

Índice General

	<i>Página</i>
EL AUTOR. UN ARQUITECTO DE RESILIENCIA EN LA ERA DE LA IA.....	29
TRANSPARENCIA METODOLÓGICA Y AUTORÍA. SISTEMA DE ICONOGRAFÍA HMC (<i>HUMAN-MACHINE COLLABORATION</i>)	31
PRÓLOGO.....	33
PREFACIO DEL AUTOR. GOBERNAR LA TECNOLOGÍA CUANDO LA RESPONSABILIDAD NO ES DELEGABLE.....	35

PARTE I FUNDAMENTOS NORMATIVOS DEL NUEVO PARADIGMA

CAPÍTULO 1

INTRODUCCIÓN Y GOBERNANZA ESTRATÉGICA DE LA CIBERSEGURIDAD.....	39
1.1. Políticas generales de seguridad y procedimientos.....	42
1.1.1. <i>La Directiva NIS2 como obligación estructural de gobernanza del riesgo digital.....</i>	44
1.1.2. <i>El Reglamento de Inteligencia Artificial (AI Act) y la tensión regulatoria de los sistemas autónomos.....</i>	47
1.1.3. <i>El Data Act. Soberanía, interoperabilidad y acceso de terceros.....</i>	50
1.2. <i>Zero Trust</i> como respuesta arquitectónica a la insuficiencia regulatoria y técnica.....	51

	<u>Página</u>
1.3. El marco estratégico del CISO moderno. Más allá de los controles técnicos	55
1.4. El CISO como directivo. Responsabilidad, imputación y límites en la gobernanza del riesgo digital.	58
1.5. La síntesis del escudo. Hacia una arquitectura de gobernanza integrada	64
1.6. Contexto operativo	65
1.6.1. <i>La genealogía del consenso y los principios de confiabilidad. Hacia una ontología de la IA pública</i>	65
1.6.2. <i>Traducción operativa. La transmutación de la norma en arquitectura de control</i>	66
1.6.3. <i>El CISO como traductor institucional y garante de la soberanía</i>	68
1.6.4. <i>La transición hacia el rigor metodológico. El diseño como respuesta a la incertidumbre</i>	70
1.7. Marco metodológico	72
1.7.1. <i>Enfoque epistemológico. realismo jurídico-tecnológico</i>	72
1.7.2. <i>Frameworks de gobernanza y arquitecturas IAM</i>	73
1.7.3. <i>Estrategia de investigación. El ciclo de validación de la soberanía</i>	74
Key takeaways de la Parte I.	77
Glosario síntesis interseccional	77
Transición a Parte II.	84

PARTE II
LA EVOLUCIÓN DEL ROL DEL CISO Y LA
EMERGENCIA DE LAS IDENTIDADES ARTIFICIALES

CAPÍTULO 2

LA EVOLUCIÓN DEL ROL DEL CISO	87
2.1. Ciclo de vida técnico.	88
2.2. El nexos de la responsabilidad	89
2.3. Emergencia de las identidades artificiales	89

	<i>Página</i>
2.4. Gobernanza de identidades artificiales. Imputación jurídica y responsabilidad del CISO	92
2.5. Imputación jurídica y responsabilidad administrativa en entornos con identidades artificiales	94
2.6. Identidad consciente de la privacidad (Privacy-Aware Identity)	98
2.7. Riesgos democráticos y organizativos de las identidades artificiales	100
2.8. De la identidad como acceso a la identidad como poder...	103
CAPÍTULO 3	
IDENTIDAD DIGITAL, AGENTES DE IA Y NUEVOS MODELOS DE RESPONSABILIDAD	105
3.1. De la identidad digital clásica a la identidad operativa ...	105
3.1.1. <i>Identidad, acción y poder en entornos digitales</i>	106
3.1.2. <i>El desbordamiento del modelo IAM tradicional</i>	106
3.1.3. <i>Identidades técnicas y responsabilidad difusa</i>	107
3.1.4. <i>Hacia una concepción ampliada de la identidad</i>	107
3.2. El nacimiento de los agentes de IA como sujetos operativos	108
3.2.1. <i>De la automatización clásica a la agencia algorítmica</i>	109
3.2.2. <i>Opacidad decisional e indefensión ante el cumplimiento</i> ..	110
3.2.3. <i>Comportamientos emergentes y el radio de explosión</i>	111
3.2.4. <i>La ilusión de control y la abdicación de la supervisión</i>	111
3.2.5. <i>De la herramienta al actor regulado</i>	112
3.3. Identidades artificiales. Definición, tipología y riesgos ...	112
3.3.1. <i>La identidad como vector de escalada de privilegios autónoma</i>	113
3.3.2. <i>El secuestro de la identidad artificial y la manipulación del propósito</i>	114
3.3.3. <i>Volatilidad y pérdida de la trazabilidad de responsabilidad</i>	114
3.3.4. <i>Riesgos y trazabilidad. El colapso de la confianza implícita</i>	114

