

ESTUDIOS

# EL GOBIERNO DE LA CIBERSEGURIDAD

ROBERTO FERNÁNDEZ CASTILLA  
DAVID VELÁZQUEZ VIOQUE  
COORDINADORES

URÍA  
MENÉNDEZ

esade | Law  
School  
UNIVERSIDAD RAMON LLUL

ARANZADI

© Roberto Fernández Castilla, David Velázquez Vioque (Coords.) y autores, 2025  
© ARANZADI LA LEY, S.A.U.

**ARANZADI LA LEY, S.A.U.**

C/ Collado Mediano, 9  
28231 Las Rozas (Madrid)  
www.aranzadilaley.es

**Atención al cliente:** <https://areacliente.aranzadilaley.es/publicaciones>

**Primera edición:** noviembre 2025

**Depósito Legal:** M-24739-2025

**ISBN versión impresa con complemento electrónico:** 978-84-1085-483-3

**ISBN versión electrónica:** 978-84-1085-484-0

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.

*Printed in Spain*

© ARANZADI LA LEY, S.A.U. 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, ARANZADI LA LEY, S.A.U., 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](http://www.cedro.org)) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no asumirán ningún tipo de responsabilidad que pueda derivarse frente a terceros como consecuencia de la utilización total o parcial de cualquier modo y en cualquier medio o formato de esta publicación (reproducción, modificación, registro, copia, explotación, distribución, comunicación pública, transformación, publicación, reutilización, etc.) que no haya sido expresa y previamente autorizada.

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.

ARANZADI LA LEY 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, ARANZADI LA LEY se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.

ARANZADI LA LEY 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.

ARANZADI LA LEY 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 ARANZADI LA LEY, S.A.U., 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 General

Página

### PRÓLOGO

JOSÉ MIGUEL GORDILLO LUQUE.....	17
---------------------------------	----

### CAPÍTULO 1.

#### MARCO REGULATORIO DE LA CIBERSEGURIDAD

#### I

#### **LA ESTRATEGIA EUROPEA DE CIBERSEGURIDAD: LA LEGISLACIÓN DE LA UE QUE LA DESARROLLA**

LETICIA LÓPEZ-LAPUENTE .....	25
<b>1. Introducción: una transformación digital europea cibersegura en un entorno de amenazas complejo .....</b>	<b>25</b>
<b>2. Los principios rectores de la Estrategia Europea de Ciberseguridad.....</b>	<b>27</b>
<b>3. La principal legislación en ciberseguridad de la UE .....</b>	<b>31</b>
3.1. <i>Directivas sobre medidas para un alto nivel común de ciberseguridad en la Unión (Directivas NIS1 y NIS2).....</i>	31
3.2. <i>ENISA y el Reglamento de Ciberseguridad .....</i>	35
3.3. <i>El Reglamento de Ciberresiliencia.....</i>	36
3.4. <i>El Reglamento de Cibersolidaridad .....</i>	37
3.5. <i>Reglamento DORA .....</i>	37
3.6. <i>Directiva Europea sobre la Resiliencia de Entidades Críticas.</i>	37

**NORMATIVA COMUNITARIA PARA LA CIBERSEGURIDAD  
EN EL SECTOR ELÉCTRICO**

ROBERTO FERNÁNDEZ CASTILLA.....	39
<b>1. Introducción: El sector eléctrico y su exposición a un mundo digitalizado .....</b>	<b>39</b>
<b>2. Regulación en materia de ciberseguridad en el sector de la electricidad.....</b>	<b>41</b>
2.1. <i>Reglamento 2019/941: Preparación frente a los riesgos en el sector de la electricidad.....</i>	43
a. Razonamiento detrás del enfoque basado en riesgos.....	43
b. Evaluación y análisis de riesgos: los planes de preparación.....	44
c. Integración de la ciberseguridad en la seguridad del suministro.....	45
d. Conclusión: la importancia del Reglamento 2019/941 en la ciberseguridad del sistema eléctrico .	45
2.2. <i>Reglamento (UE) 2019/943: Mercado interior de la electricidad .....</i>	46
a. Consideraciones en materia de ciberseguridad .....	47
b. Conclusión .....	48
2.3. <i>Reglamento Delegado (UE) 2024/1366: Complemento del Reglamento (UE) 2019/943 en materia de ciberseguridad.....</i>	49
a. Objetivos específicos y medidas que implementa .	49
b. <i>Ámbito</i> subjetivo de aplicación .....	50
c. Disposiciones específicas en materia de ciberseguridad .....	52
d. Conclusión: Relevancia y aportación al sistema eléctrico europeo .....	54

II

**LEGISLACIÓN NACIONAL ESPECÍFICA EN MATERIA DE SEGURIDAD NACIONAL, CIBERSEGURIDAD, RESILIENCIA OPERATIVA**

ROSA ORTUÑO .....	55
-------------------	----

**LEGISLACIÓN PENAL ESPECÍFICA CON IMPACTO EN CIBERSEGURIDAD**

DAVID VELÁZQUEZ .....	81
-----------------------	----

<b>1. Normativa aplicable .....</b>	<b>81</b>
<b>2. Delitos que afectan a la ciberseguridad en la legislación penal española .....</b>	<b>87</b>
2.1. <i>Acceso ilegal a sistemas informáticos .....</i>	87
2.2. <i>Interceptación ilegal de datos informáticos .....</i>	90
2.3. <i>Daños en datos, programas informáticos o documentos electrónicos .....</i>	90
2.4. <i>Delitos de abuso de dispositivos (artículos 197 ter y 264 ter).</i>	92
2.5. <i>Otros delitos relacionados con la ciberseguridad .....</i>	94

III

**OTRAS NORMATIVAS DISTINTAS DE CIBERSEGURIDAD CON IMPACTO EN LA REGULACIÓN DE LA SEGURIDAD DE LAS EMPRESAS**

ROSA ORTUÑO .....	95
-------------------	----

<b>1. Datos: protección de datos (RGPD) y Estrategia Europea de Datos (Data Act, Data Governance Act) .....</b>	<b>95</b>
<b>2. Seguridad de la información: Cyber resilience Act.....</b>	<b>106</b>
<b>3. Inteligencia artificial: IA Act.....</b>	<b>106</b>
<b>4. El nuevo Reglamento sobre Seguridad de los Productos .....</b>	<b>110</b>
<b>5. Ejemplo de normativa específica de productos por sector: Sector sanitario: Reglamento de productos sanitarios .....</b>	<b>111</b>
<b>6. Responsabilidad por daños por productos defectuosos .....</b>	<b>112</b>
<b>7. Nota Final .....</b>	<b>113</b>

