



DERECHOS
DIGITALES

Declaración de Deberes y Responsabilidades Digitales

Marzo de 2026



fundaciónHermes
derechos de
ciudadanía
digital



Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA GENERAL
DE POLÍTICAS
ECONÓMICAS Y
INDUSTRIALES

red.es



Plan de
Recuperación,
Transformación
y Resiliencia

CONTENIDO

PREÁMBULO	4
DECÁLOGO DE LA DECLARACIÓN DE DEBERES Y RESPONSABILIDADES DIGITALES	6
CAPÍTULO I: DEBERES RELATIVOS AL ACCESO DIGITAL Y LA CIBERSEGURIDAD	8
Sección 1. Acceso universal y brechas digitales	9
Sección 2. Igualdad, no discriminación y accesibilidad	9
Sección 3. Ciberseguridad	10
CAPÍTULO II: DEBERES RELATIVOS A LA IDENTIDAD DIGITAL	11
Sección 1. Principios generales	12
Sección 2. Deberes de los poderes públicos	12
Sección 3. Deberes de los prestadores de servicios digitales y de las plataformas	12
Sección 4. Deberes de los particulares	12
CAPÍTULO III: DEBERES RELATIVOS A LA PROTECCIÓN DE DATOS PERSONALES	13
Sección 1. Principios generales	14
Sección 2. Deberes de los poderes públicos	14
Sección 3. Deberes de los prestadores de servicios digitales y de las plataformas	14
Sección 4. Deberes de los particulares	15
CAPÍTULO IV: DEBERES RELATIVOS A LOS CONTENIDOS Y A LA LIBERTAD DE EXPRESIÓN E INFORMACIÓN	16
Sección 1. Libertad de expresión e información en entornos digitales	17
Sección 2. Libertad de creación y acceso a la cultura	17
Sección 3. Transparencia informativa y lucha contra la desinformación	18
CAPÍTULO V: DEBERES RELATIVOS A LA PARTICIPACIÓN CIUDADANA POR MEDIOS DIGITALES	19
Sección 1. Participación ciudadana digital y servicios electrónicos	20
Sección 2. Accesibilidad digital, participación inclusiva y alfabetización tecnológica	20
CAPÍTULO VI: DEBERES RELATIVOS A LA ACTIVIDAD ECONÓMICA:	
LIBERTAD DE EMPRESA Y ENTORNO LABORAL	21
Sección 1. Libertad de empresa en el entorno digital	22
Sección 2. Entorno laboral digital	23

CAPÍTULO VII: DEBERES RELATIVOS A LA PROTECCIÓN DE LOS MENORES Y LA EDUCACIÓN	24
Sección 1. Educación y alfabetización digital	25
Sección 2. Protección activa de los menores en el entorno digital	25
CAPÍTULO VIII: DEBERES RELATIVOS AL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL	26
Sección 1. Principios generales	27
Sección 2. Obligaciones de los diseñadores y desarrolladores de algoritmos	27
Sección 3. Obligaciones de los usuarios de sistemas de inteligencia artificial	27
SUJETOS OBLIGADOS EN EL ÁMBITO DIGITAL	28
Sección 1. Poderes públicos	30
Sección 2. Plataformas y empresas proveedoras de contenidos y servicios digitales	32
Sección 3. Empresas y particulares	33
GLOSARIO	33

Preámbulo

El siglo XXI está marcado por la digitalización. Este proceso ha transformado de manera profunda nuestras sociedades, no solo en el plano tecnológico y económico, sino también en los hábitos, las relaciones sociales y las formas de vida, afectando tanto a la esfera pública como a la personal. La digitalización plantea desafíos de amplio alcance, ante los cuales los poderes públicos tienen la obligación de ofrecer respuestas eficaces o, cuando menos, de afrontarlos de forma responsable.

Una de las primeras respuestas institucionales a esta transformación ha sido el reconocimiento y desarrollo de los derechos en el entorno digital. Ese paso es esencial: los Estados de Derecho deben reflexionar y actuar sobre los efectos que las tecnologías pueden tener en los derechos y libertades de las personas. Esta orientación ha guiado también la acción de organizaciones internacionales y de instituciones regionales como la Unión Europea, que ha situado la regulación del entorno digital entre sus prioridades.

En los últimos años, tanto a nivel nacional como internacional, se ha desplegado una intensa actividad normativa orientada a formular y garantizar los derechos digitales, en un momento de aceleración tecnológica y de creciente dependencia social y económica de los servicios digitales. En el ámbito europeo, la Unión Europea ha reforzado este impulso regulatorio como parte de su agenda estratégica. En España, la aprobación de la Carta de Derechos Digitales constituye un referente en este esfuerzo y expresa la voluntad de contribuir, desde el marco constitucional, a una protección efectiva de las personas en el entorno digital.

Sin embargo, el reconocimiento de derechos resulta insuficiente si no se acompaña de condiciones efectivas para su ejercicio. Igual que sucede en el ámbito analógico, un Estado social y democrático de Derecho no puede limitarse a declarar derechos: debe también identificar responsabilidades y deberes que hagan posible su vigencia real. Estos deberes corresponden, en primer lugar, a los poderes públicos, y también, con distinta intensidad, a los actores privados que diseñan, despliegan u operan servicios digitales con impacto significativo. En ningún caso puede situarse a la ciudadanía en un plano equivalente al de las grandes plataformas tecnológicas o al de los poderes públicos como sujetos de deberes en términos homogéneos. Ello no se corresponde con las asimetrías reales de posición e influencia existentes en el ecosistema digital: determinadas plataformas controlan infraestructuras, datos y arquitecturas algorítmicas con capacidad de condicionamiento sistémico; los poderes públicos ejercen funciones de regulación, garantía y supervisión; mientras que la ciudadanía dispone, por regla general, de un margen de actuación más limitado y no siempre puede ejercerlo con plena autonomía por razones técnicas, económicas o de diseño. En consecuencia, las obligaciones más exigentes deben recaer sobre quienes ostentan mayor capacidad de diseño, control y escala, así como de prevención de riesgos.

