

Ciberseguridad

Un nuevo reto para el Estado
y los Gobiernos Locales

Directora

Dolors Canals Ametller

© De los autores, 2021
© Wolters Kluwer España, S.A.

Wolters Kluwer
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@wolterskluwer.es
<http://www.wolterskluwer.es>

Primera edición: Abril 2021

Depósito Legal: M-7649-2021
ISBN versión impresa: 978-84-7052-846-0
ISBN versión electrónica: 978-84-7052-847-7

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S.A.
Printed in Spain

© **Wolters Kluwer España, S.A.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, Wolters Kluwer España, S.A., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

WOLTERS KLUWER no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, u cualesquiera otras herramientas de participación. Igualmente, WOLTERS KLUWER se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.

WOLTERS KLUWER queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.

WOLTERS KLUWER se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **Wolters Kluwer España, S.A.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

ÍNDICE SISTEMÁTICO

CAPÍTULO INTRODUCTORIO.....	21
PRIMERA PARTE. CIBERESPACIO, CIBERSEGURIDAD Y ESTADO DE DERECHO.....	27
CAPÍTULO 1. CIBERSEGURIDAD EN UN MUNDO HIPERCONNECTADO. Ángel GÓMEZ DE ÁGREDÁ.....	27
I. LOS CUATRO ELEMENTOS.....	29
II. UN MUNDO MEDIADO.....	30
III. VEINTE AÑOS NO ES NADA.....	32
IV. LAS CIUDADES Y EL MUNDO INTELIGENTES.....	34
V. RIESGOS Y AMENAZAS.....	37
VI. ESCONDIENDO LA MANO.....	43
VII. UN MUNDO ENREDADO.....	44
VIII. LA EXPERIENCIA COMO PRODUCTO.....	48
IX. LIBERTAD POR ENCIMA DE REALIDAD.....	50
X. FRENTE AL ESPEJO.....	51
XI. UN MUNDO FALAZ.....	54
BIBLIOGRAFÍA.....	56
CAPÍTULO 2. LA SEGURIDAD EN EL ENTORNO DIGITAL. Dolors CANALS AMETLLER.....	61
I. INTRODUCCIÓN. ENTORNO DIGITAL Y ESTADO DE DERECHO.....	63

II.	EL ENTORNO CIBERNÉTICO: UN ECOSISTEMA TECNOLÓGICO DE BASE PRIVADA CON PROYECCIÓN PÚBLICA	65
III.	LA SEGURIDAD DIGITAL COMO SERVICIO PÚBLICO-PRIVADO	70
1.	Ciberseguridad y ciberresiliencia	70
2.	De la seguridad pública, a la colaboración privada y la autoseguridad individual	72
IV.	ANÁLISIS DE RIESGOS DE SEGURIDAD DIGITAL INDIVIDUAL Y COLECTIVA	76
1.	Protección de libertades y derechos fundamentales	76
2.	La garantía de la seguridad jurídica frente a la desinformación	77
3.	Identidad digital: acreditación y certificación	78
4.	Protección de servicios esenciales e infraestructuras críticas	80
5.	Seguridad en redes y sistemas de información	82
V.	LAS ESTRATEGIAS DE CIBERSEGURIDAD	83
	BIBLIOGRAFÍA Y DOCUMENTOS DE INTERÉS	84
CAPÍTULO 3. SISTEMA JUDICIAL Y CIBERDELINCUENCIA. Susanna OROMÍ I VALL-LLOVERA		89
I.	EL IMPACTO DE LA CIBERDELINCUENCIA EN EL SISTEMA JUDICIAL	91
II.	PROBLEMAS DEL SISTEMA JUDICIAL PARA HACER FRENTE A LA CIBERDELINCUENCIA Y CLAVES DE SOLUCIÓN	98
III.	EL DESARROLLO DE LA TECNOLOGÍA EN LOS PROCESOS FRENTE AL AVANCE DE LA CIBERDELINCUENCIA	104
1.	Ventajas e inconvenientes del uso de la tecnología en el proceso penal	106
2.	Las principales medidas tecnológica utilizadas en la investigación de la ciberdelincuencia	111
IV.	LA NECESARIA COLABORACIÓN CON EL SECTOR PRIVADO: UN RIESGO DE PRIVATIZACIÓN DEL SISTEMA JUDICIAL	116
V.	A MODO DE CONCLUSIÓN. UNO DE LOS DESAFÍOS DE LA JUSTICIA	122

