Delegado de Protección de Datos
Camino hacia la certificación y la excelencia

Normativa General de Protección de Datos

Ainhoa Juárez Carreño - Jorge Badiola Guerra

AUTORES

Ainhoa Juárez Carreño

Letrada colegiada en el Ilustre Colegio de Abogados de Madrid, Máster de Práctica Jurídica en Centro de Estudios e Investigaciones Jurídicas Madrid (CEIJ).

Cuenta con una larga experiencia en procesos judiciales de diferentes materias y especialidades.

Experta reconocida por el Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias del Banco de España.

Con amplia experiencia en normativas relativas al cumplimiento normativo empresarial (compliance) y las nuevas tecnologías, ha escrito e impartido diversos cursos relativos a estas materias, formando a auditores y consultores así como redes comerciales.

Dirige durante años, proyectos de valoración de puestos de trabajo, sucesión en pymes, protocolos en las empresas familiares, fusiones y escisiones de empresas, impartiendo además formación en las citadas materias, formando a formadores.

Destaca su carrera profesional desde hace 15 años en entidades relacionadas con la empresa en el ámbito de la privacidad y las nuevas tecnologías, llegando a ocupar puestos de relevancia en todas ellas.

Su anterior desempeño profesional se desarrolló en la Fundación Española para la Protección de Datos en la que ha dirigido el departamento jurídico y consultoría técnica.

Posee la certificación IRCA (ISO 27001) (International Register of Certificated Auditors).

En materia de Prevención del Blanqueo de Capitales y Financiación del Terrorismo, ha elaborado distintos cursos y desarrollado el primer software específico de aplicación de esta normativa en los sujetos obligados.

Jorge Badiola Guerra

Profesional con más de 20 años de experiencia en el área de gestión y dirección empresarial, realizó sus estudios de Ciencias Empresariales en la Universidad Complutense de Madrid.

Desde el año 1992, comenzó su andadura empresarial en diversos ámbitos hasta que finalmente, se especializó en las nuevas tecnologías, su aplicación normativa y de seguridad de la información.

Pionero desde la entrada de internet en España, en al año 1994 desarrolló su primer sitio web, evolucionando hacia el momento actual en el que se ha centrado completamente en el área de la seguridad de datos y privacidad.

En 2009, fue nombrado presidente de la Fundación Española para la Protección de Datos, a través de la cual, ha desarrollado protocolos de actuación y profesionalización del sector de las nuevas tecnologías, coordinando más de 30 centros y empresas profesionales en toda España.

Relativo a la Prevención del Blanqueo de Capitales y Financiación del Terrorismo, es experto externo reconocido por el Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias del Banco de España.

Colaboró como presidente en la Comunidad de Madrid de ASEBLAC, la primera y más importante Asociación Española de Sujetos Obligados en Prevención del Blanqueo de Capitales.

Actualmente ha fundado y preside la Asociación Española de Delegados de Protección de Datos.

Autor de varias publicaciones sobre la materia, ha impartido cursos y conferencias en diversos foros profesionales y empresariales difundiendo la normativa y las buenas prácticas en su aplicación.

ISBN - 978-84-697-6081-9

Impreso por Martinco Impresión

Calle de Narváez, 67 – 28009 Madrid

mpm@martinco.es – www.martinco.es

Impreso en España – Printed in Spain

1ª edición - Septiembre 2017

Tipografías utilizadas: familias Tahoma y Estrangelo Edessa

Correspondencia: administracion@fundacionprotecciondedatos.es

PRESENTACIÓN

Cuando hablamos de Protección de Datos nos referimos a conceptos tan trascendentes como privacidad, identidad, intimidad, protección de nuestra imagen, y la de nuestras familias, el derecho a tener una vida sin intrusiones indeseadas. En definitiva la frontera entre controlar nuestra vida o perder el control de la misma, quizás la última frontera con la libertad.

El artículo 18 de nuestra carta magna garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Pero realmente, además de que en las leyes está escrito el derecho a la intimidad, ¿quién es el ejecutor real de este derecho?

Los Delegados de Protección de Datos son la figura clave para auxiliar en el cumplimiento de este derecho. Una grandiosa misión, como enorme es el derecho a proteger.

En línea con la importancia de la tarea, debe estar la importancia de la preparación y de la vocación de los profesionales que abanderan esta labor.

Hemos pretendido desarrollar un libro que permita cumplir con 2 objetivos esenciales: formar a las personas que van a desempeñar una función que consideramos fundamental en nuestro estado de derecho; y en segundo lugar, que ofrezca una visión práctica sobre el cometido a realizar, una visión que traslade confianza y seguridad en la labor realizada, métodos de trabajo eficaces y contrastados, basados en la experiencia de años de profesión.

Queremos con esta obra proporcionar la garantía al sujeto obligado, que los profesionales de la privacidad estarán a la altura de sus necesidades, y a la población en general, que su derecho a la intimidad se deposita en manos de una red de expertos que conocen, respetan y defienden su derecho fundamental a la protección de su intimidad con verdadera vocación, aptitud y disposición.

El contenido del libro, sigue rigurosamente los aspectos requeridos por el Esquema de Certificación de la Agencia Española de Protección de Datos y es un método de estudio y preparación para la realización de la prueba de aptitud exigida a los profesionales que lo requieran.

A su vez, este texto no pretende ser una acotación del conocimiento ni de la experiencia de los profesionales de la protección de datos y por ello, está completado con una sección documental necesaria para aumentar y complementar el aprendizaje.

Finalmente, como es lógico, estamos ante una obra que por la naturaleza de su contenido y el objetivo con el que nace, no puede ser estática, sino que debe convertirse en un documento vivo con futuras ediciones que complementen y actualicen su contenido. Un proceso de aprendizaje que se convierta en una correspondencia *biunívoca* entre el lector y los autores que posibilite mejorar una herramienta con vocación de utilidad y servicio social.

Si estás convencido de iniciar este camino, tan sólo podemos advertir de un riesgo: la protección de datos crea adicción, y una vez que caes en sus garras, no tiene escapatoria. Bienvenidos a este mundo maravilloso de la privacidad.

ÍNDICE

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 LORD. 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 LORD. 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 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 GTart. 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. LSS!, 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) n5 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.

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. Segundad de la información.

2.4.1. Marco normativo. Esquema Nacional de Seguridad y directiva MIS: 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 (EIPD) 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.

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 Segundad 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

Curso preparatorio para el examen de certificación según el programa temario del Esquema Oficial de Certificación de la Agencia Española de Protección de Datos

Primera edición Septiembre 2017