Por ello, en el ámbito digital resulta necesario articular un catálogo de deberes y responsabilidades formulado de manera autónoma y específica. La complejidad propia de la digitalización exige criterios claros de asignación: las obligaciones deben graduarse conforme al papel de cada actor, su capacidad de prevención de daños y su impacto sobre derechos fundamentales, incluyendo exigencias de transparencia, diligencia debida (prevención, evaluación y mitigación de riesgos) y rendición de cuentas. Estos deberes se formulan como criterios de responsabilidad y prevención de daños, y no como una traslación impropia de cargas a quienes carecen de control real sobre los sistemas digitales.

Un aspecto decisivo es, por tanto, la determinación de los sujetos obligados. En el entorno analógico, los poderes públicos eran los principales responsables de cumplir y hacer cumplir los deberes. En el entorno digital, junto a ellos adquieren un papel central nuevos actores privados, en particular plataformas y grandes prestadores de servicios digitales, cuyo impacto sistémico hace indispensable asignarles deberes claros y verificables en relación con los servicios que prestan y los riesgos que generan.

Si se pretende que los derechos digitales sean plenamente efectivos, finalidad última de esta Declaración, resulta imprescindible reconocer y ordenar estas responsabilidades. De lo contrario, el texto quedaría incompleto y con escasa capacidad orientadora en un entorno donde la arquitectura técnica y las decisiones privadas influyen de manera directa en el ejercicio de los derechos.

Por ello, la presente Declaración de Deberes y Responsabilidades Digitales se estructura en tres partes: una disposición preliminar, un catálogo de deberes y un apartado final sobre los sujetos obligados, tanto públicos como privados. Su propósito es establecer un referente común para orientar la actuación responsable de los distintos actores y reforzar la garantía y el ejercicio efectivo de los derechos de las personas en el entorno digital.

Decálogo de la Declaración de Deberes y Responsabilidades Digitales

En los últimos años, el entorno digital ha pasado de ser un ámbito principalmente tecnológico a convertirse en una infraestructura cotidiana que requiere reglas claras y garantías fiables. En Europa, ese cambio ha impulsado un marco de referencia cada vez más definido para proteger a las personas y dar seguridad a quienes operan servicios digitales. España ha contribuido a este avance con la Carta de Derechos Digitales, que fija un punto de partida sobre lo que debe protegerse.

Esta Declaración se apoya en ese trabajo y lo complementa con la otra pieza imprescindible para que los derechos sean efectivos: responsabilidades concretas y proporcionadas para quienes diseñan, operan y gobiernan lo digital. Su objetivo es práctico: traducir principios en obligaciones aplicables, reforzar la transparencia, la diligencia debida y la rendición de cuentas, y consolidar un entorno de confianza que favorezca la innovación responsable. Este decálogo resume la Declaración en diez compromisos claros y verificables, pensados para la ciudadanía y para quienes toman decisiones en administraciones, empresas y plataformas.

1. Más poder, más responsabilidad

Las obligaciones más exigentes recaen en quienes diseñan, operan y escalan servicios digitales, especialmente plataformas y grandes prestadores con capacidad de influir en datos, algoritmos y condiciones de acceso.

2. Acceso digital para todos, sin brechas

Las administraciones deben asegurar conectividad asequible y de calidad y políticas activas para reducir desigualdades por territorio, edad, discapacidad o situación socioeconómica.

3. Lo público debe ser digital

Los servicios públicos y la participación digital deben facilitar derechos. Cuando lo digital sea una barrera, deben existir alternativas para garantizar el acceso efectivo.

4. Alfabetización digital para ejercer derechos

Las administraciones deben impulsar capacitación digital inclusiva y evaluable. Centros, empresas y plataformas deben contribuir a un uso comprensible, seguro y accesible.

5. Tus datos bajo control

Administraciones, empresas y plataformas deben tratar datos con licitud, minimización y transparencia, con protección desde el diseño y por defecto y seguridad adecuada.

6. Ciberseguridad como estándar de confianza

Poderes públicos deben supervisar y fortalecer capacidades. Prestadores, en especial plataformas, deben prevenir, detectar, responder y recuperarse de incidentes con medidas proporcionales al riesgo y canales claros.

7. Igualdad, accesibilidad y decisiones automatizadas con garantías

Quien diseñe o use sistemas automatizados debe identificar y mitigar sesgos, evitar discriminación, asegurar accesibilidad y garantizar intervención humana significativa cuando haya efectos relevantes.

8. Identidad digital protegida

Debe prevenirse la suplantación y la vulneración de identidades. Debe permitirse el uso de seudónimos salvo necesidad legal o de seguridad.

9. Libertad de expresión con moderación responsable y transparente

Las plataformas deben proteger la expresión lícita, actuar frente a lo ilícito con diligencia y procedimiento, motivar decisiones y ofrecer mecanismos accesibles de reclamación y revisión.

10. Menores, neurotecnologías e inteligencia artificial con responsabilidades reforzadas

Los servicios accesibles a menores deben aplicar protección reforzada. El uso de neurodatos debe evitar discriminación y manipulación ilícita. La IA debe aplicarse con enfoque basado en riesgos, supervisión humana, documentación cuando proceda y límites normativos claros.

CAPÍTULO I: Deberes relativos al acceso digital y la ciberseguridad



CAPÍTULO I: DEBERES RELATIVOS AL ACCESO DIGITAL Y LA CIBERSEGURIDAD

Sección 1. Acceso universal y brechas digitales

1. Las autoridades competentes deberán garantizar que todas las personas dispongan de un acceso asequible, de calidad, continuo y no discriminatorio a los servicios básicos de conexión a Internet de alta capacidad.
2. Dicho acceso se ajustará a los requisitos del servicio universal vigentes en cada momento.
3. El cumplimiento de estos deberes por parte de los poderes públicos no supondrá, en ningún caso, que se prive a la ciudadanía de la facultad de no emplear medios digitales para el ejercicio de sus derechos.

Políticas públicas para la inclusión digital.

Las autoridades competentes deberán desarrollar e implementar políticas públicas activas que permitan:

- a) Asegurar la conectividad digital en todo el territorio, con especial atención a las zonas rurales o insuficientemente atendidas.
- b) Garantizar la accesibilidad universal a los servicios, contenidos y plataformas digitales, de acuerdo con los estándares técnicos aplicables.
- c) Reducir las desigualdades de acceso y uso derivadas de factores socioeconómicos, de género, edad o discapacidad.
- d) Promover la disponibilidad de dispositivos y recursos tecnológicos esenciales.
- e) Impulsar la capacitación digital de toda la población, con especial atención a las personas mayores, con baja autonomía o en riesgo de exclusión.

