Universidad de Alcalá

Estudio Propio: **EXPERTO EN GESTIÓN DE LA CIBERDEFENSA**

Código Plan de Estudios: **EL33**

Año Académico: **2018-2019**

ESTRUCTURA GENERAL DEL PLAN DE ESTUDIOS:

CURSO	Obligatorios		Optativos		Prácticas Externas	Memoria/ Proyecto	Créditos
	Créditos	Nº Asignaturas	Créditos	Nº Asignaturas	Créditos	Créditos	
1º	18	6					18
2º							
3º							
ECTS TOTALES	**18**	**6**					**18**

PROGRAMA TEMÁTICO:

ASIGNATURAS OBLIGATORIAS

Código Asignatura	Curso	Denominación	Carácter OB/OP	Créditos
702210	1	BASES DE CIBERSEGURIDAD	OB	3
702211	1	INTRODUCCIÓN A LA CIBERDEFENSA	OB	3
702212	1	ASPECTOS LEGALES, POLÍTICOS Y ÉTICOS DEL CIBERESPACIO	OB	3
702213	1	ASPECTOS DOCTRINALES. PLANEAMIENTO DE OPERACIONES	OB	3
702216	1	ANÁLISIS DE RIESGOS ESTÁTICO Y DINÁMICO	OB	3
702221	1	CONCIENCIA DE LA SITUACIÓN Y COMPARTICIÓN INFORMACIÓN	OB	3

Carácter: OB - Obligatoria; OP – Optativa

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2018-2019	
Estudio	Experto en Gestión de la Ciberdefensa (EL33)	
Nombre de la asignatura	BASES DE CIBERSEGURIDAD	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Bernardo Alarcos Alcázar	
Idioma en el que se imparte	Español	

1. DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

2. CONTENIDOS (Temario)

UD1. INTRODUCCIÓN A LA CRIPTOGRAFÍA

- Criptografía Clásica.
- Criptografía de Clave Simétrica.
- Criptografía de Clave Asimétrica.
- Criptografía Cuántica.

UD2. MECANISMOS CRIPTOGRÁFICOS

- Introducción a los sistemas criptográficos.
- Funciones Hash.
- Firma digital.
- Infraestructuras de clave pública.
- Funciones HMAC.
- Protocolos de autenticación.

UD3. APLICACIONES CRIPTOGRÁFICAS

- Comercio Electrónico.
- Redes Privadas Virtuales (VPN).
- Correo Electrónico Seguro.
- Seguridad en la Web.
- Establecimiento de sesiones seguras.
- Seguridad WIFI.

3. EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

4. BIBLIOGRAFÍA

Enlaces

1. Kriptopolis. http://www.kriptopolis.com/
   - Web dedicado a la criptografía en donde podrás mantenerte actualizado de los avances en este campo.
2. Hispasec. http://www.hispasec.com/
   - Web dedicado a la seguridad en general en donde puedes mantenerte actualizado sobre nuevas vulnerabilidades y noticias relacionadas con la seguridad.

Lecturas complementarias

1. Algoritmo AES (Anexo I de la Unidad I)
   - Descripción detallada del algoritmo AES.
2. Métodos de cifrado simétrico. (Anexo II de la Unidad I)
   - Descripción sobre la formas de usar los algoritmos simétricos, es necesario conocerlos para saber cuándo se requiere el uso de vector de inicialización en un algoritmo.
3. Intercambio de clave de Diffie Helmann. (Anexo III de la Unidad I)
   - Descripción detallada del funcionamiento de estos mecanismos para intercambiar un valor secreto.
4. Algoritmo RSA. (Anexo IV de la Unidad I).
   - Descripción detallada del algoritmo de clave simétrica más utilizado, el algoritmo RSA.
5. Criptografía basada en Curvas Elípticas. (Anexo V de la Unidad I).
   - Descripción detallada de los algoritmos basados en curvas elípticas y su uso y ventajas en la criptografía.

Bibliografía recomendada y complementaria

En la Unidad se hace referencias a bibliografía, que permite ampliar los conceptos tratados en el lugar de la referencia.

