1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad en Infraestructura de Tecnologías de Información
Clave de la asignatura:	SID-1303
Créditos (Ht-Hp_ créditos):	2-3-5
Carrera:	Ingeniería en Informática.

2. Presentación

Caracterización de la asignatura
La asignatura aporta al perfil del egresado de la Carrera de Ingeniería Informática los conocimientos y habilidades para implementar y desarrollar aplicaciones de seguridad y acordes a la normas de tecnologías de la información. *Con la creciente de los sistemas, negocios enfocados al uso de internet (globalización), la materia de Seguridad en infraestructura de T. I., permite que el estudiante conozca las funciones y algoritmos criptográficos de la seguridad para proteger los sistemas y recursos. Permitiendo la implementación de Protocolos y Estándares.* *La asignatura se encuentra estructurada de tal manera que el aprendizaje sea evolutivo en el conocimiento adquirido iniciando con los conceptos básicos de seguridad y las principales funciones, algoritmos y aplicaciones a las que se encuentran expuestos las aplicaciones web. La asignatura nos permitirá conocer los temas actuales relacionados con la Seguridad de T. I., que permitan conocer y tener la habilidad de aplicarlas de acuerdo a las necesidades de cada organización.* *Esta materia se imparte en el V Semestre considerando que el estudiante ya cuenta con los conocimientos adquiridos de las materias de Redes, Programación, Seguridad; con lo cual tiene la habilidad y capacidad de desarrollar, implementar e instalar las normas, estándares en tecnológicas para proteger los activos de la organización.*

Intención didáctica
El temario se agrupo en seis temas, distribuyendo los conceptos teóricos y practico, que ayudan a lograr el adecuado entendimiento e interpretación de la materia, lo cual permitirá el óptimo desarrollo y alcance de las competencias de esta asignatura. *En el primer tema se aborda los aspectos generales de las funciones Hash, la cual incluye una breve introducción a las funciones matemáticas, aplicadas a dichas funciones para darles seguridad a la cadena de datos. Al estudiar cada función, se hace un énfasis muy especial en la utilidad que tendrá para más adelante, tanto del desarrollo de la asignatura como de la carrera en general.* *El segundo tema comprende los diferentes mecanismos de las firmas digitales y subtemas relacionados a los aspectos de la Seguridad Informática en la web que permitirá a los estudiantes adquieran conocimientos, habilidades y a su vez logren implementar herramientas a través de software especializados en la protección de los datos.* *En el tercer tema correspondiente a los tipos de certificados digitales como herramientas de seguridad, los subtemas relacionados están enfocados a los estándares de los componentes, creación y lista de certificados digitales, servirá como un ejemplo y ejercicio introductorio a este importante aspecto de seguridad en la web, incluyendo una revisión de los diferentes tipos de Certificados Digitales* *En el cuarto tema se aborda los aspectos generales de la creación de llaves sus funcione, algoritmos técnicas y transporte de los datos. Al estudiar estos temas, se hace un énfasis muy especial en la utilidad de dichas llaves para su aplicación en el siguiente tema.* *En el quinto tema se abordan la infraestructura de las llaves públicas, la cual incluye los componentes, modelos, generación estándares y protocolos a dicho tema. Al estudiar cada función, se hace un énfasis muy especial en la utilidad que tendrá en la generación de la infraestructura de llaves públicas.* *El temario culmina con el estudio y conocimiento de las aplicaciones de las Norma, Estándares y protocolos para la seguridad en la infraestructura de la tecnología de la información.*

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Dirección General de Educación Superior Tecnológica, 21 y 22 Febrero de 2013	Tecnológico de Estudios Superiores de Ecatepec. Instituto Tecnológico Superior Teziutlán,	Reunión para el Análisis por Competencias Profesionales de la Especialidad.

	Puebla. Instituto Tecnológico Superior de Ciudad Serdán, Puebla. Tecnológico de Estudios Superiores de Cuautitlán Izcalli.	

