Guía Docente: Dirección de Proyectos de Seguridad Corporativos

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Grado en Ingeniería Informática
Plan de estudios	2012
Especialidad/Mención	Mención en Criptología y Seguridad de la Información
Materia	Criptología y Seguridad de la Información
Carácter	Optativo
Período de impartición	Segundo Trimestre
Curso	Cuarto
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	Ninguno

DATOS DEL PROFESORADO			
Profesor Responsable	Juan Agustín Fraile Nieto	**Correo electrónico**	juanagustin.fraile@ui1.es
Área	Tecnología Electrónica	**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	About.me LinKedin Twitter		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Auditoría y seguridad avanzada de sistemas y redes de comunicaciones • Autenticación y Sistemas Biométricos • Criptografía y Criptoanálisis • Dirección de Proyectos de Seguridad Corporativos • Técnicas de Análisis Forense • Técnicas de auditoría, ataque y programación segura de aplicaciones web
Contexto y sentido de la asignatura en la titulación y perfil profesional	En la asignatura de **Dirección de proyectos de seguridad corporativos**, el objetivo es que el alumnado adquiera los conocimientos necesarios para dirigir proyectos de seguridad informática en el contexto empresarial. Más concretamente, que sea capaz de: • Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente en lo referente a la protección de datos personales. • Ejercer las habilidades necesarias en los sectores y puestos profesionales vinculados al campo de la dirección y gestión informática. La dirección de proyectos en general, y de aquellos que involucran seguridad en los sistemas y datos informáticos, en particular, está regulada por normas (o buenas prácticas) y debe de cumplir cierta legislación. Por lo tanto, las tareas a llevar a cabo en esta asignatura, se apoyan en metodologías y estándares para los que ha sido probada su efectividad. Así se pretende aportar al alumno el conocimiento suficiente para afrontar la dirección de un proyecto de seguridad corporativo. El alumno debe tener en cuenta todos los conceptos que se tratan en la asignatura. La asignatura está relacionada con las materias que proporcionan los conocimientos básicos sobre sistemas de información, bases de datos y redes de comunicaciones.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CT06: Capacidad de trabajo en equipo. • CT09: Capacidad para innovar y generar nuevas ideas. • CU02: Identificar y dar valor a las oportunidades tanto personales como profesionales, siendo responsables de las actuaciones que se pongan en marcha, sabiendo comprometer los recursos necesarios, con la finalidad de realizar un proyecto viable y sostenible para uno mismo o para una organización. • CU03: Utilizar la expresión oral y escrita de forma adecuada en contextos personales y profesionales. • CU04: Utilizar las Tecnologías de la Información y la Comunicación (TICs) para poner en marcha procesos de trabajo ajustados a las necesidades de la sociedad actual. • CU15: Utilizar una adecuada estructura lógica y un lenguaje apropiado para el público no especialista y escribir con corrección. • CU16: Saber transmitir un informe técnico de la especialidad. • CMC05: Capacidad para identificar, comprender y solucionar las principales vulnerabilidades que afectan a las aplicaciones Web, así como para diseñar y programar éstas de forma segura. • CMC06: Capacidad para concebir, desarrollar y desplegar proyectos globales y políticas de seguridad corporativas, teniendo en cuenta criterios organizacionales, económicos y aspectos legales.
Resultados de aprendizaje de la asignatura	• Conoce el procedimiento adecuado para la implantación de una política de seguridad corporativa, e involucra convenientemente a la dirección de la empresa y al resto de recursos humanos. • Concibe, desarrolla y despliega proyectos globales y políticas de seguridad corporativas, teniendo en cuenta criterios organizacionales, económicos y aspectos legales. • Conoce los sistemas de información corporativos, sus principales diferencias con sistemas de menor tamaño, y las consecuencias de la incorporación de nuevas políticas de seguridad.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	Con el fin de cubrir también los aspectos relacionados con la dirección de proyectos de seguridad en la formación del estudiante, esta asignatura estudiará conceptos como medidas de seguridad física de los Sistemas de Información, la prevención de delitos corporativos o los aspectos de la legislación vigente relacionados con la seguridad.
Contenidos	**UD1: Normativas de Gestión de la Seguridad** • Introducción • Normas ISO • Serie ISO 20000 • Serie ISO 27000 • Metodología ITIL: Librería de infraestructuras de las tecnologías de la información. • Servicios de Internet y protección de datos de carácter personal. **UD2: Normativa sobre servicios de la sociedad de la información y protección de datos de carácter personal** • Servicios de la sociedad de la información • La protección de datos de carácter personal