IV

**ESTRATEGIAS Y MARCO NORMATIVO DE CIBERSEGURIDAD DE ESTADOS UNIDOS, AUSTRALIA, REINO UNIDO, BRASIL Y MÉXICO**

NOHAILA EL MOUDEN JAADOUNI.....	117
<b>1. Introducción.....</b>	<b>117</b>
<b>2. Estrategias nacionales de ciberseguridad: análisis comparado.</b>	<b>118</b>
2.1. <i>La relevancia del análisis de las Estrategias Nacionales de Ciberseguridad</i> .....	118
a) Estados Unidos: <i>The National Cybersecurity Strategy</i> (2023) .....	119
b) Australia: <i>The 2023-2030 Australian Cyber Security Strategy</i> (2023-2030).....	122
c) Reino Unido: <i>The Government Cyber Security Strategy</i> (2022-2030) .....	124
d) Brasil: <i>Política Nacional de Cibersegurança (PNCiber)</i> (2023) .....	126
e) México: <i>La Estrategia Nacional de Ciberseguridad</i> (2017).....	127
2.2. <i>Sobre la necesidad de una mayor cooperación internacional...</i>	129

**CAPÍTULO 2.  
GOBIERNO DE LA CIBERSEGURIDAD**

I

**LA CIBERSEGURIDAD Y LA DIRECTIVA NIS 2**

RAFAEL SEBASTIÁN .....	133
<b>1. Introducción.....</b>	<b>133</b>
1.1. <i>La amenaza fantasma: cómo actúan los piratas informáticos .</i>	135
1.2. <i>Tendencias en materia de ciberseguridad</i> .....	139
1.3. <i>La ciberseguridad. Una defensa activa</i> .....	140
1.4. <i>Una mirada al futuro</i> .....	142
<b>2. El marco normativo</b> .....	<b>143</b>

	<i>Página</i>
2.1. <i>Legislación aplicable</i> .....	143
2.2. <i>Panorama institucional</i> .....	147
2.3. <i>El código de buen gobierno</i> .....	148
<b>3. Ciberseguridad y gobierno corporativo</b> .....	<b>150</b>
3.1. <i>Notificación de ciberincidentes</i> .....	151
3.2. <i>La gobernanza de la ciberseguridad y la Directiva NIS 2</i> .....	153
3.3. <i>Los deberes de los administradores en materia de ciberseguridad</i>	155
3.4. <i>Asignación de la ciberseguridad a una comisión especializada</i> .	158
3.5. <i>Responsabilidad del Consejo</i> .....	159
3.6. <i>Responsabilidad de la Comisión de Auditoría</i> .....	161
<b>4. Conclusiones</b> .....	<b>162</b>
<b>Bibliografía</b> .....	<b>165</b>

CAPÍTULO 3.  
COLABORACIÓN PÚBLICO-PRIVADA  
EN MATERIA DE CIBERSEGURIDAD

I

**MODELOS DE COLABORACIÓN PARA LA PREVENCIÓN  
Y LA RESPUESTA COORDINADA ANTE INCIDENTES DE  
SEGURIDAD**

DAVID VELÁZQUEZ .....	171
-----------------------	-----

II

**LA CIBERSEGURIDAD DESDE LA PERSPECTIVA DE LA  
ADMINISTRACIÓN PÚBLICA: PARTICULARIDADES  
EXISTENTES Y ESTADÍSTICAS RELEVANTES.  
RESPONSABILIDAD Y COLABORACIÓN DE LOS ÓRGANOS  
DE SUPERVISIÓN Y CONTROL Y LA PROMOCIÓN DE  
LA SEGURIDAD. NOVEDADES Y CAMBIOS DERIVADOS  
DEL ANTEPROYECTO DE LA LEY DE COORDINACIÓN Y  
GOBERNANZA DE LA CIBERSEGURIDAD**

DAVID FRANCISCO BLANCO .....	183
------------------------------	-----

<b>1. La Ciberseguridad desde la Perspectiva de la Administra- ción Pública: Particularidades Existentes</b> .....	<b>184</b>
------------------------------------------------------------------------------------------------------------------------	------------

	<i>Página</i>
1.1. <i>Introducción</i> .....	184
1.2. <i>Particularidades existentes</i> .....	185
1.3. <i>Estadísticas relevantes</i> .....	189
<b>2. Responsabilidad y Colaboración de los Órganos de Supervisión, Control y la Promoción de la Seguridad</b> .....	<b>191</b>
2.1. <i>Centro Criptológico Nacional</i> .....	191
2.2. <i>Centro Nacional de Protección de Infraestructuras y Ciberseguridad</i> .....	195
2.3. <i>Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos</i> .....	197
2.4. <i>Mando Conjunto del Ciberespacio</i> .....	198
2.5. <i>Instituto Nacional de Ciberseguridad de España</i> .....	199
<b>3. Novedades y cambios derivados del Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad</b> .....	<b>204</b>

## CAPÍTULO 4

### GESTIÓN Y RESPUESTA ANTE INCIDENTES DE CIBERSEGURIDAD

MARIO MONTES SANTAMARÍA .....	211
<b>1. Reacción penal frente a los incidentes de ciberseguridad</b> .....	<b>211</b>
<b>2. Riesgos penales asociados al pago en casos de <i>ransomware</i></b> .....	<b>218</b>

## CAPÍTULO 5

### IMPLICACIONES DE CIBERSEGURIDAD EN LA CONTRATACIÓN DE PRODUCTOS Y SERVICIOS TECNOLÓGICOS

FRANCISCO JAVIER GARCÍA Y MARC CALVO CARMONA.....	225
<b>1. La digitalización del sector eléctrico y la creciente importancia de la ciberseguridad</b> .....	<b>225</b>
<b>2. El papel de los proveedores en la ciberseguridad de los operadores eléctricos</b> .....	<b>228</b>

	<i>Página</i>
<b>3. Pautas a seguir por los operadores eléctricos en la contratación de proveedores tecnológicos.....</b>	<b>229</b>
3.1. <i>Primer paso: determinación del régimen aplicable en materia de ciberseguridad.....</i>	<i>230</i>
3.2. <i>Segundo paso: redacción del contrato.....</i>	<i>233</i>
a) Cláusulas contractuales en cumplimiento del RD 2024/1366.....	233
b) Cláusulas contractuales de conformidad con el RGPD.....	235
c) Garantías de cumplimiento .....	236
d) Definición de las medidas de seguridad .....	237
e) Facultades de supervisión .....	238
f) Asunción de responsabilidad .....	238
g) Confidencialidad.....	239
h) Restricciones a la subcontratación .....	239
i) Notificación de incidentes y deber de colaboración .....	239
j) Facultad de terminación.....	241
k) Jurisdicción .....	241
<b>4. Conclusiones.....</b>	<b>245</b>

## CAPÍTULO 6

### **CIBERAMENAZAS EN EL SECTOR ELÉCTRICO**

JOSEP PEGUEROLES VALLÉS, FCO. JAVIER GARCÍA PÉREZ Y ROBERTO FERNÁNDEZ CASTILLA.....	249
<b>1. La red eléctrica como infraestructura crítica. Seguridad IT y seguridad OT.....</b>	<b>250</b>
<b>2. La generación, distribución y comercialización inteligente de energía eléctrica. Vulnerabilidades intrínsecas de la <i>Smart Grid</i> .....</b>	<b>251</b>

