Guía Docente: Dirección de Proyectos de Seguridad Corporativos

DATOS GENERALES	
Facultad	Facultad de Criminología
Titulación	Grado en Criminología
Plan de estudios	2012
Especialidad/Mención	Mención en Ciberseguridad
Materia	Informática
Carácter	Optativo
Período de impartición	Tercer Trimestre
Curso	Tercero
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No existen requisitos previos para esta asignatura.

DATOS DEL PROFESORADO			
Profesor Responsable	Juan Agustín Fraile Nieto	**Correo electrónico**	juanagustin.fraile@ui1.es
Área	Tecnología Electrónica	**Facultad**	Facultad de Criminología
Perfil Profesional 2.0	Doctor en Informática con amplia experiencia como docente de asignaturas relacionadas con las TIC y como tutor de proyectos de grado/máster. He colaborado en proyectos de investigación del ámbito de los sistemas inteligentes, las tecnologías móviles (NFC) y la gestión de proyectos. Además, realizo tareas como consultor en procesos de implantación de software. Emprendedor, con gran iniciativa y voluntad de abordar proyectos formativos innovadores. Acreditado como profesor contratado doctor y profesor de universidad privada por la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA). **About.me** **LinKedin** **Twitter**		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Aplicación de las TIC a la Práctica Profesional • Auditoría y seguridad avanzada de sistemas y redes de comunicaciones • Autenticación y Sistemas Biométricos • Dirección de Proyectos de Seguridad Corporativos • Fundamentos de Seguridad de la Información
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 corporativa 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 de proyectos. La dirección de proyectos en general, y de aquellos que involucran seguridad en los sistemas y datos corporativos, 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.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CU-04: 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. • CU-05: Realizar investigaciones basándose en métodos científicos que promuevan un avance en la profesión. • CU-06: Aprender a trabajar individualmente de forma activa. • CU-07: Valorar lo que suponen las nuevas formas de trabajo actuales, como es el teletrabajo y el trabajo en red y saber trabajar de forma colaborativa en ellas. • CU-08: Entender las prácticas y el trabajo colaborativo como una forma de aplicar la teoría y como una manera de indagar sobre la práctica valores teóricos. • CG-01: Capacidad de análisis, síntesis y organización. • CG-02: Comunicación oral y escrita en la lengua nativa. • CG-03: Conocimientos de una lengua extranjera y/o de informática, relativos al ámbito de estudio. • CG-04: Capacidad de gestión de la información. • CG-05: Resolución de problemas. • CG-06: Razonamiento crítico y aprendizaje autónomo. • CG-07: Motivación por la calidad. • CB-01 Poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio. • CB-03: Reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética. • CB-04: Transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. • CB-05: Desarrollar aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. • CE-16: Organizar y/o programar a su nivel el trabajo de la unidad/gabinete, adaptando procedimientos, produciendo información o instrucciones, previendo, asignando o distribuyendo tareas, recursos y materiales. • CMB-02: Capacidad para plantear, desarrollar y dirigir el proceso de auditoría de un sistema en red, de forma manual y a través del uso de herramientas automáticas, generando un informe que resume los resultados. • CMB-03 Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto, de acuerdo con los conocimientos adquiridos, la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas. • CMB-04: Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas. • CMB-06: Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión. • CMB-07: Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional. • CMB-08: Conocer y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos. • CMB-09 Conocer de las características, funcionalidades y estructura de los Sistemas Operativos y diseñar e implementar aplicaciones basadas en sus servicios.
Resultados de aprendizaje de la	• Busca y localiza información digital relevante para aplicarla a su ámbito de conocimiento.

asignatura	• Aplica herramientas y recursos para buscar información. • Presenta y difunde información a través de medios digitales con una calidad profesional. • Aplica correctamente estrategias de comunicación y de difusión de información en la red. • Domina los conceptos, las funciones y aplicaciones básicas, dispositivos e interrelación entre programas. • Aplica estrategias de comunicación e interacción en entornos virtuales correctamente. • Usa y aplica críticamente y de forma segura las TIC. • Es capaz de plantear, redactar, organizar y desarrollar proyectos de seguridad y auditoria informática. • Conocer las características, funcionalidades y estructura de los sistemas operativos, implementar aplicaciones así como diseñar soluciones a los problemas. • Conocer y tener la capacidad de analizar y valorar el impacto social y medioambiental de las soluciones técnicas, así como resolver los problemas con iniciativa, autonomía y creatividad. • Ser capaz de identificar, valorar y relacionar los activos de una organización con las amenazas a las que están expuestos. • Ser capaz de desarrollar y desplegar proyectos globales y políticas de seguridad corporativas, teniendo según el alcance establecido. • Conocer y saber utilizar las principales herramientas que permite obtener vulnerabilidades en los sistemas. • Conocer y saber utilizar las principales herramientas de análisis de red. • Conocer los principios generales sobre los cortafuegos, sus diferentes componentes, tipos diferentes y capacidad para poder crear reglas propias.

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** 1.1. Normas ISO. 1.2. Serie ISO 20000. 1.3. Serie ISO 27000. 1.4. Metodología ITIL: Librería de infraestructuras de las tecnologías de la información. 1.5. 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** 2.1. Servicios de la sociedad de la información. 2.2. La protección de datos de carácter personal.

