MANUAL DE GESTIÓN DE PROTECCIÓN DE DATOS

GUÍA PRÁCTICA PARA PYMES

Javier Casal Tavasci

COLEX READER
COLEX AUDIO
COLEX

MANUAL DE GESTIÓN DE PROTECCIÓN DE DATOS

GUÍA PRÁCTICA PARA PYMES

Javier Casal Tavasci
Abogado

COLEX 2025

Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, 15004, A Coruña (Galicia)
info@colex.es
www.colex.es

I.S.B.N.: 979-13-7011-160-1
Depósito legal: C 814-2025

SUMARIO

CAPÍTULO III
NOVEDADES DEL RGPD

CAPÍTULO IV
ÁMBITO DE APLICACIÓN DEL RGPD

CAPÍTULO V
FIGURAS Y RESPONSABILIDADES EN EL TRATAMIENTO DE DATOS PERSONALES

CAPÍTULO VI
PRINCIPIOS RELATIVOS AL TRATAMIENTO

CAPÍTULO VII
CATEGORÍAS DE DATOS PERSONALES

CAPÍTULO VIII
REGISTROS DE LAS ACTIVIDADES DE TRATAMIENTO

CAPÍTULO IX
PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTOS

CAPÍTULO X
ANÁLISIS DE RIESGOS

CAPÍTULO XI
EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS

CAPÍTULO XII
POLÍTICAS, REGLAS Y ESTÁNDARES DE SEGURIDAD

CAPÍTULO XIII
SEGURIDAD PERIMETRAL INFORMÁTICA

CAPÍTULO XIV
BRECHAS DE SEGURIDAD

CAPÍTULO XV
GESTIÓN DE INCIDENCIAS

CAPÍTULO XVI
AUTORIDADES DE CONTROL

CAPÍTULO XVII
PROCEDIMIENTOS ANTE LA AUTORIDAD DE CONTROL Y RECURSO ANTE LA VÍA JURISDICCIONAL

CAPÍTULO XVIII
RÉGIMEN SANCIONADOR

CAPÍTULO XIX
DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS

CAPÍTULO XX
GARANTÍA DE LOS DERECHOS DIGITALES

BIBLIOGRAFÍA

PRESENTACIÓN

La información para cualquier organización es un activo de gran valor, fundamental para adoptar decisiones informadas y mejorar la eficiencia operativa.

Asegurar la información es un desafío para las pequeñas y medianas empresas (PYMES), pero es esencial, no solo para cumplir con la legalidad, sino también para obtener una ventaja competitiva. Poniendo en valor la seguridad de la información como un activo estratégico, las empresas refuerzan su imagen reputacional, brindándoles una oportunidad para ampliar su red de clientes y establecer alianzas sólidas.

En un entorno regulatorio en constante evolución, donde las normativas sobre privacidad son cada vez más estrictas, es comprensible que las empresas se sientan abrumadas. Muchas PYMES optan por la externalización de servicios, convencidas de que esta es la solución más eficiente y menos problemática, aunque esta percepción no siempre es acertada. Por ejemplo, un delegado de protección de datos que trabaja desde una posición externa enfrentará mayores dificultades para garantizar el cumplimiento normativo en comparación con un delegado interno, quien tiene un conocimiento más profundo de la organización. Esta ventaja permite al delegado interno identificar riesgos y oportunidades que podrían pasar desapercibidos desde una perspectiva externa, así como adaptar las estrategias de protección de datos a las necesidades específicas de la organización.

Un delegado interno puede que tenga menos experiencia que un delegado externo, sobre todo si este último se dedica profesionalmente a la protección de datos, pero esto no limita la valía del delegado interno, que puede fortalecer su labor a través del asesoramiento de expertos, por ejemplo, para realizar tareas complejas como una evaluación de impacto relativa a la protección de datos.

El perfil de un delegado de protección de datos debe corresponder a una persona con formación y experiencia en este ámbito. Además, deberá reunir una combinación de habilidades como iniciativa y proactividad, imparcialidad e independencia, integridad y ética personal, capacidad para la gestión y la coordinación de equipos y dotes para la negociación y la resolución de conflictos.