4. Competencias a desarrollar

Competencia general de la asignatura
• Analiza y evalúa los protocolos, algoritmos y sistemas criptográficos, métodos y técnicas encaminadas a proteger la infraestructura de tecnologías de la información para solucionar problemas específicos de seguridad informática dentro de la organización.
Competencias específicas
• Analiza las distintas técnicas y directrices de funciones Hash de la seguridad informática para implementar soluciones integradoras en la protección. • Aplicar las técnicas de Firma Digitales en la seguridad informática en aplicaciones web. • Configura e Implementa técnicas de los Certificados Digitales en aplicaciones y productos web. • Analiza la teoría y las técnicas de la Gestión de llaves aplicadas a la seguridad informática. • Analiza las distintas técnicas y directrices de la Infraestructura de llaves publicas aplicadas a la seguridad informática para implementar soluciones integradoras en la protección. • Implementa y configura la seguridad en aplicaciones Web, para implementar soluciones integradoras en la protección de las tecnologías de la información.
Competencias genéricas
• Capacidad de aplicar los conocimientos en la práctica. • Capacidad de comunicación oral y escrita. • Habilidades en el uso de las tecnologías de la información y de la

comunicación.
- Habilidades en el uso de protocolos y aplicaciones de seguridad.
- Capacidad para identificar, plantear y resolver problemas.
- Capacidad para tomar decisiones.
- Capacidad de trabajo en equipo.
- Habilidades interpersonales.

5. Competencias previas de otras asignaturas

Competencias previas
• Conoce de Fundamentos de programación. • Conoce de Métodos y Algoritmos Matemáticos. • Dominio de las metodologías para la solución de problemas mediante la construcción de algoritmos. • Dominio de las técnicas de diseño de algoritmos. • Analiza los componentes y la funcionalidad de diferentes sistemas de comunicación para evaluar las tecnologías utilizadas actualmente como parte de la solución de un proyecto. • Aplica e identifica el proceso administrativo para la gestión, diseño, evaluación e implementación de una propuesta de TIC. • Analiza las necesidades y determinar los requerimientos para la implementación

6. Temario

Temas		Subtemas
No.	Nombre	
1.	Funciones hash criptográficas.	1.1. Clasificación y propiedades. 1.2. Códigos de detección de modificación (MDC). 1.3. Algoritmos MD5 y SHA. 1.4. Códigos de autenticación de mensajes. (MAC). 1.5. Integridad de datos y autenticación de mensajes.
2.		2.1. Mecanismos de firmas digitales. 2.2. Esquema de firma RSA.

	Firmas digitales.	2.3. Esquemas de firma digital de FIAT-SHAMIR. 2.4. Esquema de firma DSA. 2.5. Firmas digitales con funcionalidad adicional.
3.	Certificados digitales.	3.1. Autoridad certificadora. 3.2. Certificado digital. 3.3. Componentes de un certificado digital. 3.4. Creación de certificados digitales. 3.5. Lista de certificados revocados. 3.6. Certificados X.509.
4.	Gestión de la llave.	4.1. Análisis de los protocolos de establecimiento de llave. 4.2. Transporte y acuerdo de llave basados en técnicas simétricas. 4.3. Transporte y acuerdo de llave basados en técnicas asimétricas. 4.4. Técnicas de gestión de la llave. 4.5. Técnicas para distribución de llaves públicas y confidenciales.
5.	Infraestructura de llave pública.	5.1. Conceptos básicos. 5.2. Componentes de una infraestructura de llave pública. 5.3. Modelos de confianza. 5.4. Generación de llaves del usuario/servidor y firmado. 5.5. Estándar y especificaciones PKI.
6.	Aplicaciones de la criptografía.	6.1. Autenticación e identificación. 6.2. Esquemas de compartición de secretos. 6.3. Situaciones de desconfianza mutua. 6.4. Dinero electrónico. 6.5. Elecciones electrónicas. 6.6. Expectativas a futuro. 6.7. PGP. 6.7.1. Fundamentos e historia de PGP. 6.7.2. Estructura de PGP. 6.7.3. Vulnerabilidades de PGP.

