridad.**
- **Clasificación y control de activos.**
- **Seguridad ligada al personal.**
- **Seguridad física.**
- **Seguridad lógica.**
- **Control de accesos.**
- **Mantenimiento y desarrollo de los sistemas.**
- **Continuidad de negocio.**
- **Cumplimiento con la legislación vigente.**

Norma UNE-ISO/IEC 17799:2002

Código de buenas prácticas en Seguridad de la Información (contenido)

Introducción a los conceptos de gestión de la seguridad.

10 secciones

36 objetivos de seguridad

127 controles de seguridad

Especificaciones / / Guía / / Referencias

Cubre aspectos de Gestión, Jurídicos y Técnicos

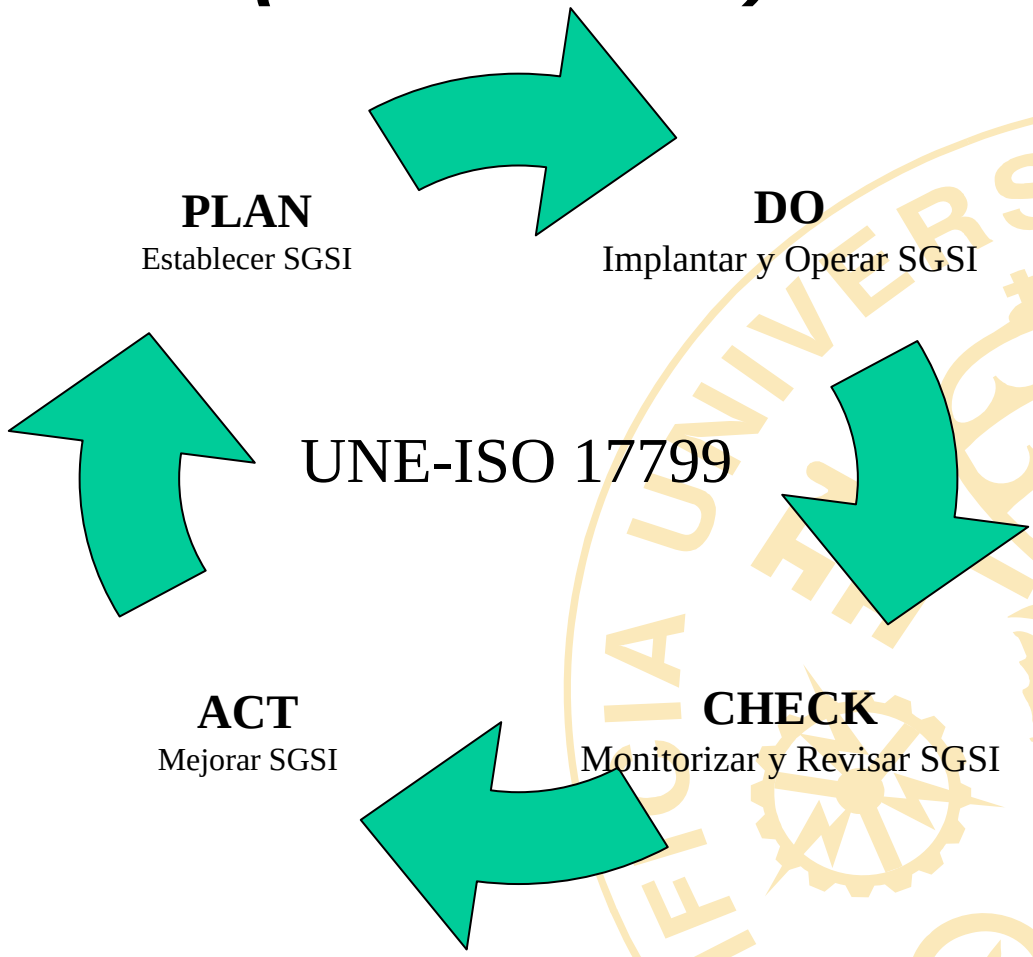
UNE 71502 / ISO 27001

Especificaciones para los Sistemas de Gestión de la Seguridad de la Información

- Especifica los requisitos para establecer, implantar, documentar y evaluar un SGSI de acuerdo con UNE-ISO 17799
- Define los controles de seguridad a revisar
- Define un marco general del SGSI
- Cómo se debe implantar el SGSI
- Cómo se realiza la explotación
- Cómo debe realizarse la revisión y mejora del SGSI

Norma UNE 71502:2004 - SGSI

Sistema de Gestión de la Seguridad de la Información (Modelo PDCA)



Criterios de Certificación de productos de Seguridad

Antecedentes: Orange Book - TCSEC

- 1985. Trusted Computer Security Evaluation Criteria (TCSEC - Orange Book - Criterios Norteamericanos)
- Recomendaciones del Departamento de Defensa (DoD). Parte de una serie de recomendaciones sobre SI denominada “Rainbow Series”
- Se especifican criterios de seguridad del Hw y Sw básico, así como metodologías de evaluación de la seguridad en los SI
- Permiten examinar el sistema comprobando si las funciones de seguridad están presentes y si funcionan correctamente
- Los fabricantes someten sus productos a evaluación por una Agencia Gubernamental

