TEMARIO MÁSTER EN PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

ORGANIZA

UNIVERSIDAD COMPLUTENSE MADRID

isms forum

DIPLOMATURA ESPECIALIZACIÓN EN PROTECCIÓN DE DATOS (180H - 36 SESIONES) - 24 ECTS	
Dominio	Subdominio
	DOMINIO 1: NORMATIVA GENERAL DE PROTECCIÓN DE DATOS
	Conferencia magistral Presentación máster
1.1. Contexto normativo.	1.1.1. Privacidad y protección de datos en el panorama internacional. 1.1.2. La protección de datos en Europa. 1.1.3. La protección de datos en España. 1.1.4. Estándares y buenas prácticas.
1.2. El Reglamento Europeo de Protección de datos y actualización de LOPD. Fundamentos	1.2.1. Ámbito de aplicación. 1.2.2. Definiciones. 1.2.3. Sujetos obligados.
1.3. El Reglamento Europeo de Protección de datos y actualización de LOPD. Principios	1.3.1. El binomio derecho/deber en la protección de datos. 1.3.2. Licitud del tratamiento. 1.3.3. Lealtad y transparencia. 1.3.4. Limitación de la finalidad. 1.3.5. Minimización de datos. 1.3.6. Exactitud.
1.4. El Reglamento Europeo de Protección de datos y actualización de LOPD. Legitimación	1.4.1. El consentimiento: otorgamiento y revocación. 1.4.2. El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado. 1.4.3. Consentimiento de los niños. 1.4.4. Categorías especiales de datos. 1.4.5. Datos relativos a infracciones y condenas penales. 1.4.6. Tratamiento que no requiere identificación. 1.4.7. Bases jurídicas distintas del consentimiento.
1.5. Derechos de los individuos.	1.5.1. Transparencia e información. 1.5.2. Acceso, rectificación, supresión (olvido). 1.5.3. Oposición. 1.5.4. Decisiones individuales automatizadas. 1.5.5. Portabilidad. 1.5.6. Limitación del tratamiento. 1.5.7. Excepciones a los derechos.
1.6. El Reglamento Europeo de Protección de datos y actualización de LOPD. Medidas de cumplimiento	1.6.1. Las políticas de protección de datos. 1.6.2. Posición jurídica de los intervinientes. Responsables, co-responsables, encargados, subencargado del tratamiento y sus representantes. Relaciones entre ellos y formalización. 1.6.3. El registro de actividades de tratamiento: identificación y clasificación del tratamiento de datos.
1.7. El Reglamento Europeo de Protección de datos y actualización de LOPD. Responsabilidad proactiva.	1.7.1. Privacidad desde el diseño y por defecto. Principios fundamentales. 1.7.2. Evaluación de impacto relativa a la protección de datos y consulta previa. Los tratamientos de alto riesgo. 1.7.3. Seguridad de los datos personales. Seguridad técnica y organizativa. 1.7.4. Las violaciones de la seguridad. Notificación de violaciones de seguridad. 1.7.5. El Delegado de Protección de Datos (DPD). Marco normativo. 1.7.6. Códigos de conducta y certificaciones.

1.8. El Reglamento Europeo de Protección de datos. Delegados de Protección de Datos (DPD, DPO o Data Privacy Officer)	1.8.1. Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses. 1.8.2. Obligaciones y responsabilidades. Independencia. Identificación y reporte a dirección. 1.8.3. Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones. 1.8.4. Comunicación con la autoridad de protección de datos. 1.8.5. Competencia profesional. Negociación. Comunicación. Presupuestos. 1.8.6. Formación. 1.8.7. Habilidades personales, trabajo en equipo, liderazgo, gestión de equipos.
	Práctica 1 Dominio 1
1.9. El Reglamento Europeo de Protección de datos y actualización de LOPD. Transferencias internacionales de datos	1.9.1. El sistema de decisiones de adecuación. 1.9.2. Transferencias mediante garantías adecuadas. 1.9.3. Normas Corporativas Vinculantes. 1.9.4. Excepciones. 1.9.5. Autorización de la autoridad de control. 1.9.6. Suspensión temporal. 1.9.7. Cláusulas contractuales.
1.10. El Reglamento Europeo de Protección de datos y actualización de LOPD. Las Autoridades de Control	1.10.1. Autoridades de Control. 1.10.2. Potestades. 1.10.3. Régimen sancionador. 1.10.4. Comité Europeo de Protección de Datos. 1.10.5. Procedimientos seguidos por la AEPD. 1.10.6. La tutela jurisdiccional. 1.10.7. El derecho de indemnización.
1.11. Directrices de interpretación del RGPD	1.11.1. Guías del GT art. 29. 1.11.2. Opiniones del Comité Europeo de Protección de Datos. 1.11.3. Criterios de órganos jurisdiccionales.
	Práctica 2 Dominio 1
1.12. **Normativas sectoriales** afectadas por la protección de datos	1.12.1. Sanitaria, Farmacéutica, Investigación. 1.12.2. Protección de los menores. 1.12.3. Solvencia Patrimonial. 1.12.4. Telecomunicaciones. 1.12.5. Videovigilancia. 1.12.6. Seguros. 1.12.7. Publicidad, etc.
1.13. **Normativa española** con implicaciones en protección de datos	1.13.1. LSSI, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. 1.13.2. LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. 1.13.3. Ley firma-e, Ley 59/2003, de 19 de diciembre, de firma electrónica.