7. Actividades de aprendizaje

Competencia específica y genéricas (a desarrollar y fortalecer por tema)

Específica:

- Analiza las distintas técnicas y directrices de funciones Hash de la seguridad informática para implementar soluciones integradoras en la protección.

Genéricas:

- Capacidad de aplicar los conocimientos en la práctica.
- Capacidad de comunicación oral y escrita.
- Habilidades en el uso de las tecnologías de la información y de la comunicación.
- Habilidades en el uso de protocolos y aplicaciones de seguridad.
- Capacidad para identificar, plantear y resolver problemas.
- Capacidad de trabajo en equipo.
- Habilidades interpersonales.

Tema	Actividades de aprendizaje
Tema 1: Funciones hash criptográficas.	• Investigar el concepto de funciones hash y la clasificación de este tipo de funciones y entregar documento impreso. • Elaborar mapas conceptuales y cuadros sinópticos con la información recabada. • Desarrollar aplicación software que

Competencia específica y genéricas (a desarrollar y fortalecer por tema)

Específica:

- Analiza las distintas técnicas y directrices de las Firma Digitales aplicadas a la seguridad informática para implementar soluciones integradoras en la protección.

Genéricas:

- Capacidad de aplicar los conocimientos en la práctica.
- Capacidad de comunicación oral y escrita.
- Habilidades en el uso de las tecnologías de la información y de la comunicación.
- Habilidades en el uso de protocolos y aplicaciones de seguridad.
- Capacidad para identificar, plantear y resolver problemas.
- Capacidad de trabajo en equipo.
- Habilidades interpersonales.

Tema	Actividades de aprendizaje

<table>
<tr><td>Tema 2: Firmas digitales.</td><td>• Investigar el concepto de Firmas Digitales y su clasificación de este tipo de Firmas Digitales.
• Elaborar mapas conceptuales y cuadros sinópticos con la información recabada.
• Investigar e instalar aplicación software que realice la Firma Digital en aplicaciones Web para el entendimiento de la Firma.
• Instalar y evaluar distintas herramientas de seguridad en el área de Certificados Digitales.</td></tr>
<tr><td colspan="2">Competencia específica y genéricas (a desarrollar y fortalecer por tema)</td></tr>
<tr><td colspan="2">Específica:
• Analiza las distintas técnicas y directrices de los Certificados Digitales de la seguridad informática para implementar soluciones integradoras en la protección.

Genéricas:
• Capacidad de aplicar los conocimientos en la práctica.
• Capacidad de comunicación oral y escrita.
• Habilidades en el uso de las tecnologías de la información y de la comunicación.
• Habilidades en el uso de protocolos y aplicaciones de seguridad.
• Capacidad para identificar, plantear y resolver problemas.
• Capacidad de trabajo en equipo.
• Habilidades interpersonales.</td></tr>
<tr><td>Tema</td><td>Actividades de aprendizaje</td></tr>
<tr><td>Tema 3: Certificados digitales.</td><td>• Investigar el concepto de Certificado Digitales y su clasificación de este tipo de Certificados Digitales.
• Elaborar mapas conceptuales y cuadros sinópticos con la información recabada.
• Investigar e instalar aplicación software que realice el Certificado Digital en aplicaciones Web.
• Investigar el concepto de Autoridad</td></tr>
</table>

<table>
<tr><td colspan="2">Competencia específica y genéricas (a desarrollar y fortalecer por tema)</td></tr>
<tr><td colspan="2">Específica:
• Analiza las distintas técnicas y directrices de la Gestión de llaves aplicadas a la seguridad informática para implementar soluciones integradoras en la protección.