Laboratorio de criptografía

Se aconseja usar las herramientas didácticas cryptools versión 1 y 2 para hacer prácticas sobre los algoritmos criptográficos clásicos y modernos y poder usar herramientas de criptoanálisis.
https://www.cryptool.org/en/

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2018-2019	
Estudio	Experto en Gestión de la Ciberdefensa (EL33)	
Nombre de la asignatura	INTRODUCCIÓN A LA CIBERDEFENSA	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Ángel Gómez de Ágreda	
Idioma en el que se imparte	Español	

1. DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

2. CONTENIDOS (Temario)

UD1. EL CIBERESPACIO
- Introducción
- Definición y características
- El ciberespacio como escenario social y geoestratégico

UD2. CIBERSEGURIDAD Y CIBERDEFENSA
- Conceptos y estrategias.
- Amenazas en y desde el ciberespacio.

UD3. CIBERDEFENSA
- Conflicto en el ciberespacio.
- Aproximaciones internacionales a la ciberdefensa.
- Prospectiva sobre una posible evolución del ciberespacio.

3. EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

4. BIBLIOGRAFÍA

Enlaces

1. Asociación de Diplomados en Altos Estudios de la Defensa Nacional. Antiguos alumnos del CESEDEN. http://adalede.org/videoteca/videos-adalede/
2. "Cybersecurity" and Why Definitions Are Risky

http://isnblog.ethz.ch/intelligence/cybersecurity-and-the-problem-of-definitions

3. Cyber Security by the Numbers

http://www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html?goback=%2Egde_1836487_member_5800147705443401730#%21

4. La mano que mueve el ratón

http://revistasic.es/index.php?option=com_content&view=article&id=837&Itemid=820

5. Documento de opinión: Ciberespacio

http://www.ieee.es/contenido/noticias/2013/06/DIEEEO57-2013.html

6. La ciberseguridad: un riesgo, pero también una garantía para la libertad

http://abcblogs.abc.es/ley-red/public/post/la-ciberseguridad-un-riesgo-pero-tambien-una-garantia-para-la-libertad-15860.asp/

7. Cybersecurity: Authoritative Reports and Resources, by Topic

http://www.fas.org/sgp/crs/misc/R42507.pdf

Lecturas complementarias

- Monografías del CESEDEN

http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf

- El ciberespacio como entorno social y de conflicto

http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO17_CiberespacioConflicto_Agreda.pdf

- Why Cibersecurity must be defined by processs, not tech

http://blogs.wsj.com/cio/2014/12/11/why-cybersecurity-must-be-defined-by-process-not-tech/

- Miradas sobre el control de nuestras vidas: Huxley y Orwell

https://www.youtube.com/watch?v=vqTiSXnWD90, http://ssociologos.com/2013/10/18/miradas-sobre-el-control-de-nuestras-vidas-huxley-y-orwell/

- IV Jornadas de Estudios de Seguridad

http://iugm.es/publicaciones/colecciones/libros-investigacion/?id=142

- Center on Public Diplomacy

http://uscpublicdiplomacy.org/blog/hacking-diplomacy

- Geopolíticas en la nube

http://www.blog.rielcano.org/el-espectador-global-geopolitica-en-la-nube/

- The Strategic Significance of the Internet Commons

http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?lng=en&id=182692

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2018-2019	
Estudio	Experto en Gestión de la Ciberdefensa (EL33)	
Nombre de la asignatura	ASPECTOS LEGALES, POLÍTICOS Y ÉTICOS DEL CIBERESPACIO	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Ángel Gómez de Ágreda	
Idioma en el que se imparte	Español	

1. DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

2. CONTENIDOS (Temario)

UD1. ASPECTOS ÉTICOS, POLÍTICOS Y JURÍDICOS DEL CIBERESPACIO

- Introducción.
- Ética y Ciberespacio.
- Política y Ciberespacio.

UD2. ASPECTOS JURÍDICOS DE DERECHO NACIONAL

- La normativa sobre Ciberseguridad.
- El estado de la cooperación sobre ciberseguridad.
- La normativa española sobre ciberseguridad.

UD3. ASPECTOS JURÍDICOS DE DERECHO INTERNACIONAL

- El principio de prohibición del uso y de la amenaza de la fuerza.
- El derecho internacional de los conflictos armados.

3. EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

4. BIBLIOGRAFÍA

Enlaces

- BARRET JR., Barrington M., “Information Warfare: China’s Response to U.S. Technological Advantages”, International Journal of Intelligence and Counterintelligence 18, número 4 (2005), páginas 682–706. http://www.tandfonline.com/doi/abs/10.1080/08850600500177135
- BUCKLAND, Benjamin, "Democratic Governance Challenges of Ciber Security", DCAF, 2015. http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security

- COOK, Tim, "A message to our custormers", 16/02/2016, web de Apple:

http://www.apple.com/customer-letter/

- DEIBERT, Ronald, "The growing dark side of cyberspace", Penn State Journal of Law and International Affairs, volumen 1, tomo 2, noviembre de 2012.

http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1012&context=jlia

- FORSYTH, James W. y POPE, B., "Structural Causes and Cyber Effects. Why International Order is Inevitable in Cyberspace", Strategic Studies Quarterly, número de invierno de 2014.

http://www.au.af.mil/au/ssq/digital/pdf/winter_14/forsyth.pdf

- GARCÍA MEXÍA, Pablo, "Internet: el nuevo campo de batalla", Foro de la sociedad civil,

http://www.forosociedadcivil.org/internet-el-nuevo-campo-de-batalla-pablo-garcia-mexia/

- GARCÍA MEXÍA, Pablo, "La Ley en la Red", Blog de ABC.es.

http://abcblogs.abc.es/ley-red/

- International Strategy for Cyberspace,

https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

- JESCHKE, Rebecca, "EFF to Apple Shareholders: Your Company Is Fighting for All of Us", Electronic Frontier Foundation, 26/02/2016:

https://www.eff.org/es/deeplinks/2016/02/eff-apples-shareholders-meeting-statement-support

- KRUGER, L.G., "Internet governance and Developing countries: implications for India". RIS Policy Brief, núm. 63, marzo de 2014.

http://www.ris.org.in/sites/default/files/pdf/RIS%20Policy%20Brief-63.pdf

- KRUGER, L.G., "Internet governance and domain names system. Issues for Congress", Congressional Research Service, 23 de marzo de 2016.

https://www.fas.org/sgp/crs/misc/R42351.pdf

- LERIG, Lawrence, "Code", versión 2.0.

http://codev2.cc/download+remix/Lessig-Codev2.pdf

- LESSIG, Lawrence, "El código y otras leyes del ciberespacio", Taurus Digital, 2001.

http://www.nodo50.org/lecturas/lessig_el_codigo.htm

- LEWIS, J.A., "Internet Governance: Inevitable Transitions", CIGI (Center for International Governance Innovation), paper número 4, octubre de 2013.

https://www.cigionline.org/publications/2013/10/internet-governance-inevitable-transitions

- MAZANEC, B., "Why International Order in Cyberspace Is Not Inevitable", Strategic Studies Quarterly, verano de 2015.

http://www.au.af.mil/au/ssq/digital/pdf/Summer_2015/mazanec.pdf

- PERRY BARLOW, John, "A Declaration of Independence of Cyberspace". 8 de febrero de 1996. Disponible en

https://www.eff.org/es/cyberspace-independence

- SÁNCHEZ DE ROJAS, Emilio, "Cooperación internacional en temas de ciberseguridad", capítulo 5 de la Monografía 137 del CESEDEN "Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa, un reto prioritario", página 262. Publicaciones de Defensa, 2013, ISBN 978-84-9781-862-9Consultado el 22 de marzo de 2016.

http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/137_NECESIDAD_DE_UNA_CONCIENCIA_NACIONAL_DE_CIBERSEGURIDAD_LA_CIBERDEFENSA_UN_RETO_PRIORITARIO.pdf

- Sentencia del TJUE sobre el "Derecho al olvido".

http://www.abogacia.es/wp-content/uploads/2014/05/Sentencia-131-12-TJUE-derecho-al-olvido.pdf