1.14. **Normativa europea** con implicaciones en protección de datos	1.14.1. Directiva e-Privacy: Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas) o Reglamento e-Privacy cuando se apruebe. 1.14.2. Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores. 1.14.3. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
	Práctica 3 Dominio 1
	DOMINIO 2: RESPONSABILIDAD ACTIVA
2.1. Análisis y gestión de riesgos de los tratamientos de datos personales	2.1.1. Introducción. Marco general de la evaluación y gestión de riesgos. Conceptos generales. 2.1.2. Evaluación de riesgos. Inventario y valoración de activos. Inventario y valoración amenazas.Salvaguardas existentes y valoración de su protección. Riesgo resultante. 2.1.3. Gestión de riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo inasumible.
	2.2. Metodologías de análisis y gestión de riesgos
	Práctica 1 Dominio 2
2.3. Programa de cumplimiento de Protección de Datos y Seguridad en una organización	2.3.1. El Diseño y la implantación del programa de protección de datos en el contexto de la organización. 2.3.2. Objetivos del programa de cumplimiento. 2.3.3. Accountability: La trazabilidad del modelo de cumplimiento.
2.4. Seguridad de la información	2.4.1. Marco normativo. Esquema Nacional de Seguridad y directiva NIS: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Ámbito de aplicación, objetivos, elementos principales, principios básicos y requisitos mínimos.
	2.4.2. Ciberseguridad y gobierno de la seguridad de la información. Generalidades, Misión, gobierno efectivo de la Seguridad de la Información (SI). Conceptos de SI. Alcance. Métricas del gobierno de la SI. Estado de la SI. Estrategia de SI.
	2.4.3. Puesta en práctica de la seguridad de la información. Seguridad desde el diseño y por defecto. El ciclo de vida de los Sistemas de Información. Integración de la seguridad y la privacidad en el ciclo de vida. El control de calidad de los SI.
	Práctica 2 Dominio 2
2.5. Evaluación de Impacto de Protección de Datos “EIPD”	2.5.1. Introducción y fundamentos de las EIPD: Origen, concepto y características de las EIPD. Alcance y necesidad. Estándares.
	2.5.2. Realización de una evaluación de impacto. Aspectos preparatorios y organizativos, análisis de la necesidad de llevar a cabo la evaluación y consultas previas.
	Práctica 3 Dominio 2

	DOMINIO 3: TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS
3.1. La auditoría de protección de datos	3.1.1. El proceso de auditoría. Cuestiones generales y aproximación a la auditoría. Características básicas de la Auditoría. 3.1.2. Elaboración del informe de auditoría. Aspectos básicos e importancia del informe de auditoría. 3.1.3. Ejecución y seguimiento de acciones correctoras.
3.2. Auditoría de Sistemas de Información	3.2.1. La Función de la Auditoría en los Sistemas de Información. Conceptos básicos. Estándares y Directrices de Auditoría de SI. 3.2.2. Control interno y mejora continua. Buenas prácticas. Integración de la auditoria de protección de datos en la auditoria de SI. 3.2.3. Planificación, ejecución y seguimiento.
3.3. La gestión de la seguridad de los tratamientos	3.3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI). 3.3.2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación. 3.3.3. Recuperación de desastres y Continuidad del Negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación del Desastres.
	Práctica 1 Dominio 3
3.4. Otros conocimientos	3.4.1. El cloud computing. 3.4.2. Los Smartphones. 3.4.3. Internet de las cosas (IoT). 3.4.4. Big data y elaboración de perfiles. 3.4.5. Redes sociales. 3.4.6. Tecnologías de seguimiento de usuario.
	3.4.7. Protección de Datos e Inteligencia Artificial
	Práctica 2 dominio 3
	Conferencia cierre - La práctica del DPO