Genéricas:
• Capacidad de aplicar los conocimientos en la práctica.
• Capacidad de comunicación oral y escrita.
• Habilidades en el uso de las tecnologías de la información y de la comunicación.
• Habilidades en el uso de protocolos y aplicaciones de seguridad.
• Capacidad para identificar, plantear y resolver problemas.
• Capacidad de trabajo en equipo.
• Habilidades interpersonales.</td></tr>
<tr><td>Tema</td><td>Actividades de aprendizaje</td></tr>
<tr><td>Tema 4: Gestión de la llave.</td><td>• Investigar el concepto de Gestión de Llaves y su clasificación.
• Elaborar mapas conceptuales y cuadros sinópticos con la información recabada.
• Investigar el concepto de Transporte, Técnicas y Tendencias de la Gestión de Llaves. Exponer en clase los distintos ejemplos de su aplicación.</td></tr>
<tr><td colspan="2">Competencia específica y genéricas (a desarrollar y fortalecer por tema)</td></tr>
<tr><td colspan="2">Específica:
• Analiza las distintas técnicas y directrices de la Infraestructura de llaves publicas aplicadas a la seguridad informática para implementar soluciones integradoras en la protección.

Genéricas:
• Capacidad de aplicar los conocimientos en la práctica.
• Capacidad de comunicación oral y escrita.
• Habilidades en el uso de las tecnologías de la información y de la</td></tr>
</table>

comunicación.
- Habilidades en el uso de protocolos y aplicaciones de seguridad.
- Capacidad para identificar, plantear y resolver problemas.
- Capacidad de trabajo en equipo.
- Habilidades interpersonales.

Tema	Actividades de aprendizaje
Tema 5: Infraestructura de llave pública.	• Investigar el concepto de Llaves Públicas y su clasificación de este. • Elaborar mapas conceptuales y cuadros sinópticos con la información recabada. • Investigar e instalar aplicación software que realice la Llave Pública en aplicaciones Web. • Investigar el concepto de Componentes, Modelos, Generación, Protocolos de Llaves Públicas. Exponer en clase los distintos ejemplos de su aplicación. • Investigar el concepto de PKI estándar y explicarlo en clase. • Instalar y evaluar distintas herramientas de seguridad en el área de Llaves públicas.

Competencia específica y genéricas (a desarrollar y fortalecer por tema)

Específica:
- Analiza las distintas técnicas y desarrollo de aplicaciones Web aplicadas a la seguridad informática para implementar soluciones integradoras en la protección.

Genéricas:
- Capacidad de aplicar los conocimientos en la práctica.
- Capacidad de comunicación oral y escrita.
- Habilidades en el uso de las tecnologías de la información y de la comunicación.
- Habilidades en el uso de protocolos y aplicaciones de seguridad.
- Capacidad para identificar, plantear y resolver problemas.
- Capacidad de trabajo en equipo.

• Habilidades interpersonales.	
Tema	Actividades de aprendizaje
Tema 6: Aplicaciones de la criptografía.	• Investigar el concepto de criptografía enfocada a Aplicaciones Web. • Elaborar mapas conceptuales y cuadros sinópticos con la información recabada. • Investigar e instalar aplicación software enfocadas a seguridad Web. • Investigar el concepto de Dinero Electrónico y exponer en clase los distintos ejemplos de su aplicación. • Investigar el concepto de Elecciones Electrónicas y exponer en clase los distintos ejemplos de su aplicación. • Investigar el concepto de Correo

8. Prácticas (para fortalecer las competencias de los temas y de la asignatura)

Tema 1:

- Analizar, Instalar y experimentar diferentes herramientas de software especializados en temas de funciones hash para que de forma grupal seleccionemos la que mejores beneficios le ofrezca a las empresas.
- Identificar en lluvia de ideas las empresas líderes en desarrollo de soluciones hash acordes a la seguridad de informática.
- Realizar pruebas de ataque-defensa utilizando un conjunto de herramientas previamente seleccionadas para conocer los principales funciones hash.