- SINGH, Parminder Jeet, “India’s Proposal Will Help Take the Web out of U.S. Control,” Hindu Online, 17 de mayo de 2012,

http://www.thehindu.com/opinion/op-ed/article3426292.ece

- YANAKOGEORGOS, Panayotis A., "Internet governance and National Security", Strategic Studies Quarterly, volumen 6, número 3, otoño de 2012,

http://www.au.af.mil/au/ssq/2012/fall/yannakogeorgos.pdf

Bibliografía recomendada y complementaria

- LIBICKI, Martin, "Conquest in Cyberspace", New York, Cambridge University Press, 2007
- WU, Tim, "The Master Switch: The Rise and Fall of Information Empires", New York, Alfred A. Knopf, 2010, ISBN 978-0307390998
- ABBATE, Janet, "Inventing the Internet", The MIT Press, 1999, ISBN 9780262011723

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2018-2019	
Estudio	Experto en Gestión de la Ciberdefensa (EL33)	
Nombre de la asignatura	ASPECTOS DOCTRINALES. PLANEAMIENTO DE OPERACIONES	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Javier Lopez de Turiso y Sánchez	
Idioma en el que se imparte	Español	

1. DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

2. CONTENIDOS (Temario)

UD1. EL CIBERESPACIO COMO ENTORNO OPERATIVO

- Introducción a los instrumentos de poder de los estados.
- El instrumento de poder militar.
- El campo de batalla operativo: el ciberespacio.
- Conceptos del empleo militar en el ciberespacio.
- Doctrinas de empleo del poder militar en el ciberespacio

UD2. CAPACIDADES DE LA CIBERDEFENSA

- Capacidades requeridas para operar en el ciberespacio.
- Fuerzas de ciberdefensa. Estructura y organización.

UD3. OPERACIONES MILITARES EN EL CIBERESPACIO

- Operaciones en el ciberespacio. Carácter estratégico, operacional y táctico.
- Operaciones específicas, conjuntas y combinadas (necesidad de autoridad de control del CS).
- Guerra electrónica y ciberespacio.
- Planeamiento de operaciones en el ciberespacio.

3. EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

4. BIBLIOGRAFÍA

Cyber Doctrine Towards a coherent evolutionary framework for learning resilience
JP MacIntosh, J Reid and LR Tyler

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2018-2019	
Estudio	Experto en Gestión de la Ciberdefensa (EL33)	
Nombre de la asignatura	ANÁLISIS DE RIESGOS ESTÁTICO Y DINÁMICO	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Juan Ramón Bermejo Higuera	
Idioma en el que se imparte	Español	

1. DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

2. CONTENIDOS (Temario)

UD1. INTRODUCCIÓN AL ANÁLISIS Y GESTIÓN DEL RIESGO ESTÁTICO Y DINÁMICO

- Introducción al Análisis y gestión de Riesgos.
- Sistemas de Gestión de Seguridad de la Información.
- Metodologías de Análisis y gestión de Riesgos.
- Modelado de amenazas en Aplicaciones.

UD2. PROYECTOS DE ANÁLISIS Y GESTIÓN DE RIESGOS

- Proyectos de Análisis y gestión de Riesgos AARR.
- Herramienta PILAR.

UD3. ANÁLISIS Y GESTIÓN DEL RIESGO DINÁMICO (DRA)

- Introducción al Análisis y Gestión del riesgo dinámico.
- Arquitecturas y tecnologías DRA.
- DRA framework: Sistema CAESARS.

3. EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:

- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

4. BIBLIOGRAFÍA

Enlaces

1. SGSI: NIST RMF:
    - Risk management framework del NIST.

http://csrc.nist.gov/groups/SMA/forum/documents/Forum-121410-Continuous-Monitoring-AJohnson.pdf

2. SGSI: ISO 27001:
    - Portal en español de la ISO 27001

http://www.iso27000.es/sgsi.html

3. SGSI: ENS:
    - Esquema Nacional de Seguridad

http://ametic.es/sites/default/files//media/INTECO%20-%20Implantaci%C3%B3n%20del%20ENS.pdf
https://www.ccn-cert.cni.es/publico/ens/ens/index.html?n=2.html

4. GUÍA STIC 825 sobre el Esquema Nacional de Seguridad:
    - https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html

5. GUÍA STIC 801 Responsabilidades y funciones en el ENS:
    - https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

6. MAGERIT. Ministerio de Administraciones Públicas de España MAP.
    - MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. Actualizada en 2012 en su versión