	<i><u>Página</u></i>
3. <b>Agentes implicados, atacantes, amenazas híbridas, geopolíticas</b> .....	254
4. <b>Cumplimiento en medidas de ciberseguridad</b> .....	259
5. <b>Medidas de ciberseguridad para la <i>Smart Grid</i></b> .....	261
6. <b>Conclusiones</b> .....	262
7. <b>Referencias</b> .....	263

# Normativa comunitaria para la ciberseguridad en el sector eléctrico

ROBERTO FERNÁNDEZ CASTILLA  
*Abogado en Uría Menéndez*

SUMARIO: 1. INTRODUCCIÓN: EL SECTOR ELÉCTRICO Y SU EXPOSICIÓN A UN MUNDO DIGITALIZADO. 2. REGULACIÓN EN MATERIA DE CIBERSEGURIDAD EN EL SECTOR DE LA ELECTRICIDAD. 2.1. *Reglamento 2019/941: Preparación frente a los riesgos en el sector de la electricidad.* a. Razonamiento detrás del enfoque basado en riesgos. b. Evaluación y análisis de riesgos: los planes de preparación. c. Integración de la ciberseguridad en la seguridad del suministro. d. Conclusión: la importancia del Reglamento 2019/941 en la ciberseguridad del sistema eléctrico. 2.2. *Reglamento (UE) 2019/943: Mercado interior de la electricidad.* a. Consideraciones en materia de ciberseguridad. b. Conclusión. 2.3. *Reglamento Delegado (UE) 2024/1366: Complemento del Reglamento (UE) 2019/943 en materia de ciberseguridad.* a. Objetivos específicos y medidas que implementa. b. *Ámbito* subjetivo de aplicación. c. Disposiciones específicas en materia de ciberseguridad. d. Conclusión: Relevancia y aportación al sistema eléctrico europeo.

## 1. INTRODUCCIÓN: EL SECTOR ELÉCTRICO Y SU EXPOSICIÓN A UN MUNDO DIGITALIZADO

Nuestra Ley del Sector Eléctrico<sup>1</sup> abre su preámbulo afirmando que “[e]l suministro de energía eléctrica constituye un servicio de interés económico general, pues la actividad económica y humana no puede entenderse hoy en día sin su existencia”. En efecto, las actividades principales que encontramos en nuestro sistema eléctrico (actividades de generación, transporte, distribución y comercialización —como decimos, las principales, pero no las únicas—) se alzan como esenciales para el correcto funcionamiento diario de un mundo

---

1. Ley 24/2013, de 26 de diciembre, del Sector Eléctrico.

globalizado, esto es, para un escenario en el que las industrias participan cada vez más en mercados internacionales, para unos servicios públicos que cada vez más están interconectados y que cooperan de manera transfronteriza con otros territorios, sistemas de transporte e infraestructuras que unen distintos países, y un largo etcétera de actividades básicas, todas ellas altamente digitalizadas y con el mismo común denominador: el suministro de electricidad como pilar para su desenvolvimiento.

No es difícil atisbar, a partir de lo anterior, que la correcta operación del sistema eléctrico, la garantía de prestar un adecuado suministro de energía, y en definitiva, su aseguramiento y continuidad, se tornan en una cuestión crítica. En efecto, la dependencia de la energía es cada vez mayor, y por tanto, la seguridad y la estabilidad en la entrega de energía son cruciales.

A este respecto, las interrupciones en el suministro no solo podrían afectar, de manera puntual o específica, a los procesos económicos y productivos de una determinada compañía o grupo de éstas, sino que su impacto puede ir más allá, generando daños mucho más profundos: imaginen por un momento que, con motivo de un (ciber)ataque, el sistema eléctrico de un Estado se viese afectado de tal manera que su sistema de defensa o los sistemas que hacen funcionar adecuadamente los mercados financieros existentes en ese país se viesan perjudicados; sin duda, esto generaría resultados negativos estructurales y a largo plazo, alterando la confianza de los distintos agentes que participan en nuestra sociedad. Esta hipótesis se agrava teniendo en cuenta que la mayoría de las fases de gestión del sistema eléctrico, como decíamos, están digitalizadas mediante tecnologías avanzadas. En definitiva, la integración de servicios, la digitalización de procesos y el uso de redes inteligentes en el marco del suministro de energía aportan un indudable valor en aras de una eficiente gestión de nuestro funcionamiento diario, pero sin duda, su protección supone un reto de seguridad global, y en especial, a los efectos de dotarnos de un sistema eléctrico robusto y resiliente para responder a amenazas tanto físicas como digitales.

Esta realidad ha supuesto que el regulador (comunitario) haya decidido dotar al sector, paulatinamente, de un cuerpo normativo cada vez más riguroso en materia de (ciber)seguridad, lo que se ha materializado en la implementación de regulaciones específicas destinadas a abordar cómo han de ejecutarse los procesos de operación para el suministro de energía, primando su salvaguarda y continuidad. A este respecto, y son las normas que se van a analizar en este capítulo, encontramos el Reglamento (UE) 2019/941, orien-

tado a la preparación frente a los riesgos en el sector eléctrico; el Reglamento (UE) 2019/943, que regula el mercado interior de la electricidad; y el Reglamento Delegado (UE) 2024/1366, que complementa el anterior con medidas específicas sobre la ciberseguridad de los flujos transfronterizos de electricidad. Estas normas buscan garantizar la protección del sistema, promoviendo la interoperabilidad y su protección en un entorno cada vez más digitalizado.

Esta doble exigencia —de asegurar la continuidad operativa y de proteger los sistemas contra (ciber)ataques— es el motor que impulsa la adopción de estas normativas europeas. La implementación de estos marcos legales fortalece la capacidad de anticipar y mitigar riesgos, estableciendo protocolos que permiten una respuesta coordinada y eficaz ante incidentes, garantizando así la protección de infraestructuras críticas en un entorno cada vez más complejo y dinámico.

## 2. REGULACIÓN EN MATERIA DE CIBERSEGURIDAD EN EL SECTOR DE LA ELECTRICIDAD

Por tanto, podemos afirmar sin temor a equivocarnos que la seguridad (también, la “ciber”) se ha convertido en una preocupación central en la operativa de los mercados de la electricidad dada su exposición a los entornos globales, habiéndose ampliado exponencialmente el espectro de amenazas o ciberataques a sus infraestructuras.

Esta realidad trata de ser capturada, para su anticipación, detección, y en su caso, mitigación, mediante la implementación de normativas y protocolos de ciberseguridad frente a posibles incidentes. Como se indicaba, los tres principales instrumentos normativos a nivel europeo que abordan estos aspectos son los siguientes:

- **Reglamento (UE) 2019/941**<sup>2</sup>: Este Reglamento está destinado a la preparación frente a los riesgos en el sector de la electricidad. Su principal objetivo es fortalecer la resiliencia de las infraestructuras eléctricas mediante la implementación de medidas preventivas y protocolos de respuesta ante incidentes, incluyendo aquellos de origen cibernético. La normativa fomenta la identificación y evaluación continua de riesgos, asegurando que las medidas de contingencia

---

2. Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la Directiva 2005/89/CE (“**Reglamento 2019/941**”) <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32019R0941>

y la coordinación entre actores sean efectivas ante posibles (ciber) amenazas.