Tema 2:

- Analizar, Instalar y experimentar diferentes herramientas de software especializados en temas de seguridad ocupando Firmas Digitales para seleccionemos la que mejores beneficios le ofrezca a las empresas de acuerdo a sus necesidades.
- Realizar pruebas a nivel Aplicaciones e Internet ocupando los mecanismos y esquemas de las Firmas Digitales.
- Identificar en lluvia de ideas las empresas líderes en desarrollo de soluciones informáticas de seguridad.

- Realizar pruebas de vulnerabilidad utilizando un conjunto de herramientas previamente seleccionadas para conocer los principales métodos de ataque a los que estamos expuestos y las Firmas Digitales.

Tema 3:
- Analizar, Instalar y experimentar diferentes Certificados Digitales, y su funcionamiento en aplicaciones Web.
- Realizar pruebas de seguridad a Certificaciones Digitales ocupando mecanismos de revocación a dichos certificados.

Tema 4:
- Analizar las diferentes técnicas de Infraestructura de Llaves Publicas para el uso en aplicaciones Web.

Tema 5:
- Analizar, Instalar y experimentar diferentes protocolos y estándares de Gestión de Llaves.
- Realizar pruebas al estándar PKI para su uso en generación de llaves.

Tema 6:
- Analizar e Identificar las principales aplicaciones en el mercado para:
  Autenticación.
  Dinero Electrónico.
  Elecciones Electrónicas.
  PGP.
  Para conocer sus características, costos, requisitos de instalación para desarrollar soluciones a la medida.

9. Proyecto integrador (Para fortalecer las competencias de la asignatura con otras asignaturas)

Panorama general del proyecto integrador

El proyecto integrador para esta asignatura se puede contemplar en varias capas que por los contenidos involucran a varias asignaturas anteriores y actuales:

0. **Base de datos:** Se enfocará a la adquisición de datos del mundo real para trasladarlos a un sistema de base de datos, creando una estructura completa para el manejo de información.

Relación con las asignaturas:
Taller de bases de datos *y* ***tópicos de bases de datos.***

1. **Adaptador:** Se enfocará a las rutinas diversas de conexión dependiendo de las tecnologías de desarrollo que se estén usando en el proyecto.

Relación con la asignaturas:
Fundamentos de gestión de servicios de TI** y **administración de servidores.

2. **Interfaces:** Se designará el uso de herramientas para diseño de las GUI (Interfaces de usuarios) que permitan interactuar con el usuarios del sistema.

Relación con la asignaturas:
Desarrollo de aplicaciones web** y **calidad en los sistemas de información

3. **Presentación:** Se contemplará el uso de modelos generales de presentación de datos usando la ergonomía para la interpretación intuitiva de los sistemas.

Relación con la asignaturas:
Desarrollo de aplicaciones web** y **calidad en los sistemas de información

Objetivo general

Desarrollar una aplicación WEB cliente/servidor para implementar las diversas técnicas de encriptación. El proyecto puede implementar los lenguaje ASP, PHP, Java, JavaScript, Python, o cualquier otro disponible para aplicaciones WEB.

Es importante que se determine que SGBD (Sistema Gestor de Base de Datos) se usará, ya que de esto depende los diversos componentes para el adaptador conocido como conector entre la aplicación y la base de datos. También se debe determinar que servidor WEB se usará, entre los que podemos elegir: Apache, Tomcat, IIS y Django.

En la unidad 1, se deben determinar los diversos campos que pueden ser creados en la base de datos para implementar un método criptográfico como lo es el MD5 o el SHA1.

En las unidades 2 y 3, se debe hacer una práctica para la identificación de los recursos tales como documentos y/o programas que puedan ser descargados, y determinar si son válidos o si han sufrido alguna modificación post descargar.