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VDUaiU0cTUA

7. STRIDE de Microsoft. Security Risk Management Guide, de Microsoft.
    - Método de modelado de amenazas de la empresa Microsoft.

http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx
http://www.microsoft.com/en-us/download/details.aspx?id=14719

8. OWASP thread modeling en aplicaciones web:

https://www.owasp.org/index.php/Application_Threat_Modeling
https://www.owasp.org/index.php/Modelado_de_Amenazas

9. Microsoft thread modeling en aplicaciones web:
    - https://msdn.microsoft.com/en-us/library/ff648644.aspx

10. Diversos métodos de modelado de amenazas en aplicaciones en comparación:
    - http://fortinux.com/wp-content/uploads/2010/12/Analisis-y-Modelado-de-Amenazas.pdf

11. Information Technology Baseline Protection Manual
    - Sitio web donde se puede encontrar catálogos de salvaguardas

http://en.wikipedia.org/wiki/IT_Baseline_Protection_Catalogs

12. ISO/IEC 13335-1:2004
    - Norma ISO donde se puede encontrar catálogos de salvaguardas.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39066

13. BugTraq.
    - Foros de discusión de seguridad públicos sobre análisis de riesgos.

http://www.securityfocus.com/archive/1
http://catless.ncl.ac.uk/Risks

14. VulnWatch.
    - Listas de direcciones públicas de sistemas atacados

http://www.vulnwatch.org/

Lecturas complementarias

1. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método. Ministerio de Hacienda y Administraciones Públicas.
    - Método de análisis de riesgos de MAGERIT.
    - http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.U2_oe2CKB2E.

2. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos. Método. Ministerio de Hacienda y Administraciones Públicas.
    - Catálogo de elementos de tipos de activos, dimensiones de valoración, criterios de valoración, dimensiones de valoración, amenazas, y salvaguardas.
    - http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.U2_oe2CKB2E.

3. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas. Método. Ministerio de Hacienda y Administraciones Públicas.
    - Describe algunas técnicas utilizadas en análisis y gestión de riesgos
    - http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.U2_oe2CKB2E.

4. Herramienta PILAR de análisis de riesgos de uso obligatorio en la Administración pública de España, y oficial en la OTAN (Organización del Tratado del Atlántico Norte).
    - Manual de usuario de la herramienta de análisis de riesgos PILAR
    - Herramienta de análisis de riesgos de la Administración pública del Estado. Español y oficial en la OTAN (Organización del Tratado del Atlántico Norte). Permite analizar los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (accountability).
    - http://www.ar-tools.com/es/index.html
    - https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/pilar.html

5. CIGITAL's architectural risk analysis process.
    - Método de análisis de riesgo arquitectónico para aplicaciones.

https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/architecture/10-BSI.html

6. ASSET (Automated Security Self-Evaluation Tool). National Institute on Standards and Technology (NIST).
    - Método de análisis de riesgos del NIST de los EEUU.

http://csrc.nist.gov/archive/asset/index.html

7. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). SEI de la Universidad Carnegie Mellon.
    - Método de análisis de la Universidad Carnegie Mellon.

http://www.sei.cmu.edu/library/abstracts/reports/99tr017.cfm

8. CRAMM. CCTA Risk Analysis and Management Method.
    - Metodología de análisis de riesgos del Reino Unido
    - http://www.cramm.com/

9. Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers. Guía NIST SP 800-53. Recommended Security Controls for Federal Information Systems.
- Contiene un catálogo de salvaguardas.
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

10. NIST 800-30 rev1 Risk Management Guide for Information Technology Systems, 2012.
- Guía del NIST para la realización de análisis de riesgos. 2012
- http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Vídeos recomendados y complementarios

1. Lección 11: Análisis y gestión de riesgos (intypedia)
   - Video que indica los pasos que hay que seguir para realizar un correcto análisis de las amenazas a las que puede enfrentarse un sistema de información, su impacto y la consiguiente gestión de riesgos, recomendando algunas metodologías.

https://www.youtube.com/watch?v=EgiYIIJ8WnU

2. SGSI - 07 Los activos de Seguridad de la Información.
   - La implantación de un SGSI tiene como objetivo proteger la información, el activo más importante en una empresa. Para ello una de las tareas principales en su implantación es analizar las dependencias y la relevancia de los activos.