BIBLIOGRAFÍA.....	123
-------------------	-----

CAPÍTULO 4. FACTOR HUMANO Y PREVENCIÓN DEL CIBER-FRAUDE. ANÁLISIS DEL ENGAÑO EN EL CIBERESPACIO DESDE LA PERSPECTIVA AMBIENTAL Y LA VULNERABILIDAD PSICOLÓGICA DE LA VÍCTIMA. José R. AGUSTINA SANLLEHÍ Aina M. GASSÓ MOSER.....	127
---	-----

I. INTRODUCCIÓN	129
II. EL ARTE DE ENGAÑAR... EN UN LUGAR LLAMADO «CIBERESPACIO»	131
III. <i>MODUS OPERANDI</i> : ALGUNOS EJEMPLOS DE CIBER-FRAUDES.....	133
IV. LA VICTIMOLOGÍA COMO EJE CENTRAL DE LAS ESTRATEGIAS DE PREVENCIÓN: ESPECIAL RELEVANCIA ANTE LOS CIBERFRAUDES	139
V. PSICOLOGÍA Y CIBERESPACIO.....	143
VI. CARACTERÍSTICAS Y PATRONES PSICOLÓGICOS DE VÍCTIMAS Y OFENSORES EN EL CIBERESPACIO.....	145
1. Comportamientos	146
2. Experiencias vitales	146
3. Conocimiento	146
VII. TÉCNICAS DE INGENIERÍA SOCIAL: DINÁMICA Y ASPECTOS EMOCIONALES	150
BIBLIOGRAFÍA.....	155

CAPÍTULO 5. FOMENTANDO LA DENUNCIA DE LOS CIBER-DELITOS ECONÓMICOS Y UNA CULTURA DE CIBERSEGURIDAD MEDIANTE EL TRABAJO EN EQUIPO. Steven KEMP	159
--	-----

I. INTRODUCCIÓN	161
II. ¿POR QUÉ ES IMPORTANTE DENUNCIAR LAS CIBERAMENAZAS Y LOS CIBERDELITOS ECONÓMICOS?.....	162
1. La ciberdelincuencia económica y su impacto	162
2. Denunciar y la cultura de ciberseguridad	163
III. ¿QUÉ SABEMOS SOBRE LA DECISIÓN DE DENUNCIAR?..	167

1.	La denuncia de la ciberdelincuencia en comparación con la delincuencia tradicional	167
2.	El reporte del <i>phishing</i>	168
3.	Las denuncias del fraude en la época digital	169
IV.	LA CIBERSEGURIDAD Y LA TEORÍA DE LA MOTIVACIÓN A LA PROTECCIÓN (TMP)	171
1.	<i>Protection Motivation Theory</i>	171
2.	TMP aplicada a la ciberseguridad	173
3.	TMP y la denuncia del ciberdelito económico	174
3.1.	Gravedad percibida	174
3.2.	Vulnerabilidad percibida	175
3.3.	Autoeficacia	175
3.4.	Eficacia de la respuesta	176
3.5.	Costes de responder	177
V.	MEJORANDO Y FOMENTANDO LAS DENUNCIAS	178
VI.	CONCLUSIONES	181
	BIBLIOGRAFÍA	182
 SEGUNDA PARTE. CIBERSEGURIDAD: UN NUEVO RETO PARA LOS GOBIERNOS LOCALES.		193
 CAPÍTULO 1. INCIDENTES DE SEGURIDAD INFORMÁTICA EN ENTIDADES LOCALES: PANORÁMICA Y PROPUESTAS DE ACTUACIÓN. Enrique BENÍTEZ PALMA		193
I.	INTRODUCCIÓN	195
II.	CIBERSEGURIDAD: AMENAZA GLOBAL, DEBILIDAD LOCAL	196
III.	INCIDENTES DE CIBERSEGURIDAD EN ENTIDADES LOCALES ESPAÑOLAS	200
1.	Ciberataques a entidades locales en 2019	202
2.	Ciberataques a entidades locales en 2020 y 2021	203
IV.	¿DÓNDE PONER EL FOCO?	207
V.	CONCLUSIONES Y PROPUESTAS CONCRETAS	210
1.	Analizar el estado de la cuestión	210