En las microempresas puede resultar complicado encontrar el perfil adecuado para designar a un delegado de protección de datos. Si optan por externalizar este servicio es crucial que el profesional se integre en la organización, lo que le permitirá comprender sus fortalezas y abordar sus vulnerabilidades con mayor efectividad.

La alternativa a la externalización es la autogestión, que ofrece innumerables beneficios: permite a la organización responder de forma directa y con mayor agilidad a los desafíos que se le presentan, al tiempo que incrementa el compromiso de los trabajadores con la seguridad de la información al sentirse participes del proceso de gestión, fomenta un entorno colaborativo que potencia la coordinación entre equipos y el intercambio de ideas, incrementa la satisfacción de los clientes al demostrar un compromiso activo con la protección de datos, etc.

El camino hacia la autogestión requiere cierto esfuerzo. Para empezar la empresa deberá realizar una inversión económica para dotarse de los recursos humanos y técnicos necesarios y es probable que, en esta fase inicial, necesiten recurrir a expertos para adaptar la organización al marco regulador pero, una vez adaptada, deberían ser capaces de gestionar la protección de datos por sí mismos con las herramientas que se le han proporcionado.

La autogestión también exige compromiso, determinación, constancia y responsabilidad, desde la alta dirección hasta el último trabajador con acceso a la información. Cuando la autogestión se consolida en la empresa, la protección de datos se integra de manera natural en las operaciones diarias como una rutina o un hábito de trabajo más.

Este libro, diseñado para guiar a las PYMES en el camino hacia la autogestión, está dirigido a profesionales del área de protección de datos y responsables de cumplimiento normativo. También puede ser de interés para quienes se preocupan por la privacidad, ya que cada vez más personas son conscientes de la importancia de proteger sus datos personales.

En sus capítulos se analizan las novedades que introdujo el Reglamento General de Protección de Datos en el ecosistema de datos. Se examina su ámbito de aplicación, se describen las figuras clave en el tratamiento de datos personales, se abordan aspectos cruciales como los principios relativos al tratamiento, los conceptos de protección de datos «desde el diseño» y «por defecto», el registro de las actividades de tratamiento, las metodologías para el análisis de riesgos y las evaluaciones de impacto.

La obra profundiza en la implementación de políticas y estándares de seguridad y estrategias de defensa perimetral para controlar las amenazas que se ciernen sobre las organizaciones, al tiempo que enseña cómo gestionar los incidentes de seguridad.

También ofrece una visión clara sobre los derechos que la normativa reconoce a los titulares de datos personales, analizando los procedimientos

asociados y el papel de las autoridades de control, incluyendo un estudio del régimen sancionador a partir de ejemplos reales y casos prácticos.

Asimismo, aborda temas complejos como las transferencias de datos personales a terceros países u organizaciones internacionales. La guía se complementa con anexos que refuerzan su enfoque práctico.

Para finalizar, quiero expresar mi más sincero agradecimiento a COLEX por su confianza, así como a todas las personas que han contribuido con sus conocimientos y consejos a la elaboración de este libro. Sus aportaciones han enriquecido significativamente su contenido y me han permitido abordar los temas con mayor claridad y profundidad. Dado que son muchas las personas involucradas, prefiero no mencionarlas individualmente para evitar el riesgo de omitir a alguna, lo cual consideraría una falta imperdonable de mi parte. Confío en que cada una de ellas sabrá sentirse reconocida.

Quiero dedicar este libro a mi familia, sin cuya comprensión y apoyo incondicional nada de esto habría sido posible.

Javier Casal Tavasci

SOBRE EL AUTOR

Javier Casal Tavasci es licenciado en Derecho por la Universidad Europa de Madrid.

Realizó sus primeros estudios de postgrado (Máster) en Asesoría Jurídica de Empresas y en Asesoría Fiscal entre los años 2000 y 2002 en la Universidad Pontificia Comillas de Madrid.

En el año 2015 cursó el Máster en Gestión y Dirección Laboral de la Universidad de Vigo.

En el año 2019 realizó el Curso de Delegado de Protección de Datos de la Universidad Antonio de Nebrija, completando su formación académica en el año 2021 con el Máster en Compliance Officer en el mismo centro.

