INFORME Nº 001 /2021-2022/CESIP-OCDE-CR

El presente informe versa sobre las actividades realizadas en el viaje de Representación a la Reunión Organizada por la Red Parlamentaria Global de la OCDE del 30 de junio al 1° de julio del 2022 en la ciudad de Riga, Letonia, siendo la temática de la reunión "Construir un futuro digital seguro e inclusivo en un mundo post – COVID".

I. ANTECEDENTES:

Con fecha 03 de junio del 2022, fue recepcionado un correo electrónico remitido por la Srta. Silvia Terrón, Responsable de los Asuntos Públicos de la Dirección de Asuntos Públicos y Comunicación de la OCDE mediante el cual comunica que los miembros de la Comisión Especial de Seguimiento de la Incorporación del Perú a la Organización para la Cooperación y el Desarrollo Económicos (CESIP -OCDE) del Congreso de la República del Perú habían sido considerados miembros de la Red Parlamentaria Global de la OCDE y, como tales, hacía extensiva la invitación para participar de la reunión a realizarse durante los días 30 de junio al 1 de julio en la ciudad de Riga, Letonia.

La invitación fue puesta en conocimiento de todos los miembros de la Comisión. La señorita congresista Yessica Rosselli Amuruz Dulanto y el suscrito expresamos nuestro interés en participar de la reunión y adjuntamos los requerimientos. Se oficializó la solicitud de autorización correspondiente a la Presidencia del Congreso.

La Mesa Directiva del Congreso de la República, en su sesión de fecha 27 de junio del año en curso, y mediante Acuerdo Nº 106-2021-2022/MESA-CR, autorizó a la congresista Yessica Rosselli Amuruz Dulanto y al suscrito a participar de la reunión de la Red Parlamentaria Global de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), a realizarse en la ciudad de Riga, Letonia, del 30 de junio al 1º de julio de 2022, procediendo en ese sentido a cumplir los trámites pertinentes como la confirmación de participación al evento, los pasajes y estadía.

El viaje se inició con nuestra partida del Aeropuerto Internacional "Jorge Chávez", la noche del martes 28 de junio, desarrollando las actividades que detallo en las páginas siguientes y culminó con nuestro retorno, el sábado 02 de julio.

II. SOBRE LA REUNIÓN DE LA RED PARLAMENTARIA GLOBAL:

En el desarrollo de las jornadas parlamentarias, se cumplió estrictamente con el programa, cuya copia se adjunta al presente, y que giró sobre el tema de la construcción de un futuro digital seguro e inclusivo en un mundo post – COVID, conforme al siguiente detalle:

JUEVES 30 DE JUNIO:

La reunión parlamentaria inició el día 30 de junio en el edificio del Parlamento de Riga, contando con la participación de 66 legisladores de diferentes países del mundo.

En la primera conversación se realizó un taller parlamentario denominado: ***"Hacia una respuesta a los desafíos de la transformación digital en los procesos democráticos",*** que inició con la expresión de la preocupación del impulso de la revolución tecnológica digital en el mundo, que como es de público conocimiento, la digitalización va a abarcar en el corto o mediano plazo todas las esferas y los organigramas de los estados a nivel mundial.

Con este fin, se están implementando programas de digitalización en todos los países, por ser estos los medios que se utilizan en estos momentos; además que nos facilitan reducir tanto las barreras burocráticas como las brechas que existen en diferentes sectores. La digitalización y el impulso de la tecnología son los medios que van a ser parte de nuestra vida en los próximos años.

Respecto a la ***reserva de la información en los medios digitales*** y en las redes sociales, en la reunión se mencionó que existe mucha preocupación sobre la desinformación que circula en los medios de comunicación, debido a que normalmente se extraen datos e información de las redes sociales y de las aplicaciones, sin ningún sustento.

Los miembros participantes de la Red Parlamentaria Global y los expositores mencionaron su preocupación en el tema de la transparencia de la información, debido a que existe un punto débil que es la información sin sustento y/o la información falsa, la misma que se puede viralizar en las redes sociales y en los medios digitales. Ello puede generar tendencias y, en muchos casos, no tienen asidero sólido, y al ser expuestas en las redes a nivel masivo, ocasionan caos social y económico, e inclusive pueden llegar a incidir en las bolsas de valores de los países donde se producen los hechos y situaciones antes descritas.

Asimismo, los expositores manifestaron su preocupación debido a la guerra entre Ucrania y Rusia, ya que se ha iniciado una campaña de

desinformación sobre noticias de economía contra políticos, empresas y respecto de los países que se oponen a Rusia.

En ese sentido, existe la inquietud por la privacidad y la veracidad de la información que se pueda captar u obtener en las redes sociales y en los medios digitales, al existir el temor de que puede ser utilizado por mafias, para la comisión de delitos vinculados a estos temas, o utilizar estas herramientas digitales para sus propios beneficios.

VIERNES 1° DE JULIO:

El día viernes 1° de julio, la reunión se realizó en el Ayuntamiento de Riga (Rigas Dome), siendo el primer tema de la jornada *"**Espacios digitales seguros: gobernanza de datos para mejorar el acceso y el intercambio**"*, cuya presentación estuvo a cargo de Christian Reimsbach – Kounatze, economista, analista de Políticas, Gobernanza de datos y Privacidad – Seguridad en la Economía Digital, División de Políticas de Economía Digital, Dirección de Ciencia, Tecnología e Innovación, OCDE.

A continuación, se abordó el tema ***"Gobernar y legislar en la era digital"***, que estuvo a cargo de la Sra. Bárbara Ubaldi, Jefa de la Unidad de Datos y gobierno Digital, división de gobierno Abierto e Innovador, Dirección de Gobernanza Pública, OCDE.

La reunión continuó con la exposición de Janis Karlsbergs, Director de Publicaciones y Políticas, Centro de Excelencia de Comunicaciones Estratégicas de la OTAN con el tema de ***"Combatir la desinformación digital: visión desde el Frente Oriental"***

Finalizando el programa de exposiciones, se abordó el tema ***"Ciberseguridad y seguridad digital: gestión de riesgos y abordaje de vulnerabilidades"*** a cargo nuevamente, del señor Christian Reimsbach – Kounatze.

Por último, se expusieron las observaciones finales y los próximos pasos a seguir.

En general, las presentaciones fueron interesantes y propiciaban el intercambio de ideas y debates entre los parlamentarios asistentes, en ellas, nuestra participación fue activa dejando en evidencia los avances de nuestro país en esta materia.

Es importante resaltar que los miembros participantes de la Red Parlamentaria Global así como los expositores en sus intervenciones presentaron preocupación respecto de la desinformación que existe en los medios digitales, medios de información y/o en las redes sociales sobre las noticias falsas y campañas de desprestigio que pueden existir en los

medios digitales, así como en las redes sociales. Se evidenció que cuando se manejan estos datos en forma inadecuada y desvirtuando el sentido de la información, podrían llegar a interferir en la gobernanza y la democracia de un país.

La paradoja de que exista una cuarta revolución industrial tecnológica digital tiene como una de sus problemáticas la privacidad de la información personal; si bien es cierto ella nos facilita las posibilidades que tenemos para la adquisición de un bien o un producto, corremos el riesgo de que las empresas puedan acceder a nuestra información personal y utilizarla para su propio beneficio al no existir un debido control y fiscalización con los datos que se almacenan en las aplicaciones y/o redes sociales. En ese sentido, la pregunta es ¿Cómo se respalda esa información?, ¿Cuál sería el esquema de la privacidad de la información?

La Organización para la Cooperación y el Desarrollo Económicos – OCDE - está solicitando opinión respecto al tema a los miembros de la Red Parlamentaria Global, para poder adoptar las medidas necesarias y de esta forma se pueda controlar y fiscalizar esta situación.

Finalmente, hago de su conocimiento que el día 13 de julio del presente año he realizado la rendición de cuentas por los viáticos asignados ante la Oficina de Logistica del Congreso de la República.

III. Anexos

- Programa del evento y fotografías de la Reunión Parlamentaria Global de la OCDE.

Sin otro particular, aprovecho la oportunidad de expresarle mi especial consideración y estima personal.