Sección 2. Igualdad, no discriminación y accesibilidad

1. Toda persona física o jurídica que diseñe, implemente, gestione o preste servicios o plataformas digitales, deberá garantizar el respeto efectivo del principio de igualdad, evitando cualquier forma de discriminación o exclusión por razón de sexo, género, edad, origen étnico, discapacidad u otra circunstancia personal o social.
2. Deberán adoptar, en particular, medidas para:
 - a) Incorporar la perspectiva de género en el diseño y uso de tecnologías digitales.
 - b) Identificar y corregir posibles sesgos en los datos, algoritmos o procesos de decisión automatizada.

3. Responsabilidad de las administraciones públicas

Las administraciones públicas, en sus funciones de regulación, supervisión y contratación tecnológica, deberán garantizar el cumplimiento de los deberes establecidos en esta sección, promoviendo la transparencia, la equidad algorítmica y el desarrollo de tecnologías inclusivas.

Sección 3. Ciberseguridad

1. Obligaciones de los poderes públicos

- a) Supervisar el cumplimiento de las obligaciones de ciberseguridad previstas en la normativa europea y nacional.
- b) Impulsar la sensibilización y la formación de la sociedad en materia de ciberseguridad.
- c) Implementar políticas robustas que incluyan análisis de riesgos, gestión de crisis y planes de formación y continuidad de negocio.

2. Obligaciones de los prestadores de servicios y gestores de plataformas digitales

Quienes presten servicios digitales deberán adoptar medidas proporcionales al nivel de riesgo, a fin de garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de los datos y servicios.

Las empresas deberán implementar políticas sólidas que incluyan análisis de riesgos, gestión de crisis y planes de formación y continuidad de negocio.

Deberán, además, establecer canales claros y funcionales para la comunicación de incidentes por parte de los usuarios. Asimismo, deberán contar con procedimientos de prevención, detección, respuesta y recuperación ante incidentes, incluyendo, cuando proceda, la notificación de incidentes significativos a las autoridades competentes conforme a la normativa aplicable

CAPÍTULO II: Deberes relativos a la identidad digital





CAPÍTULO II: DEBERES RELATIVOS A LA IDENTIDAD DIGITAL

Sección 1. Principios generales

1. Todas las personas físicas o jurídicas, públicas o privadas, deberán respetar la identidad digital de terceros conforme a lo establecido en el ordenamiento jurídico nacional, europeo e internacional.

Sección 2. Deberes de los poderes públicos

1. Los poderes públicos deberán garantizar que el respeto a la identidad digital se integre en la normativa y en las políticas públicas, incluyendo medidas de prevención, protección y reparación frente a su vulneración.

Sección 3. Deberes de los prestadores de servicios digitales y de las plataformas

1. Los prestadores de servicios digitales y las plataformas deberán:
 - a) Permitir el acceso y uso de sus entornos mediante seudónimos o identificadores indirectos, siempre que la identificación personal no sea necesaria ni proporcionada para fines legítimos del servicio, para garantizar derechos de terceros o cumplir obligaciones legales de verificación o seguridad.
 - b) Adoptar medidas para prevenir la vulneración de la identidad digital de los usuarios.

Sección 4. Deberes de los particulares

1. Los particulares deberán respetar la identidad digital de terceros en todas sus interacciones en entornos digitales.

CAPÍTULO III: Deberes relativos a la protección de datos personales



CAPÍTULO III: DEBERES RELATIVOS A LA PROTECCIÓN DE DATOS PERSONALES

Sección 1. Principios generales

1. Todas las personas físicas o jurídicas, públicas o privadas, que traten datos personales deberán respetar los principios de licitud, lealtad, transparencia, minimización, exactitud, integridad y confidencialidad, limitación de la finalidad y del plazo de conservación, así como los de responsabilidad proactiva y protección de datos desde el diseño y por defecto
2. En particular, el desarrollo de neurotecnologías y el tratamiento de neurodatos deberán respetar los derechos fundamentales, especialmente la dignidad, la privacidad, la autonomía, la identidad personal y el libre desarrollo de la personalidad. Queda prohibido el uso discriminatorio de neurodatos y toda práctica de manipulación mental o que menoscabe la autonomía de la persona, en particular cuando se realice sin información suficiente o sin base jurídica o consentimiento válido, según corresponda.

Sección 2. Deberes de los poderes públicos

1. Los poderes públicos deberán fomentar la formación y la concienciación en materia de protección de datos, con especial atención a los menores de edad.
2. Asimismo, deberán establecer marcos jurídicos claros sobre el desarrollo y uso de las neurotecnologías, establecer marcos jurídicos claros sobre el desarrollo y uso de las neurotecnologías, tratando los neurodatos como datos especialmente sensibles y asegurando, cuando proceda, el nivel reforzado de protección previsto para categorías especiales, y prevenir desigualdades sociales en el acceso a dichas tecnologías

Sección 3. Deberes de los prestadores de servicios digitales y de las plataformas

1. Los prestadores de servicios digitales y las plataformas deberán:
 - a) Informar de manera clara y accesible sobre la finalidad y condiciones de los tratamientos de datos y, en su caso, sobre la lógica aplicada, especialmente cuando existan decisiones automatizadas o perfilado con efectos relevantes.
 - b) Implantar medidas de seguridad adecuadas para prevenir accesos no autorizados, pérdidas, alteraciones o usos indebidos
 - c) Diseñar tecnologías respetuosas con la dignidad, la autonomía y la privacidad de las personas.
 - d) Abstenerse de comercializar o tratar ilícitamente neurodatos, así como de desarrollar o desplegar sistemas que interfieran en la autonomía o el libre desarrollo de la personalidad.

Sección 4. Deberes de los particulares

1. Además de los deberes previstos en los apartados anteriores que les sean de aplicación, los particulares deberán:
 - a) Actuar con veracidad y responsabilidad al aportar datos personales.
 - b) Respetar la confidencialidad de los datos a los que accedan.
 - c) No emplear neurotecnologías con fines ilícitos ni obtener ventajas indebidas mediante el uso ilegítimo de dichas tecnologías.