Junto a su desempeño profesional como abogado desde el año 2003, asesorando a empresas en diferentes campos, en el año 2019 creó un proyecto multidisciplinar: PROTECCIÓN DATA, centrado en la implantación de programas de cumplimiento normativo en empresas, el impulso de negocios digitales y la defensa del derecho a la privacidad.

Correo (electrónico): abogado@protecciondata.es

Página web: www.protecciondata.es

ABREVIATURAS

ACPD	Autoridad Catalana de Protección de Datos
AEPD	Agencia Española de Protección de Datos
AESIA	Agencia Española de Supervisión de la Inteligencia Artificial
ARCO	Acceso, Rectificación, Cancelación y Oposición
ARCP-POL	Acceso, Rectificación, Cancelación (ahora, Supresión), Oposición, Portabilidad y Limitación del tratamiento
ART	Artículo
AVPD	Autoridad Vasca de Protección de Datos
BOE	Boletín Oficial del Estado
CC	Código Civil
CCN	Centro Criptológico Nacional
CE	Constitución Española
CEPD	Comité Europeo de Protección de Datos
CP	Código Penal
DOUE	Diario Oficial de la Unión Europea
DPD	Delegado de Protección de Datos
DUDH	Declaración Universal de los Derechos Humanos
EEE	Espacio Económico Europeo
EE.UU.	Estados Unidos
EIPD	Evaluación de Impacto en Protección de Datos
ENS	Esquema Nacional de Seguridad
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
FJ	Fundamento Jurídico
GT29	Grupo de Trabajo del Artículo 29 de la Directiva 95/47/CE
IA	Inteligencia Artificial
INCIBE	Instituto Nacional de Ciberseguridad
LGT	Ley 9/2014, de 9 de mayo, General de las Telecomunicaciones
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal

LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
LPAC	Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
LSSICE	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
N.º	Número
PdD	Privacidad desde el diseño
PIDCP	Pacto Internacional de los Derechos Civiles y Políticos
PpD	Privacidad por defecto
PS	Procedimiento Sancionador
PYME	Pequeña y mediana empresa
RAT	Registro de las actividades de tratamiento
RD	Real Decreto
RDLeg.	Real Decreto Legislativo
RGPD	Reglamento General de Protección de Datos
RLOPD	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD
SAN	Sentencia de la Audiencia Nacional
SEPD	Supervisor Europeo de Protección de Datos
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
TEDH	Tribunal Europeo de Derechos Humanos
TIC	Tecnologías de la Información y las Comunicaciones
TJUE	Tribunal de Justicia de la Unión Europea
TC	Tribunal Constitucional
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia
UE	Unión Europea

CAPÍTULO I

ANTECEDENTES HISTÓRICOS

SUMARIO.- 1.1. Introducción. 1.2. Declaración Universal de los Derechos Humanos. 1.3. Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales. 1.4. Pacto Internacional de Derechos Civiles y Políticos. 1.5. Datenschutzgesetz. 1.6. Datalagen. 1.7. Convenio n.º 108 del Consejo de Europa. 1.8. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. 1.9. Directiva 95/46/CE. 1.10. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. 1.11. Carta de los Derechos Fundamentales de la Unión Europea. 1.12. Directiva 2002/58/CE. 1.13. Tratado de Lisboa. 1.14. Resoluciones de Naciones Unidas sobre el derecho a la privacidad en la era digital. 1.15. Reglamento (UE) 2016/679, General de Protección de Datos. 1.16. Protocolo Adicional y Protocolo modificativo del Convenio n.º 108. 1.17. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

1.1. Introducción

Dice un antiguo proverbio Zen: «Si no sabes a dónde vas, regresa para saber de dónde vienes»; de forma que, en este primer capítulo, vamos a adentrarnos en la historia de la protección de datos personales a través de los instrumentos jurídicos más destacados.

No pretendo hacer un estudio detallado de todos y cada uno de los instrumentos dictados a lo largo de la historia, porque eso nos alejaría del objetivo, que no es otro que acercarle al mundo de la protección de datos, pero sin abrumarle. Empecemos, pues.