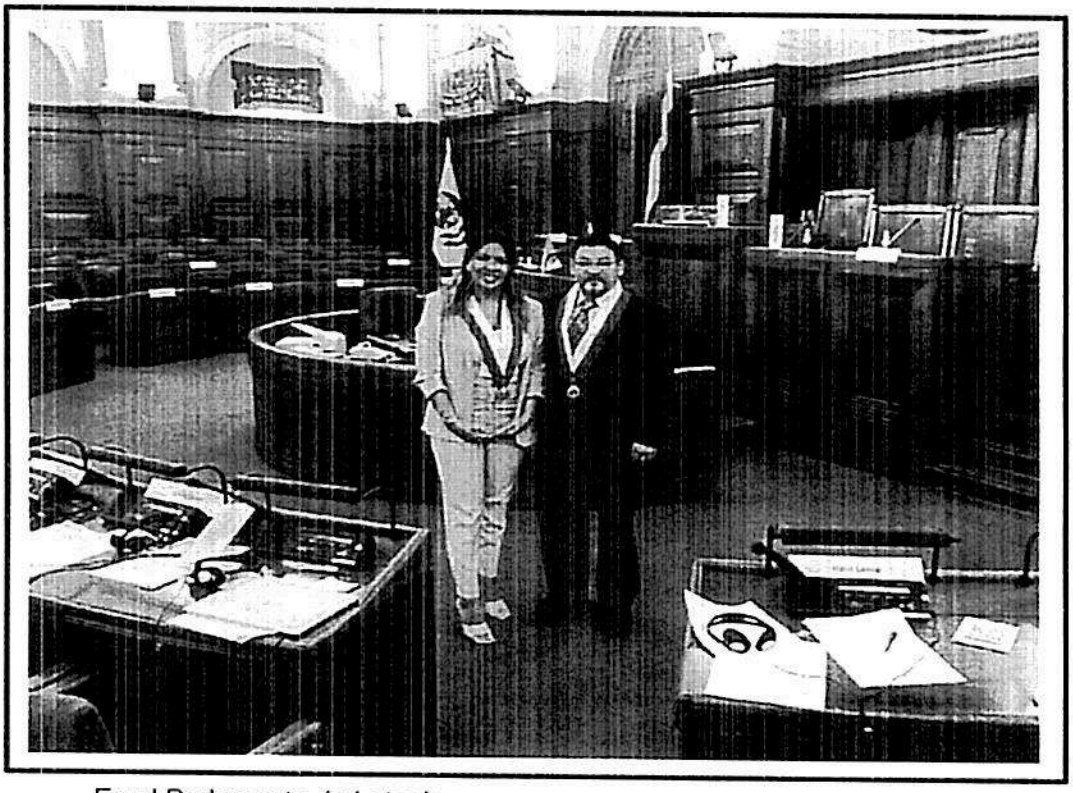
Atentamente,

Lima, 14 de Julio de 2022

CONGRESO DE LA REPÚBLICA
CESIP - OCDE

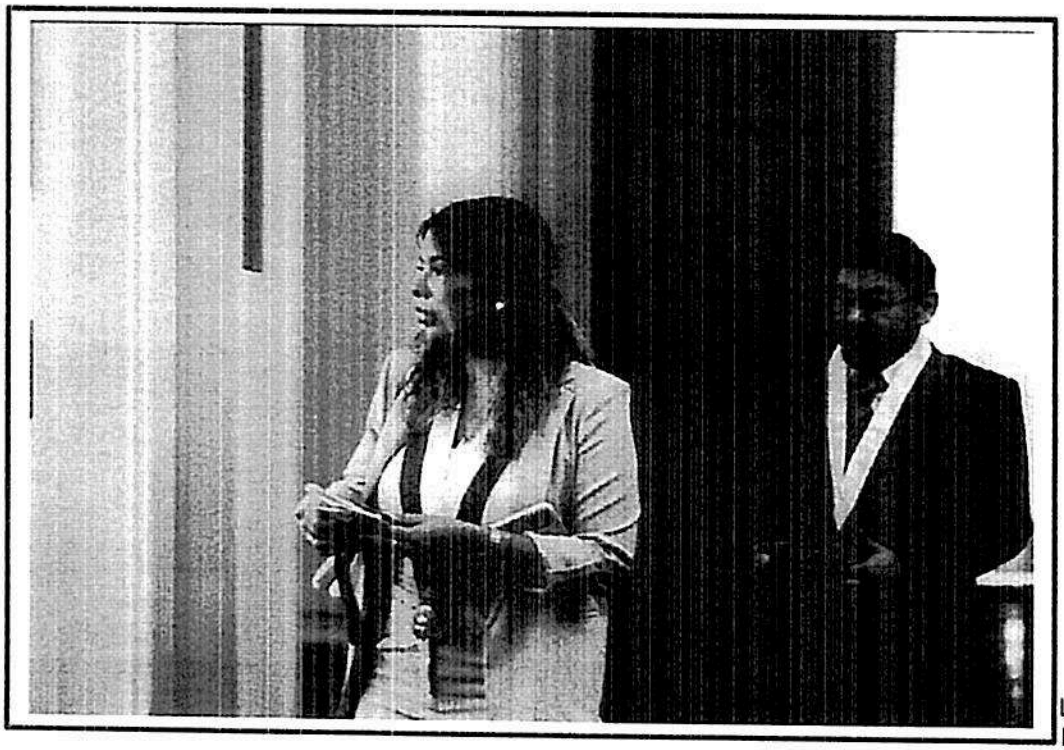
L. GUSTAVO CORDERO JON TAY
Congresista de la República
Presidente de la Comisión Especial de
Seguimiento de la Incorporación del Perú a la
Organización para la Cooperación y el Desarrollo Económicos
CESIP - OCDE

- Anexos fotográficos



En el Parlamento de Letonia

Inauguración del evento



Jr. Azángaro N°468–Cercado de Lima
Lima Perú
Central Telefonica:311 - 7777

PROYECTO DE PROGRAMA

Reunión itinerante de la Red Parlamentaria Global de OCDE

el 30 junio y 1 julio del 2022

Saeima de la República de Letonia

Jēkaba iela 11, Rīga

«Construir un futuro digital seguro e inclusivo en un mundo post-COVID»

Jueves 30 de junio del 2022

16:30	Café de bienvenida
17:00 - 19:00	**Taller parlamentario – Hacia una respuesta a los desafíos de la transformación digital en los procesos democráticos**
20:00	Recepción Museo Nacional de Arte de Letonia

Viernes 1 de julio del 2022

09:00 - 09:30 Palabras de bienvenida

- ***Ināra Mūrniece***, *Presidenta de la Saeima (parlamento), Letonia*
- ***Rihards Kols***, *Presidente, Comisión de Asuntos Exteriores, Saeima de la República de Letonia*
- ***Artūrs Toms Plešs***, *Ministro de Protección Ambiental y Desarrollo Regional, Letonia*
- ***Anthony Gooch***, *Director de Asuntos Públicos y Comunicaciones, OCDE, y Presidente de la Red Parlamentaria Global, OCDE*

09:30 - 11:00	**Espacios digitales seguros: gobernanza de datos para mejorar el acceso y el intercambio** ***Christian Reimsbach-Kounatze,*** *Economista, Analista de Políticas, Gobernanza de Datos y Privacidad-Seguridad en la Economía Digital, División de Políticas de Economía Digital, Dirección de Ciencia, Tecnología e Innovación, OCDE* Comentarista especial. Desde la perspectiva de Letonia ***Jekaterina Macuka,*** *Directora, Data State Inspectorate [Inspectoría de Datos del Estado] (Letonia)*
11:00 - 11:30	Pausa café
11:30 - 13:00	**Gobernar y legislar en la era digital** ***Barbara Ubaldi,*** *Jefa de la Unidad de Datos y Gobierno Digital, División de Gobierno Abierto e Innovador, Dirección de Gobernanza Pública, OCDE*
13:00 - 13:15	Foto grupal
13:15 - 14:30	Almuerzo
14:30 - 16:30	**Combatir la desinformación digital: visión desde el Frente Oriental** ***Janis Karlsbergs,*** *Director de Publicaciones y Políticas, Centro de Excelencia de Comunicaciones Estratégicas de la OTAN*
16:30 – 18:00	**Ciberseguridad y seguridad digital: gestión de riesgos y abordaje de vulnerabilidades** ***Christian Reimsbach-Kounatze,*** *Economista, Analista de Políticas, Gobernanza de Datos y Privacidad-Seguridad en la Economía Digital, División de Políticas de Economía Digital, Dirección de Ciencia, Tecnología e Innovación, OCDE*
18:00 – 18:15	**Observaciones finales y próximos pasos**

CONGRESO
REPÚBLICA

COMISIÓN ESPECIAL DE SEGUIMIENTO DE LA INCORPORACIÓN DEL PERÚ A LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (CESIP - OCDE)

"Año del Fortalecimiento de la Soberanía Nacional"

RV895207

MEMORANDO N° 026 - 2021-2022/CESIP-OCDE-CR

A : **Sr. Hugo Rovira Zagal**
Oficial Mayor del Congreso de la República

DE : **Sr. Congresista Luis Gustavo Cordero Jon Tay**
Presidente de la Comisión Especial CESIP – OCDE

ASUNTO : Solicitud de Traducción

FECHA : 08 de julio de 2022

Mediante el presente me dirijo a usted, para solicitarle se sirva gestionar ante el área correspondiente y a la mayor brevedad posible la traducción al castellano de los documentos adjuntos al presente, que se encuentran en idioma inglés:

1. Programa de la reunión realizada por la Red Parlamentaria Global de la OCDE del 30 de junio de 2022 al 01 de julio de 2022.
2. Cuatro Diapositivas de la Red Parlamentaria Global de la OCDE de fecha 30 de junio de 2022 y 01 de julio de 2022.