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

3.1. Ley orgánica de protección de datos y garantía de derechos digitales (LOPDGDD).

3.2. Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (RD 1720/2007).

3.3. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización.

3.4. Reglamento General de Protección de Datos (RGPD).

3.5. Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007.

3.6. 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)

4.1. ¿Para qué la ISO/IEC 27001?

4.2 Características de la norma.

4.3. Terminología.

4.4. Estructura de la norma.

4.5. Proceso de Implementación.

4.6. El proceso de Certificación.

UD5: Metodología ITIL

5.1. La Librería.

5.2. ITIL® v4 en la práctica.

5.3. Las certificaciones ITIL® v4.

UD6: Transacciones con BlockChain en IoT

6.1. Las cadenas de bloques.

6.2. Internet de las cosas - IoT.

6.3. Blockchain en redes IoT.

6.4. Los contratos inteligentes.

6.5. 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. **Cuestionarios:** En formato tipo test que sirvan de repaso al alumno y además le permitan prepararse para el examen final. **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. 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. 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. **Prueba de Evaluación de Competencias (PEC):** Además, en el caso de optar por esta opción de evaluación (PEC+ examen final), el estudiante tendrá que realizar la prueba de evaluación de competencias (PEC). Esta prueba se define como una actividad integradora a través de la cual el estudiante deberá demostrar la adquisición de competencias propuestas en la asignatura, vinculadas principalmente al «saber hacer». Para ello hará entrega de un conjunto de evidencias en respuesta a los retos propuestos en esta prueba. La entrega se realizará antes de finalizar la asignatura.

EVALUACIÓN	
Sistema evaluativo	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.

Características de los exámenes

Los exámenes constarán de 30 ítems compuestos por un enunciado y cuatro opciones de respuesta, de las cuales solo una será la correcta. Tendrán una duración de 90 minutos y la calificación resultará de otorgar 1 punto a cada respuesta correcta, descontar 0,33 puntos por cada respuesta incorrecta y no puntuar las no contestadas. Después, con el resultado total, se establece una relación de proporcionalidad en una escala de 10.

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	Drogseth, D. (2014). ITIL Resources Adoptions and Priorities: A Global View. Enterprise Management Associates (EMA). 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 llevo 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. Marzo Portera, A., Macho-Quevedo Pérez-Victoria, A. (2004). *La auditoría de seguridad en la protección de datos de carácter personal.* Barcelona: Ed. Experiencia. La novedad más importante que en materia de seguridad ha introducido el Reglamento de la Ley de Protección de Datos ha sido, por un lado, la regulación de la medidas de

	seguridad que se deben aplicar a los datos contenidos en expedientes o ficheros manuales en papel y por otro lado, la obligación de auditar cada dos años el cumplimiento de estas medidas. Además refuerza las obligaciones de seguridad auditoría respecto de los ficheros y tratamientos de datos personales en soportes automatizados, obligando asimismo a auditar estos sistemas de información e instalaciones de tratamiento y almacenamiento de datos, al amenos cada dos años, y con carácter extraordinario siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.
Bibliografía complementaria	Gómez Fernández, L., Fernández Rivero, P.P. (2018). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.* Madrid: AENOR Ediciones. Recuperado de https://www.aenor.com/normas-y-libros/buscar-libros/detalle?c=3a8a528f-9180-e911-a84e-000d3a2fe6cc Calder, A., Watkins, S. G (2012). IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Ed. IT Governance Public. Fernández Sánchez, C. M. y Piattini Velthuis, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*. AENOR Ediciones. Gómez Fernández, L. y Andrés Álvarez, A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. AENOR. Holtsnider, B. & Jaffe, B.D. (2012). *IT Manager's Handbook*. Elsevier. Moreno Pérez, J.M. y Ramos Pérez, A.F. (2014). *Gestión de Servicios en el Sistema Informático. Certificado de Profesionalidad (MF0490_3).* Ed. RAMA. Saltor, C.E. (2013). La Protección de Datos Personales: Estudio Comparativo Europa-América con especial análisis de la situación Argentina. *Tesis Doctoral*. Watkins, S. G. (2013). An Introduction to Information Security and ISO27001:2013. It Governance. Ed. IT Governance Public. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, 6-10. Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, *10*(4), 983-994.
Otros recursos	• Gómez Martínez, J. A. (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 • Nextel, SA (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://es.scribd.com/doc/106390415/Glosario-de-Terminos-y-Acronimos-ITIL-v3 • 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

- Sorrius, M. M. Seguridad en la Internet de las cosas. Estudio de IOTA para el Internet of Things.
- López, J. M. M., & Herrero, C. R. Cutrecoin: cómo programar una criptodivisa desde cero y no morir en el intento.
- Weber, M. Cryptocurrencies and the Block Chain.
- Siewert, S. (2018). Why software engineers and developers should care about blockchain technology. *white paper, April*.
- Malviya, H. (2016). How Blockchain will Defend IOT.
- Karst, J. J., & Brodar, G. (2017). Connecting multiple devices with blockchain in the internet of

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.