ASIGNATURA DE MÁSTER:

SEGURIDAD INFORMÁTICA DE DATOS, SISTEMAS Y COMUNICACIONES

Curso 2012/2013

(Código:28803222)

1.PRESENTACIÓN

Hoy en día en la mayoría de redes industriales y de sistemas de procesos de control industrial, la mayor parte de las aplicaciones utilizan la red conocida popularmente como TCP/IP (redes basadas en el Internet Protocol o IP). Esto significa que cualquiera de los datos relevantes desde el punto de vista industrial, sea cual sea la aplicación, utiliza este transporte en red.

Esto hace particularmente importante que se tenga en cuenta siempre, como variable necesaria en el diseño y el uso de cualquier red que se utilice en cualquier proceso industrial, la seguridad asociada a los sistemas informáticos sobre los que funcionan las aplicaciones, también a los dispositivos de comunicaciones típicos de estas redes, especialmente encaminadores y conmutadores y, en general, la seguridad vista como un servicio básico que garantice la disponibilidad, fiabilidad y continuidad de las redes utilizadas.

Es desde esta óptica que se presenta esta asignatura, que pretende conseguir que los alumnos obtengan una serie de conocimientos fundamentales en el sentido citado de seguridad de datos, sistemas y comunicaciones, que serán muy necesarios en su trabajo profesional. Igualmente la asignatura pretende que los alumnos alcancen una serie de competencias relacionadas con el análisis de seguridad de las redes habituales, la creación de una política de seguridad particular para cada instalación y el mantenimiento y cumplimiento de la citada política de seguridad, siguiendo el criterio práctico de estándares internacionales como el existente sobre Sistemas de Gestión de Seguridad Informática, conocido como ISO/IEC 27001.

2.CONTEXTUALIZACIÓN

Esta asignatura forma parte del Módulo II que corresponde a los contenidos específicos optativos del itinerario o especialidad en “Ingeniería Telemática”. Esta asignatura, junto a las demás incluidas en el mismo itinerario, constituye la oferta de contenidos específicos que permiten al estudiante particularizar o diseñar según su interés su formación investigadora. Teniendo en cuenta la lógica relación que hay entre los contenidos de las asignaturas que forman cada especialidad, cada itinerario se ha definido como una materia que está compuesta por seis asignaturas, de 5 ECTS cada una, de las que el estudiante debe elegir y cursar cuatro.

La asignatura viene a completar y ampliar los conocimientos adquiridos por los alumnos durante sus estudios de grado, en particular de disciplinas tales como “Automatización industrial”, “Electrónica digital”, “Sistemas digitales avanzados y microprocesadores” y “Comunicaciones industriales”. Por tanto desarrolla, con más extensión temática y con un mayor nivel de intensidad conceptual y aplicativa, los aspectos científicos y tecnológicos de las aplicaciones industriales de las comunicaciones y sistemas en general.

Las principales competencias que se pretenden alcanzar son:

- Conocimiento teórico y práctico de lo que son los procesos de seguridad informática en una organización, tanto en los aspectos técnicos, como en los físicos y organizativos.
- Conocimiento de los distintos estándares involucrados en la disciplina, de los criptográficos (FIPS, RSA, X.509, etc.) como de los organizativos (ISO/IEC 27001, ISO/IEC 15480, CobIT) y de la legislación más importante aplicable en España, la LOPD (Ley Orgánica de Protección de Datos) y la LSSICE (Ley de Servicios de la Sociedad de la Información y Comercio Electrónico).

- Conocimiento de la clasificación de distintos tipos de ataques a la seguridad de sistemas y datos: denegación de servicio, acceso no permitido a datos, escalado de privilegios, etc. Clasificación de problemas actuales de seguridad para sistemas individuales: spam, virus, phishing, spyware, etc.
- Conocimiento y destreza técnica en el análisis de los principales problemas de seguridad asociados con los sistemas operativos de servidores y estaciones de trabajo, especialmente en el entorno de sistemas UNIX/LINUX.
- Conocimiento y destreza técnica en el análisis de los principales problemas de seguridad asociados con los sistemas operativos de dispositivos de comunicaciones, especialmente de encaminadores y conmutadores.
- Conocimiento de las principales herramientas dde seguridad en redes: cortafuegos, sistemas de detección de intrusiones (IDS) y analizadores de vulnerabilidades.
- Conocimiento práctico de las principales características de seguridad buscadas para los datos, ya sea estáticos en dispositivos de almacenamiento o dinámicos en su tráfico por la red. Análisis de la confidencialidad, integridad, autenticación y no repudio.
- Conocimiento básico de algoritmos criptográficos simétricos, asimétricos y funciones de una sola vía y destreza práctica para la decisión sobre dónde aplicarlos.
- Conocimiento práctico de protocolos criptográficos y de sistemas criptográficos: PGP, SSL, SET y su uso en comercio electrónico, IPSec y redes privadas virtuales.
- Conocimiento práctico de algunas herramientas de seguridad informática en sistemas, como nmap, tripwire, TCP wrappers, SpamAssasin, etc.
- Conocimiento de los problemas de disponibilidad de sistemas, almacenamiento y redes y de los protocolos y soluciones de alta disponibilidad para redes.
- Conocimiento en detalle de las soluciones actuales de alta disponibilidad para almacenamiento de datos: SAN (Storage Area Networks) y NAS (Network Available Storage).