1.2. Declaración Universal de los Derechos Humanos

Tras la Segunda Guerra Mundial, en un mundo polarizado y dividido en dos bloques antagonistas —el socialista y el capitalista— la Organización de las Naciones Unidas promovió la **Declaración Universal de los Derechos Humanos**[1] (DUDH).

El proyecto de Declaración se sometió a votación el 10 de diciembre de 1948 en el Palacio de Chaillot de París, y a pesar de que las circunstancias no eran las propicias para lograr el apoyo unánime de los 58 Estados miembros de las Naciones Unidas, la Asamblea General aprobó la Declaración con 48 votos a favor, 8 abstenciones (Unión Soviética, Yugoslavia, Checoslovaquia, Ucrania, Bielorrusia, Polonia, Arabia Saudí y Sudáfrica) y las ausencias de Honduras y Yemen.

El texto aprobado por la Asamblea General, mediante la Resolución 217 A (III), no se formalizó como un tratado internacional, sino como una declaración de intenciones, carente de fuerza jurídica, lo que no le resta valor ni importancia.

La DUDH ha sido traducida a más de 550 idiomas y dialectos de todo el mundo, algunos casi extintos como el «náhuat», última lengua indígena viva en El Salvador. En 1999, el Libro Guinness de los Records reconoció a la DUDH como el documento más traducido del planeta.

El valor de la DUDH reside en el hecho de ser el primer documento de la historia de la humanidad aprobado por la comunidad internacional que considera a todos los seres humanos libres e iguales en dignidad y derechos, sin distinción de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

Eleanor Roosevelt, presidenta de la Comisión de Derechos Humanos de las Naciones Unidas, encargada de redactar el proyecto de Declaración, durante la presentación del proyecto a la Asamblea General, calificó la Declaración Universal de Derechos Humanos de «Carta Magna de la Humanidad».

Con el tiempo, la mayoría de países signatarios de la DUDH han incorporado sus preceptos a sus respectivas Constituciones. Tal es el caso de España.

El artículo 10, apartado 2, de la Constitución de 1978 —bajo el título «De los derechos y deberes fundamentales»— establece: «Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las materias ratificados por España».

1. Naciones Unidas. Declaración Universal de los Derechos Humanos. Resolución 217 A [III], París, de 10 de diciembre de 1948. [https://www.un.org/es/about-us/universal-declaration-of-human-rights].

Volviendo a la DUDH, el artículo 12 dice: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

La DUDH no reconoce la protección de los datos personales como un derecho fundamental, más bien, se refiere al derecho a la privacidad de toda persona física que engloba el derecho al honor (honra y reputación), a la intimidad personal y familiar (vida privada), incluida la inviolabilidad del domicilio y el secreto de las comunicaciones (correspondencia), frente a las injerencias o ataques de cualquier tipo.

Cuando la zona espiritual, íntima y reservada de una persona física se ve atacada hablamos de «intimidad». Todo lo relativo a la intimidad concierne a la privacidad, pero no todo lo que atañe a la vida privada forma parte, necesariamente, del espacio de lo íntimo. Si entran en juego los datos personales de una persona física, estos estarían protegidos por el derecho a la privacidad, que la DUDH reconoce como un derecho fundamental, independiente, intransferible e irrenunciable de toda persona física.

1.3. Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales

El Consejo de Europa (no lo confundan con el Consejo de la Unión Europea) aprobó en Roma, el 4 de noviembre de 1950, el **Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales**[2], más conocido como «Convención Europea de Derechos Humanos» (CEDH), que entró en vigor el 3 de septiembre de 1953.

Estamos ante el primer instrumento internacional que otorgó fuerza vinculante a los derechos que la DUDH había enunciado y reconocido previamente.

El CEDH, en su artículo 8, apartado 1, dispone: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia». No obstante, en su apartado 2 admite la posibilidad de injerencia por parte de la autoridad pública cuando «esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

2. Consejo de Europa. Convenio Europeo de Derechos Humanos, Roma, de 4 de noviembre de 1950 («BOE», n.º 243, de 10 de octubre de 1979). [https://www.echr.coe.int/documents/convention_spa.pdf]

La DUDH y la CEDH reconocen, expresamente, los derechos civiles y políticos del ser humano, pero dejaron al margen los derechos sociales y económicos que, tiempo después, fueron reconocidos por el Consejo de Europa en la «Carta Social Europea» aprobada en Turín el 18 de octubre de 1961. El texto original fue revisado en Estrasburgo el 3 de mayo de 1996.