- **Reglamento (UE) 2019/943**<sup>3</sup>: Por su parte, este Reglamento se enfoca a la regulación del mercado interior de la electricidad. Este instrumento normativo tiene como meta principal la liberalización y la eficiencia del mercado europeo, promoviendo la integración de energías renovables y garantizando la seguridad del suministro. En términos de ciberseguridad, establece directrices para la interoperabilidad de las redes, la integridad de los flujos de información y la protección de sistemas de comunicación y control esenciales para el funcionamiento del mercado, asegurando así la fiabilidad en el intercambio de datos y la operatividad transfronteriza.
- **Reglamento Delegado (UE) 2024/1366**<sup>4</sup>: Complementario al Reglamento 2019/943, este reciente reglamento aborda específicamente los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad. Su objetivo es definir estándares mínimos y protocolos de comunicación seguros entre los diferentes actores involucrados en el intercambio comunitario de electricidad, reduciendo vulnerabilidades y asegurando que los puntos de conexión entre países cuenten con medidas robustas de protección. Así, se refuerza la capacidad de respuesta y la coordinación a nivel europeo ante incidentes que puedan comprometer la integridad de la red eléctrica transnacional.

Estas normas, al conjugarse, ofrecen un marco integral que aborda tanto la preparación y mitigación de riesgos como la seguridad operativa en el mercado y la protección de las interconexiones transfronterizas, constituyendo así una respuesta coordinada y adaptada a las complejas amenazas del entorno digital actual.

---

3. Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, relativo al mercado interior de la electricidad (versión refundida) (“**Reglamento 2019/943**”)

<https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32019R0943>

4. Reglamento Delegado (UE) 2024/1366 de la Comisión, de 11 de marzo de 2024, por el que se completa el Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo mediante el establecimiento de un código de red sobre normas sectoriales específicas para los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad (“**Reglamento Delegado 2024/1366**” o “**Reglamento Delegado**”)

<https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32024R1366>

## 2.1. REGLAMENTO 2019/941: PREPARACIÓN FRENTE A LOS RIESGOS EN EL SECTOR DE LA ELECTRICIDAD

El Reglamento 2019/941 tiene como propósito fundamental fortalecer la seguridad del suministro eléctrico a través de una preparación frente a diversos riesgos. Este instrumento normativo se enmarca dentro del *Paquete de Energía Limpia para todos los Europeos*<sup>5</sup>, y se orienta a garantizar la robustez y continuidad en la prestación de servicios eléctricos mediante una gestión integral tanto amenazas físicas como digitales.

### a. Razonamiento detrás del enfoque basado en riesgos

El Reglamento 2019/941 comienza su preámbulo afirmando que la mejor garantía para la seguridad del suministro eléctrico es, precisamente, que los mercados y sistemas eléctricos funcionen adecuadamente, y en donde las interconexiones eléctricas sean siempre las óptimas. No obstante, incluso cuando los sistemas funcionan adecuadamente, el Reglamento reconoce que el sistema eléctrico se enfrenta a múltiples escenarios de crisis (que además, pueden afectar simultáneamente a distintas regiones europeas), y es por ello por lo que es necesario adoptar un enfoque preventivo y basado en análisis de contingencias.

Para lo anterior el Reglamento 2019/941:

- **Establece la obligación de los Estados miembros de evaluar los riesgos existentes:** Una de las primeras previsiones que recoge este instrumento normativo<sup>6</sup> es que cada Estado miembro debe llevar a cabo una evaluación de riesgos de carácter periódico (cada cuatro años) basada en la metodología que se apruebe por el conjunto de los gestores de red<sup>7</sup>.

Esta medida se fundamenta en la necesidad de anticipar amenazas potenciales antes de que se materialicen, permitiendo identificar vulnerabilidades específicas de cada territorio<sup>8</sup>. Esta evaluación debe actualizarse por los distintos Estados, reflejando la realidad y la nueva experiencia generada.

- **Los Estados miembros deben incluir en el espectro de amenazas todas aquellas que sean potenciales con independencia de su**

5. [https://ec.europa.eu/commission/presscorner/detail/es/ip\\_16\\_4009](https://ec.europa.eu/commission/presscorner/detail/es/ip_16_4009)

6. Artículo 6 del Reglamento 2019/941.

7. Artículo 5 del Reglamento 2019/941.

8. Artículo 6 del Reglamento 2019/941.

**naturaleza<sup>9</sup>, y por tanto, entre ellas, las cibernéticas:** En un mundo interconectado, las amenazas informáticas representan un riesgo real. En la práctica, y en una interpretación finalista del Reglamento y el contexto actual en el que nos encontramos, los Estados miembros están viéndose obligados a valorar nuevas modalidades de amenazas, lo que implica considerar potenciales daños los derivados de la utilización de sistemas digitales, como los ciberataques, los cuales deben ser listados como un posible tipo de evento disruptivo. En este sentido, el Reglamento 2019/941 establece que los escenarios de riesgo deberán ser los más relevantes y pertinentes para cada territorio, no especificando cuáles ni en qué ámbitos.

#### **b. Evaluación y análisis de riesgos: los planes de preparación**

A partir de la evaluación de riesgos, cada Estado miembro debe elaborar y mantener actualizado un **plan nacional de preparación frente a riesgos<sup>10</sup>**. España ha preparado el suyo como se puede ver en el siguiente enlace a pie de página<sup>11</sup>.

La elaboración de estos planes se basa en la idea de que la preparación permite no solo mitigar el impacto de incidentes, sino también responder de manera coordinada y efectiva ante situaciones de crisis. Estos planes deben cumplir con los siguientes elementos:

- **Actualización y revisión periódica<sup>12</sup>:** Cada plan debe actualizarse de forma regular para incorporar las últimas evaluaciones de riesgo y adaptarse a las evoluciones del entorno y sus eventuales amenazas, incluyendo la dinámica de los riesgos cibernéticos.
- **Cooperación y coordinación<sup>13</sup>:** Se debe fomentar una estrecha coordinación tanto a nivel nacional y regional como entre Estados miembros. Esto incluye la comunicación entre operadores de sistemas, autoridades competentes y organismos europeos, lo que permite una respuesta conjunta ante incidentes de gran escala.
- **Medidas preventivas y de respuesta<sup>14</sup>:** Los planes deben contemplar medidas técnicas, organizativas y operativas para prevenir y

---

9. Artículo 7 del Reglamento 2019/941.

10. Capítulo III del Reglamento 2019/941 sobre planes de preparación frente a riesgos.

11. Plan de Preparación frente a los Riesgos en el Sector Eléctrico en España.

12. Artículo 10 del Reglamento 2019/941.

13. Artículo 12 y 15 del Reglamento 2019/941.

14. Artículo 11 y 14 del Reglamento 2019/941.

mitigar los riesgos previstos. Entre estas medidas se incluye la adopción de protocolos de respuesta ante emergencias, la realización de simulacros y la implementación de estrategias de ciberseguridad específicas que aseguren la protección de infraestructuras críticas.