2.	Concienciación básica	210
3.	Explotación de datos del CCN-CERT	211
4.	Detección y actuación sobre las vulnerabilidades	211
5.	Definir el modelo a seguir	212
	BIBLIOGRAFÍA Y DOCUMENTOS DE INTERÉS	213

CAPÍTULO 2. ETAPAS EN LA IMPLANTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD EN EL ÁMBITO DE LA ADMINISTRACIÓN LOCAL. Carlos VAZ CALDERÓN 217

I.	LA CONCEPCIÓN DE LA CIBERSEGURIDAD EN EL ORDENAMIENTO JURÍDICO	219
II.	LOS RIESGOS DE LA CIBERSEGURIDAD	223
III.	IMPLANTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD EN EL ÁMBITO LOCAL	225
1.	Determinación del ámbito subjetivo de aplicación del ENS	227
2.	Funciones y responsabilidades en el ENS	229
3.	La formulación de un Plan de adecuación	232
A.	Principios básicos y requerimientos mínimos. La política de seguridad	232
B.	Identificación y categorización de la información y los servicios prestados	236
C.	El análisis de riesgos	238
D.	La declaración de aplicabilidad	241
E.	Insuficiencias del sistema y el plan de mejora continua	242
4.	La implementación del Plan de adecuación y de las medidas de seguridad	243
5.	La realización de auditorías de seguridad	246
6.	La conformidad con el ENS	248
7.	La implantación conjunta del ENS para el ámbito local	249
	BIBLIOGRAFÍA Y DOCUMENTOS DE INTERÉS	251

CAPÍTULO 3. CONTROLES BÁSICOS DE CIBERSEGURIDAD EN LOS AYUNTAMIENTOS DE MAYOR POBLACIÓN: LA EXPERIENCIA DE LA COMUNIDAD VALENCIANA. Antonio MINGUILLO ROY	253
I. INTRODUCCIÓN	255
1. El actual entorno de administración electrónica de las entidades locales.....	256
2. El impacto de la COVID-19.....	258
3. Efecto en el auditor externo y metodología	260
4. Alineación con el Esquema Nacional de Seguridad...	262
5. Los controles básicos de ciberseguridad (CBCS) en la metodología de auditoría de los órganos de control externo de las comunidades autónomas	264
II. LA SINDICATURA DE COMPTES DE LA COMUNIDAD VALENCIANA.....	270
1. Plan Estratégico y auditorías de ciberseguridad de los mayores Ayuntamientos de la Comunidad.	270
2. Ámbito subjetivo, objetivo y temporal de las auditorías de ciberseguridad	271
3. Primera conclusión	272
4. Segunda conclusión	277
5. Situación al máximo nivel de detalle.....	280
6. Insatisfactorio grado de cumplimiento normativo	283
7. Situación de las Diputaciones provinciales	283
BIBLIOGRAFÍA Y DOCUMENTOS DE INTERÉS.....	286
 CAPÍTULO 4. SISTEMAS DE CIBERSEGURIDAD Y BUENAS PRÁCTICAS EN MUNICIPIOS DE POCA POBLACIÓN. Virginia MORENO BONILLA	289
I. INTRODUCCIÓN	291
II. DIGITALIZACIÓN DE LAS ADMINISTRACIONES LOCALES: CIBERSEGURIDAD EN EL PROCESO INTEGRAL DE LA ADMINISTRACIÓN ELECTRÓNICA Y EL TELETRABAJO.....	295