CAPÍTULO IV: Deberes relativos a los contenidos y a la libertad de expresión e información

IV.

CAPÍTULO IV: DEBERES RELATIVOS A LOS CONTENIDOS Y A LA LIBERTAD DE EXPRESIÓN E INFORMACIÓN

Sección 1. Libertad de expresión e información en entornos digitales

1. Todas las personas deberán ejercer su libertad de expresión en entornos digitales respetando el ordenamiento jurídico y los derechos de terceros.
2. Queda prohibida la difusión de contenidos ilícitos, de acuerdo con la normativa aplicable.
3. Las personas responderán cuando proceda civil y penalmente por los contenidos que difundan cuando vulneren el ordenamiento jurídico o los derechos de terceros.

Obligaciones de los prestadores de servicios digitales y de las plataformas.

Los prestadores de servicios digitales y las plataformas deberán:

- a) Abstenerse de interferir en la expresión lícita de los usuarios.
- b) Retirar o inutilizar el acceso a contenidos ilícitos con diligencia, tras adquirir conocimiento efectivo de su existencia o recibir la correspondiente orden o notificación conforme a los procedimientos aplicables, garantizando mecanismos de reclamación y revisión.
- c) Aplicar políticas de moderación con transparencia y proporcionalidad, incluyendo información y motivación suficientes sobre las decisiones de moderación, y garantizando mecanismos de reclamación accesibles.
- d) Proteger los derechos de propiedad intelectual mediante procedimientos y medidas adecuadas y proporcionadas para prevenir y reaccionar frente a infracciones, sin interferir indebidamente en la expresión lícita.

Sección 2. Libertad de creación y acceso a la cultura

1. Las personas físicas y jurídicas que operen en el ámbito cultural digital deberán respetar la libertad de creación y los derechos morales y patrimoniales de los autores.
2. Los poderes públicos deberán desarrollar políticas activas para fomentar la cultura en el entorno digital, combatiendo las brechas culturales digitales y garantizando la pluralidad de voces creativas y el acceso universal a los contenidos culturales.

3. Obligaciones de las administraciones culturales

Las administraciones competentes en materia cultural deberán:

- a) Digitalizar el patrimonio cultural público y garantizar su disponibilidad en formatos accesibles.
- b) Asegurar el acceso libre a las obras en dominio público y difundirlas mediante plataformas abiertas.
- c) Establecer directrices para preservar la integridad y la autoría de las obras accesibles digitalmente.

Sección 3. Transparencia informativa y lucha contra la desinformación

1. Obligaciones de los medios de comunicación y de las plataformas digitales

Las plataformas digitales y los prestadores de servicios informativos deberán:

- a) Informar de manera clara cuando los contenidos hayan sido generados o manipulados mediante sistemas automatizados, especialmente cuando puedan inducir a error sobre su autenticidad, incluidos los *deepfakes*.
- b) Advertir de la priorización informativa basada en el perfilado de datos personales, en particular cuando se utilicen sistemas de recomendación o ranking personalizado.
- c) Identificar de forma inequívoca los contenidos patrocinados o publicitarios.

2. Deberes de los prestadores de servicios digitales y de las plataformas digitales

Los prestadores de servicios digitales y las plataformas digitales que difundan contenidos deberán habilitar mecanismos eficaces para que las personas usuarias puedan solicitar la rectificación, actualización o supresión de información lesiva, errónea o desactualizada, conforme a la normativa aplicable, y, cuando proceda, ejercer los derechos vinculados a la desindexación o al denominado derecho al olvido

3. Responsabilidad de los medios de comunicación

Además de los deberes anteriores, los medios de comunicación digitales con responsabilidad editorial deberán garantizar el derecho de las personas a la rectificación, conforme a la normativa aplicable.

CAPÍTULO V: Deberes relativos a la participación ciudadana por medios digitales

V.

**CAPÍTULO V:
DEBERES RELATIVOS A LA PARTICIPACIÓN CIUDADANA
POR MEDIOS DIGITALES****Sección 1. Participación ciudadana digital y servicios electrónicos**

1. Los poderes públicos deberán desarrollar, mantener y actualizar canales digitales que hagan efectivo el derecho de participación de la ciudadanía, sin perjuicio de garantizar vías no digitales cuando resulte necesario para evitar exclusión o asegurar la efectividad de los derechos.
2. En particular, dichos canales deberán permitir y facilitar a las personas:
 - a) El acceso a los servicios públicos.
 - b) La participación activa en la toma de decisiones públicas.
 - c) La formulación de propuestas.
 - d) El acceso a la información institucional.

3. Principios de los procesos de participación digital

Los procesos de participación digital promovidos por entidades públicas o privadas, cuando se vinculen a procesos de participación pública o a la prestación de servicios de interés general, deberán observar:

- a) Transparencia procedimental y documental.
- b) Trazabilidad e integridad de las aportaciones.
- c) Igualdad y no discriminación en el acceso y en la influencia.
- d) Accesibilidad tecnológica universal y diseño inclusivo.
- e) Respeto a la pluralidad ideológica y a la libertad de opinión.
- f) Garantía del secreto del voto, y de la integridad del proceso, cuando así lo exija la legislación aplicable

Sección 2. Accesibilidad digital, participación inclusiva y alfabetización tecnológica

1. Los proveedores de servicios o plataformas digitales, tanto públicos como privados, deberán garantizar que los entornos digitales, sus contenidos e interfaces sean accesibles y comprensibles para todas las personas, especialmente en el caso de servicios esenciales o financiados con fondos públicos.
2. Obligaciones de las administraciones públicas

Las administraciones públicas deberán asegurar que todos los canales y plataformas de participación en asuntos públicos, incluidos los procedimientos electrónicos y las herramientas de consulta ciudadana, sean plenamente accesibles y utilizables para todas las personas, incluidas las personas con discapacidad, teniendo en cuenta las posibles barreras tecnológicas.

CAPÍTULO VI:
Deberes
relativos
a la actividad
económica:
libertad de
empresa y
entorno laboral

VI.

