Seguridad del documento digital

Curso Académico: (2023 / 2024) **Fecha de revisión: 18-05-2023**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: FUENTES GARCIA ROMERO DE TEJADA, JOSE MARIA DE

Tipo: Obligatoria Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

No es imprescindible haber superado ninguna materia

OBJETIVOS

El estudiante tras la superación de la materia deberá:
- Conocer y comprender los objetivos de la seguridad de la información y las amenazas y las vulnerabilidades de los sistemas de información.
- Conocer y comprender los problemas de la autenticación e integridad del documento electrónico y las herramientas para garantizarlas.
- Conocer aspectos jurídicos esenciales relacionados con la ciberseguridad y particularmente la seguridad del documento digital.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

El objetivo primordial es que el estudiante reconozca a la seguridad como una faceta insoslayable de la información digital y de los sistemas que intervienen en su gestión. Subordinado a este objetivo global, se pretende que el alumno identifique las dimensiones de la seguridad (confidencialidad, integridad y disponibilidad), las amenazas (técnicas o físicas) a las que está expuesta información digital y conozca y sepa usar las principales herramientas para protegerla.
El programa se divide en cinco grandes bloques:
PRIMERA PARTE: Se expondrán las dimensiones de la seguridad (confidencialidad, integridad, disponibilidad) haciendo hincapié en su importancia relativa según los entornos e introducirán las medidas de seguridad específicas para cada una de ellas. A continuación, se expondrán las amenazas de distintos tipos que padece la información y las vulnerabilidades de los sistemas que la tratan.
SEGUNDA PARTE: Se analizarán los problemas de conservación del documento electrónico y estudiarán los sistemas de protección, para seguidamente hacer lo propio con la destrucción segura de la información y los soportes que la alojan antes de ser desechados o reutilizados.
TERCERA PARTE: Se estudiará el cifrado de datos como herramienta fundamental de la seguridad, exponiendo los distintos sistemas y su utilidad según su uso previsto.
CUARTA PARTE: Se tratará la firma y los certificados digitales como herramienta básica de integridad y autenticidad del documento, así como su uso para evitar el rechazo de su autoría.
QUINTA PARTE: Se expondrán los problemas de seguridad que conlleva la información ubicada en sistemas accesibles mediante redes de ordenadores y los mecanismos de protección específicos para la transmisión segura de información.

Así, el programa se compone de los siguientes temas y epígrafes:
1.- La seguridad del documento electrónico

1.1.- Objetivos de la seguridad
1.2.- Mecanismos de seguridad: legales, administrativos, físicos y técnicos
1.3.- Programas malignos
1.4.- Seguridad de los sistemas informáticos. Vulnerabilidades

2.- El documento electrónico. Integridad y destrucción
2.1.- Integridad. El uso de funciones resumen
2.2.- Destrucción segura del documento electrónico
2.3.- Condiciones legales de conservación y destrucción de soportes de información conteniendo datos personales.

3.- Cifrado de datos
3.1.- Introducción a las técnicas de ocultación de la información
3.2.- Esquema de un cifrador. Ejemplos
3.3.- Cifrados de clave secreta y pública. Ejemplos
3.4.- Cifrado en aplicaciones ofimáticas comunes (Microsoft Office, PDF, etc.)
3.5.- Programas específicos de cifrado

4.- Firma y autenticación de usuarios
4.1.- Introducción a la firma digital. Diferencias con la manuscrita
4.2.- Sellado de tiempo
4.3.- Certificados digitales. Tipos
4.4.- Autoridades de certificación. Ejemplos. El DNI-e
4.5.- La revocación de certificados
4.6.- Autenticación de usuarios

5.- Seguridad en redes de ordenadores
5.1.- Amenazas a las redes de ordenadores.
5.2.- Protocolos seguros de conexión con servidores. TLS/SSL

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS DEL PLAN DE ESTUDIOS REFERIDAS A MATERIAS

AF1 Trabajo individual para el estudio de materiales teóricos y prácticos elaborados y aportados por el profesor (40 h)
AF3 Clases presenciales/online síncronas teórico-prácticas (3 h)
AF4 Tutorías
AF5 Trabajo en grupo (47 h)

METODOLOGÍAS DOCENTES

MD1 Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
MD3 Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo
MD5 Elaboración de trabajos e informes de manera individual o en grupo
MD6 Lectura de materiales docentes teóricos y prácticos

Los horarios de las tutorías, ajustados a lo dispuesto por la Universidad, se podrán consultar en el espacio propio de la asignatura en la plataforma de enseñanza y aprendizaje (Aula Global). Incluirán al menos dos tramos, uno para atención presencial y otro para atención en línea, que deberán ser solicitados (y posteriormente confirmados) por correo electrónico con antelación suficiente. Además de estas tutorías fijadas oficialmente para la asignatura, los alumnos pueden solicitar y concertar con el profesor tutorías presenciales o en línea fuera de esos horarios.