Atentamente,

CONGRESO DE LA REPÚBLICA
CESIP - OCDE

LUIS GUSTAVO CORDERO JON TAY
Presidente
COMISIÓN ESPECIAL DE SEGUIMIENTO DE LA INCORPORACION DEL PERU A LA ORGANIZACIÓN PARA LA COOPERACION Y EL DESARROLLO ECONÓMICOS
(CESIP - OCDE)

CONGRESO DE LA REPÚBLICA
V°B°
F. RIVERA
Secretaría Técnica de la Oficialía Mayor

OFICIALÍA MAYOR

DGP		PROTOCOLO	
DGA		PARTICIPACIÓN CIUDADANA	
LEGAL Y CONSTITUCIONAL		PREV. Y SEGURIDAD	
CENTRO DE ESTUDIOS		COMUNICACIONES	
COOPERACIÓN INTERNACIONAL		FONDO EDITORIAL	
PLANEAMIENTO Y PRESUPUESTO		ENLACE	
PROCURADURÍA			
TRÁMITE CORRESPONDIENTE	☒	AUTORIZADO	
CONOCIMIENTO Y FINES PERTINENTES	☐	ARCHIVO	
ATENDER SEGÚN PROCEDIMIENTOS INTERNOS	☐	INFORME	☐

Av. Abancay cdra. 5 s/n - Cercado de Lima
Lima – Perú
Central Telefónica: 311 - 7777

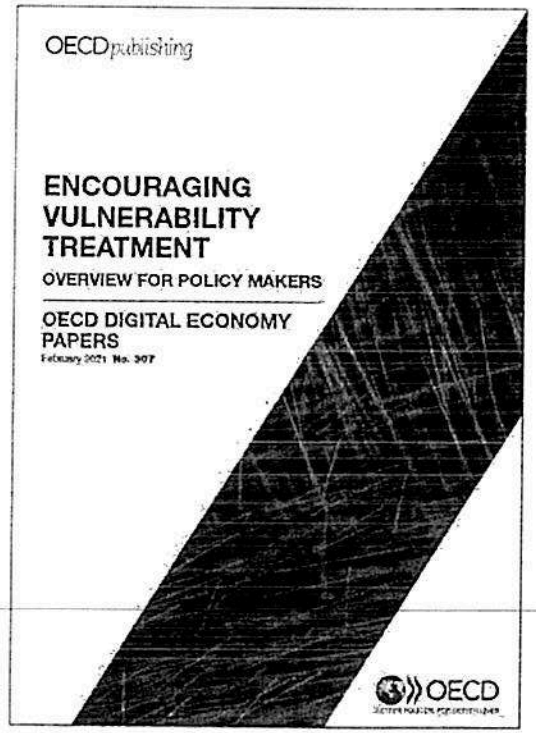
¿Busca más información?

Vea nuestro sitio web:
https://oe.cd/security

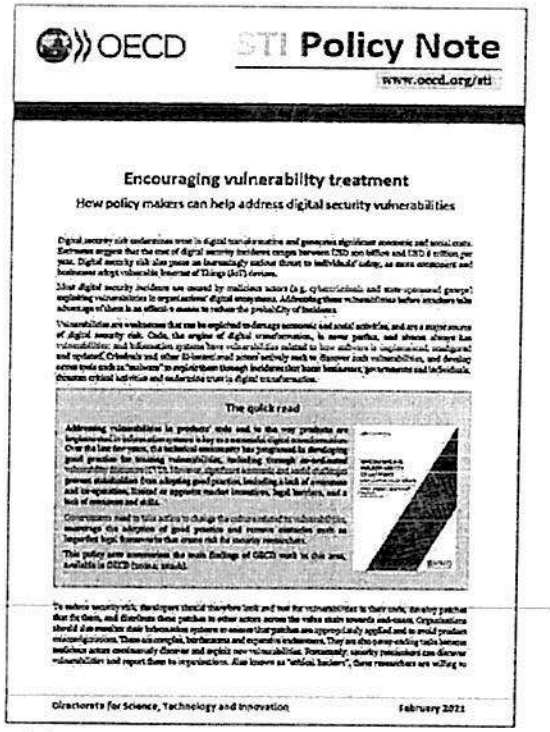
Contacte a la Secretaría de la OECD:
digitalsecurity@oecd.org

¡Gracias!

Trabajo analítico de la OCDE sobre vulnerabilidades



Informe



Nota de política

Principales hallazgos para los responsables de elaborar las políticas públicas

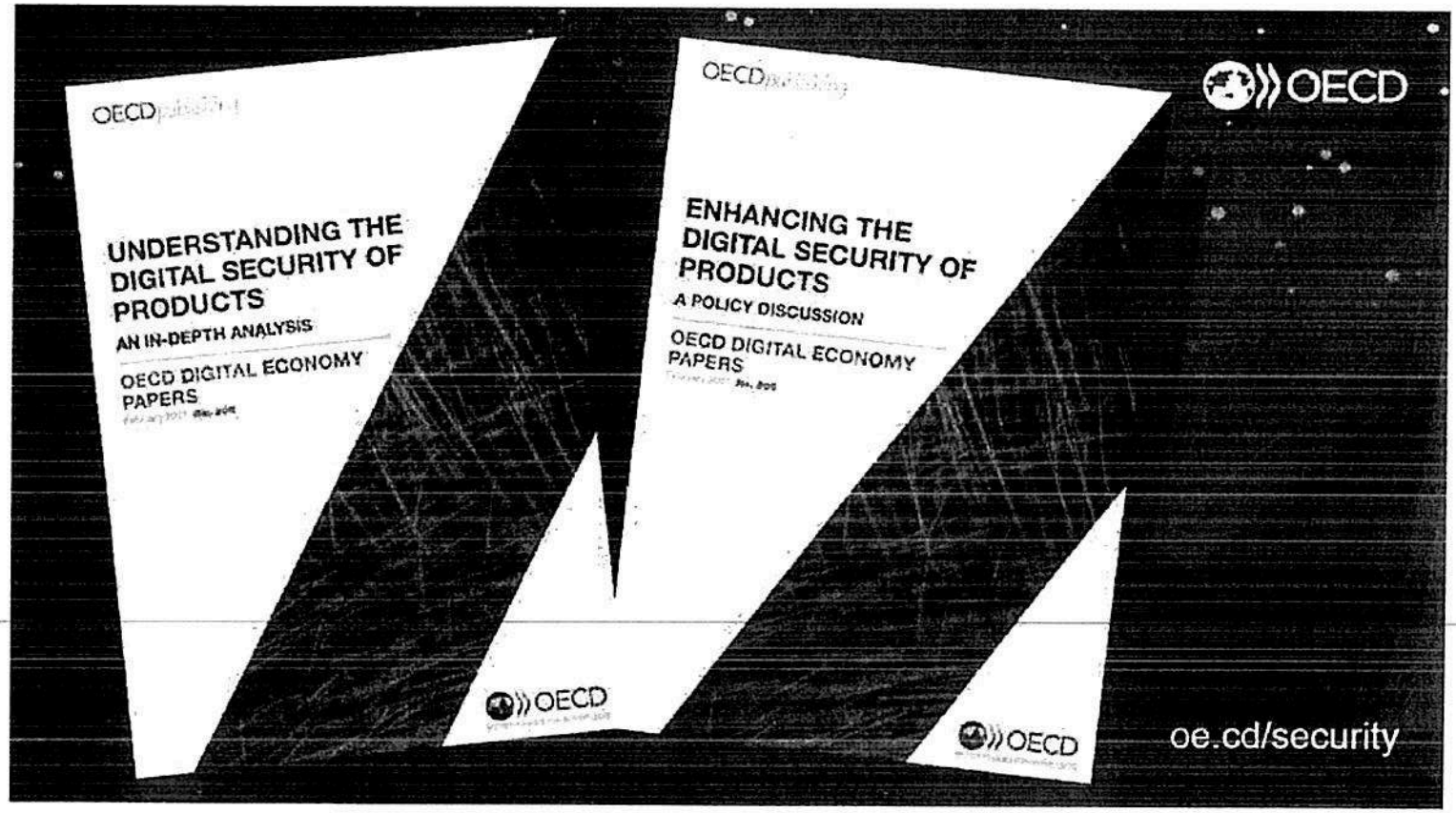
- **No todas las vulnerabilidades son iguales**
  - Código versus vulnerabilidades de sistemas
  - Severidad versus riesgo
- **Las vulnerabilidades son un hecho en la vida digital**
  - No es posible erradicarlas
  - Pero enfrentarlas es un oportunidad clave para reducir el riesgo para todos
- **Los importantes retos económicos y sociales impiden que las partes interesadas traten las vulnerabilidades con eficacia**
  - No es solo una cuestión técnica
  - El riesgo legal para los investigadores de seguridad es un obstáculo importante