Para garantizar que los Estados miembros cumplan las obligaciones impuestas por la CEDH, en 1959 se creó el Tribunal Europeo de Derechos Humanos (TEDH) con sede en Estrasburgo (Francia).

El TEDH ha examinado varios asuntos referidos a la posible vulneración del derecho fundamental a la vida privada, en concreto, al secreto de las comunicaciones[3], métodos de vigilancia[4] y protección contra el almacenamiento de datos personales por las autoridades públicas[5].

1.4. Pacto Internacional de Derechos Civiles y Políticos

El 16 de diciembre de 1966, la Asamblea General de las Naciones Unidas aprobó en Nueva York el **Pacto Internacional de Derechos Civiles y Políticos**[6] (PIDCP). Entró en vigor el 23 de marzo de 1976. Forman parte del tratado un total de 173 países.

Inspirándose en la DUDH, el artículo 17, apartado 1, del PIDCP dispone: «Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación», añadiendo su apartado 2 que «toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques».

---

3. TEDH, Malone vs. Reino Unido, n.º 8691/79, de 26 de abril de 1985; Kruslin vs. Francia, n.º 11801/85, de 24 de abril de 1990; Halford vs. Reino Unido, n.º 20605/92, de 25 de junio de 1997; Lambert vs. Francia, n.º 23618/94, de 24 de agosto de 1998; Amann vs. Suiza [GS], n.º 27798/95, de 16 de febrero de 2000; Cotlet vs. Rumanía, n.º 38565/97, de 3 de junio de 2003; Copland vs. Reino Unido, n.º 62617/00, de 3 de abril de 2007; Liberty y otros vs. Reino Unido, n.º 58243/00, de 1 de julio de 2008; Szuluk vs. Reino Unido, n.º 36936/05, de 2 de junio de 2009.

4. Klass y otros vs. Alemania, n.º 5029/71, de 6 de septiembre de 1978; Rotaru vs. Rumanía [GS], n.º 28341/95, de 4 de mayo de 2000; Taylor-Sabori vs. Reino Unido, n.º 47114/99, de 22 de octubre de 2002; Allan vs. Reino Unido, n.º 48539/99, de 5 de noviembre de 2002; Vetter vs. Francia, n.º 59842/00, de 31 de mayo de 2005; Bykov vs. Rusia [GS], n.º 4378/02, de 10 de marzo de 2009; Kennedy vs. Reino Unido, n.º 26839/05, de 18 de mayo de 2010; Uzun vs. Alemania, n.º 35623/05, de 2 de septiembre de 2010; Association «21 Décembre 1989» y otros vs. Rumanía, n.º 33810/07 y 18817/08, de 24 de mayo de 2011.

5. TEDH, Leander vs. Suecia, n.º 9248/81, de 26 de marzo de 1987; TEDH, S. and Marper vs. Reino Unido, n.º 30562/04 y n.º 30566/04, de 4 de diciembre de 2008.

6. Naciones Unidas. Pacto Internacional de Derechos Civiles y Políticos. Resolución 2200 A (XXI), Nueva York, de 16 de diciembre de 1966. [https://www.ohchr.org/sites/default/files/ccpr_SP.pdf].

1.5. Datenschutzgesetz

En 1970, el Land de Hesse de la República Federal Alemana aprobó la **Datenschutzgesetz**[7], que se traduce, literalmente, como «Ley de Protección de Datos». Para algunos el título era completamente inapropiado, pues la ley no protegía los datos, sino los derechos de las personas cuyos datos se estaban tratando. Sea como fuere, el término «protección de datos» se mantuvo y, actualmente, se emplea en todo el mundo.

La Ley de Protección de Datos del Land de Hesse quería brindarle protección a las personas físicas frente a la amenaza que representaba el tratamiento informatizado de los datos personales por las autoridades y distintas administraciones públicas, por otras personas jurídicas de derecho público sujetas a la supervisión del Estado federado y por empresas del sector privado que tratasen datos de carácter personal por cuenta de organismos soberanos.