3.REQUISITOS PREVIOS RECOMENDABLES

La asignatura no tiene requisitos específicos, si bien para su adecuado seguimiento y aprovechamiento se precisan conocimientos, a nivel de grado universitario, de algunas de las siguientes disciplinas: “Redes de ordenadores con protocolos TCP/IP”, “Electrónica digital” y “Comunicaciones industriales”.

4.RESULTADOS DE APRENDIZAJE

En esta asignatura de Master se analiza una amplia panorámica de los principales problemas de seguridad relacionados con sistemas, comunicaciones en redes IP y datos. Se estudian las vulnerabilidades técnicas de seguridad más habituales, haciendo énfasis en las más peligrosas por ser los más habituales y tratando de crear un espíritu crítico necesario para trabajar en este entorno intrínsecamente dinámico. Se clasifican los distintos tipos de ataques y las posibles defensas técnicas, tanto las que no utilizan la criptografía como herramienta como las que se basan en la misma. En este sentido, se analiza cómo los distintos tipos de algoritmos criptográficos permiten crear protocolos criptográficos y sistemas que permiten alcanzar las propiedades de seguridad más necesarias, como la autenticación, la privacidad y la integridad. Se pretende conseguir, en concreto, un conocimiento práctico sobre qué es y cómo se utiliza la firma digital. Se estudia cómo usar, y cuándo, algunas herramientas habituales de seguridad en sistemas abiertos como LINUX. Se pretende conseguir un conocimiento suficiente de los estándares de gestión de seguridad más extendidos, como el ISO/IEC 27001, así como de la legislación aplicable en España, como la LOPD. Por último se analizan los principales problemas de la disponibilidad de datos, sistemas y redes y sus soluciones más usadas, haciendo especial énfasis en soluciones de almacenamiento de datos en redes, como SAN o NAS.

A partir de este objetivo básico, se establecen los resultados del aprendizaje que debe alcanzar el estudiante:

- Identificar los diferentes tipos de ataques a redes, sistemas y datos en una organización, así como las soluciones más habituales empleadas para tratar de soslayarlos. Estudiar los diferentes protocolos de uso posible en las redes de comunicación estudiadas.
- Identificar los principales estándares de seguridad informática y la legislación española aplicable, que se utilizan para la creación de una política de seguridad de una organización concreta.

- Identificar las herramientas de seguridad más habituales como cortafuegos, IDS o aplicaciones de análisis de vulnerabilidades.
- Efectuar simulaciones de ataques y defensas sencillas en sistemas y redes.
- Entender, desde un punto de vista práctico, las diferentes aplicaciones de la criptografía a la seguridad informática, tanto en protocolos como en sistemas criptográficos, de manera que se comprenda cómo usar la firma digital o cómo se configura una red privada virtual.
- Identificar, y entender cómo funcionan, las soluciones más habituales al problema de la disponibilidad de sistemas, redes y almacenamiento de datos.
- Integrar las comunicaciones inalámbricas dentro de las redes analizadas y llevar a cabo un diseño concreto.

5.CONTENIDOS DE LA ASIGNATURA

Los contenidos temáticos para la asignatura "*Seguridad Informática de datos, sistemas y comunicaciones"* son los siguientes:

1-Introducción a los problemas de seguridad informática en sistemas, datos y redes de comunicación.
2-Clasificación de los distintos tipos de ataques a datos, sistemas y dispositivos de comunicación en redes.
3-Gestión de la seguridad, procesos organizativos, estándares y legislación aplicable.
4-La política de seguridad de sistemas y redes como herramienta organizativa.
5-Herramientas de seguridad en sistemas operativos.
6-Dispositivos de seguridad en redes: cortafuegos e IDS.
7-Introducción a la criptografía aplicada: algoritmos criptográficos básicos.
8-Autenticación y sistemas de firma digital.
9-Protocolos criptográficos: SSL, SET e IPSec. Redes Privadas Virtuales.
10-Problemas de disponibilidad de sistemas y de redes y sus soluciones.
11-Soluciones de alta disponibilidad para el almacenamiento de datos: SAN y NAS

6.EQUIPO DOCENTE

- GABRIEL DIAZ ORUETA
- MANUEL ALONSO CASTRO GIL
- ELIO SAN CRISTOBAL RUIZ

7.METODOLOGÍA

La asignatura "*Seguridad Informática de datos, sistemas y comunicaciones"* tiene las siguientes características generales:

1. Es una asignatura "a distancia" según modelo metodológico implantado en la UNED. Al efecto se dispondrá de los recursos incorporados al *Curso virtual* de la asignatura al que se tendrá acceso a través del portal de enseñanza virtual *UNED-e*. A través de los foros generales del curso virtual y del contacto personal mediante del correo electrónico, se le guiará y aconsejará sobre el ritmo de trabajo que debe llevar para que el seguimiento de la asignatura sea lo más regular y constante posible.
2. Dado que las actividades síncronas son reducidas, la planificación de su seguimiento y estudio permite su adaptación a estudiantes con diversas circunstancias personales y laborales. No obstante, en este sentido, suele ser aconsejable que en la medida de sus posibilidades, cada estudiante establezca su propio modelo de estudio y seguimiento lo más regular y constante posible.
3. Tiene un carácter predominantemente práctico, por lo que los planteamientos teóricos irán siempre

seguidos de la resolución de ejercicios.