Nivel técnico: Conceptos erróneos comunes sobre las vulnerabilidades; un área más compleja de lo que parece

Creíamos que...	Cuando en realidad...
Solo se trata de días cero	Hay que considerar las vulnerabilidades del código y del sistema
Es solo sobre la divulgación coordinada de vulnerabilidades (CVD)	Es necesario un enfoque holístico, de ahí el tratamiento de las vulnerabilidades
Las recompensas por errores son el santo remedio	Una herramienta más entre otras
Es un problema técnico	Los obstáculos son económicos ('mercado gris', incentivos), legales (puertos seguros), culturales (tabú de la vulnerabilidad).
El Gobierno siempre es neutral	La confianza en el gobierno puede ser un reto

Visión general de los instrumentos de la OCDE en seguridad digital

OCDE publicó dos informes en febrero del 2021



Los factores económicos desempeñan un papel clave en la seguridad digital de los productos

- **Incentivos de mercado mal alineados:** el tiempo de comercialización y la rentabilidad suelen tener prioridad sobre la seguridad.
- **Asimetrías de información:** los clientes no pueden evaluar el nivel de seguridad digital de los productos inteligentes.
- **Externalidades negativas:** los productos inseguros afectan a terceros y a la sociedad (por ejemplo, ataques DDoS y botnets).
- **Las cadenas de valor complejas y globales** dificultan la asignación de responsabilidades.
- **No hay seguridad «absoluta»:** no se puede alcanzar el 100% de seguridad y hay que equilibrarla con otros objetivos.

=>Esto lleva al fracaso del mercado, es decir, es poco probable que la dinámica del mercado por sí sola ofrezca un nivel óptimo de ciberseguridad en los productos inteligentes.

Seguridad digital de los productos: ¿Por qué es importante?

Con la transformación digital:

- **El código está en todas partes:** cada vez más productos son **«inteligentes», es decir, contienen código** y pueden conectarse.
- El código casi siempre contiene **vulnerabilidades**: en promedio, cada día se descubren 40 nuevas vulnerabilidades en productos muy utilizados, como Windows, iOS y Android.
- **Nuestra dependencia digital** de los productos inteligentes es cada vez mayor, como pone de manifiesto la pandemia **COVID-19.**

  En consecuencia, el **impacto** de los ataques a la seguridad digital que aprovechan las vulnerabilidades de los productos está aumentando considerablemente.

=> La (in)seguridad digital de los productos ha sido noticia en los últimos años:

- En **2016**, los botnets **Mirai** infectaron millones de dispositivos **IoT** «inseguros por su diseño», permitiendo ataques masivos de DDoS.
- En **2017**, **WannaCry y NotPetya** aprovecharon las vulnerabilidades de los **sistemas operativos** Windows sin parches, lo que provocó daños por valor de miles de millones de dólares.
- En **2018**, se encontraron las vulnerabilidades **Meltdown y Spectre** en **microprocesadores**: ¿Vulnerabilidades «sistémicas»?

=> ¿Cuáles son los principales factores (técnicos y económicos) que explican esta situación, y qué recursos pueden utilizar los responsables políticos para mejorar la seguridad digital de los productos?

Seguridad digital de las actividades fundamentales:
Proceso de canalización

Evaluación nacional de riesgos

Considerar todas las actividades económicas y sociales

Identificados por el gobierno

Identificadas por cada operador como parte de su ciclo de gestión de riesgo empresarial

Entorno digital que apoya las funciones cruciales de los operadores durante la cadena de valor de las actividades fundamentales

Evaluación y tratamiento de riesgos de seguridad digital (2015 Rec.)

- Reducir, transferir, impedir, aceptar
- Proteger, detectar y responder, crear resiliencia

Nivel de mercado: Reforzar la seguridad digital sin inhibir la prosperidad

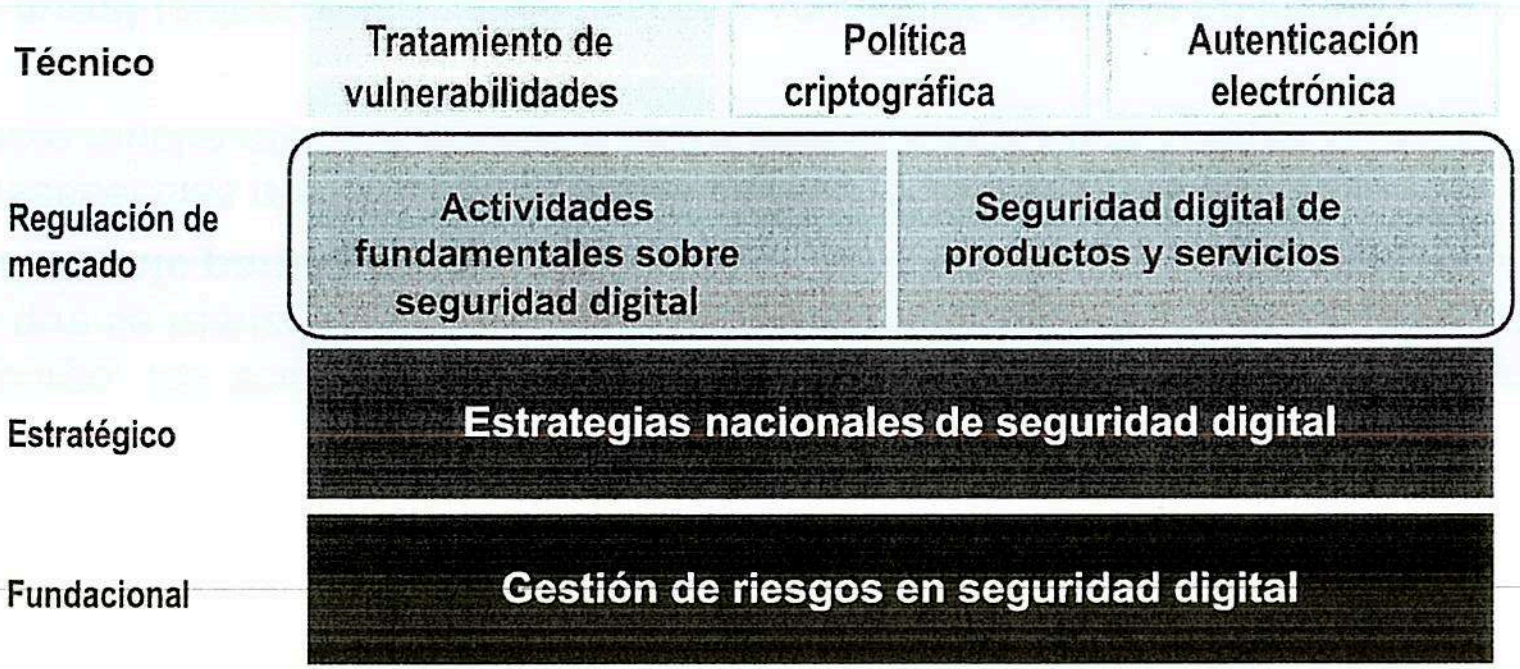
- Las partes interesadas deben asumir la responsabilidad de gestionar los riesgos de la seguridad digital según su función y sus capacidades.
- Sin embargo, los actores pueden gestionar los riesgos de seguridad digital de manera que se reduzcan al nivel **que consideran aceptable para ellos, pero no necesariamente para la sociedad**.

➢ Las consecuencias económicas y sociales de los incidentes pueden extenderse mucho más allá de estos actores y pueden ser catastróficas para todos.

➢ **Peligro moral** (externalidad de los riesgos): «cualquier situación en la que una persona toma la decisión sobre cuánto riesgo asumir, mientras que otra asume el coste si las cosas van mal» (Krugman, 2009).

