

CAPÍTULO PRIMERO  
INTRODUCCIÓN

CAPÍTULO SEGUNDO  
EL VALOR DE LA SEGURIDAD  
EN LAS ORGANIZACIONES

- 1. Los objetivos de seguridad
- 2. La transformación del entorno tecnológico: el ciberespacio y las ciber amenazas
- 3. El nuevo marco de seguridad de la información: ISO 27001:2022
- 4. Cambios significativos de la versión ISO 27001:2013 a ISO 27001:2022/2023
- 5. Modificaciones del Anejo A: Controles de seguridad de la información ISO/IEC 27001:2022

CAPÍTULO TERCERO  
EL ESQUEMA NACIONAL DE  
SEGURIDAD: LA SEGURIDAD EN LAS  
ADMINISTRACIONES PÚBLICAS

- 1. El objetivo de la seguridad de la información en las administraciones públicas
- 2. La regulación del Esquema Nacional de Seguridad según el Real Decreto 311/2022, de 3 de mayo
- 3. Objetivos y ámbito de aplicación del Esquema Nacional de Seguridad
- 4. Aspectos esenciales y requisitos mínimos del Esquema Nacional de Seguridad
- 5. Las medidas de seguridad del Esquema Nacional de Seguridad y su aplicación en los distintos niveles de seguridad
- 6. Principales novedades y cambios en las medidas de seguridad del nuevo Esquema Nacional de Seguridad, de 2022
- 7. Relación entre el Reglamento General de Protección de Datos y el Esquema General de Seguridad
- 8. Medidas de seguridad para encargados del tratamiento
- 9. Objetivo: la seguridad de la información

CAPÍTULO CUARTO  
EL *CLOUD COMPUTING*, LA SEGURIDAD  
Y LA NORMATIVA EN MATERIA DE  
PROTECCIÓN DE DATOS PERSONALES

- 1. Una nueva forma de trabajar: cuestiones previas
- 2. El *cloud computing* y el acceso a datos por cuenta de terceros (artículo 28 RGPD)
- 3. El análisis de riesgos previo a la contratación de los servicios de *cloud computing*
- 4. Aplicación de la normativa en materia de protección de datos personales en el *cloud computing*
- 5. Medidas de cumplimiento en el *cloud computing* ante la nueva normativa en materia de protección de datos personales
- 6. Posibles riesgos en los servicios de *cloud computing*
- 7. El *cloud computing* y las medidas del Esquema Nacional de Seguridad

CAPÍTULO QUINTO  
LA INTELIGENCIA ARTIFICIAL Y LA  
PROTECCIÓN DE DATOS PERSONALES

- 1. Algunas nociones básicas sobre los sistemas de inteligencia artificial
- 2. El impacto de la inteligencia artificial en la protección de datos personales
- 3. Medidas de seguridad para garantizar el cumplimiento normativo

BIBLIOGRAFÍA

ÍNDICE DE FIGURAS



Este libro puede considerarse la segunda parte del publicado en 2022 bajo el título “Seguridad del tratamiento: aspectos técnicos”. En este segundo volumen se aborda la cuestión de la seguridad en el tratamiento de la información desde distintas perspectivas, combinando marcos normativos, estándares internacionales, regulación y avances tecnológicos que inciden directamente en la gestión de la seguridad de la información y en el derecho a la protección de datos personales.

En todo caso, y a pesar de la complejidad para garantizar la seguridad, esta no debe entenderse como un obstáculo para la innovación, sino más bien como un valor esencial que garantiza la continuidad para las organizaciones. La confianza de los usuarios depende, en gran medida, de la garantía de que los datos que confían a las organizaciones serán tratados de manera responsable, confidencial y segura. En este sentido, el valor de la seguridad no se mide únicamente en términos de cumplimiento normativo, sino también como un activo estratégico capaz de generar ventajas competitivas, reforzar la reputación institucional y consolidar relaciones de confianza en entornos de creciente incertidumbre y, en ocasiones, de inseguridad jurídica.