III.	ESQUEMA NACIONAL DE SEGURIDAD (ENS). ADECUACIÓN	299
1.	Elaboración de una Política de Seguridad de la Información	303
2.	Identificación de la información y los servicios. Determinación de la Categoría del Sistema	303
3.	El Análisis de Riesgos	303
4.	La declaración de aplicabilidad (SoA)	304
5.	El informe de insuficiencias	304
6.	El Plan de Mejora de la Seguridad	304
IV.	LAS CLAVES	305
V.	CÓMO HACERLO EN AYUNTAMIENTOS PEQUEÑOS.	306
1.	Fases	306
2.	Características más comunes en un Ayuntamiento pequeño tipo.	308
A.	Equipamiento	308
B.	Ámbito de aplicación	309
C.	Figura del Responsable de Seguridad	310
D.	Medidas de seguridad.	311
E.	Notificación de Incidentes de Seguridad.	317
F.	Evaluación y mejora continua.	317
VI.	PROPUESTA PARA GESTIÓN DE CIBERSEGURIDAD NORMALIZADA EN AYUNTAMIENTOS PEQUEÑOS	318
	BIBLIOGRAFÍA.	319

CAPÍTULO 5. GARANTÍAS DE SEGURIDAD EN LOS SERVICIOS DE COMPUTACIÓN EN NUBE. Carmen SERRANO DURBÁ

I.	QUÉ ES LA NUBE Y TIPOS DE NUBE	323
II.	MODELOS DE DESPLIEGUE Y DE SERVICIOS.	324
III.	CONDICIONES OBLIGATORIAS DE LA NUBE	328
IV.	LA NUBE COMO ACELERADOR DE LA TRANSFORMACIÓN DIGITAL	328
V.	SEGURIDAD EN LA NUBE.	329
A.	Riesgos derivados del uso de la nube	330

B.	Vulnerabilidades de los servicios en la nube	331
VI.	CUMPLIMIENTO EN LA NUBE	335
VII.	ASPECTOS DE SEGURIDAD Y CUMPLIMIENTO EN LA CONTRATACIÓN PÚBLICA	335
	BIBLIOGRAFÍA Y DOCUMENTOS DE INTERÉS.	345
CAPÍTULO 6. LAS CIBERAMENAZAS EN LOS AYUNTAMIENTOS. Genís MARGARIT I CONTEL		347
I.	INTRODUCCIÓN. LA REALIDAD TAL CUAL	349
II.	TENER LAS PERSONAS ADECUADAS	355
III.	UN PROBLEMA «GLOCAL»	357
IV.	LA INTELIGENCIA ARTIFICIAL PARA ATACAR Y PARA PROTEGERSE.	358
V.	APRENDER DE LOS ERRORES	359
VI.	POR RESPETO A LAS PERSONAS	361
A.	Plan de ciberseguridad	363
B.	Cultura de Seguridad	364
C.	Política de Seguridad	365
D.	Normativa de Seguridad	365
E.	Evaluación y gestión de riesgos	365
F.	Liderazgo	366
CAPÍTULO 7. LA ESTRATEGIA DE CIBERSEGURIDAD DE CATALUNYA Y EL MUNDO LOCAL. Oriol TORRUELLA TORRES		369
I.	INTRODUCCIÓN	371
II.	LA ESTRATEGIA DE CIBERSEGURIDAD	374
1.	Digitalización	377
2.	Liderazgo en ciberseguridad	378
3.	Transformación digital de la Administración	379
4.	Ciudadanía digital	380
5.	Sector estratégico	381
6.	Pilares	382

7.	Fundamentos	384
8.	Un país ciberseguro.	386
9.	Servicio público de ciberseguridad	387
10.	Administración cibersegura	390
11.	Cultura de ciberseguridad	393
12.	Innovación, talento y actividad económica de la ciberseguridad.	395
III.	ESTADO DE LA CIBERSEGURIDAD EN EL MUNDO LOCAL	398
1.	Algunos datos relevantes	398
2.	El Plan Nacional para una Sociedad Digital y la Administración local	401
3.	Modelo de ciberseguridad e iniciativas para la Administración local	403
	A. Portal o hub de ciberseguridad	403
	B. Plataforma de ciberseguridad en la nube	404
	C. Catalonia-CERT	404
4.	Otros proyectos que deben mejorar la ciberseguridad en la Administración local.	405