**CAPÍTULO VI:
DEBERES RELATIVOS A LA ACTIVIDAD ECONÓMICA:
LIBERTAD DE EMPRESA Y ENTORNO LABORAL****Sección 1. Libertad de empresa en el entorno digital**

1. Las empresas que operen en el entorno digital deberán desarrollar sus actividades conforme a los principios de equidad, transparencia, seguridad, interoperabilidad y sostenibilidad, de manera proporcionada a su tamaño, capacidad e impacto, respetando los derechos de las personas y las normas de competencia.

2. Sistemas internos de cumplimiento normativo

La transformación digital de las empresas exige establecer sistemas internos de cumplimiento normativo, adecuados y proporcionales, que aseguren el respeto a:

- a) La protección de datos y la privacidad.
- b) La igualdad.
- c) La accesibilidad tecnológica.
- d) Los derechos laborales.
- e) La transparencia algorítmica, cuando se utilicen sistemas automatizados con efectos relevantes.

3. Obligaciones de las plataformas digitales

Las plataformas digitales, en el ejercicio de su actividad, deberán, en función de su papel, tamaño e impacto, y conforme a la normativa aplicable:

- a) Respetar el principio de transparencia.
- b) Garantizar el tratamiento lícito de los datos personales y, cuando proceda, la revisión humana de decisiones automatizadas.
- c) Garantizar la interoperabilidad y la portabilidad de los datos, en los términos previstos por la normativa aplicable, facilitando, cuando proceda, la transferencia entre plataformas.
- d) Evitar prácticas, anticompetitivas, incluidas la autopreferencia o el bloqueo injustificado de aplicaciones alternativas.
- e) Informar de manera clara sobre los criterios de visibilidad y priorización de contenidos, bienes o servicios, según corresponda.
- f) Establecer mecanismos accesibles y eficaces para la resolución de conflictos.

4. Obligaciones de los poderes públicos en el ámbito económico

Los poderes públicos deberán diseñar políticas económicas y regulatorias que garanticen y favorezcan un entorno digital competitivo, innovador y libre de prácticas abusivas, e impulsar la creación de entornos controlados de experimentación jurídica supervisada para tecnologías emergentes.

Sección 2. Entorno laboral digital

1. Las personas físicas o jurídicas empleadoras, públicas o privadas, deberán respetar la dignidad y garantizar los derechos fundamentales y la seguridad y salud de las personas trabajadoras
2. Obligaciones específicas de las personas empleadoras

En el desarrollo y gestión de la actividad laboral en entornos digitales, las personas empleadoras deberán:

- a) Respetar de modo efectivo el derecho a la desconexión digital.
- b) Proteger los derechos de las personas trabajadoras a la intimidad personal y familiar, al honor, a la imagen, a la protección de datos y al secreto de las comunicaciones.
- c) Cumplir la normativa aplicable al uso de sistemas de control, videovigilancia, grabación sonora, geolocalización, monitoreo, biometría o inteligencia artificial en el entorno laboral, asegurando que se proporciona a las personas trabajadoras información previa y suficiente.
- d) Garantizar que el uso de tecnologías para la toma de decisiones automatizadas en la selección, evaluación, promoción o desvinculación de personal respete los principios de licitud, transparencia, proporcionalidad, no discriminación e intervención humana significativa, incluyendo información suficiente y mecanismos de revisión o impugnación.
- e) Promover la capacitación digital de las personas trabajadoras y proporcionarles los recursos tecnológicos necesarios, en condiciones adecuadas y seguras, para el desempeño de su actividad laboral, ya sea presencial o a distancia.
- f) Prevenir, detectar y sancionar el acoso laboral, sexual o por razón de género a través de medios digitales.

3. Teletrabajo

En el teletrabajo, las personas empleadoras deberán garantizar:

- a) El carácter voluntario del acuerdo de teletrabajo, conforme a la normativa aplicable, asegurando la plena efectividad de las condiciones laborales.
- b) La protección de la intimidad personal y familiar de la persona trabajadora.
- c) El respeto a los derechos de conciliación del trabajo con la vida personal y familiar.

CAPÍTULO VII: Deberes relativos a la protección de los menores y la educación

VII.

CAPÍTULO VII: DEBERES RELATIVOS A LA PROTECCIÓN DE LOS MENORES Y LA EDUCACIÓN

Sección 1. Educación y alfabetización digital

1. Uso de medios tecnológicos en el sistema educativo

Las autoridades y los centros educativos deberán garantizar que la integración de medios tecnológicos adecuados en el sistema educativo, en el marco de una educación integral, facilite la competencia digital del alumnado, garantizando su bienestar, seguridad y protección de datos, de acuerdo con su edad y necesidades.

2. Programas de alfabetización digital inclusiva

Las autoridades competentes deberán diseñar e implementar programas efectivos y evaluables de alfabetización digital inclusiva, orientados a superar las brechas digitales y a garantizar la adquisición, por parte de la ciudadanía, de las habilidades necesarias para el ejercicio de los derechos fundamentales en el entorno digital con especial énfasis en la alfabetización digital y en inteligencia artificial de toda la población, adaptada a las distintas etapas y colectivos: desde la educación escolar y universitaria hasta programas para personas adultas y mayores, así como formación específica para familias, sector público y empresas.

Sección 2. Protección activa de los menores en el entorno digital

1. Responsabilidades de los representantes legales

Los representantes legales de las personas menores de edad deberán promover y ejercer un acompañamiento activo en su relación con las tecnologías digitales, con el objetivo de salvaguardar su desarrollo integral, el ejercicio progresivo de su autonomía y la preservación de su dignidad e intimidad.

2. Obligaciones de las entidades que ofrecen servicios digitales a menores

Las entidades públicas o privadas que ofrezcan servicios o gestionen plataformas digitales accesibles a menores deberán implementar medidas de protección reforzada bajo los principios de privacidad y seguridad por diseño que incluyan:

- a) El tratamiento lícito de sus datos personales, conforme a su edad y nivel de madurez.
- b) La implementación de sistemas efectivos de verificación de edad y control parental, apropiados y proporcionales al riesgo, y diseñados para minimizar la recogida de datos, preservando la privacidad; es decir, que protejan la privacidad y no supongan la recolección masiva de datos biométricos.
- c) La evitación de prácticas de perfilado respecto de menores con fines persuasivos, manipulativos o de publicidad ilegal.
- d) El diseño de mecanismos accesibles de denuncia, rectificación y retirada de contenidos.
- e) El acceso a información clara, adaptada y formativa sobre el uso seguro y consciente de los servicios digitales.