3.4. El vacío de cumplimiento. NIS2, AI Act y la crisis de la evidencia	115
3.4.1. <i>La insuficiencia del log tradicional ante la NIS2</i>	115
3.4.2. <i>El mito de la supervisión humana en el AI Act</i>	116
3.4.3. <i>La crisis de la evidencia y la carga de la prueba</i>	116
3.5. Gobernanza de identidades en el sector público europeo .	116
3.5.1. <i>El ENS y la identidad como arquitectura de legalidad</i>	117
3.5.2. <i>NIS2 y eIDAS2. La soberanía frente al riesgo sistémico</i> ...	117
3.5.3. <i>Zero Trust como modelo de integridad institucional</i>	117
3.5.4. <i>Gobernar identidades es gobernar legitimidad</i>	118
3.6. Identidad consciente de la privacidad (Privacy-Aware Identity)	118
3.6.1. <i>El poder informacional y la protección desde el diseño</i>	118
3.6.2. <i>Minimización, transparencia y separación de contextos</i> ...	118
3.6.3. <i>Trazabilidad proporcionada y calidad institucional</i>	119
3.6.4. <i>La transparencia y la trazabilidad como activos estratégicos</i>	119
3.7. Identidad, poder y legitimidad en la administración digital	120
3.7.1. <i>La delegación de autoridad y el control del riesgo</i>	120
3.7.2. <i>Contra la despersonalización. Rendición de cuentas y soberanía corporativa</i>	120
3.7.3. <i>Identidad, confianza y rendición de cuentas</i>	121
3.7.4. <i>La responsabilidad como eje de la soberanía</i>	121
3.8. Identidad consciente de la privacidad	125
3.8.1. <i>Fundamento conceptual y ruptura paradigmática</i>	125
3.8.2. <i>Arquitectura técnico-normativa de componentes</i>	126
3.8.3. <i>Validación mediante caso de uso técnico</i>	139
3.8.4. <i>Proyección de impacto y transferibilidad</i>	148
3.8.5. <i>Conclusiones y agenda futura</i>	151
Key takeaways de la Parte II	155
Glosario síntesis interseccional	155

	<u>Página</u>
Transición a Parte III.....	165

**PARTE III
ARQUITECTURAS OPERATIVAS, BLINDAJE
JURÍDICO-INSTITUCIONAL Y SOBERANÍA DIGITAL**

CAPÍTULO 4

CÓMO BLINDAR AL CONSEJO (Y A TI MISMO) ANTE NIS2 Y DORA	169
4.1. Filosofía <i>Zero Trust</i> como doctrina jurídico-técnica	173
4.1.1. <i>La integración de la firma electrónica cualificada en el flujo Zero Trust</i>	<i>178</i>
4.1.2. <i>El conflicto entre interoperabilidad y desconfianza</i>	<i>182</i>
4.1.3. <i>Análisis forense en entornos de confianza cero</i>	<i>186</i>
4.1.4. <i>Zero Trust como doctrina</i>	<i>189</i>
4.2. Obligaciones NIS2 para administraciones públicas.....	192
4.2.1. <i>Análisis de riesgos y seguridad de sistemas de información</i>	<i>193</i>
4.2.2. <i>Gestión de incidentes de ciberseguridad</i>	<i>198</i>
4.2.3. <i>Continuidad operativa y gestión de crisis</i>	<i>203</i>
4.2.4. <i>Seguridad de la cadena de suministro de tecnologías de la información y comunicación</i>	<i>206</i>
4.2.5. <i>Controles técnicos fundamentales de ciberseguridad.....</i>	<i>211</i>
4.2.6. <i>Gobernanza, supervisión directiva y formación en ciberseguridad</i>	<i>218</i>
4.3. DORA. Resiliencia operativa digital en sector financiero y extensibilidad a administraciones públicas	229
4.3.1. <i>DORA como laboratorio regulatorio de supervisión intensiva</i>	<i>229</i>
4.3.2. <i>Los cinco pilares arquitectónicos de resiliencia operativa bajo DORA</i>	<i>230</i>
4.3.3. <i>Extensibilidad de principios DORA a administraciones públicas</i>	<i>233</i>
4.3.4. <i>Aplicabilidad específica a entidades financieras públicas..</i>	<i>235</i>