Entre sus méritos destaca el reconocimiento al interesado del derecho a ser informado sobre el tratamiento informatizado de sus datos personales y a corregir estos en caso de ser erróneos, así como la previsión de precauciones técnicas y de personal adecuadas para evitar que los documentos, datos y resultados cubiertos por la protección de datos pudieran ser vistos, modificados, accedidos o destruidos por personas no autorizadas.

Otra novedad, quizá la más curiosa, fue la aparición por primera vez en la historia de la figura del «Datenschutzbeauftragter», que se traduce como «Delegado de Protección de Datos», al que se hace responsable de velar por el cumplimiento de la ley.

El autor principal de la norma fue el jurista greco-alemán Spiros Simitis (19.10.1934-18.03.2023), a quien, a menudo, se hace referencia como el «padre de la protección de datos».

Con motivo de la aprobación de esta ley, el entonces primer ministro de Hesse, Albert Osswald, declaró: «La visión orwelliana de un Estado omnisciente que explora los rincones más íntimos de la vida humana no se hará realidad en nuestro país». En la actualidad, lo tendría difícil para afirmar lo mismo.

En 1976, la República Federal Alemana aprobaba la «Bundesdatenschutzgestez», esto es, la «Ley Federal de Protección de Datos» inspirada en la Datenschutzgesetz de Hesse. A diferencia de la ley de Hesse, que se centraba en el sector público, esta ley amplió su ámbito de aplicación para incluir tanto al sector público como al privado, estableciendo así un marco legal integral para la protección de los datos personales en Alemania.

---

7. «Hessisches Datenschutzgesetz». *Gesetz-und Verordnungsblatt für das Land Hessen*, 12.10.1970. N.º 41.

MANUAL DE GESTIÓN DE PROTECCIÓN DE DATOS

GUÍA PRÁCTICA PARA PYMES

Esta obra tiene como objetivo facilitar a las PYMES su adaptación al marco regulatorio y permitirles gestionar de manera autónoma la protección de datos.

En sus capítulos se analizan las novedades que introdujo el Reglamento General de Protección de Datos. Se examina su ámbito de aplicación, se describen las figuras clave en el tratamiento de datos personales, se abordan los principios relativos al tratamiento, los conceptos de protección de datos «desde el diseño» y «por defecto», el registro de las actividades de tratamiento, las metodologías para el análisis de riesgos y las evaluaciones de impacto.

La obra profundiza en la implementación de políticas y estándares de seguridad, al tiempo que enseña cómo gestionar los incidentes de seguridad. También ofrece una visión clara sobre los derechos que la normativa reconoce a los titulares de datos personales, analizando los procedimientos asociados y el papel de las autoridades de control. Incluye un estudio del régimen sancionador a partir de casos reales, lo que permite comprender las implicaciones legales del incumplimiento, y aborda temas complejos como las transferencias internacionales de datos. La guía se complementa con formularios prácticos.

Con un enfoque accesible y orientado a la acción, el contenido de esta obra facilita la adaptación a los requisitos legales y promueve una cultura de protección de datos en el entorno empresarial.

JAVIER CASAL TAVASCI

Licenciado en Derecho por la Universidad Europea de Madrid. Realizó sus primeros estudios de postgrado (Máster) en Asesoría Jurídica de Empresas y en Asesoría Fiscal entre los años 2000 y 2002 en la Universidad Pontificia Comillas de Madrid. En 2015 cursó el Máster en Gestión y Dirección Laboral de la Universidad de Vigo y en 2021 completó su formación con el Máster en Compliance Officer en la Universidad Antonio de Nebrija.

Ejerce como abogado desde 2003, asesorando a empresas en diversos ámbitos. En 2019, fundó PROTECCIÓN DATA, un proyecto multidisciplinar enfocado en la implantación de programas de cumplimiento normativo, el impulso de negocios digitales y la defensa del derecho a la privacidad.

Autor de más de 500 artículos sobre protección de datos y seguridad de la información que podrá encontrar escaneando el siguiente código QR:

PVP: 50,00 €

ISBN: 979-13-7011-160-1

9 791370 111601