CAPÍTULO VIII: Deberes relativos al uso de sistemas de inteligencia artificial

VIII.

CAPÍTULO VIII: DEBERES RELATIVOS AL USO DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

Sección 1. Principios generales

1. Las plataformas y demás prestadores de servicios digitales, así como los responsables del diseño, desarrollo o despliegue de sistemas de inteligencia artificial, deberán garantizar, conforme a un enfoque basado en riesgos y a la normativa aplicable, que dichos sistemas se desarrollen conforme a los principios de agencia y supervisión humanas, solidez técnica y seguridad, gestión de la privacidad y de los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y ambiental, y rendición de cuentas.
2. Estos principios deberán aplicarse en todas las fases del ciclo de vida de los sistemas de inteligencia artificial, desde su diseño, despliegue y seguimiento, hasta su eventual retirada del mercado.

Sección 2. Obligaciones de los diseñadores y desarrolladores de algoritmos

1. Los diseñadores y desarrolladores de algoritmos deberán ejercer sus obligaciones profesionales con arreglo a la ley y a los principios éticos y deontológicos, con pleno respeto a los derechos fundamentales.
2. En particular, deberán procurar la identificación, evaluación y corrección de los sesgos de género, edad, origen social y otros que los sistemas de inteligencia artificial puedan producir.
3. En cuanto a la discriminación y el sesgo algorítmico debe considerarse cada fase del ciclo de vida algorítmico: diseño (evaluaciones de impacto algorítmico antes del despliegue, análisis de representatividad de datos, obligatoriedad de documentación técnica),entrenamiento (calidad, diversidad y ausencia de sesgos en los conjuntos de datos; trazabilidad de fuentes, pruebas de no discriminación antes de poner el modelo en producción) pre-despliegue y despliegue (monitoreo continuo de sesgos y rendimiento diferencial entre grupos, protocolos obligatorios de retirada o recalibración cuando se detecten sesgos y supervisión posterior (auditorías periódicas internas y externas y mecanismos de reclamación directa).

Sección 3. Obligaciones de los usuarios de sistemas de inteligencia artificial

1. El uso de sistemas de inteligencia artificial por parte de cualquier usuario deberá realizarse conforme a la normativa aplicable y de manera proporcionada al rol del usuario y al riesgo del uso, con pleno respeto a los derechos fundamentales y a la legislación vigente.
2. Los usuarios profesionales deberán abstenerse de emplear sistemas de inteligencia artificial con fines ilícitos, discriminatorios o contrarios a los principios de transparencia, equidad y seguridad tecnológica, incluida la elusión deliberada de salvaguardas o controles del sistema.

Sujetos obligados en el ámbito digital



SUJETOS OBLIGADOS EN EL ÁMBITO DIGITAL

Como se ha señalado, una característica esencial de los deberes digitales es la determinación de los sujetos obligados. Junto a los sujetos clásicos, los poderes públicos, en el entorno digital adquieren relevancia otros actores que inciden de forma directa en la garantía de derechos: la ciudadanía, las empresas en general y, de manera destacada, las plataformas y los prestadores de servicios digitales que, por su posición y escala, ocupan un papel estructural en el ecosistema digital, más allá de su condición de meros proveedores de servicios.

El elemento diferencial de esta categoría de actores reside en que, en un periodo muy breve, algunas plataformas han alcanzado posiciones de dominio en la economía digital con un nivel de concentración y capacidad de influencia poco comparable con el de gran parte de la economía tradicional. Ello genera una asimetría estructural no solo frente a la ciudadanía y otras empresas, sino también, y esta es la novedad, frente a los propios poderes públicos y reguladores, al convertirse en ocasiones en reguladores de facto mediante decisiones sobre diseño, acceso, moderación o distribución de contenidos.

Si las asimetrías han justificado tradicionalmente la aplicación de principios de derecho de la competencia, incluida la limitación de conductas abusivas por parte de empresas con posición de dominio, y en ciertos casos la introducción de regulación ex ante, esta necesidad es aún más acuciante respecto de plataformas con impacto sistémico. En consecuencia, deben estar sujetas a un conjunto de obligaciones y responsabilidades específicas en el ejercicio de su actividad, acordes con su capacidad de control e incidencia sobre derechos fundamentales.

Esta realidad exige asimismo un papel central de los poderes públicos, especialmente a escala europea, garantizando una regulación clara y aplicable que defina con precisión el papel de las plataformas y los límites de su actividad. Del mismo modo, debe resaltarse el papel de las organizaciones de la sociedad civil, tales como universidades, corporaciones profesionales u organizaciones de consumidores y usuarios, cuya participación resulta necesaria como colaboración estructurada con los poderes públicos: no solo como transmisores de sensibilidad social, sino también como agentes de detección temprana, evaluación y alerta sobre problemas y riesgos derivados del uso de tecnologías digitales por ciudadanía, empresas y profesionales.

Sección 1. Poderes públicos

1. Los poderes públicos, en todos sus niveles, deberán promover, asegurar en su ámbito de actuación y supervisar conforme a la normativa aplicable:
 - a) El acceso digital y la conectividad en todo el territorio, mediante el establecimiento y mantenimiento del servicio universal.
 - b) La transparencia y la equidad algorítmica.
 - c) La ciberseguridad y la resiliencia de las administraciones, y el impulso y supervisión de la ciberseguridad en el sector privado conforme a la normativa aplicable.
 - d) El respeto a la identidad en el entorno digital.
 - e) El tratamiento de los datos conforme a los principios de licitud, lealtad, transparencia, minimización, exactitud, integridad, confidencialidad y limitación de finalidad y del plazo de conservación.
 - f) El uso responsable de los neurodatos, garantizando transparencia, responsabilidad, mitigación de sesgos y prohibición de usos discriminatorios.
 - g) La libertad de creación y el acceso a la cultura en el entorno digital, combatiendo las brechas y promoviendo la digitalización del patrimonio público.
 - h) La participación ciudadana digital, la Administración electrónica y el acceso a los servicios públicos por medios digitales.
 - i) Un entorno digital competitivo, innovador y libre de prácticas abusivas.
 - j) El uso de medios tecnológicos adecuados en el sistema educativo, así como la alfabetización digital inclusiva.
 - k) La protección reforzada de los menores en el entorno digital.
 - l) El uso adecuado de la inteligencia artificial, conforme a un enfoque basado en riesgos y a la normativa aplicable, bajo principios de transparencia, control del riesgo y supervisión humana.