➢ **¿Cómo abordar este peligro moral para mejorar la seguridad digital sin frenar la innovación y reducir los beneficios de la digitalización?**

Visión general de los instrumentos de la OCDE en seguridad digital



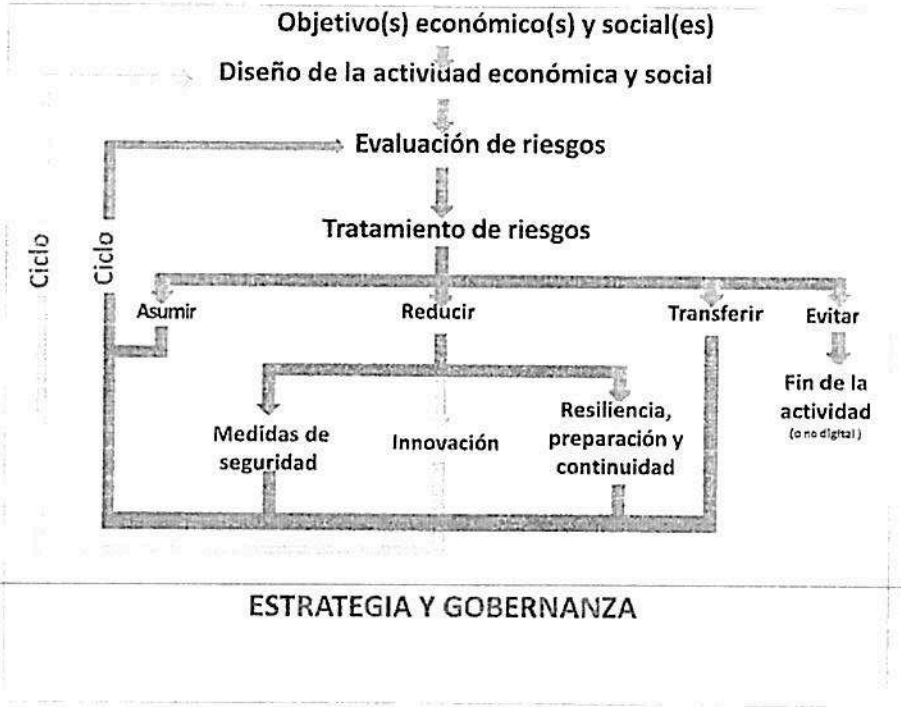
Nivel estratégico: Estrategias nacionales de seguridad digital que establecen el marco institucional para gestionar los riesgos de la seguridad digital

- **Mejora de la coordinación gubernamental a nivel operativo y de políticas:** La responsabilidad para elaborar y aplicar políticas de ciberseguridad se está asignando claramente dentro del gobierno.
- **Cooperación reforzada entre el sector público y el privado**: Reconocer que el ciberespacio es en gran medida propiedad del sector privado y está gestionado por este, y que los usuarios también desempeñan un papel fundamental.
- **Mejora de la cooperación internacional:** Reflejar la necesidad de mejorar las alianzas y asociaciones con países afines o aliados, incluso facilitando el desarrollo de capacidades de los países menos desarrollados.
- **Respeto por los valores fundamentales:** Fuerte énfasis en la necesidad de que las políticas de ciberseguridad respeten los valores fundamentales, que generalmente incluyen la privacidad, la libertad de expresión y el libre flujo de información.

Visión general de los instrumentos de la OCDE en seguridad digital

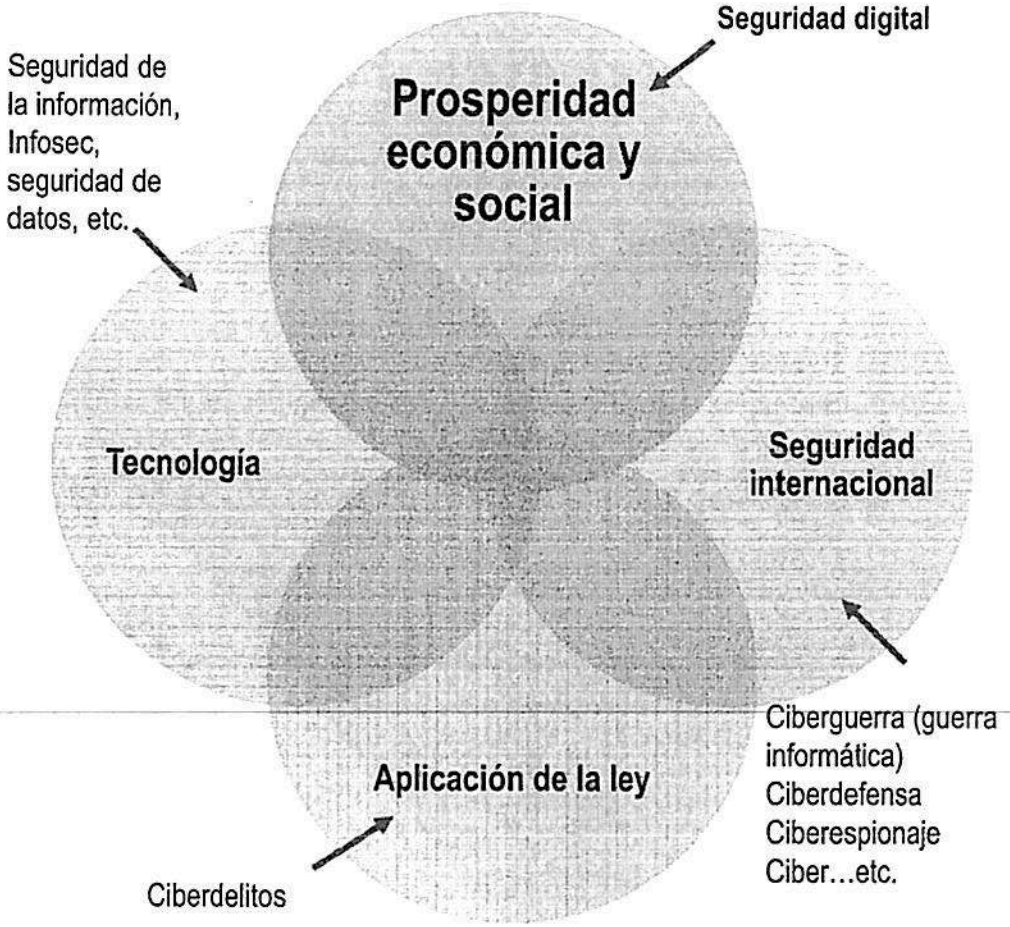
NIVEL BÁSICO: Gestión de riesgos de seguridad digital

- ¿Qué es la seguridad digital?
  - Seguridad digital como dimensión económica y social de ciberseguridad
  - Elementos fundamentales de la seguridad digital, p. ej.
    - CID (confianza, integridad y disponibilidad)
    - Amenazas, vulnerabilidades, incidentes
    - **Riesgos económicos y sociales versus riesgos técnicos**
- Principios de gestión de riesgos



Visión general de los instrumentos de la OCDE en seguridad digital

Seguridad digital: un reto económico y social



- **¿Por qué seguridad 'digital' y no 'ciberseguridad'?**
  - Porque los riesgos de seguridad digital son económicos y sociales
  - « Digital » tiene connotaciones económicas (p. ej.: tecnologías, economía, transformación…y seguridad *digital)*)
  - «Ciber» tiene connotaciones relacionadas con la soberanía (ciberguerra, ciberespionaje, ciberdefensa, etc.)
- **Grupo de trabajo sobre Seguridad en Economía Digital (SDE)**
  - Promueve un enfoque de gestión de riesgos económicos y sociales en cuanto a la seguridad digital
  - Tiene como base casi 40 años de experiencia de la OCDE en seguridad, privacidad y confianza digital
  - Reúne a la comunidad de responsables de la creación de políticas en seguridad digital centrándose en los aspectos económicos y sociales
  - Informa al Comité de Políticas de la Economía Digital (CDEP) de la OCDE.

RED PARLAMENTARIA GLOBAL DE OCDE

«Construir un futuro digital seguro e inclusivo en un mundo post-COVID»

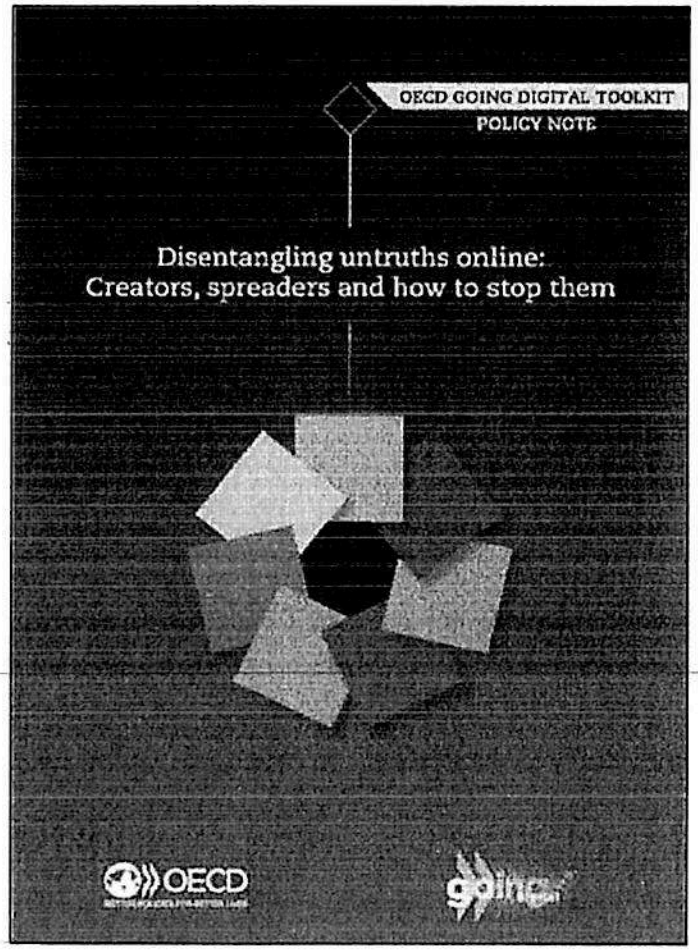
Saeima de la República de Letonia, Jēkaba iela 11, Rīga

1 julio del 2022

TRABAJO DE LA OCDE EN POLÍTICAS PÚBLICAS SOBRE SEGURIDAD DIGITAL

Documento traducido por la Biblioteca del Congreso, con fines meramente informativos. Como es usual, el documento original puede estar sujeto a derechos de autor.