UD3: Aplicación de la normativa de protección de datos de carácter personal

- Ley orgánica de protección de datos y garantía de derechos digitales (LOPDGDD).
- Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (RD 1720/2007).
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización.
- Reglamento General de Protección de Datos (RGPD)
- Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
- Realización de la auditoría bienal obligatoria de Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal

UD4: Sistemas de Gestión de Seguridad de la Información (SGSI)

- ¿Para qué la ISO/IEC 27001?
- Características de la norma
- Terminología
- Estructura de la norma
- Proceso de Implementación
- El proceso de Certificación

UD5: Metodología ITIL

- La Librería
    - ServiceStrategy - Estrategia de Servicios (SE)
    - ServiceDesign - Diseño de servicios (SD)
    - ServiceTransition - Transición de Servicios (ST)
    - ServiceOperation – Operaciones de Servicios (SO)
    - ContinualServiceImprovement - Mejora Continua de Servicios (CSI)
- ITIL® v4 en la práctica
- Las certificaciones ITIL® v4

UD6: Transacciones con BlockChain en IoT

- Las cadenas de bloques
- Internet de las cosas - IoT
- Blockchain en redes IoT
- Los contratos inteligentes
- Implementaciones y casos de uso

METODOLOGÍA	
Actividades formativas	La evaluación continua de la asignatura **Dirección de proyectos de seguridad corporativos** se articula sobre cuatro tipos básicos de actividades: **Estudios de caso:** En tres de las UD se plantea la realización de un estudio y un trabajo con algún tema de interés propio de la Unidad. Se trata de que el alumnado utilice los recursos necesarios para investigar y conocer determinados aspectos relacionados con los contenidos tratados en cada Unidad Didáctica. A partir de ahí, debe realizar una síntesis de su investigación y plasmarlo en un trabajo que siempre tiene en cuenta su aplicación en la práctica. **Actividades de contenidos teóricos:** Los contenidos básicos de la asignatura comprenden 6 unidades didacticas para el estudio de la materia. Cada unidad didáctica contiene actividades de autoevaluación y enlaces a recursos de interés para el aprendizaje. Además se pueden sugerir lecturas o resolución de ejercicios que no son objeto de evaluación pero facilitan y complementan el aprendizaje. En el aula virtual está disponible un espacio de recursos, en el que encontrar bibliografía complementaria o información útil para la ampliación de la teoría. **Foros de debate:** En este tipo de actividad se valora **la participación activa del alumnado y la interacción con los compañeros**, más que la mera aportación de una respuesta individual. Es recomendable antes de participar en foros de debate abiertos, revisar las aportaciones previas de otros compañeros, evitar repetir respuestas y mostrar capacidad de análisis objetivo del tema planteado. Además se plantean foros no evaluables que pueden guardar relación con noticias o cuestiones de interés para la asignatura. **Trabajos colaborativos:** Se trata de una sugerencia de indagación personal y en grupo en la propia red con el método, fundamentalmente, del trabajo colaborativo. En el desarrollo de cada actividad, en el aula, se establecen las características específicas de entrega, plazos, puntuación y cualquier otra información útil para su realización.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.* El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*.

El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera:

Sistema de evaluación convocatoria ordinaria

Opción 1. Evaluación continua

Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua.

Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de**

	evaluación de competencias que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final. Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria. Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior. En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado. En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura. Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	D. Drogseth. ITIL Resources Adoptions and Priorities: A Global View. Enterprise Management Associates (EMA). 2014 Recuperado de https://es.bluebottlebiz.com/resource/itil-resources-adoptions-and-priorities-a-global-view-1 Con la creación de Axelos en 2013, una empresa conjunta entre Capita y la Oficina de Proyectos del Reino Unido, surgió la posibilidad de reinvertir en la IT Infrastructure Library (ITIL) como la principal fuente mundial de mejores prácticas para la gestión de servicios. El crecimiento silencioso de ITIL durante la década de 1990 llevó a un crecimiento en los primeros años del nuevo siglo. Esto se produjo a medida que las organizaciones de TI intentaron hacerse cargo de sus servicios de una manera más cohesiva, más alineada con los negocios, más medida y más transversal que en el pasado. Los resultados de la investigación reafirman en gran medida el valor de ITIL, y lo hacen frente a esas mismas fuerzas, como la nube y agile, que algunos expertos de la industria afirman que hacen que ITIL sea menos relevante. Las investigaciones también sugieren claras prioridades sobre cómo las organizaciones de TI, los ejecutivos de TI y los profesionales pueden optimizar mejor el uso de los recursos de ITIL, y cómo ITIL podría evolucionar para apoyar la evolución continua de la gestión de servicios de TI. L. Gómez Fernández, P.P. Fernández Rivero. Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. Madrid: AENOR Ediciones. 2015. Recuperado de https://es.bluebottlebiz.com/resource/como-implantar-un-sgsi-segun-une-iso-iec-27001-2014-y-su-aplicacion-en-el-esquema-nacional-de-seguridad