Sección 2. Plataformas y empresas proveedoras de contenidos y servicios digitales

1. Las plataformas y empresas proveedoras de contenidos y servicios digitales deberán cumplir y aplicar, en función de su papel, tamaño e impacto, y conforme a la normativa aplicable:
 - a) La diligencia en el diseño y gestión de sistemas digitales, identificando y mitigando sesgos algorítmicos, documentando cuando proceda las decisiones automatizadas con efectos relevantes y aplicando políticas de igualdad.
 - b) Que sus sistemas cuenten con un nivel adecuado de ciberseguridad y resiliencia frente a ataques.
 - c) El tratamiento de los datos conforme a los principios de protección previstos en la normativa, actuando con plena transparencia frente a los usuarios.
 - d) El respeto a la identidad digital, permitiendo el uso de seudónimos o identificadores indirectos, cuando sea compatible con fines legítimos, obligaciones legales de verificación o requisitos de seguridad.
 - e) El uso lícito de los neurodatos, absteniéndose de su comercialización ilícita y evitando prácticas discriminatorias o barreras injustificadas de acceso.
 - f) Mecanismos de moderación que permitan la retirada de contenidos ilícitos, respetando la libertad de expresión, la creación cultural y los derechos de autor, garantizando mecanismos accesibles de reclamación y revisión.
 - g) La transparencia informativa, la protección frente a la desinformación y la garantía de los derechos de rectificación, actualización y olvido de los usuarios así como la gestión responsable de los modelos de negocio basados en la maximización del tiempo de uso.
 - h) La accesibilidad universal de los contenidos e interfaces, especialmente para las personas con discapacidad.
 - i) La transparencia en el ejercicio de su actividad económica, evitando prácticas anticompetitivas como la autopreferencia o el bloqueo de aplicaciones competidoras, y permitiendo, en los términos previstos por la normativa aplicable, la portabilidad y transferencia de datos entre plataformas.
 - j) El uso de la inteligencia artificial conforme a los principios de transparencia, supervisión humana y control del riesgo, identificando y mitigando sesgos, documentando las medidas cuando proceda, y respetando los límites normativos.

Sección 3. Empresas y particulares

1. Las empresas y las personas físicas deberán respetar:
 - a) Las normas de seguridad y ciberhigiene en su vida digital.
 - b) Los datos y neurodatos de terceros, manteniendo su confidencialidad y recabando el consentimiento informado cuando proceda.
 - c) La identidad digital ajena.
 - d) La libertad de expresión en el entorno digital, evitando la difusión de contenidos ilícitos o de información deliberadamente engañosa cuando pueda causar perjuicios, y respetando los derechos morales y económicos de los autores.
 - e) Los derechos de rectificación y actualización de contenidos cuando actúen como difusores o responsables de publicaciones en el ámbito de la comunicación, conforme a la normativa aplicable.
 - f) En la actividad empresarial, la protección y seguridad de los datos de empleados y clientes, el respeto a las normas de competencia y la formación digital de sus órganos directivos.
 - g) En el entorno laboral, los principios de desconexión digital, la limitación de sistemas de control intrusivos, el suministro de medios tecnológicos adecuados y la posibilidad de teletrabajo cuando proceda, en condiciones dignas y conforme a la normativa aplicable.
 - h) En la negociación colectiva, la promoción de estos principios por parte de las organizaciones sindicales y empresariales, favoreciendo la digitalización responsable de las empresas.
 - i) En el ámbito educativo, el uso responsable de las tecnologías, transmitiendo su importancia social y económica, y garantizando, junto a las familias, la protección de los menores en el entorno digital.
 - j) En el uso de la inteligencia artificial, el respeto a los principios de transparencia, ética y legalidad, evitando sistemas prohibidos y respetando las limitaciones aplicables a los sistemas de alto riesgo.

Glosario



Glosario

A efectos de esta Declaración, los términos que siguen se entenderán en el sentido indicado, sin perjuicio de las definiciones establecidas en la normativa aplicable.

Accesibilidad universal

Condición que deben cumplir los entornos, procesos, bienes, productos y servicios, así como objetos, instrumentos y dispositivos, para ser comprensibles, utilizables y practicables por todas las personas en condiciones de seguridad y comodidad y de la forma más autónoma posible.

Agencia y supervisión humanas

Principio por el cual el uso de sistemas digitales o de inteligencia artificial no anula la capacidad humana de comprender, decidir, corregir y rendir cuentas, especialmente cuando existen efectos relevantes sobre personas.

Alfabetización digital

Conjunto de competencias técnicas y críticas necesarias para usar tecnologías digitales de forma segura y autónoma, comprender riesgos, derechos y deberes, y participar en el entorno digital.

Arquitectura de amplificación (recomendación/ranking)

Mecanismos (recomendadores, priorización, ranking, tendencias) que aumentan o reducen el alcance de contenidos, información o servicios, condicionando su visibilidad.

Ciberhigiene

Prácticas básicas de seguridad aplicables a personas y organizaciones según su rol (actualizaciones, autenticación, gestión de contraseñas, prevención de fraudes, etc.).

Ciberseguridad

Medidas técnicas y organizativas destinadas a proteger sistemas, redes y datos frente a accesos no autorizados, pérdida, alteración, interrupción o uso indebido.

Contenido ilícito

Contenido cuya difusión o puesta a disposición está prohibida por la normativa aplicable o por resolución/orden de autoridad competente.

Contenido legal potencialmente dañino

Contenido no necesariamente ilícito que puede causar perjuicios relevantes (por ejemplo, por manipulación, acoso o engaño deliberado) y que exige respuestas proporcionadas distintas de la retirada automática.

Conocimiento efectivo

Situación en la que un prestador o plataforma dispone de información suficientemente concreta y fundada para apreciar la posible ilicitud de un contenido o actividad, conforme a los procedimientos aplicables.

Consentimiento informado

Manifestación de voluntad válida, libre y específica, basada en información suficiente y comprensible, cuando el consentimiento sea el fundamento aplicable para un tratamiento o actuación.