Antecedentes: Orange Book - TCSEC

- Los productos se clasifican en diferentes niveles, obteniendo la certificación correspondiente:
  - Nivel D (Menor nivel de seguridad)
  - Nivel C1, C2
  - Nivel B1, B2, B3
  - Nivel A1 (Mayor nivel de seguridad)
- La mayoría de Sistemas Operativos comerciales están en el nivel C2
- Pueden añadirse módulos específicos de seguridad para aumentar el nivel
- Problemática:
  - Excesivo coste y duración (1 a 3 años)
  - Excesiva orientación a S.O.
  - Demasiado énfasis en confidencialidad y no en el resto

Antecedentes: ITSEC (white book)

- 1991. Information Technology Security Evaluation Criteria (ITSEC - White Book - Criterios Europeos)
- Inicialmente propuestos por Alemania, Francia, Reino Unido y Holanda, mezclando recomendaciones propias
- Posteriormente se publicó ITSEM (Metodología)
- Se aborda la seguridad como confidencialidad, integridad y disponibilidad
- Se definen productos (Hw y Sw) para una diversidad de entornos y sistemas para entornos específicos
- Los productos dispondrán de funciones de seguridad como: controles acceso, auditoría, recuperación de errores, etc
- Se evalúa la corrección con la que están desarrollados, la operatividad funcional de las medidas y su efectividad contra potenciales amenazas

Antecedentes: ITSEC (white book)

- Define 10 clases de funcionalidades, de las cuales 5 equivalen a niveles de TCSEC:
  - ITSEC: F-C1, F-C2, F-B1, F-B2, F-B3
  - TCSEC: C1, C2, B1, B2, B3/A1
- Las otras 5 funcionalidades están orientadas a aplicaciones
- Un producto o sistema a evaluar se denomina TOE (Target of Evaluation) y se verifica contra un objetivo de seguridad (ej. Funcionalidad F-B1)
- Primero se evalúa la corrección del TOE en cuanto a construcción y operación, clasificándolo en 7 niveles (E0 a E6 de menor a mayor)
- Posteriormente se examina la efectividad de sus funciones para adaptarse al objetivo de seguridad
- Problemática:
  - Evaluación larga aunque menor que TCSEC (9 meses)
  - Falta de reconocimiento entre paises
  - Falta de interés del sector privado por productos certificados

Actualidad: Common Criteria

- 1996. V1.0 Common Criteria (Criterios comunes USA-EUR)
- Iniciativa conjunta para armonizar TCSEC e ITSEC
- Reconocimiento mutuo de la certificación
- Mayor interés del sector privado en productos certificados
- Actualmente en vigor V2.0 de 1998
- `www.commoncriteriaportal.org`

Common Criteria

- EAL1
  - Nivel básico. Se evalúa la utilización apropiada de lasfunciones de seguridad, pero no su correcta implantación
- EAL2
  - Nivel moderado de seguridad. Se analizan las funciones de seguridad utilizando especificaciones funcionales
- EAL3
  - Nivel medio de seguridad. Se analizan las funciones de seguridad y su diseño a alto nivel
- EAL4 (Ejemplos EAL4+: Windows Server 2003, Windows XP, Windows 2000, SuSE, Solaris 9)
  - Nivel alto de seguridad. Se analizan las funciones de seguridad y su diseño a alto y bajo nivel, su correcta implantación

El estándar FIPS-140-1

- Certificación de productos criptográficos

  FIPS : Federal Information Processing Standard

  140-1: Security Requirements for Crypto Modules

- Se verifican los siguientes parámetros
  - Diseño y documentación del módulo cripto
  - Interfaces, roles-servicios, modelo utilizado
  - Seguridad física y del software
  - Seguridad del sistema operativo
  - Gestión de claves
  - Algoritmos criptográficos
  - Emisiones electromagnéticas (EMI/EMC)
  - Auto tests

El estándar FIPS-140-1 Niveles

NIVEL 1

- Puede ser Sw
- Algoritmos FIPS
- G. Claves FIPS
- Descripción módulo cripto
- Especificación software

NIVEL 2

- Detección intrusión
- Autentic. Operador
- Nivel C2

NIVEL 3

- Prevención intrusión
- Identificación Operador
- Nivel B1
- Seguridad física claves
- Puertos E/S separados
- E/S claves cifradas

NIVEL 4

- Prevención y borrado claves con intrusión
- Seguridad física completa
- Seguridad emisiones
- Nivel B2