	Este libro facilita una descripción de los conceptos y requisitos para la implantación efectiva de un Sistema de Gestión de Seguridad de la Información (SGSI), según la norma UNE-ISO/IEC 27001:2014; presentando ejemplos y casos prácticos. Asimismo, explica en qué consiste el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de obligado cumplimiento en el ámbito de la Administración Electrónica, y su aplicación mediante un sistema de gestión de seguridad de la información.
Bibliografía complementaria	A. Calder, S.G. Watkins. IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Ed. IT Governance Public. 2012 C.M. Fernández Sánchez y M. Piattini Velthuis. Modelo para el gobierno de las TIC basado en las normas ISO. Madrid: AENOR Ediciones. 2012. Recuperado de https://es.bluebottlebiz.com/resource/modelo-para-el-gobierno-de-las-tic-basado-en-las-normas-iso L. Gómez Fernández y A. Álvarez Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Madrid: AENOR Ediciones. 2012. Recuperado de https://es.bluebottlebiz.com/resource/guia-de-aplicacion-de-la-norma-une-iso-iec-27001-sobre-seguridad-en-sistemas-de-informacion-para-pymes B. Holtsnider y B.D. Jaffe. IT Manager's Handbook. Elsevier. 2012 Recuperado de https://es.bluebottlebiz.com/resource/it-manager-s-handbook J.M. Moreno Pérez y A.F. Ramos Pérez. Gestión de Servicios en el Sistema Informático. Certificado de Profesionalidad (MF0490_3). Ed. RAMA. 2014. Recuperado de https://es.bluebottlebiz.com/resource/gestion-de-servicios-en-el-sistema-informatico C.E. Saltor. La Protección de Datos Personales: Estudio Comparativo Europa-América con especial análisis de la situación Argentina. Tesis Doctoral. 2013. Recuperado de http://eprints.ucm.es/22832/1/T34731.pdf S.G. Watkins. An Introduction to Information Security and ISO27001:2013. It Governance. Ed. IT Governance Public. 2013. I. Lee y K. Lee. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440. 2015 M. Crosby, P. Pattanayak, S. Verma y V. Kalyanaraman. Blockchain technology: Beyond bitcoin. Applied Innovation, 2, 6-10. 2016 Y. Zhang y J. Wen. The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10(4), 983-994. 2017.
Otros recursos	J.A. Gómez Martínez (AENOR), Sistemas de Gestión Integrados. http://aenormas.aenor.es/es/mas-valor/todoslosvideos/sistemas-de-gestion-integrados Canal Youtube de la AEPD. https://www.youtube.com/user/desdelaAEPD/videos AEPD. Guía del Responsable de Ficheros https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf S.A. Nextel(2015) 5 aspectos importantes sobre la implantación ISO 27001 https://www.youtube.com/watch?v=wHT0n8ojTWw AENOR (2014) ISO 27001 Sistemas de Gestión de Seguridad de la Información https://www.youtube.com/watch?v=Tit3mCFBo2M Glosario de términos ITIL® v3 https://itservice.com.co/wp-content/uploads/Glosario-t%C3%A9rminos-y-definiciones-ITIL-4.pdf Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630 M.M. Sorrius. Seguridad en la Internet de las cosas. Estudio de IOTA para el Internet of Things. J.M. López y C.R. Herrero. Cutrecoin: cómo programar una criptodivisa desde cero y no morir en el intento. M. Weber. Cryptocurrencies and the Block Chain. S. Siewert. Why software engineers and developers should care about blockchain technology. white paper, April. 2018. H. Malviya. How Blockchain will Defend IOT. 2016. J.J. Karst y G. Brodar. Connecting multiple devices with blockchain in the internet of Thing. 2017.

COMENTARIOS ADICIONALES

La Seguridad de la Información describe actividades relacionadas con la protección de la información y de los activos de la infraestructura donde se encuentra la información, contra los riesgos de pérdida, uso erróneo, acceso indebido o daño. La Gestión de la Seguridad de la Información (Information Security Management -ISM-) describe los controles que debe implementar una organización para asegurarse de que está manejando esos riesgos. La ISM tiene una importancia crucial porque casi cualquier compañía realiza su trabajo usando redes internas para intercambiar información, pero además usan Internet.

Afronta esta materia con mente abierta y espíritu crítico. A partir de los conceptos, herramientas y definiciones básicas que asimiles debes ser capaz de realizar un toma de requisitos óptima que te ayude en la implementación de un producto de calidad.