	<i>Página</i>
4.4. Síntesis arquitectónica de blindaje institucional	236
4.4.1. <i>Del cumplimiento fragmentado a la arquitectura integrada</i>	236
4.4.2. <i>Mapeo de convergencias normativas</i>	237
4.4.3. <i>Arquitectura técnica de referencia para blindaje institucional</i>	241
4.4.4. <i>Roadmap de implementación gradual</i>	245
4.5. Arquitectura de blindaje institucional bajo NIS2/DORA/ENS	249
CAPÍTULO 5	
LA GRADUACIÓN DE LA AUTONOMÍA	257
5.1. La automatización como desafío a la imputabilidad clásica	257
5.2. Taxonomía operativa de niveles de autonomía algorítmica	260
5.2.1. <i>Nivel 0. Sin automatización</i>	261
5.2.2. <i>Nivel 1. Asistencia informacional</i>	262
5.2.3. <i>Nivel 2. Recomendación automatizada</i>	265
5.2.4. <i>Nivel 3. Automatización supervisada</i>	271
5.2.5. <i>Nivel 4. Automatización autónoma con aprendizaje continuo</i>	279
5.2.6. <i>Nivel 5. Autonomía general (AGI): prohibido</i>	287
5.2.7. <i>Tabla comparativa de los cinco niveles</i>	290
5.2.8. <i>Árbol de decisión para clasificación de sistemas</i>	291
5.2.9. <i>Casos frontera y resolución</i>	291
5.2.10. <i>Conclusión de Sección 5.2.</i>	292
5.3. Régimen de responsabilidad administrativa por nivel de autonomía	292
5.3.1. <i>Responsabilidad en Nivel 1. Asistencia informacional</i>	293
5.3.2. <i>Responsabilidad en Nivel 2. Recomendación automatizada</i>	295
5.3.3. <i>Responsabilidad en Nivel 3. Automatización supervisada</i>	298

	<i><u>Página</u></i>
5.3.4. <i>Responsabilidad en Nivel 4. Automatización autónoma con aprendizaje</i>	301
5.3.5. <i>Tabla de responsabilidad por nivel</i>	303
5.3.6. <i>Principios transversales de responsabilidad</i>	304
5.3.7. <i>Conclusión de Sección 5.3.</i>	306
5.4. Validación de la taxonomía mediante casos ilustrativos ..	306
5.4.1. <i>Caso 1: Sistema VioGén - Nivel 2 (Recomendación automatizada)</i>	307
5.4.2. <i>Caso 2: Sistema de asignación de plazas escolares - Nivel 3 (Automatización supervisada)</i>	316
5.4.3. <i>Conclusión de Sección 5.4.</i>	325
5.5. Automatización algorítmica y principios constitucionales de buena administración	326
5.5.1. <i>Tensión 1: Eficacia administrativa versus supervisión humana exhaustiva</i>	326
5.5.2. <i>Tensión 2: Imparcialidad y objetividad versus sesgos algorítmicos</i>	329
5.5.3. <i>Tensión 3: Seguridad jurídica versus aprendizaje continuo.</i>	333
5.5.4. <i>Tensión 4: Tutela judicial efectiva versus opacidad algorítmica.</i>	335
5.5.5. <i>Conclusión de sección 5.5.</i>	339
5.6. Hacia una ley de transparencia algorítmica. La iconografía HMC como estándar de evidencia en el sector público español.	340
5.6.1. <i>Insuficiencia del marco actual. El vacío de comunicación al ciudadano</i>	341
5.6.2. <i>El sistema de iconografía HMC. Del estándar Dubai al derecho español</i>	343
5.6.3. <i>Propuesta de reforma legislativa. Nuevo artículo 41bis de la Ley 39/2015.</i>	349
5.6.4. <i>Techos de automatización por tipo de trámite</i>	355
5.6.5. <i>Implementación y verificación. El rol de AESIA.</i>	361
5.6.6. <i>Sinergia iconografía HMC y arquitectura X-FAIT</i>	367