### c. Integración de la ciberseguridad en la seguridad del suministro

Aunque el Reglamento 2019/941 no se dedica específicamente a la ciberseguridad del sector eléctrico, su enfoque integral reconoce que la estabilidad del sistema eléctrico depende en gran parte de la protección de las infraestructuras críticas frente a ataques de cualquier naturaleza, como pueden ser los informáticos. En efecto, el Reglamento, como reconoce su parte expositiva (en complemento de la Directiva 2022/2555<sup>15</sup> NIS2) asegura que los ciberincidentes estén debidamente recogidos como un riesgo y que las medidas adoptadas para abordarlos queden debidamente reflejadas en los planes de preparación mencionados.

A través de esta consideración, los Estados miembros de la Unión deben incorporar en sus planes de actuación, por un lado, **medidas concretas en ciberseguridad, contemplando** que los operadores de sistemas y las autoridades deban incluir en sus estrategias medidas de **detección temprana, notificación y respuesta** ante incidentes cibernéticos. Esto se justifica dado que la interconexión digital de los sistemas de control y gestión incrementa el potencial de vulnerabilidades.

**Para lo anterior, el Reglamento 2019/941 prevé e impulsa** la realización de simulacros de crisis para evaluar la eficacia de los protocolos establecidos. Estas pruebas van a permitir detectar debilidades en la respuesta ante ciberincidentes, promoviendo la mejora constante de los procesos de seguridad.

### d. Conclusión: la importancia del Reglamento 2019/941 en la ciberseguridad del sistema eléctrico

En definitiva, en un plano de la ciberseguridad en la operativa del sector eléctrico, el enfoque que adopta el Reglamento 2019/941 se fundamenta en la idea de que la preparación y la respuesta coordinada ante riesgos son esenciales para garantizar la seguridad del suministro eléctrico. Al integrar la

---

15. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) <https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32022L2555>

ciberseguridad dentro de este marco, se reconoce que las amenazas digitales pueden tener consecuencias tan disruptivas como cualquier otro tipo de riesgo. La lógica subyacente es que, mediante evaluaciones periódicas y planes de contingencia bien estructurados, se puede minimizar el impacto de posibles ciberataques, fortaleciendo así la resiliencia global del sistema eléctrico.

Esta visión integral es crucial en un sector donde la interdependencia tecnológica y operativa ha hecho que la ciberseguridad deje de ser un componente aislado para convertirse en un pilar esencial de la seguridad y la estabilidad de nuestros sistemas eléctricos.

## 2.2. REGLAMENTO (UE) 2019/943: MERCADO INTERIOR DE LA ELECTRICIDAD

El Reglamento (UE) 2019/943<sup>16</sup> se centra en la creación y el fortalecimiento del mercado interior de la electricidad, con el objetivo de garantizar un suministro seguro y competitivo, promover la integración de las energías renovables y aumentar la eficiencia y transparencia en la operación de la red eléctrica europea. Este instrumento normativo, adoptado en el marco de los esfuerzos por alcanzar una mayor cohesión y competitividad en el sector, establece directrices y medidas que repercuten tanto en el aspecto económico como en la gestión técnica y operativa de la electricidad en el territorio comunitario.

El reglamento tiene como metas esenciales:

- **Liberalización y eficiencia del mercado:** La normativa busca eliminar barreras y crear condiciones equitativas para que los operadores y proveedores de energía puedan competir en igualdad de condiciones, fomentando una mayor integración de las diferentes infraestructuras y sistemas eléctricos europeos.
- **Integración de energías renovables:** Se promueve un entorno favorable para la adopción de fuentes de energía renovable, facilitando el acceso y la incorporación de estas a la red, lo que contribuye a la descarbonización del sector.
- **Seguridad y estabilidad del suministro:** A través de medidas que aseguran la interoperabilidad y la integridad de los flujos eléctricos,

---

16. Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, relativo al mercado interior de la electricidad (“**Reglamento 2019/943**”)  
<https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32019R0943>

el reglamento incide en la confiabilidad del sistema. Este aspecto adquiere una relevancia especial en la era digital, donde la protección de la información y la seguridad de las infraestructuras son cruciales para evitar interrupciones.

La definición del “mercado interior de la electricidad” en el reglamento abarca tanto el intercambio de electricidad entre los Estados miembros como la coordinación de las operaciones transfronterizas, marcando un avance en la integración de los mercados eléctricos nacionales en una red cohesionada y moderna.

#### a. Consideraciones en materia de ciberseguridad

Aunque el principal enfoque del Reglamento 2019/943 se orienta hacia la organización y el funcionamiento del mercado eléctrico, se incluyen disposiciones importantes relacionadas con la seguridad de las tecnologías de la información y la protección de la infraestructura crítica:

- **Interoperabilidad y seguridad en las comunicaciones:** El reglamento establece directrices para garantizar que los sistemas de medición, control y gestión que facilitan el intercambio de electricidad operen de manera segura. La integridad en el flujo de información es vital para asegurar una respuesta coordinada ante incidentes y evitar que vulnerabilidades en los sistemas de comunicación interfieran con el funcionamiento del mercado.
- **Requisitos para la protección de la infraestructura digital:** Se hace hincapié en la necesidad de que los operadores adopten medidas que aseguren la confidencialidad, integridad y disponibilidad de los datos, aspecto que adquiere especial importancia en el contexto de la transformación digital del sector eléctrico. La protección contra posibles ciberamenazas se convierte en un componente indispensable para mantener la estabilidad de los servicios de intercambio eléctrico.

En este sentido, se destaca que uno de los elementos centrales del Reglamento 2019/943 en cuanto a ciberseguridad es el desarrollo y la aplicación de los códigos de red<sup>17</sup>. Estos códigos, enmarcados en la literalidad del propio reglamento, están diseñados para asegurar que todos los procesos digitalizados, especialmente aquellos con un impacto crítico o alto en los flujos de electricidad internacionales, se sometan a un proceso recurrente de evaluación de riesgos en materia de ciberseguridad.

17. Artículo 59 del Reglamento 2019/943.

En concreto, el artículo 59 de esta norma se erige como uno de los preceptos clave en este ámbito. De manera específica, este artículo establece el marco para la elaboración y la actualización de los códigos de red, que deben incluir disposiciones para garantizar la protección de las infraestructuras digitales y la continuidad del sistema eléctrico. Este precepto exige que se adopten medidas que aseguren la integridad, confidencialidad y disponibilidad de la información que circula a lo largo de la red, poniendo especial foco en la necesidad de integrar criterios de ciberseguridad en la planificación y gestión de las infraestructuras.