SISTEMA DE EVALUACIÓN

SE2 Trabajos individuales o en grupo realizados durante el curso
SE4 Examen o Trabajo final*

* El examen o trabajo final se realizará en modalidad presencial, en la universidad Carlos III que garantice la identidad del estudiante, y deberá superarlo para poder aprobar la materia/asignatura correspondiente.

Se establece el siguiente sistema de evaluación:

La evaluación de la asignatura se compone de la evaluación continua del trabajo desarrollado por el alumno (50%), el peso del examen final (25%) y el de una entrega final (25%).
1. Convocatoria ordinaria

Trabajo(s) teórico(s)
- Representarán el 25% de la nota final
- Obligatorio
- En grupos, salvo indicación en contrario al inicio del curso

Trabajo(s) práctico(s)
- Representarán el 25% de la nota final
- Obligatorio
- En grupos, salvo indicación en contrario al inicio del curso

Práctica final
- Representará el 25% de la nota final
- Tendrá carácter práctico
- Obligatorio e Individual

Examen final
- Representará el 25% de la nota final
- Tendrá carácter Teórico/Práctico
- Individual y de superación obligatoria

Consideraciones para superar la asignatura:
- La nota mínima en el examen será de 5.0
- Deberán entregarse todos los trabajos.

2. Convocatoria extraordinaria
La calificación de los estudiantes en la convocatoria extraordinaria se ajustará a las siguientes reglas:

a. El examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de los trabajos teórico/prácticos y la nota obtenida en el examen final. Dicho examen deberá aprobarse, en todo caso. Si se superó la práctica final no habrá de repetirse.
b. Si el estudiante no entregó los trabajos y prácticas, tendrá derecho a realizarlos (no necesariamente con el mismo enunciado) siguiendo el mismo esquema que los descritos en la convocatoria ordinaria.

En todo caso, serán criterios de evaluación para todos los entregables de los alumnos:
- La adecuada presentación formal de los documentos.
- El uso correcto del lenguaje, ateniéndose a las normas gramaticales, ortográficas y de estilo adecuada para documentos académicos.
- La utilización apropiada de la terminología técnica relacionada con la seguridad de la información
- La justificación de las decisiones tomadas y la actitud crítica frente a las mismas.
- La crítica constructiva de elementos, sistemas y mecanismos existentes, así como la propuesta de mejora que demuestre la aportación personal del alumno.
- La originalidad de los contenidos y el uso adecuado de referencias solventes que soporten los argumentos en los que se apoya el alumno.

Peso porcentual del Examen Final:	50
Peso porcentual del resto de la evaluación:	50

BIBLIOGRAFÍA BÁSICA

- Caballero, Pino Introducción a la criptografía (capítulo 4), Ra-Ma.
- Fúster, A.; De la Guía, D.; Hernández, L.; Montoya, F.; Muñoz, J. Técnicas Criptográficas de Protección de Datos (Capitulos 1, 2, 3 y 5), Ra-Ma.
- José Luis Blasco Díaz, Modesto J. Fabra Valls. El documento electrónico : aspectos jurídicos, tecnológicos y archivísticos, Centro de publicaciones Univ. Jaume I.
- Monografías Aranzadi Guía práctica de Ciberseguridad, Aranzadi Thomson Reuters, 2019

- Morant J.L; Ribagorda A.; Sancho J. Seguridad y Protección de la Información. , Centro de Estudios Ramón Areces, 1997
- Paar, C.; Pelzl, J. Understanding Cryptography, Springer, 2010
- Ronald L. Mendell Document Security: Protecting Physical and Electronic Content., Charles C Thomas Pub Ltd, 2007
- Sainz Peña, Rosa María Ciberseguridad: la protección de la información en un mundo digital, Ariel: Fundación Telefónica, 2016

BIBLIOGRAFÍA COMPLEMENTARIA

- Charlie Kaufman, Radia Perlman, Mike Speciner Network Security: Private Communication in a Public World (Chap. 2), Prentice Hall, Second edition (2002)
- Christoph Paar, Jan Pelzl Understanding cryptography (Chap. 1 & 6), Springer-verlag, 2010

RECURSOS ELECTRÓNICOS BÁSICOS

- Adobe, Inc. . A primer document on electronic document security: http://www.adobe.com/security/pdfs/acrobat_livecycle_security_wp.pdf
- Aula virtual de criptografía y seguridad de la información Crypt4you . Curso de privacidad y protección de comunicaciones digitales.: http://www.crypt4you.com/
- España. Boletín Oficial del Estado . Código de Derecho de la Ciberseguridad: https://www.boe.es/legislacion/codigos/codigo.php?id=173&modo=2&nota=0
- J. Manuel Lucena. . Criptografía y seguridad en computadores.: http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto
- J. Ramió . Libro Electrónico de Seguridad Informática y Criptografía (Cap. 2 y 3): http://www.criptored.upm.es/guiateoria/gt_m001a.htm
- VV.AA. . Intypedia, Enciclopedia de Seguridad de la Información (Cap. 1, 2 y 3): http://www.intypedia.com