CAPÍTULO 6

SOBERANÍA DIGITAL Y GOBERNANZA DE DATOS. EL PATRIMONIO DE LA ADMINISTRACIÓN EN LA ERA DE LA IA.....

377

6.1. La Reconceptualización de la Soberanía en el Espacio de Datos Europeo

377

6.2. Arquitecturas de Datos Soberanas. Del *Cloud* Centralizado al *Edge* Administrativo.....

378

6.2.1. Tipología de entornos de datos en la Administración

378

6.2.2. La nube pública global: eficiencia a costa de soberanía condicional

379

6.2.3. El cloud soberano europeo como compromiso estructural ..

380

6.2.4. El edge administrativo como garantía última de proximidad y control

381

6.2.5. Matriz comparativa: on-prem, nube global, cloud soberano y edge administrativo

382

6.3. Gobernanza de datos explotables por IA. Calidad, integridad y propiedad intelectual.....

383

6.3.1. Calidad de los datos: métricas operativas para IA pública .

383

6.3.2. Integridad de datos: linaje y controles de transformación ..

384

6.3.3. Propiedad intelectual: el conocimiento institucional como activo crítico

384

6.4. El anclaje de supervivencia. Resiliencia de datos ante ataques de envenenamiento (Adversarial AI).....

385

6.4.1. Taxonomía operativa de ataques adversariales a datos ...

386

6.4.2. Arquitectura del anclaje de supervivencia.....

386

6.5. Ética de los datos y el derecho a la explicabilidad.....