El libro también dedica un capítulo a la seguridad de la información y al tratamiento de datos personales en el sector público y, más en concreto, en las administraciones públicas. Explica el Esquema Nacional de Seguridad, de 2022, como herramienta clave para la protección de la información en el ámbito de las Administraciones Públicas. Se presenta como una herramienta que no solo refuerza la seguridad del sector público, sino que también establece un modelo homogéneo que aporta seguridad, facilita la interoperabilidad, la confianza mutua entre administraciones y la adecuada protección de los datos personales gestionados por entidades públicas. Se evidencia la vinculación entre el RGPD y el ENS de modo que mientras el primero protege los derechos de las personas, el segundo asegura que los sistemas de información donde se albergan y tratan dichos datos cuentan con los niveles adecuados de protección.

Otro de los aspectos que se abordan en el libro es el estudio del impacto que tienen los servicios de *cloud computing* o computación en la nube sobre la seguridad y la protección de los datos personales. Se estudia como la migración de infraestructuras, aplicaciones y servicios hacia entornos *cloud* ofrece múltiples ventajas en términos de eficiencia, escalabilidad y flexibilidad. Sin embargo, también plantea nuevos riesgos vinculados al acceso a datos por cuenta de terceros, la ubicación de los datos en distintos países continentes, la dependencia de enormes proveedores globales y la necesidad de garantizar que las medidas de seguridad aplicadas cumplan con los estándares exigidos por la normativa europea y nacional.

Por último, también se aborda la relación entre la inteligencia artificial y la protección de datos personales, cuestión de creciente actualidad y enorme trascendencia. La inteligencia artificial plantea enormes oportunidades en términos de eficiencia, personalización de servicios y análisis masivo de información, pero también introduce riesgos inéditos para la privacidad de las personas.



COLECCIÓN MONOGRAFÍAS  
PROTECCIÓN DE DATOS PERSONALES



Víctor Cazurro Barahona

Seguridad del tratamiento:  
Aspectos técnicos  
y organizativos  
(Parte II)

PRÓLOGO  
Victor Cazurro Barahona



VÍCTOR CAZURRO  
BARAHONA

Doctor en Derecho con Mención Europea, con sobresaliente cum laude por unanimidad, por la Universidad de Valladolid. Acreditado por ANECA y Diplomado en la Escuela de Práctica Jurídica de la misma universidad.

Abogado en ejercicio desde 2004, especializado en Derecho de la Información, Derecho de Internet y Protección de Datos Personales; también es Delegado de Protección de Datos en diversas entidades.

En la Universidad ha ocupado las responsabilidades de Decano de la Facultad de Derecho, Vicerrector de Investigación y Relaciones Internacionales y la dirección de diversas titulaciones de Grado y Máster, siempre en el ámbito del Derecho (2013-2020).

Es Profesor universitario de *Derecho Constitucional* y de *Derecho de la Información* desde 2005. Hoy es profesor de *Derecho de Internet* en el Grado en Derecho y de diversas asignaturas en el Máster Universitario de Protección de Datos, y *Director de Innovación y Mejora Continua* de la Facultad de Derecho de la Universidad Internacional de La Rioja. También ha sido docente en materia de datos personales para el Instituto Nacional de la Administración Pública (INAP).

Es experto en docencia digital, plataformas de teleformación y en los procesos de enseñanza-aprendizaje online.

Cuenta con una amplia experiencia docente, tanto en universidades nacionales (Universidad de Valladolid, Universidad Europea Miguel de Cervantes, Universidad de Barcelona) como internacionales: Universit  Cattolica del Sacro Cuore di Milano. Tambi n ha sido colaborador de la Universit  degli Studi di Foggia y la Universit  del Salento. Ha realizado varias estancias internacionales de investigaci n en el  mbito del derecho a la protecci n de datos personales y la privacidad en la Universit  del Salento, Lecce (Italia).