https://www.youtube.com/watch?v=THnQ2FH7NtU

3. SGSI - 08 Análisis y valoración de riesgos. Metodologías.
   - Video del INTECO. Un negocio debe hacer frente al análisis y valoración de riesgos a los que está expuesto. Esta tarea, aplicando las distintas metodologías, permitirá delimitar claramente las áreas que deben ser protegidas así como el impacto económico y la probabilidad realista de que ocurra un incidente de cada uno de ellos. También se realiza una demostración de los ataques populares.

https://www.youtube.com/watch?v=g7EPuzN5Awg

4. SGSI - 09 Gestión y tratamiento de los riesgos
   - Video del INTECO. A la hora de implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) es necesario conocer en qué consiste la gestión de riesgos y cómo se deben escoger y documentar los controles que se van a aplicar.

https://www.youtube.com/watch?v=9T9X0q2y6vQ

5. SGSI - 10 Seguimiento, monitorización y registro de las operaciones de sistema.
   - Video del INTECO. Uno de los requisitos más importantes de la Norma UNE/ISO-IEC 27001 es la revisión que la dirección de la organización debe realizar con una cierta periodicidad, como mínimo anual, al Sistema de Gestión de Seguridad de la Información.

https://www.youtube.com/watch?v=Z5vaQn7bGhA

6. SGSI - 11 Gestión de la continuidad de negocio
   - Video del INTECO. Con el fin de no comprometer la actividad normal de una empresa se desarrollan diseños que constan de varias tareas encaminadas a la obtención de un plan de continuidad eficaz y viable que permita a la organización recuperarse tras un incidente.

https://www.youtube.com/watch?v=KbwhvivHNDI

7. SGSI - 12 Proceso de certificación.

- Video del INTECO. Certificar un SGSI según la Norma UNE/ISO-IEC 27001 significa obtener un "Documento" que reconoce y avala la correcta adecuación del Sistema de Gestión de Seguridad de la Información mejorando la confianza de clientes y proveedores.

https://www.youtube.com/watch?v=OQCVpiVCR9k

8. Threat Modeling Tool 2014 Demo
    - Emil Karafezov explica las nuevas características de nueva herramienta de modelado de amenazas: Microsoft Modeling Tool 2014.

https://www.youtube.com/watch?v=G2reie1skGg

9. Threat Modeling Tool principles
    - Interesante vídeo sobre la herramienta de modelado de amenazas de Microsoft.

https://www.youtube.com/watch?v=wUt8gVxmO-0

Bibliografía recomendada y complementaria

1. Marta Castellaro, Susana Romaniz, Juan Carlos Ramos, Carlos Feck, Ivana Gaspoz. Aplicar el Modelo de Amenazas para incluir la Seguridad en el Modelado de Sistemas. Argentina, Universidad Tecnológica Nacional, Facultad Regional Santa Fe. Disponible: http://docplayer.es/1665552-Aplicar-el-modelo-de-amenazas-para-incluir-la-seguridad-en-el-modelado-de-sistemas.htmlmodelado-de-sistemas.html

2. Carlos Ignacio Feck. Modelado de Amenazas, una herramienta para el tratamiento de la seguridad en el diseño de sistemas. UTN – Facultad Regional Santa Fe. Disponible en: http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3(2).pdf

3. Daniel P.F. Análisis y Modelado de Amenazas. Una revisión detallada de las metodologías y herramientas emergentes. Metal AT/DOT hacktimes.com. Año 2006. Disponible: https://fortinux.com/wp-content/uploads/2010/12/Analisis-y-Modelado-de-Amenazas.pdf

4. M. Castellaro, S. Romaniz, J.C. Ramos,C. Feck e I. Gaspoz, “Aplicar el Modelo de Amenazas para incluir la Seguridad en el Modelado de Sistemas”, CIBSI, 2009.