Cliente

VPN-IP

CA

Otros estándares y normas

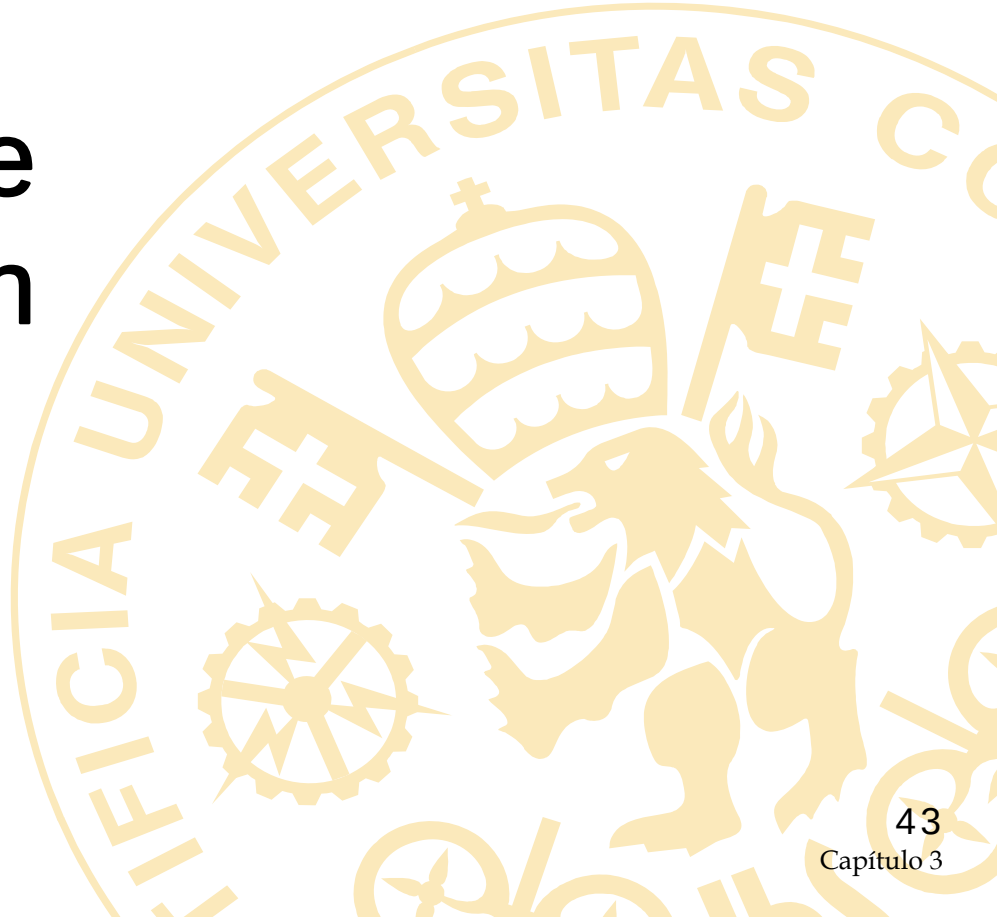
Otros estándares y normas (1)

- Normativas de seguridad
  - ISO 7498/2; ISO 17799;
- Algoritmos criptográficos simétricos:
  - DES, 3DES, IDEA, AES
- Algoritmos criptográficos asimétricos:
  - DH, RSA,DSA
- Funciones Hash
  - MD5, SHA-1, RIPEMD
- Certificados digitales
  - X.509v3

Otros estándares y normas (2)

- Public Key Cryptography Standards
  - PKCS#1 al 15
- Protocolos
  - SSL (Web)
  - S/MIME (e-Mail)
  - IPSec (ESP, AH, IKE)
- Certificaciones de seguridad
  - FIPS-140-1
  - TCSEC, ITSEC, Common Criteria
- ETSI (Instituto Europeo de Estándares de Telecomunicaciones)
  - RFC 3039 Certificados cualificados
- Estándares de firma electrónica
  - XML Dsign, XADES, CADES
- Otros organismos y grupos de estandarización

Otros grupos de estandarización



Otros grupos de estandarización

- ISO: International Standard Organization
  - Generales: ISO 7498.2, ISO 17799
  - TC68/SC2: Subcomité del Comité Técnico 68
    - WG8: Estandarización tecnología de clave pública
  - SC27: Subcomité sobre seguridad genérica
    - WG1: Identificar necesidades criptográficas
    - WG2: Definir técnicas y mecanismos
    - WG3: Establecer criterios de seguridad
- ITU: International Telecommunications Union
  - X.2xx Protocolos de seguridad (X.273, X.274)
  - X.4xx Seguridad en mensajería
  - X.5xx Directorio. (X.509)
  - X.7xx Gestión del modelo OSI. (X.737, X.740...)
  - X.8xx Arquitectura seguridad para OSI

Otros grupos de estandarización

- ANSI X3 y X9:
  - Grupos de normas para aplicaciones financieras:
    - X9F (seguridad), X9F1 cripto, X9F3 protocolos, X9F5 firma
  - X3.92 (DES), X9.52 (3DES),
  - X9.9, X9.19 (Autenticación de Mensajes)
  - X9.17 (Gestión de claves)
- FIPS: Federal Information Processing Standars
  - FIPS 46-2 (DES)
  - FIPS 112 (passwords), 186 (DSS), 197 (AES).
- IEFT: RFCs
  - PKIX.
  - TLS
  - S/MIME.