DIPLOMATURA EN ESPECIALIZACIÓN EN CIBERSEGURIDAD (150H - XX SESIONES) - 20 ECTS	
Dominio	Subdominio
	Módulo 1
	Conferencia magistral
1. GOBIERNO DE SEGURIDAD	1.1 Arquitecturas de Seguridad 1.2 Introducción y Gestión de Ciberseguridad
	1.3 Organización Roles y Responsabilidades 1.4 Gobierno de ciberseguridad 1.5 Auditoría y control de la seguridad 1.6 Certificación y acreditación de productos y sistemas
	1.7 Seguridad en entornos Cloud (IaaS, PaaS, SaaS): Modelos y Controles exigibles
2. ANÁLISIS Y GESTIÓN DE RIESGOS	2.1 La identificación y gestión de riesgos 2.2 Análisis y gestión de riesgos y amenazas 2.3 Riesgos Tecnológicos
3. CUMPLIMIENTO LEGAL Y NORMATIVO	3.1 Cumplimiento Legal 3.2 Aspectos legales y regulatorios asociados a Privacidad, Seguridad, e IC 3.3 Técnicas, metodologías y herrramientas del compliance legal 3.4 Notificación, reporte, denuncia y presentación en juzgado 3.5 Cibercrimen y delitos informativos
	Ejercicio práctico Módulo 1
	Módulo 2
4. OPERATIVA DE CIBERSEGURIDAD	4.1 Procotolos de cifrado y aplicación criptográfica
	4.2 Monitorización de seguridad 4.3 Tecnologías de ciberseguridad 4.4 Desarrollo seguro 4.5 Criptografía
	4.6 Análisis de vulnerabilidades 4.7Hacking ético 4.8 Seguridad del Directo Activo y parque Windows 4.8.1 Directivas y GPOs 4.8.2 Configuración segura 4.8.3 Modelos de capas TIER 4.8.4 Recomendaciones de seguridad
5. CIBER INTELIGENCIA, COOPERACIÓN Y CAPACIDAD	4.9 Seguridad en el acceso Remoto y el teletrabajo. 4.9.1 Roles: Usuarios privilegiados 4.9.2 Roles: Elevación de privilegios 4.9.3 Acceso remoto: Modalidades 4.9.4 Acceso remoto: Cumplimiento y su problemática en el acceso directo a servicios y equipos. 4.9.5 Acceso remoto: Acceso Seguro a Servicios . 4.9.6 Puestos remotizados y VDIs: Arquitectura 4.9.7 Puestos remotizados y VDIs: Ventajas e inconvenientes 5.1 Relaciones con organismos nacionales e Internacionales 5.2 Intercambio de información con terceros e IoCs
	5.3 Ciberejercicios

5. CIBER INTELIGENCIA, COOPERACIÓN Y CAPACIDAD	5.4 Inteligencia Artificial y Ciberseguridad
6. GESTIÓN EFICAZ DE INCIDENTES	6.1 Análisis Forense de Sistemas 6.2 Análisis de malware
	6.3 Gestión y respuesta a incidentes de Seguridad
7. INFRAESTRUCTURAS CRÍTICAS	7.1 Ciberseguridad en IC
	7.2 OT e IoT
	7.3 Sistema Gestión Ciberseguridad Industrial, Medidas de control: 7.3.1 Inventario de activos 7.3.2 Inventario de comunicaciones 7.3.3 Servicios de teleservicio (mantenimiento y soporte) 7.3.4Ciclo de vida de componentes, equipos y dispositivos.
8. CISO Soft Skills	8.1 Estrategia de Seguridad 8.2 Planificación de una gestión de Crisis
	8.3 Softskills
	Ejercicio Práctico Ciberseguridad

Módulo 3	
1. Conceptos básicos de la Nube	1.1 Introducción y Definiciones: - El paradigma de la Nube: Definición, Historia y base tecnológica de la Nube. - Nube vs tecnologías de Nube vs Servicios en la Nube; Nube vs OnPrem - CSP vs CU, Publica vs Privada, IaaS, PaaS, SaaS, tenancy. - Ejemplos, e identificación de Servicios, - Entornos híbridos y multicloud 1.2 Servicios Avanzados en la Nube: - DRaaS, SECaaS, IDaaS, BPaaS, … - Catálogo de soluciones. - Arquitecturas cloud - Infoestructura vs. Applistructure vs. Metastructura vs. Infraestructura - Roles y responsabilidades en la Nube: Competencias y cualidades específicas de las personas para trabajo en la Nube
	1.3 Gestión de identidades en la Nube. - Ubicación, gestión centralizada, Servicios IDaaS y brokering de identidades. CIEM
2. Análisis y gestión de riesgos en la Nube	2.1 Metodologías de Análisis de Riesgos. Generales y Específicas de la nube 2.2 Nuevos Riesgos derivados del uso de la Nube
3. Cloud-Conomics	3.1 ¿Por qué la Nube no es solo tecnología? 3.2 Modelos de Negocio en La Nube. 3.3 Impactos en el Negocio de la Nube: economía, automatización, eficiencias 3.4 Modelos de Negocio basados en la Nube. 3.5 FinOps 3.6 Servicios sobre Proveedores IaaS pública 3.7 Web Service OnPrem vs Cloud SaaS 3.8 Shared responsibility modes 3.9 Otros modelos