Datos personales

Cualquier información sobre una persona física identificada o identificable.

Decisión automatizada

Decisión adoptada total o parcialmente mediante procesamiento automatizado (incluida inteligencia artificial) que produce efectos jurídicos o impactos significativos sobre una persona.

Diligencia debida

Deber de identificar, prevenir, mitigar y rendir cuentas sobre riesgos razonablemente previsibles derivados del diseño, despliegue u operación de sistemas digitales, de forma proporcional al control, alcance e impacto.

Diseño inclusivo

Enfoque de diseño que incorpora desde el inicio necesidades diversas (edad, discapacidad, alfabetización, contexto) para evitar exclusiones y barreras.

Equidad algorítmica

Objetivo de evitar y mitigar sesgos y discriminaciones injustificadas en sistemas automatizados, especialmente cuando afectan a derechos, acceso a servicios u oportunidades.

Identidad digital

Conjunto de atributos, identificadores, credenciales y trazas que representan o permiten identificar, perfilar o suplantar a una persona en entornos digitales (incluida su reputación y presencia digital).

Incidente significativo

Evento que compromete de forma relevante la confidencialidad, integridad, disponibilidad o autenticidad de datos o servicios, por su alcance, impacto o naturaleza.

Interoperabilidad

Capacidad de sistemas o servicios para interactuar e intercambiar información de forma efectiva y segura, conforme a estándares o requisitos aplicables.

Intervención humana significativa

Participación humana real (no meramente formal) que permite revisar, corregir o impugnar decisiones automatizadas cuando existen efectos relevantes.

Neurodatos

Datos sobre actividad o señales del sistema nervioso (incluidas inferencias) que permiten identificar o inferir estados, rasgos o capacidades de una persona.

Neurotecnologías

Tecnologías destinadas a registrar, analizar, modificar o interactuar con el sistema nervioso (por ejemplo, medición, estimulación o interfaces cerebro-máquina).

Perfilado

Tratamiento automatizado de datos destinado a evaluar o predecir aspectos personales (preferencias, comportamiento, salud, rendimiento, etc.), especialmente cuando se usa para segmentación o priorización.

Plataforma digital

Servicio que intermedia o organiza interacciones entre múltiples usuarios o proveedores y que puede influir en visibilidad, acceso o condiciones de participación.

Portabilidad de datos

Capacidad de obtener y transmitir datos en formato utilizable para su reutilización en otro servicio, en los términos previstos por la normativa aplicable.

Prestador de servicios digitales

Persona física o jurídica que ofrece, opera o gestiona servicios prestados por medios digitales, incluidas plataformas.

Privacidad y protección de datos desde el diseño y por defecto

Obligación de incorporar salvaguardas de privacidad y minimización desde la concepción del sistema y por configuración estándar, evitando recopilaciones innecesarias.

Resiliencia

Capacidad de resistir incidentes, mantener funciones esenciales y recuperarse con continuidad.

Seudónimo o identificador indirecto

Identificador que permite operar sin revelar identidad civil directa, cuando sea compatible con fines legítimos, obligaciones legales y requisitos de seguridad.

Sistema de inteligencia artificial

Sistema basado en máquinas diseñado para funcionar con diversos niveles de autonomía y que, para objetivos explícitos o implícitos, infiere a partir de entradas cómo generar salidas (predicciones, contenidos, recomendaciones o decisiones) que pueden influir en entornos físicos o virtuales

Sistemas de alto riesgo y sistemas prohibidos

Categorías determinadas por la normativa aplicable (enfoque basado en riesgos) que imponen obligaciones reforzadas o prohíben determinados usos por su impacto potencial.

Transparencia operativa

Transparencia verificable: información clara sobre finalidades, criterios relevantes (p. ej., priorización), tratamiento de datos cuando proceda y vías de reclamación o revisión.

Verificación o estimación de edad

Mecanismos para determinar si una persona supera un umbral de edad, ajustados al riesgo del servicio y diseñados para minimizar la recogida de datos y preservar la privacidad.

Agradecimientos

COORDINADORES

Beatriz Escriña
Carlos López Blanco

PONENTES

Margarita Castilla
José María Lassalle
José Luis Piñar

EXPERTAS/OS

Maica Amador	Ignacio Hernández
Blanca Basanta	Jaime de la Hoz
Federico Buyolo	Antonio Martín Alonso
Álvaro Cabo	Dolores Martín Villalba
Juan Fernando Campos	Pablo de Miguel
Ana Caro Muñoz	Irene Milleiro
Pablo Diego Simon	Inés Monteagudo
Aina Errando	Esther Paniagua
Carlota Escolano	Elena Pisonero
Diego Garrocho	Ana de Quinto Barbado
Daniela González	Natalia Rodríguez
Millán González	Idoia Salazar
Alberto González Pulido	María Sánchez Besga
Rodrigo González Ruiz	Mercedes Siles Molina
David Gracia	Miryam Vivar

Declaración emitida en el marco del Convenio entre la Entidad Pública Empresarial Red.es, M.P. y la agrupación de entidades formada por la Fundación Hermes; Fundación La Caixa; Fundación Telefónica; Fundación Atresmedia; Universidad San Pablo CEU; Universidad Autónoma de Madrid (UAM); Universidad Carlos III de Madrid (UC3M); Fundación para la Repoblación Sostenible; Comité Español de Representantes de Personas con Discapacidad (CERMI); Universidad Católica del Uruguay; Asociación Europea para la Transición Digital; Fundación Hiberus; Universitat de València; Observatorio del Impacto Social y Ético de la Inteligencia Artificial (ODISEIA); Universidad Santiago de Compostela (USC); Universidad de Navarra; Universidad de Comillas; Fundación Mobile World Capital y, Fundación Diario de Navarra [C043/23-OT].

La información y las opiniones expresadas en este documento son de los autores y no reflejan necesariamente la opinión oficial de las instituciones firmantes del convenio de colaboración en cuyo marco se ha realizado este documento.

Las instituciones firmantes del convenio no garantizan la exactitud de los datos incluidos en este documento. Ni estas instituciones ni ninguna persona que actúe en su nombre pueden ser considerados responsables del uso que pueda hacerse de la información contenida en el mismo.



DERECHOS DIGITALES