El contenido del artículo 59 se traduce en la obligación de:

- Incluir en los códigos de red que se aprueben un proceso recurrente de evaluación de riesgos de ciberseguridad. Este proceso tiene como fin identificar de forma sistemática a aquellas entidades y procesos digitalizados que resultan críticos o tienen un alto impacto en el intercambio transfronterizo de electricidad.
- Definir, a partir de dichas evaluaciones, las medidas de mitigación necesarias que permitan salvaguardar los sistemas de control, gestión y comunicación. De este modo, se pretende minimizar los riesgos que pudieran derivarse de posibles ciberataques o de vulnerabilidades detectadas en los sistemas digitales.
- Evaluar los riesgos relacionados con la digitalización, tanto en términos operativos como de seguridad de la información.
- Establecer mecanismos de notificación y seguimiento que permitan aplicar medidas correctivas o preventivas ante la detección de vulnerabilidades.
- Establecer de manera eficaz procedimientos a nivel europeo, de forma que la respuesta ante incidentes cibernéticos se dé de manera rápida y coordinada, protegiendo así el suministro eléctrico transfronterizo.

## **b. Conclusión**

El Reglamento (UE) 2019/943, en su letra y en la práctica, incorpora medidas que van más allá del ámbito meramente económico y organizativo del mercado eléctrico. El artículo 59 y la implementación de los códigos de red son instrumentos fundamentales que garantizan una integración sistemática de la ciberseguridad en la operativa diaria del sector.

### 2.3. REGLAMENTO DELEGADO (UE) 2024/1366: COMPLEMENTO DEL REGLAMENTO (UE) 2019/943 EN MATERIA DE CIBERSEGURIDAD

Ya hemos visto como el Reglamento 2019/941 es el instrumento que trata de garantizar, mediante los protocolos y planes de previsión precisos, los incidentes a los que pudiera verse sometidos los sistemas eléctricos comunitarios. De igual manera, lo anterior se complementa por el Reglamento 2019/943 y la Directiva 2022/2555 NIS2 en virtud de los cuáles se requiere que se adopten medidas específicas para preparar, prevenir y mitigar los riesgos cibernéticos en el sector de la electricidad, máxime cuando se trata de flujos transfronterizos.

Como resultado de lo anterior, el pasado año 2024 la Comisión Europea, a partir del mencionado artículo 59 del Reglamento 2019/943 decidió adoptar el primer código de red para la Unión Europea y sus Estados miembros sobre ciberseguridad para el sector eléctrico, aprobando para ello el Reglamento Delegado (UE) 2024/1366 de la Comisión, de 11 de marzo, por el que se completa el Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo mediante el establecimiento de un código de red sobre normas sectoriales específicas para los aspectos relativos a la ciberseguridad de los flujos transfronterizos de electricidad<sup>18</sup>. Este acto delegado es uno de los elementos críticos para concluir la necesidad de establecer un marco robusto y resiliente para las infraestructuras y los servicios energéticos críticos de la Unión.

#### a. Objetivos específicos y medidas que implementa

El Reglamento Delegado 2024/1366 se dicta como complemento de las normas analizadas en este capítulo, orientándose específicamente a reforzar la ciberseguridad en los flujos transfronterizos de electricidad. Este instrumento normativo responde a la necesidad de garantizar que el intercambio de electricidad entre Estados miembros se realice bajo condiciones de seguridad digital que protejan tanto la infraestructura física como los sistemas de gestión, control y comunicación conectados en la red.

Para lo anterior, como señala el preámbulo de esta norma<sup>19</sup> se enfatiza la necesidad de adoptar en este momento un código normativo (el *Código de Red*) destinado a regular las medidas de ciberseguridad. Este código establece un proceso recurrente de evaluación de riesgos en materia de

18. Ya definido como “Reglamento Delegado 2024/1366”.

19. Considerando 11 del Reglamento Delegado 2024/1366.

ciberseguridad, que obliga a, por un lado, a identificar de forma sistemática los procesos digitalizados críticos y aquellos que influyen directamente en los flujos transfronterizos, y por otro, definir las medidas de mitigación necesarias en función de los riesgos identificados.

### b. *Ámbito subjetivo de aplicación*

El Reglamento Delegado busca, como se ha dicho, **coordinar y estandarizar** los protocolos de ciberseguridad entre los distintos Estados miembros, de modo que la protección de la infraestructura digital resulte homogénea en todo el territorio de la UE. Para ello, esta norma define el alcance subjetivo de sus disposiciones.

En efecto, en primer lugar, este Reglamento alcanza en su aplicación a los agentes más relevantes en la operativa de los sistemas eléctricos comunitarios<sup>20</sup>, principalmente, a las empresas eléctricas, Operadores designados para el mercado eléctrico (NEMOs), gestores de red, sujetos de liquidación, proveedores de servicios de seguridad y cualquier otra entidad o tercero con responsabilidades asignadas según esta norma.

Es relevante sobre este ámbito subjetivo destacar que el Reglamento Delegado fija las condiciones y metodologías técnicas que deben adoptar los gestores de redes de transporte (“GRT”) y distribución (“GRD”) para asegurar sus infraestructuras (*críticas*). El Reglamento Delegado establece al respecto<sup>21</sup> procesos colaborativos para la elaboración normativa entre los distintos actores, así como mecanismos de consulta, fijación de criterios comunes entre los distintos agentes, priorizando la armonización técnica a escala europea.

Igualmente, es relevante poner el foco en la regulación que ofrece el Reglamento Delgado 2024/1366 sobre qué han de entenderse por entidades de impacto alto y entidades de impacto crítico<sup>22</sup> y <sup>23</sup>. En síntesis, las entidades

20. Artículo 2 del Reglamento Delegado 2024/1366.

21. Artículos 5 a 17 del Reglamento Delegado 2024/1366.

22. Considerando (7) y artículo 24 del Reglamento Delegado 2024/1366. Se establece que la definición del adjetivo “alto” y “crítico” va a depender de los umbrales ECII y del impacto crítico incluido en el informe sobre evaluación de riesgos para la ciberseguridad a la vista del artículo 19 del Reglamento Delegado.

23. El artículo 48.2 del Reglamento Delegado 2024/1366 prevé que, a más tardar el 13 de octubre de 2024, ENTSO-E, en cooperación con EUDSO ENTITY, elaborará una recomendación de un índice de impacto en la ciberseguridad de la electricidad (ECII) provisional, que será notificado a las autoridades competentes. Esta recomendación se encuentra publicada en la página de ENTSO-E [https://www.entsoe.eu/network\\_codes/nccs/](https://www.entsoe.eu/network_codes/nccs/)

de impacto alto son, en términos generales, aquellas cuyos procesos pueden provocar una degradación notable en el funcionamiento del sistema eléctrico si fueran vulnerados. Por su parte, las entidades de impacto crítico se refieren a aquellas cuya interrupción o fallo podría desencadenar consecuencias severas y amplias sobre la red, afectando tanto el ámbito nacional como el transfronterizo. España ya ha realizado este ejercicio a través de la Comisión Nacional de los Mercados y la Competencia mediante su reciente acuerdo de 13 de marzo de 2025 bajo la rúbrica de *Acuerdo relativo a la determinación de las entidades de impacto alto e impacto crítico, a los efectos del Reglamento Delegado (UE) 2024/1366, sobre ciberseguridad de los flujos transfronterizos de electricidad, según el índice de impacto provisional (DCOOR/DE/002/25)*<sup>24</sup>.