Cronológicamente el estudiante debe estudiar y preparar cada tema siguiendo el orden dado a los contenidos, ya que cada uno se apoya en los anteriores.

8.BIBLIOGRAFÍA BÁSICA

ISBN(13): 9781580535168
Título: MISSION CRITICAL NETWORK PLANNING (Octubre de 2003)
Autor/es: Liotine Matthew ;
Editorial: Artech House Publishers

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9788436249750
Título: SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN (1ª)
Autor/es: Castro Gil, Manuel Alonso ; Díaz Orueta, Gabriel ; Peire Arroba, Juan ; Mur Pérez, Francisco ;
Editorial: UNED

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

Comentarios y anexos:

Forma también parte de la Bibliografía Básica el libro "*Seguridad en UNIX y Redes*, *versión 2.1*" de A. Villalón Huerta, 2002, versión disponible en el curso virtual de la asignatura.

9.BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13): 9780471117094
Título: APPLIED CRYPTOGRAPHY (1996)
Autor/es: Bruce Schneier ;
Editorial: : JOHN WILEY & SONS

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9780471253112
Título: SECRETS AND LIES
Autor/es: Bruce Schneier ;
Editorial: : JOHN WILEY & SONS

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9788420546001
Título: EL TAO DE LA MONITORIZACIÓN DE SEGURIDAD EN REDES (2005)
Autor/es: R. Bejtlich ;
Editorial: PEARSON EDUCACIÓN

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9788497053303
Título: RIESGO Y SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
Autor/es: Julian Marcelo ;
Editorial: UNIVERSIDAD POLITÉCNICA DE VALENCIA

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9789688805411
Título: REDES GLOBALES DE INFORMACIÓN CON INTERNET Y TCP/IP
Autor/es: D. E. Comer ;
Editorial: PEARSON-PRENTICE HALL

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

10.RECURSOS DE APOYO AL ESTUDIO

Curso Virtual

La plataforma aLF de e-Learning de la UNED proporcionará el adecuado interfaz de interacción entre el alumno y sus profesores. aLF es una plataforma de e-Learning y colaboración que permite impartir y recibir formación, gestionar y compartir documentos, crear y participar en comunidades temáticas, así como realizar proyectos online. Se ofrecerán las herramientas necesarias para que, tanto el equipo docente como los estudiantes, encuentren la manera de compaginar tanto el trabajo individual como el aprendizaje cooperativo.

Videoconferencia

La videoconferencia se contempla como una posibilidad de comunicación bidireccional síncrona con los estudiantes, tal y como se recoge en el modelo metodológico de educación distancia propio de la UNED. La realización de videoconferencias se anunciara a los estudiantes con antelación suficiente en el curso virtual de la asignatura.

11.TUTORIZACIÓN Y SEGUIMIENTO

La tutorización de los alumnos se llevará a cabo a través de la plataforma de e-Learning aLF o directamente por correo electrónico con el equipo docente:

Gabriel Díaz Orueta - gdiaz@ieec.uned.es
Elio San Cristóbal Ruiz - elio@ieec.uned.es
Manuel Castro Gil - mcastro@ieec.uned.es

12.EVALUACIÓN DE LOS APRENDIZAJES

Conforme al espíritu del Espacio Europeo de Educación Superior (EEES), el proceso de evaluación es continuo a lo largo del curso y está de acuerdo con la carga de trabajo, la organización del contenido y el calendario dados en la Guía de la Asignatura. El estudiante deberá realizar una serie de ejercicios y trabajos propuestos y, al final, un trabajo crítico de síntesis de la asignatura. También existe una Prueba Presencial con dos convocatorias (ordinaria en junio y extraordinaria en septiembre).

La nota de la asignatura se obtendrá fundamentalmente a partir de todos esos ejercicios y trabajos que se realizan a lo largo del curso y que corresponden a la evaluación continua de conocimientos a distancia. La participación del estudiante en la asignatura a lo largo del curso (foros, cursos virtuales, consultas, etc.) también será tenida en cuenta.

Los pesos de estos métodos de evaluación serán: un 50% a partir de los ejercicios propuestos y el trabajo final, un 30% de la Prueba Presencial y un 20% de la participación en el curso. En cualquier caso, para aplicar estos porcentajes es necesario aprobar la Prueba Presencial.

13.COLABORADORES DOCENTES

- LAURA POZUECO ALVAREZ