Desenmarañar las falsedades en línea



Nota de herramientas

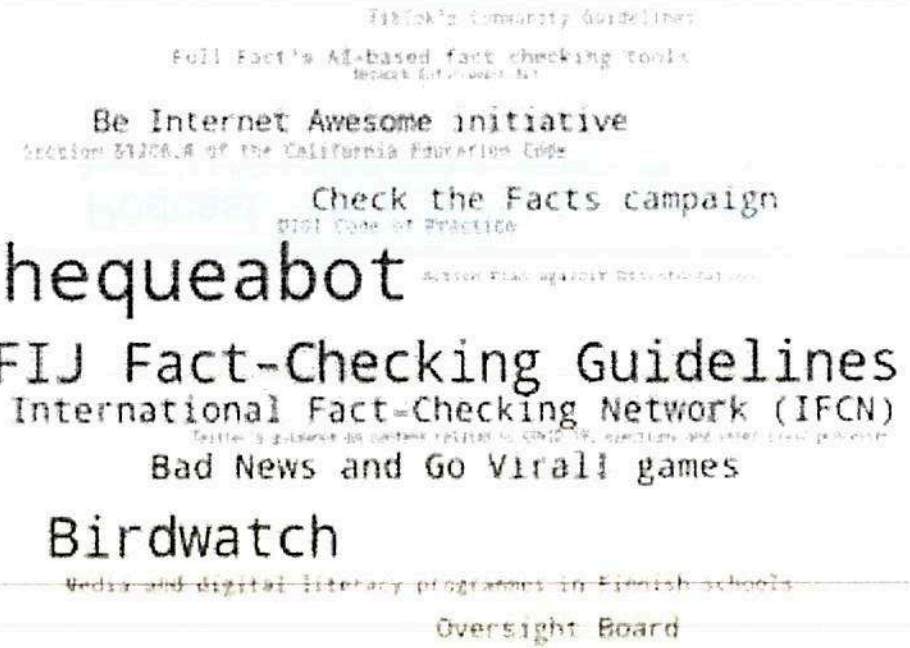
https://goingdigital.oecd.org/data/notes/No23_ToolkitNote_UntruthsOnline.pdf

Pódcast
https://soundcloud.com/oecdtopclasspodcast/disinformation-and-its-discontents

Blog
https://oecd.ai/en/wonk/untruths-online

Luchar contra las falsedades en línea

- Ampliar la alfabetización mediática digital
- Aplicar políticas de moderación de contenidos
- Integrar a los seres humanos y a las tecnologías en la lucha contra las falsedades
- Aumentar la transparencia en el gasto por concepto de publicidad política en línea
- Desarrollar una agenda para medir las falsedades en línea



Una tipología de falsedades en línea

lota de herramientas: Combatir las falsedades en línea

¿Por qué es importante acceder a información precisa?

- Derechos fundamentales
  - Libertad de expresión
  - Derecho a elecciones justas y libres
  - Derecho colectivo a la salud
  - Derecho a la protección de datos e intimidad

- Derecho de acceso a la información en materia de:
  - Cambio climático
  - Teorías conspirativas

¿Cómo se difunden las falsedades en Interne y cuáles son las consecuencias?

- Internet se ha convertido en una de las principale fuente de noticias
  - El 65% de las personas en la Unión Europea, cuya edades fluctúan entre los 16 y 75 años accedió noticias en línea en al año 2020 (Shearer y Mitchell, 2021)
- Las plataformas en línea son el principal medi para difundir falsedades
  - Cámaras de eco y filtro burbuja
- Las tecnologías digitales pueden aumentar y disminuir las falsedades en línea
  - Bots, troles y cíborgs (aumentan la difusión)
  - Las herramientas de Inteligencia artificial sirven par detectar falsedades profundas (*deepfakes*) (disminuye la difusión)

DESENMARAÑAR LAS FALSEDADES EN LÍNEA

REUNIÓN DE LA RED PARLAMENTARIA GLOBAL

1 de julio de 2022

MOLLY.LESHER@OECD.ORG

Documento traducido por la Biblioteca del Congreso, con fines meramente informativos. Como es usual, el documento original puede estar sujeto a derechos de autor.

¡Gracias!

Barbara-Chiara Ubaldi

@BarbaraUbaldi

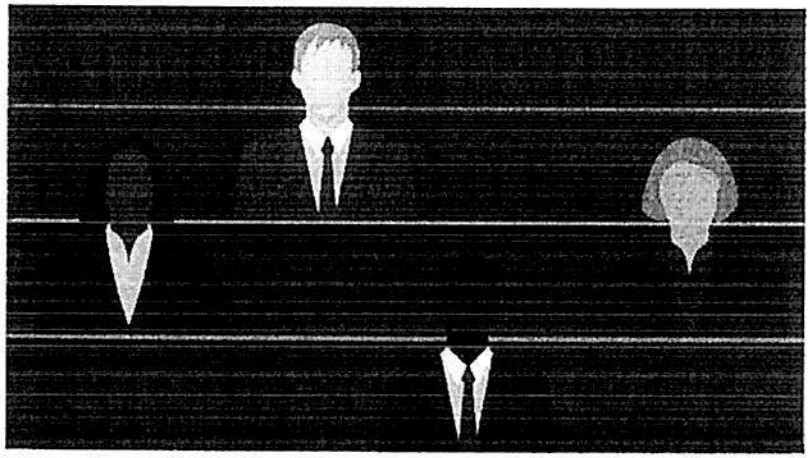
@OECDgov

#digitalgov

#opendata

#digitaltransformation

Parlamento abierto para lograr Gobiernos accesibles y con capacidad digital



Los parlamentos abiertos adoptan prácticas concretas y utilizan *herramientas y datos digitales*, para mejorar la representación, la participación y la transparencia en los procesos legislativos, lo que fomenta la confianza de los ciudadanos y refuerza la democracia.

... **brindan información** sobre el procedimiento legislativo, las agendas de los parlamentarios, las sesiones públicas, el presupuesto del Parlamento, el registro de los grupos de presión, los patrimonios de los parlamentarios y los posibles conflictos de intereses

... y **fomentan la participación** a través de mecanismos para establecer la agenda, prácticas deliberativas, la elaboración conjunta de leyes, así como consultas públicas.

Desafíos legislativos y de gobernanza en la era digital

- **La protección de los mismos** derechos humanos y principios democráticos **dentro y fuera de Internet.**

  - Reafirmación de los derechos existentes y el planteamiento de nuevos derechos.

- **Inclusión digital**

  - Garantizar el **acceso** y las **capacidades** para utilizar tecnologías digitales.
  - Brindar alternativas similares, garantizar el acceso a Internet y equilibrar la alfabetización digital de todos los ciudadanos.

- **Transformación de las instituciones y las regulaciones**
  - Nuevas instituciones especializadas: embajadores tecnológicos, especialistas en ética de datos, organismos para supervisar el uso ético y responsable de la inteligencia artificial, entre otros.
  - Transformación, fusión o creación de nuevos órganos de control para temas digitales.
  - Estructuras internacionales y nacionales de cooperación intersectorial entre los distintos órganos de control.

Temas imprescindibles: Colaboración y tecnología cívicas

- Las herramientas y los datos digitales permiten que los Gobiernos puedan **aprovechar las capacidades de la sociedad civil,** para afrontar los desafíos, mediante los aportes activos de las comunidades que cuentan con tecnologías cívicas.

- Se requiere de las siguientes condiciones clave:
  - La adopción de un enfoque de **Gobierno como plataforma** (herramientas y estándares compartidos), puede ayudar a que el sector público **fomente la colaboración con el ecosistema de tecnologías cívicas,** asegurando la integración y la estandarización.
  - Una **Gobernanza de datos sólida** permite un **acceso eficaz y fiable, así como el intercambio y uso de datos.**
  - **La difusión y fomento de la reutilización de datos de carácter público (OGD)** pueden establecer vías de colaboración concretas con el sector público, a fin de resolver los problemas sociales relevantes.

- Ejemplo: La aplicación *Vitemadose*, se utiliza para reservar citas para vacunarse contra el COVID-19 en Francia. Dicha aplicación emplea datos de gobierno abierto, que son desarrollados con tecnologías cívicas.