En las unidades 4, 5 y 6, básicamente se deben de usar servicios de compañías para poder generar algunos certificados que permitan identificar al usuarios y/o a la organización, asimismo, se debe usar las aplicaciones para la generación de las llaves tanto públicas como privadas. Para lo anterior en estas unidades propongo el uso de GNUpg, PGP, www.thawte.com y p7m.

Recomendaciones

Unidad 1 (Funciones hash criptográficas): En esta unidad, se implementaran las funciones criptográficas inicialmente para verificar si los diversos recursos (tales como documentos y/o programas) disponibles en un sistema han sido modificados o bien si son los auténticos.

p. ej: Explicar la forma de subir un recurso a un sitio público y saber si el disponible es correcto o si esta identificado.

Unidad 2 (Firmas digitales): En esta unidad, se deben identificar las aplicaciones de las firmas digitales y que aplicaciones logran crearlas. Como parte del proyecto integrador, se implementara la aplicación PGP para generar la Firma digital de documentos.

Unidad 3 (Certificados digitales): En esta unidad, se debe usar un servidor generador de certificados gratuitos, por ejemplo THAWTE (www.thawte.com), posteriormente instalar y ejecutar la aplicación p7mViewer que nos permitirá descifrar los certificados de usuarios y/o organizaciones.

Unidad 4 (Gestión de la llave): Para esta unidad, se debe explicar a detalle la forma en como trabajan las claves públicas y privadas, y que software sirve de intermediario para desencriptar los certificados importados en las aplicaciones cliente/servidor.

Unidad 5 (Infraestructura de llave pública): Para esta unidad, se realizará un ejercicio de el envío de datos usando una llave pública por medio de la Intranet o la Internet, para poder entender el funcionamiento y aplicación de las llaves públicas. Con este ejercicio, se explicará como esta compuesto el mecanismo de llave pública.

Unidad 6 (Aplicaciones de la criptográfica): Para esta unidad, se expondrán casos reales en donde se usen los métodos de criptográficos, principalmente en servicios que se usan cotidianamente, tales como bancos, tiendas, sitios de transacciones en línea, entre otras.

10. Evaluación por competencias (específicas y genéricas de la asignatura)

- La evaluación debe ser permanente y continua. Se debe hacer una evaluación diagnóstica, formativa y sumativa. Se debe aplicar la autoevaluación, coevaluación y heteroevaluación.

- Se debe generar un portafolio de evidencias, de preferencia en formato digital.

Instrumentos
- Collage
- Ensayo
- Resumen
- Mapa Mental
- Mapa Conceptual
- Mapa Cognitivo
- Tabla Comparativo
- Línea de Tiempo
- Examen
- Cuadro Sinóptico
- Cuadro Comparativo
- Análisis FODA
- Reporte de Práctica de Laboratorio
- Informe Técnico y Analítico
- Reporte de Investigación Documental

Herramientas:
- Rúbricas
- Registro Anecdótico
- Guía de Observación
- Matriz de Valoración
- Lista de Cotejo
- Guía de Proyecto
- Videos

11. Fuentes de información (actualizadas considerando los lineamientos de la APA*)

1. Konheim A. G, *Computer Security and Cryptography*, Wiley-Interscience, 2007
2. Forouzan B. A, Cryptography and Network Security, McGraw-Hill Science/Engineering/Math; 1st Edition, 2007.
3. Delfs H, Knebl H, Introduction to Cryptography: Principles and Applications (Information Security and Cryptography), Springer; 2nd Edition, 2007
4. Stallings W, *Cryptography and Network Security*, 4th Edition, 2005
5. Henk C.A. van Tilborg, *Enciclopedya of Cryptography and Security*, Springer, 2005
6. Mao W, *Modern Cryptography: Theory and Practice,* Prentice Hall PTR, 1st Edition, 2003.
7. Ferguson N, Schneier B, *Practical Cryptography,* Wiley, 2003