5. A. Shostack, “Experiences Threat Modeling at Microsoft”, Microsoft, 2008. Disponible: http://www.homeport.org/~adam/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf

6. Presentación de Microsoft. Introduction to Microsoft® Security Development Lifecycle (SDL) Threat Modeling. Disponible: http://www.microsoft.com/en-us/download/details.aspx?id=16420

7. Gary McGraw. Software Security: Building Security In. Addison Wesley Professional. Año 2005. ISBN-10: 0-321-35670-5.

8. ISO/IEC 17799:2005 – 27002:2005. Code of practice for information security management

9. UNE 71502:2004. Especificaciones para los sistemas de gestión de la seguridad de la información

10. ISO/IEC 17799:2000 | UNE-ISO/IEC 17799:2002. Código de buenas prácticas para la Gestión de la Seguridad de la Información.

11. ISI/IEC 27000 (ISMS). Information technology – Security techniques – Information security management systems

- 200x: 27000: Glossary [GMITS-1 y 2 – MICTS-1]
- 2005: 27001: Requirements [BS 7799-2 – UNE 71502]
- 2005: 27002: Code of practice for information security management [BS 7799-1 – 17799:2000 – UNE 17799:2002 – 17799:2005]
- 200x: 27003: Implementation guidance
- 200x: 27004: Measurements
- 200x: 27005: Risk management
- xxx: 27006 – 27009:

Universidad de Alcalá

GUÍA DOCENTE

Año académico	2018-2019	
Estudio	Experto en Gestión de la Ciberdefensa (EL33)	
Nombre de la asignatura	CONCIENCIA DE LA SITUACIÓN Y COMPARTICIÓN INFORMACIÓN	
Carácter (Obligatoria/Optativa)	OB	
Créditos (1 ECTS=25 horas)	3	
Modalidad (elegir una opción)		Presencial
		Semipresencial
	x	On-line
Profesor responsable	Miguel Ángel Pérez Sánchez	
Idioma en el que se imparte	Español	

1. DISTRIBUCIÓN DE CRÉDITOS (especificar en horas)

Número de horas presenciales/on-line asistencia profesor	30
Número de horas de trabajo personal del estudiante	45
Total horas	75

2. CONTENIDOS (Temario)

UD1. CAPACIDADES DE EXPLOTACIÓN. Parte I
- Introducción.
- La conciencia situacional
- Concepto de empleo de la conciencia de la situación cibernética.

UD2. CAPACIDADES DE EXPLOTACIÓN. Parte II
- Enfoque conceptual de la conciencia de la situación cibernética.
- Necesidades de la conciencia de la situación cibernética.
- Conciencia situacional para la ciberdefensa.

UD3. CAPACIDADES DE EXPLOTACIÓN. Parte III
- La conciencia situacional cibernética en apoyo al planeamiento.
- Visualización de la información.
- Colaboración y compartición de la información.

3. EVALUACIÓN

La evaluación de los alumnos se realiza teniendo en cuenta las siguientes valoraciones:
- Unidades Didácticas: 70% de la nota total de la asignatura. Controles de seguimiento conformados por una sala de debate, un test por cada unidad y un caso práctico por cada unidad
- Examen Final: 30% de la nota total de la asignatura.

4. BIBLIOGRAFÍA

Documentación complementaria
1. Enlaces de interés sobre Conciencia de la situación

https://www.dhs.gov/sites/default/files/publications/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20and%20Decision%20Support.pdf
http://www.esri.com/library/whitepapers/pdfs/situational-awareness.pdf
https://www.raes-hfg.com/crm/reports/sa-defns.pdf
https://www.nap.edu/read/6173/chapter/9
http://wikiofscience.wikidot.com/quasiscience:situational-awareness
https://www.stratfor.com/weekly/practical-guide-situational-awareness
http://www.skybrary.aero/index.php/Situational_Awareness
https://www.nap.edu/read/6173/chapter/9#182
https://www.army.gov.au/our-future/blog/situational-awareness
https://es.wikipedia.org/wiki/Consciencia_situacional

2. Textos sobre temas relativos a conciencia de la situación
a. A Review of Situation Awareness Literature Relevant to Pilot Surveillance Functions. John Uhlarik. DIANE Publishing, 2002
b. Situational Awareness. Eduardo Salas. Routledge, Julio 2017
c. Human Performance, Workload, and Situational Awareness Measures Handbook, Second Edition. Valerie J. Gawron. CRC Press, 2008