4. Cumplimiento legal y normativa aplicable	4.1 La Nube, el cumplimiento legal y Soberanía Digital. 4.2 Regulaciones aplicables en entorno cloud: privacidad, Regulaciones UE (DORA, PIC); regulaciones nacionales (ENS) 4.3 Técnicas legales aplicable. 4.4 Crime prosecution. 4.5 eDiscovery
5. Marcos de control aplicables a la Nube	5.1 Marcos de control internacionales: NIST, CSF, ISO 27017, C5, Cobit, CISA 5.2 Certificaciones aplicables a Cloud: personales, de proceso y de empresa 5.3 Guía CSA. 5.4 CCM + CAIQ + PLA + Otras
6. Medidas de seguridad específicas de la Nube	6.1 Gestión de vulnerabilidades y parcheo de servicios en la Nube vs. OnPrem Soluciones CWPP + CSPM + CNAPP 6.2 Seguridad en contenedores y MVs Aplantillado de servicios y plataformas. Gestión de la Configuración: MaaC y Automatización
	6.3 Microsegmentacion y SDNs. Gestión de movilidad y acceso ubicuo a workloads SASE, ZeroTrust y SWG 6.4 Integración de servicios Cloud en TI corporativa Entornos Multicloud y su gestión: ventajas e inconvenientes Integración de monitorización Cloud en TI corporativa 6.5 Pentesting en Cloud. Análisis Forense en Cloud Auditoria de Seguridad y Auditoria Continua en Cloud
	6.6 Respuesta ante incidentes en la Nube El rol del usuario, el rol del proveedor Modelado de playbooks en Cloud
	6.7 Cifrado: Condiciones de cifrado, gestión de claves Algoritmos de cifrado Cifrado at Rest, on Transit & on Process
7. Contratación y gestión de servicios cloud	7.1 Proceso de Adquisición de servicios. Modelos de contratación de Proveedores: modelos de compra, de subscripción, licenciamiento de servicios; Condiciones exigibles, deseables y óptimas para el Usuario de la Nube. Negociación de condiciones con el proveedor: Necesidad, capacidad

7. Contratación y gestión de servicios cloud	7.2 Gestión de Proveedores de la Nube Herramientas de seguimiento disponibles: propiedad, tipología y aplicabilidad. Gestión de servicios y gestión del proveedores en la Nube Seguimiento y Cumplimiento de SLAs. Parámetros habituales y sus valores. "Integración y Orquestacion de Gobierno y Gestión TI con proveedores Cloud: reporte, controles, herramientas." 7.3 Clausulado aplicable: privacidad, cumplimiento, autoridades y otras Documentación contractual vs documentación informativa Documentación deseable y mínima: due dilligence, privacidad, requisitos contractuales Riesgos más habituales derivados de marco contractual deficitario / incompleto / no viable Particularidades Sectoriales: Banca, Sector Público, otros Posición de riesgo y transferencias de riesgo en la Nube
8. Tendencias tecnológicas en la Nube	8.1 Edge computing, serverless, mobile computing and remote working. 8.2 Servicios basados en Datos: IA, ML; BigData. Data Gobernance en la Nube. 8.3 Cloud SecDevOps, DevOps + Security by Default en Cloud 8.4 Iot on Cloud. Infraestrucuras Críticas y Servicios Esenciales
9. Evolución de las organizaciones por la adopción de servicios en la Nube	9.1 Impacto de la Nube: Diferencias entre Outsourcing y CSP 9.2 Impacto de la Nube en Procesos de la Organización: Distribución, automatización, reingenieria 9.3 Impacto de la Nube en estrategia, presupuestos y organización. 9.4 Impacto de la Nube en personas: evolución de roles y perfiles de TI, de Seguridad y otros. Impacto 9.5 Impacto de la Nube en las tecnologias
	Ejercicio Práctico
	Sesión de cierre