Al respecto, el Reglamento profundiza en la necesidad de identificar sistemáticamente dichas entidades para enfocar los esfuerzos de mitigación y adaptar las medidas de protección a la magnitud del riesgo<sup>25</sup>.

Desde un punto de vista de las autoridades la norma establece el marco institucional a nivel nacional<sup>26</sup> para la aplicación del reglamento, definiendo las entidades responsables y los principios de cooperación entre actores clave del sector eléctrico y la ciberseguridad. Para lo anterior, el Reglamento Delegado establece la obligación de cada Estado miembro de proceder a la designación de la autoridad competente responsables de garantizar el cumplimiento del reglamento. Estas autoridades<sup>27</sup> tendrán competencia para supervisar, coordinar y hacer cumplir las medidas de ciberseguridad vinculadas a los flujos transfronterizos de electricidad.

En este sentido, se exige a los Estados miembros establecer mecanismos de coordinación entre las autoridades designadas, los GRT y GRD, los operadores de mercado y los equipos de respuesta ante incidentes de ciberseguridad (CSIRT<sup>28</sup>). El Reglamento Delegado destaca la necesidad de una interacción fluida entre los distintos niveles de gobernanza, reforzando la colaboración entre las autoridades energéticas y las entidades nacionales competentes en ciberseguridad, en particular con aquellas designadas en

24. <https://www.cnmc.es/sites/default/files/5857696.pdf>

25. Considerando (8) del Reglamento Delegado 2024/1366.

26. (artículos 4 a 7 del Reglamento Delegado)

27. De acuerdo con el artículo 4 del Reglamento Delegado 2024/1366, cada Estado miembro debe designar a una autoridad competente como responsable de llevar a cabo las tareas asignadas en la norma.

28. La red de CSIRT (*Computer Security Incident Response Team*) de la Unión Europea es una red compuesta por CSIRT designados por los Estados miembros de la UE y CERT-EU ("miembros de la red CSIRTs"). La Comisión Europea participa en la red en calidad de observador. <https://csirtnetwork.eu/>

virtud de la Directiva NIS 2. La intención es asegurar la coherencia normativa y operativa en las respuestas a incidentes.<sup>29</sup>

### c. Disposiciones específicas en materia de ciberseguridad

El texto del Reglamento Delegado 2024/1366 trata de establecer a través de su articulado un marco común de ciberseguridad en el mercado interior de la electricidad, regulando cómo van a tener que gestionarse las crisis existentes, la previsión de estos escenarios y los flujos de información, limitando el marco de funcionamiento y evaluación de los niveles de ciberseguridad según las entidades implicadas y los territorios afectados.

En concreto, este el Reglamento Delegado establece cómo han de llevarse a cabo las **evaluaciones de riesgos, sus preparación de planes y medidas de mitigación**<sup>30</sup>. En este sentido, el Reglamento impone la obligación de que los GRT, en coordinación con los de la red de distribución de la UE<sup>31</sup>, elaboren propuestas de condiciones y metodologías para abordar posible situaciones de riesgo. Con lo anterior, estos gestores de red, una vez definidas la metodología de evaluación de riesgos, deben preparar unos planes de evaluación donde se incluyan las posibles ciberamenazas que deben tenerse en cuenta, previéndose la realización de realizar evaluaciones periódicas sobre los riesgos de ciberseguridad<sup>32</sup>, centrándose en identificar aquellas vulnerabilidades que puedan comprometer la continuidad del flujo eléctrico transfronterizo<sup>33</sup>. En función de los resultados de estas evaluaciones, se deben definir las medidas de mitigación adecuadas. Este proceso sistemático se convierte en una herramienta esencial para adaptar las defensas a un entorno digital en constante cambio.

De igual forma, el Reglamento fija los **requisitos técnicos y de interoperabilidad** a los que han de quedar sujetos las entidades de impacto alto o crítico determinada por las autoridades competentes, deberá llevar a cabo una gestión d riesgos de todos sus activos con un enfoque destinado a proteger sus redes y sistemas de información<sup>34</sup>.

29. Artículos 5 y 6 del Reglamento Delegado 2024/1366.

30. Ver capítulo II del Reglamento Delegado sobre evaluación de riesgos y determinación de los riesgos para la ciberseguridad.

31. Capítulo II del Reglamento Delegado 2024/1366 bajo la rúbrica de Evaluación de riesgo y determinación de los riesgos para la ciberseguridad pertinentes.

32. Artículo 20 del Reglamento Delegado 2024/1366.

33. Artículo 19 del Reglamento Delegado 2024/1366 sobre evaluación de riesgos para la ciberseguridad a escala de la Unión.

34. Artículo 26 del Reglamento Delegado 2024/1366.

De manera consecuente, con base en lo anterior, el instrumento normativo concluye con el establecimiento **marco común de ciberseguridad en los mercados de la electricidad**, regulando modos y protocolos de actuación, dibujando los controles a ejecutar en materia de ciberseguridad<sup>35</sup> (mínimos o avanzados) seguidos de una matriz cartográfica de esos controles.

Como es de ver, una de las principales preocupaciones del Reglamento es cómo debe procederse. Por ello, además de lo anterior se fijan planes y protocolos para el **flujo de información y gestión de situaciones de crisis**<sup>36</sup> en los que se especifican las obligaciones de establecer planes de respuesta ante incidentes cibernéticos que puedan afectar a la integridad de la red. Estos protocolos deben incluir, entre otros aspectos, la notificación inmediata a las autoridades competentes, la coordinación entre operadores y la ejecución de acciones correctivas, así como, la preparación de informes sobre evaluación de esos riesgos. La finalidad es responder de manera rápida y coordinada, minimizando el impacto de los incidentes en el suministro transfronterizo de electricidad.

Como el Reglamento Delegado destaca en su composición de lugar a través del preámbulo<sup>37</sup>, se reconoce en definitiva a la importancia de armonizar conceptos y procedimientos en toda la Unión Europea para evitar discrepancias en la aplicación y garantizar una respuesta coordinada. Además, se prevé la cooperación con terceros países, facilitando la adopción de estándares comunes y permitiendo la interoperabilidad de las redes a nivel global. Estos estándares son necesarios y van a seguir para asegurar una comunicación segura y resiliente, que resista intentos de intrusión o manipulación maliciosa en un entorno altamente interconectado.

Todo lo anterior, tendrá que ejecutarse en el marco de una **actualización continua de las medidas de ciberseguridad**. En este sentido, el Reglamento Delegado reconoce la naturaleza dinámica de las amenazas cibernéticas, el reglamento destaca la importancia de que las medidas de protección se revisen y actualicen de forma periódica. Este enfoque de mejora continua garantiza que tanto los avances tecnológicos como los nuevos vectores de ataque sean considerados en la protección del sistema.