Temas imprescindibles: Inteligencia artificial para la rendición de cuentas

- Las innovaciones digitales pueden aumentar la **transparencia** y cerrar la brecha de **credibilidad política** y reducir el escepticismo sobre la **integridad de los responsables políticos.**

- Las tecnologías emergentes y la inteligencia artificial pueden ser útiles para los «**actores responsables de la integridad**» (por ejemplo, las oficinas de auditoría, las autoridades tributarias, las agencias encargadas de las adquisiciones o los organismos de control de la sociedad civil), así se podría:

  - Identificar posibles fraudes y corrupción
  - Analizar y prevenir los riesgos estratégicos
  - Empoderar a la sociedad civil (por ejemplo, tecnologías cívicas).

Temas imprescindibles: Datos y datos abiertos

- **El** acceso y uso de datos **pueden ser una herramienta de gran utilidad, para mejorar la democracia y elaborar normas confiables de diferentes formas.**
- Los datos electorales abiertos y sobre el Parlamento, así como los datos referentes al proceso legislativo, elaboración de leyes y procesos normativos son fundamentales para la transformación digital de los Parlamentos y su trabajo:
  - Datos electorales (abiertos): Por ejemplo, las mesas de votación, candidatos que postulan, circunscripciones electorales y los candidatos elegibles pueden ayudar a los ciudadanos a ejercer sus derechos (servicios)
  - Parlamento: Los datos referentes a los parlamentarios, datos de los partidos políticos (semiprivados), **datos de los grupos de presión**
  - El proceso legislativo: Los datos (legibles por máquina) de los proyectos de ley y los estatutos.
- El proceso normativo, que incluye las Evaluaciones del Impacto Regulatorio (RIAs) puede beneficiarse del libre acceso e intercambio de datos, ya que se puede aprovechar los datos provenientes de diferentes fuentes para evaluar los posibles impactos.

Temas imprescindibles: La ética y la transparencia

- Los Gobiernos deben esforzarse por promover tecnologías digitales **fiables y centradas en el ser humano**, que respeten los derechos humanos y los valores democráticos.

- El sector público se enfrenta a graves problemas en la transparencia y la rendición de cuentas.

- Algunos gobiernos están adoptando **herramientas de rendición de cuentas algorítmicas,** que permitan que el público pueda ver, comprender y supervisar el uso y el funcionamiento de los algoritmos y la información.

- La OCDE apoya a los Gobiernos a través de:

- **Los principios de inteligencia artificial de la OCDE**

- **Los principios de buenas prácticas de la OCDE en materia de ética de datos en el sector público.**

Gobernanza sólida para conseguir una transformación digital:

Marco de la OCDE sobre la gestión de un gobierno

Faceta 1: Factores contextuales

- **Dimensión 1.1** Cultura y estructura política y administrativa general
- **Dimensión 1.2** Factores socioeconómicos
- **Dimensión 1.3** Contexto tecnológico y político
- **Dimensión 1.4** Temas medioambientales y geográficos

Fase 2: Modelos institucionales

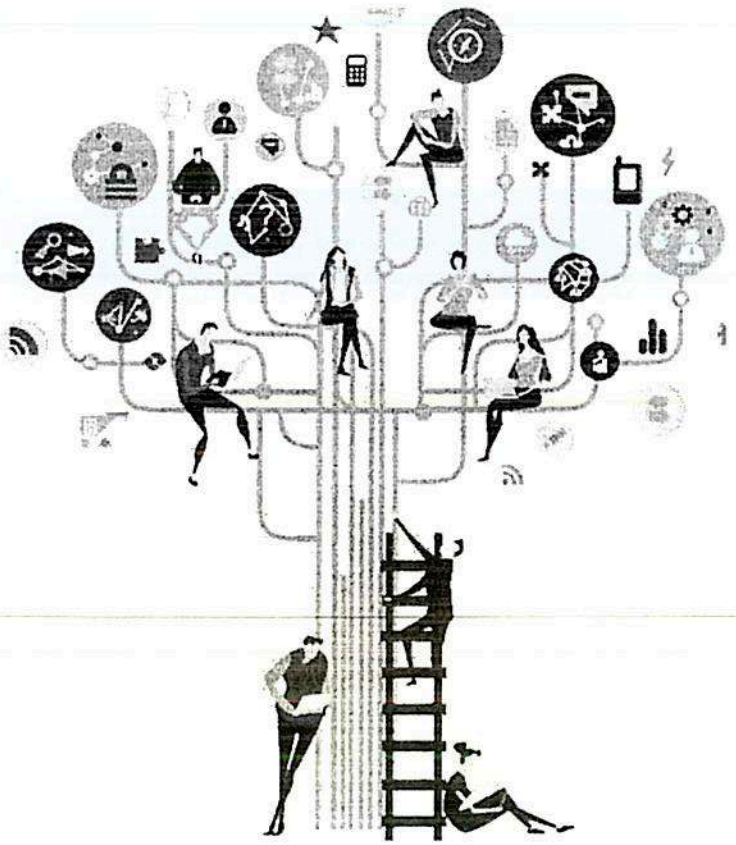
- **Dimensión 2.1** Macroestructura
- **Dimensión 2.2** Liderazgo: Posición/Función
- **Dimensión 2.3** Coordinación y cooperación
- **Dimensión 2.4** Participación y colaboración cívica

Fase 3: Instrumentos políticos

- **Dimensión 3.1** Estrategia y plan
- **Dimensión 3.2** Herramientas de gestión de proyectos
- **Dimensión 3.3** Mecanismos de gestión financiera
- **Dimensión 3.4** Regulaciones y normas

Fuente: OECD (2021), *TheE-Leaders Handbook on the Governance of Digital Government*

El mundo es digital y necesita Gobiernos digitales con experiencia



- La era digital viene generando una **transformación continua** de las necesidades y los comportamientos en las economías y las sociedades. Esta tendencia se ha hecho más evidente con el COVID-19.

- **Los Gobiernos desempeñan un papel clave en esta transformación** y en el ecosistema digital con miras a contribuir con resultados sociales más amplios y de interés público.

- **Se requiere de un Gobierno digital renovado**.
  - **Gobiernos digitales desarrollados**, que puedan equilibrar las oportunidades y riesgos, a fin de crear un gobierno que:
    - Se enfoque en las personas y que sea justo y sostenible.
    - Sea competente para enfrentar los desafíos globales.

30 de junio de 2022

Gobernar y legislar en la era digital

Barbara-Chiara Ubaldi

Jefa de la Unidad de Gobierno Digital y Datos
Jefa Adjunta de la División de Gobierno Abierto e Innovador
Dirección de Gobernanza Pública
OCDE

cumento traducido por la Biblioteca del Congreso, con fines meramente informativos. Como es usual, el cumento original puede estar sujeto a derechos de autor.

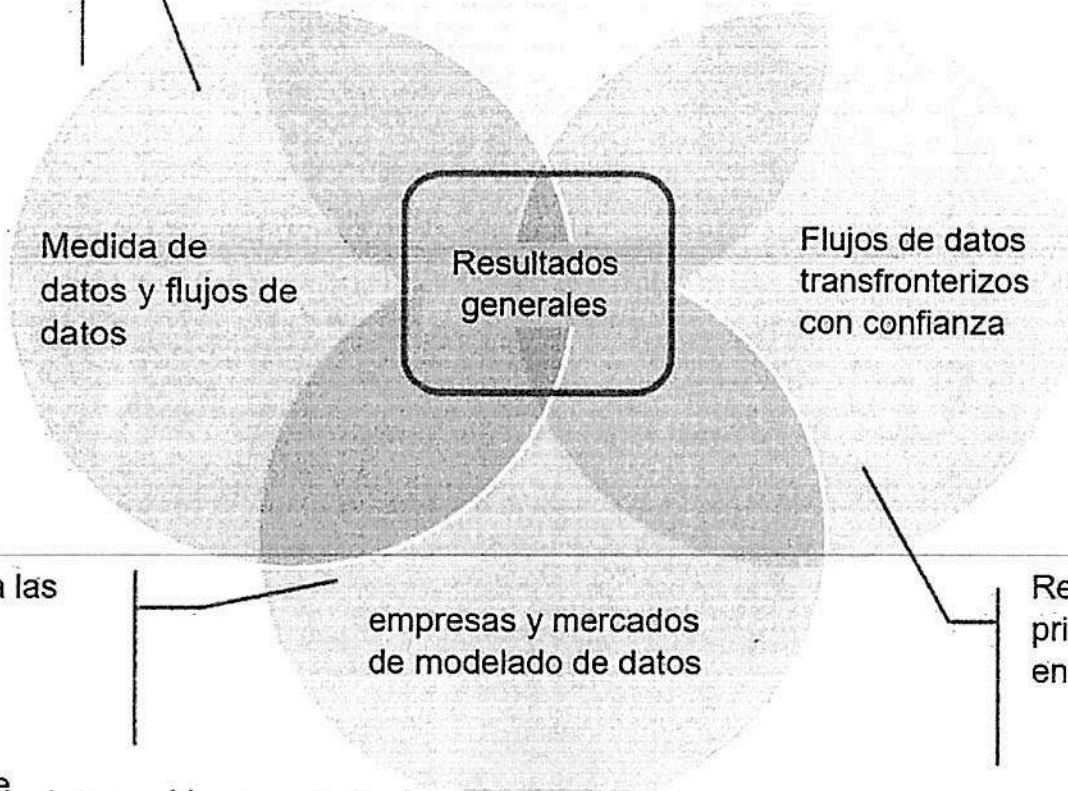
ocumentos de referencia seleccionados

- Data-driven innovation for growth and well-being (octubre 2015)
- Health in the 21st Century: Putting Data to Work for Stronger Health Systems (noviembre 2019)
- Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies [Policy note] (noviembre 2019)
- The Path to Becoming a Data-Driven Public Sector (noviembre 2019)

