PROGRAMA/TEMARIO DEL ESQUEMA

(23 de diciembre 2019. Versión 1.4)

1. Dominio 1. NORMATIVA GENERAL DE PROTECCIÓN DE DATOS. (Porcentaje temario: 50%)

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 la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. 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 la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. 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 la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. 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 la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. 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 la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. 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.

1.9. El Reglamento Europeo de Protección de datos y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. 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 la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. 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.

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.

2. Dominio 2. RESPONSABILIDAD ACTIVA.

(Porcentaje temario: 30%)

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.

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.

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.

3. Dominio 3. TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS. (Porcentaje temario: 20%)

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.

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. Blockchain y últimas tecnologías