Por último, se destaca que a través del Reglamento Delegado se pone en marcha una cultura de **simulación y entrenamiento mediante ejercicios de ciberseguridad organizados** regularmente a escala regional o transregio-

35. Capítulo III sobre el marco común de ciberseguridad, artículos 28 a 34.

36. Capítulo V sobre flujos de información, ciberataques y gestión de crisis.

37. Considerando 19 del Reglamento Delegado 2024/1366.

nal. Estas prácticas permiten no solo probar la efectividad de los planes y protocolos adoptados, sino también identificar vulnerabilidades y generar conocimiento práctico para enfrentar amenazas reales.

**d. Conclusión: Relevancia y aportación al sistema eléctrico europeo**

La incorporación de estas medidas en el Reglamento Delegado 2024/1366 tiene un impacto significativo en la seguridad global del mercado eléctrico europeo. Al centrar la atención en la protección de los flujos transfronterizos, el reglamento:

- **Fortalece la resiliencia del sistema:** Al implementar evaluaciones recurrentes de riesgos y establecer protocolos de respuesta coordinados, se minimiza la vulnerabilidad de la red frente a ciberataques, asegurando así la continuidad del suministro eléctrico en situaciones de crisis.
- **Promueve una estandarización europea:** La exigencia de implementar medidas técnicas comunes fomenta la uniformidad en la ciberseguridad a lo largo del territorio de la UE. Esto facilita la colaboración entre los Estados miembros y permite una respuesta conjunta ante amenazas que trascienden fronteras nacionales.
- **Impulsa la transformación digital segura:** Mediante la integración de estos requisitos, el reglamento no solo refuerza la seguridad del mercado eléctrico, sino que también impulsa la transformación digital del sector, estableciendo un marco que equilibra la innovación y la protección de infraestructuras críticas.

## Legislación nacional específica en materia de seguridad nacional, ciberseguridad, resiliencia operativa

ROSA ORTUÑO

*Profesora Colaboradora Esade Law School*

La normativa afectada por el anteproyecto de ley de coordinación y gobernanza de la ciberseguridad incluye varias disposiciones legales que serán derogadas o modificadas. A continuación, se detallan las principales normativas afectadas:

### **Normativa Derogada**

1. **Real Decreto-ley 12/2018, de 7 de septiembre:**
  - De seguridad de las redes y sistemas de información.
2. **Real Decreto 43/2021, de 26 de enero:**
  - Por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
  - Se exceptúa la Instrucción Nacional de Notificación y Gestión de Ciberincidentes contenida en su anexo, que seguirá vigente hasta que sea expresamente modificada, sustituida o derogada.

### **Normativa Modificada**

1. **Ley 5/2014, de 4 de abril, de Seguridad Privada:**
  - Se modifica el apartado 2 del artículo 3 para incluir al personal que realice tareas de ciberseguridad como personal acreditado.

- Se modifica el apartado 9 del artículo 2 para incluir al personal que realice tareas de ciberseguridad en los casos que legal o reglamentariamente se determine.

## **Incorporación al Derecho Español**

1. **Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022:**
  - Relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.
  - Modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972.
  - Deroga la Directiva (UE) 2016/1148.

## **Disposiciones Adicionales**

1. **Disposición adicional primera:**
  - Creación del Centro Nacional de Ciberseguridad.
2. **Disposición adicional segunda:**
  - Régimen específico del Banco de España.
3. **Disposición adicional tercera:**
  - Información sobre incidentes en el sistema financiero.
4. **Disposición adicional cuarta:**
  - Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.
5. **Disposición adicional quinta:**
  - Base de datos de incidencias de seguridad que revistan carácter de delito.
6. **Disposición adicional sexta:**
  - Salvaguarda de intereses y funciones estatales esenciales.

**7. Disposición adicional séptima:**

- Representación en el Centro Europeo de Competencia Industrial.

**8. Disposición adicional octava:**

- Autoridad Nacional de Certificación de la Ciberseguridad.

**Disposiciones Transitorias**

**1. Disposición transitoria primera:**

- Obligaciones de comunicación.

**2. Disposición transitoria segunda:**

- Registro de entidades.

**3. Disposición transitoria tercera:**

- Régimen transitorio.

**Disposición Derogatoria Única**

- Derogación normativa de las disposiciones mencionadas anteriormente.

**Disposiciones Finales**

**1. Disposición final primera:**

- Título competencial.

**2. Disposición final segunda:**

- Modificación de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

**3. Disposición final tercera:**

- Desarrollo reglamentario.

**4. Disposición final cuarta:**

- Incorporación al derecho de la Unión Europea.

5. **Disposición final quinta:**

- Entrada en vigor.

**Directivas de la UE afectadas**

1. **Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022:**

- Relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.
- Modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972.
- Deroga la Directiva (UE) 2016/1148.

2. **Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016:**

- Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Esta directiva es derogada por la Directiva (UE) 2022/2555.

3. **Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022:**

- Relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.

4. **Directiva 2009/73/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009:**

- Relativa a normas comunes para el mercado interior del gas natural.

5. **Directiva 2012/34/UE del Parlamento Europeo y del Consejo, de 21 de noviembre de 2012:**

- Por la que se establece un espacio ferroviario europeo único.

6. **Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014:**

- Relativa a los mercados de instrumentos financieros.

## ESTUDIOS

La ciberseguridad en el sector eléctrico es una cuestión de continuidad de servicio y seguridad pública. La digitalización de la red, la operación remota y la interdependencia con otros sectores críticos han ampliado la superficie de ataque. Un incidente que interrumpa el suministro no solo afecta a empresas: paraliza hospitales, transporte, finanzas y servicios esenciales.

La convergencia entre TI (Tecnologías de la Información) y TO (Tecnologías de Operación) multiplica los riesgos. Equipos de control industrial con décadas de vida útil, protocolos inseguros y cadenas de suministro complejas conviven con plataformas modernas, nube y análisis en tiempo real. Delincuencia organizada, actores estatales y hacktivismo usan ransomware, intrusiones por terceros y ataques a la integridad de datos para causar impacto rápido y ganar ventaja económica o geopolítica.

La transición energética añade complejidad. La integración masiva de renovables, almacenamiento, microrredes y millones de contadores inteligentes introduce dispositivos perimetrales expuestos, telemetría abundante y nuevos vectores de intrusión. A la vez, el mercado exige flexibilidad y visibilidad granular, elevando el valor de los datos y la necesidad de protegerlos.

La respuesta debe combinar resiliencia y cumplimiento. Segmentación de redes y «zero trust», gestión de identidades y accesos, inventario y hardening de activos, supervisión continua, copias inmutables y planes de respuesta probados con ejercicios son pilares básicos. Igual de clave es la cultura: formación, colaboración pública privada y seguridad desde el diseño en proyectos y compras. Proteger la red es en definitiva proteger la economía y la vida cotidiana.

ISBN: 978-84-1085-483-3



ER-02802005



GA-20050100