387

6.5.1. Explicabilidad técnica vs. explicabilidad jurídica.....

388

6.5.2. Protocolos de explicabilidad por diseño

388

Key takeaways de la Parte III

391

Glosario síntesis interseccional

392

Transición a Parte IV

402

**PARTE IV
GESTIÓN DE CIBERCRISIS, RESILIENCIA
INSTITUCIONAL Y APRENDIZAJE POSFALLO**

**CAPÍTULO 7
GESTIÓN DE CIBERCRISIS Y GOBERNANZA EN
ESCENARIOS DE ALTA PRESIÓN** 407

PARTE A

ARQUITECTURA DE LA RESPUESTA INSTITUCIONAL 408

7.1. Crisis y Ciber crisis. Delimitación conceptual y consecuencias jurídicas 408

7.2. Modelos de Gestión Escalonada. *Bronze, Silver y Gold* 410

7.2.1. Nivel Bronze. Táctica de integridad y verdad forense 410

7.2.2. Nivel Silver. Coordinación de Riesgos de Compliance 411

7.2.3. Nivel Gold. Soberanía decisional y responsabilidad política 412

7.3. La dimensión humana. sesgos cognitivos y el control efectivo 413

7.4. Velocidad, automatización y el límite humano 414

PARTE B

GOBERNANZA EN EL MOMENTO DE LA VERDAD. 415

7.5. Cuando la seguridad falla. La auditoría de la soberanía 415

7.6. Supervisores, autoridades y el nuevo ecosistema de control 417

7.7. Comunicación en crisis. Entre la transparencia y el pánico. 418

7.8. Errores fatales y crisis de legitimidad 419

7.9. Aprendizaje Institucional y Memoria del Error. La Inmunidad del Sistema 421

Key takeaways de la Parte IV 423

Glosario síntesis interseccional 424

Transición a Parte V. 434

PARTE V
GOBERNANZA EN INCERTIDUMBRE PERMANENTE
Y SOBERANÍA DEL MANDO ALGORÍTMICO

CAPÍTULO 8

GOBERNAR LA CIBERSEGURIDAD EN 2026. LIDERAZGO, RIESGO Y ACCIÓN RESPONSABLE	439
8.1. Del control perimetral a la arquitectura del privilegio.....	439
8.1.1. <i>Del gestor técnico al garante institucional.....</i>	439
8.1.2. <i>La traducción del riesgo técnico en valor estratégico.....</i>	440
8.1.3. <i>El CISO como facilitador de la responsabilidad directiva .</i>	440
8.1.4. <i>La legitimidad como frontera final</i>	440
8.2. Gestión del riesgo en entornos automatizados y algorítmicos.....	441
8.2.1. <i>El desplazamiento hacia el riesgo algorítmico y de identidad.....</i>	441
8.2.2. <i>El riesgo de imputación y el marco regulatorio europeo ...</i>	441
8.2.3. <i>Del análisis estático al control continuo y gobernable</i>	442
8.3. Gobernanza operativa de agentes de inteligencia artificial	442
8.3.1. <i>La Identidad Artificial como anclaje de control y supervisión</i>	442
8.3.2. <i>Sincronía con el AI Act y el ENS. Evitar las islas de automatización</i>	443
8.3.3. <i>Contra la ilusión de control. Responsabilidad y resiliencia</i>	443
8.4. Arquitecturas de identidad resilientes y el modelo Zero Trust.....	443
8.4.1. <i>La identidad como frontera dinámica y especializada</i>	444
8.4.2. <i>Zero Trust. Verificación continua y control de contexto ...</i>	444
8.4.3. <i>Zero Trust como principio de desconfianza estructural ...</i>	445
8.4.4. <i>Identidad, contexto y control continuo.....</i>	446
8.4.5. <i>Resiliencia como capacidad de contención y cumplimiento</i>	446

	<i>Página</i>
8.5. Resiliencia organizativa y toma de decisiones bajo presión	446
8.5.1. <i>La resiliencia como capacidad de decisión, no solo de recuperación</i>	446
8.5.2. <i>El piloto automático institucional y la revocación del mandato</i>	447
8.5.3. <i>El CISO como intérprete de la agencia algorítmica</i>	447
8.5.4. <i>Coherencia, legitimidad y la arquitectura de la evidencia..</i>	447
8.6. Hoja de ruta para organizaciones públicas europeas	448
8.6.1. <i>De la conformidad normativa a la capacidad institucional</i>	448
8.6.2. <i>Integración de la gobernanza de IA en el núcleo de la ciberseguridad</i>	448
8.6.3. <i>La identidad como infraestructura de fe pública</i>	448
8.6.4. <i>Liderazgo público y gestión del cambio</i>	448
8.6.5. <i>Una hoja de ruta evolutiva hacia la Arquitectura de la Evidencia</i>	450
8.7. Gobernar la complejidad. Ciberseguridad, inteligencia artificial y legitimidad democrática	450
8.8. Epílogo. ¿Quién gobierna cuando gobiernan los sistemas?	451
CAPÍTULO 9	
EL FUTURO DE LA CIBERSEGURIDAD. GOBERNAR SISTEMAS QUE YA NO CONTROLAMOS DEL TODO	
9.1. De la seguridad como función a la seguridad como sistema de gobierno	453
9.2. Europa ante el dilema de la automatización soberana	454
9.3. El nuevo contrato institucional. Ciudadanos, algoritmos y responsabilidad	457
9.4. El CISO y la alta dirección como arquitectos de confianza	458
9.5. Gobernar en incertidumbre permanente. El realismo estratégico de la ciberseguridad	460

	<i>Página</i>
9.6. Anclajes de supervivencia para una ciberseguridad legítima	461
9.6.1. <i>Responsabilidad indelegable en la toma de decisiones digitales</i>	462
9.6.2. <i>La trazabilidad como presupuesto de explicabilidad y rendición de cuentas</i>	462
9.6.3. <i>El control humano significativo en los puntos de no retorno</i>	463
9.6.4. <i>La identidad gobernada como base de imputación jurídica</i>	464
9.6.5. <i>Transparencia operativa compatible con la seguridad</i>	465
9.6.6. <i>Capacidad institucional de aprendizaje tras el fallo</i>	466
Key takeaways de la Parte V	467
Glosario síntesis interseccional	469

**PARTE VI
ANEXOS**

1. Doctrina	483
1.1. <i>Glosario completo</i>	483
1.2. <i>Referencias bibliográficas</i>	507
TABLA DE ABREVIATURAS	513