8. Menezes, P. Van, Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
9. Bruce Schneier, *Applied Cryptography: Protocols Algorithms and Source Code in C*, Second Edition, John Wiley & Sons, INC, 1996.
10. Douglas R Stinson, *Cryptography Theory and Practice*, CRC, 1995.
11. Bruce Schneier (Author), *Applied Cryptography. Protocol, Algorithms, and Source Code in C. 2da Edition.* ISBN-10: 0471117099 ISBN-13: 978-0471117094.
12. Niels Ferguson (Author), Bruce Schneier (Author), *Practical Cryptography.* ISBN-10: 0471223573 ISBN-13: 978-0471223573.
13. Alfred Menezes, Paul van Oorschot y Scott Vanstone (Editores), *Handbook of Applied Cryptography. Discrete Mathematics and its Applications.* ISBN-10: 0849385237 ISBN-13: 978-0849385230.
14. William Stallings (Author), *Cryptography and Network Security. Principal and Practice, 5ta Edition.* ISBN-10: 0136097049 ISBN-13: 978-0136097044.
15. Tom St Denis (Author), *Cryptography of Developers. ISBN*-10: 1597491047 ISBN-13: 978-1597491044.
16. Tom St Denis (Author), *BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic.* ISBN-10: 1597491128 ISBN-13: 978-1597491129.
17. Fred B. Wrixon (Author), *Codes, Ciphers, Secrets and Cryptic Communication. Making and Breaking Secret Messages from Hieroglyphs to the Internet.* ISBN-10: 1579124852 ISBN-13: 978-1579124854.
18. Simon Singh (Author), *The Code Book. The Sciences of Secrecy from Ancient Egypt to Quantum Cryptography.* ISBN-10: 0385495323 ISBN-13: 978-0385495325.
19. David Kahn (Author), *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* ISBN-10: 0684831309 ISBN-13: 978-0684831305.
20. Charles P. Pfleeger y Shari Lawrence Pfleeger, *Security in Computing 4ª edition.* Prentice Hall (2006) ISBN-10: 0132390779, ISBN-13: 978-0132390774.
21. Charlie Kaufman, Radia Perlman y Mike Speciner. Prentice Hall (2002), *Network Security: Private Communication in a Public World 2ª edition.* ISBN-10: 0130460192, ISBN-13: 978-0130460196.
22. Rick Lehtinen y G.T. Gangemi. O'Reilly, *Computer security Basics 2ª edition.* Media, Inc. (2006) ISBN-10: 0596006691, ISBN-13: 978-0596006693.
23. Dieter Gollmann. Wiley (2006), *Computer Security 2ª edition.* ISBN-10: 0470862939, ISBN-13: 978-0470862933.
24. Matt Bishop. Addison-Wesley Professional, *Introduction to Computer Security.* (November 5, 2004) ISBN-10: 0321247442, ISBN-13: 978-0321247445.
25. Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry, *Fundamentals Of Computer Security.* ISBN: 3540431012, ISBN-13: 9783540431015, 978-3540431015. Springer 2003.
26. Varios autores**,** *Seguridad de las tecnologías de la información. La construcción de la confianza para una sociedad conectada.* Editorial: AENOR.
27. Morant, José Luis; Ribagorda, Arturo; Sancho, Justo, *Seguridad y Protección de la Información.* Editorial Centro de Estudios Ramón Areces. Enero 1994. (Primera reimpresión agosto 1997).
28. Pastor, J; Sarasa, M. A. CRIPTOGRAFÍA DIGITAL. *Fundamentos y*

Aplicaciones. Colección Textos Docentes. Zaragoza, 1998.
29. Schneier, B. APPLIED CRYPTOGRAPHY. *Protocols, Algorithms and Source Code in c. 2ª Edition.* John Wiley, 1996.
30. Stallings, William. *Cryptography and Network Security.* PRINCIPLES AND PRACTICE, Prentice Hall, 1999.

* American Psychological Association (*APA*)