Para mayor información sobre nuestro trabajo, consulte a los siguientes enlaces:

https://goingdigital.oecd.org/, www.oecd.org/sti/ieconomy/privacy.htm, www.oecd.org/sti/ieconomy/protecting-children-online.htm, www.oecd.org/internet/ieconomy/enhanced-data-access.htm, www.oecd.org/digital/ieconomy/digital-security/

El III Proyecto Horizontal de la OCDE *Going digital* sobre «Gobernanza de los datos para el crecimiento y bienestar» es una gran iniciativa en este mismo sentido



'a mayor información, ingrese a este
ace https://goingdigital.oecd.org/

Disposiciones principales de la Recomendación sobre la EASD

Sección 1- Reforzar la confianza en el ecosistema de datos

III Empoderamiento y participación proactiva

IV Enfoque estratégico de todo el gobierno

Maximizar los beneficios, protegiendo los derechos y fomentando una cultura de responsabilidad

Sección 2. Estimular la inversión en materia de datos e incentivar el acceso e intercambio de datos

IV Incentivos coherentes y modelos de negocios y mercados sostenibles

Sección 3. Fomentar el acceso, intercambio y uso efectivo y responsable de datos en la sociedad

VII Mejorar las condiciones para el acceso e intercambio transfronterizo de datos

VIII Encontrabilidad, accesibilidad, interoperabilidad reutilización de datos en las organizaciones

IX Desarrollo de capacidades para el uso efectivo de los datos

Disposiciones principales de la Recomendación sobre la EASD

Sección 1- Reforzar la confianza en el ecosistema de datos

III Empoderamiento y participación proactiva

IV Enfoque estratégico de todo el gobierno

Maximizar los beneficios, protegiendo los derechos y fomentando una cultura de responsabilidad

Sección 2. Estimular la inversión en materia de datos e incentivar el acceso e intercambio de datos

IV Incentivos coherentes y modelos de negocios y mercados sostenibles

Sección 3. Fomentar el acceso, intercambio y uso efectivo y responsable de datos en la sociedad

VII Mejorar las condiciones para el acceso e intercambio transfronterizo de datos

VIII Encontrabilidad, accesibilidad, interoperabilidad reutilización de datos en las organizaciones

IX Desarrollo de capacidades para el uso efectivo de los datos

Disposiciones principales de la Recomendación sobre la EASD

Sección 1- Reforzar la confianza en el ecosistema de datos

III Empoderamiento y participación proactiva

IV Enfoque estratégico de todo el gobierno

Maximizar los beneficios, protegiendo los derechos y fomentando una cultura de responsabilidad

Sección 2. Estimular la inversión en materia de datos e incentivar el acceso e intercambio de datos

IV Incentivos coherentes y modelos de negocios y mercados sostenibles

Sección 3. Fomentar el acceso, intercambio y uso efectivo y responsable de datos en la sociedad

VII Mejorar las condiciones para el acceso e intercambio transfronterizo de datos

VIII Encontrabilidad, accesibilidad, interoperabilidad reutilización de datos en las organizaciones

IX Desarrollo de capacidades para el uso efectivo de los datos

Disposiciones principales de la Recomendación sobre la EASD

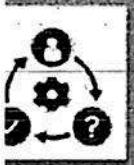
Sección 1- Reforzar la confianza en el ecosistema de datos

III Empoderamiento y participación proactiva

IV Enfoque estratégico de todo el gobierno

Maximizar los beneficios, protegiendo los derechos y fomentando una cultura de responsabilidad

Sección 2. Estimular la inversión en materia de datos e incentivar el acceso e intercambio de datos



IV Incentivos coherentes y modelos de negocios y mercados sostenibles

Sección 3. Fomentar el acceso, intercambio y uso efectivo y responsable de datos en la sociedad

VII Mejorar las condiciones para el acceso e intercambio transfronterizo de datos

VIII Encontrabilidad, accesibilidad, interoperabilidad reutilización de datos en las organizaciones

IX Desarrollo de capacidades para el uso efectivo de los datos

Disposiciones principales de la Recomendación sobre la EASD

Sección 1- Reforzar la confianza en el ecosistema de datos

III Empoderamiento y participación proactiva

IV Enfoque estratégico de todo el gobierno

V Maximizar los beneficios, protegiendo los derechos y fomentando una cultura de responsabilidad

Sección 2. Estimular la inversión en materia de datos e incentivar el acceso e intercambio de datos

IV Incentivos coherentes y modelos de negocios y mercados sostenibles

Sección 3. Fomentar el acceso, intercambio y uso efectivo y responsable de datos en la sociedad

VII Mejorar las condiciones para el acceso e intercambio transfronterizo de datos

VIII Encontrabilidad, accesibilidad, interoperabilidad reutilización de datos en las organizaciones

IX Desarrollo de capacidades para el uso efectivo de los datos

Disposiciones principales de la Recomendación sobre la EASD

Sección 1- Reforzar la confianza en el ecosistema de datos

III Empoderamiento y participación proactiva

IV Enfoque estratégico de todo el gobierno

V Maximizar los beneficios, protegiendo los derechos y fomentando una cultura de responsabilidad

Sección 2. Estimular la inversión en materia de datos e incentivar el acceso e intercambio de datos

VI Incentivos coherentes y modelos de negocios y mercados sostenibles

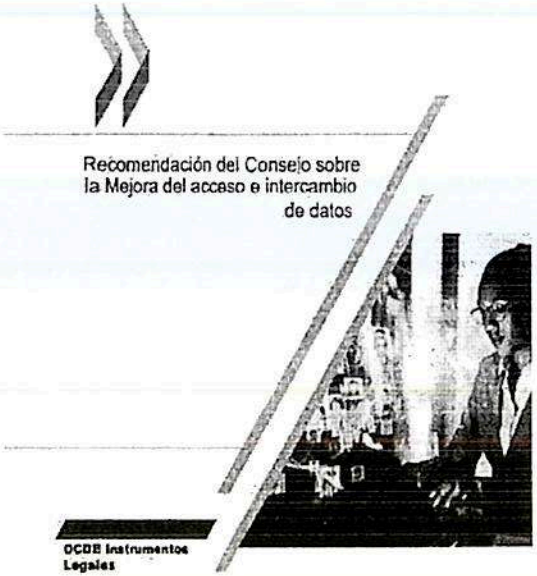
Sección 3. Fomentar el acceso, intercambio y uso efectivo y responsable de datos en la sociedad

VII Mejorar las condiciones para el acceso e intercambio transfronterizo de datos

VIII Encontrabilidad, accesibilidad, interoperabilidad y reutilización de datos en las organizaciones

IX Desarrollo de capacidades para el uso efectivo de los datos

Los Miembros de la OCDE acordaron en octubre de 2021 los principios generales para el acceso e intercambio de datos



Objetivos de la Recomendación sobre la EASD:

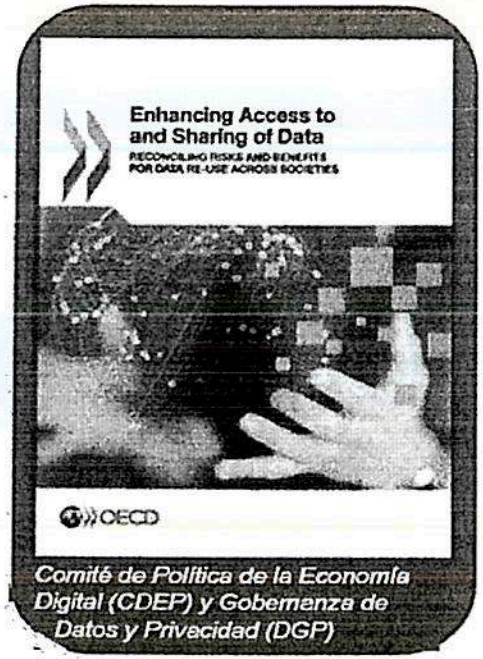
- Facilitar el acceso e intercambio de datos entre los sectores y países.
- Permitir la colaboración y la reutilización innovadora de los datos para el crecimiento y el bienestar.
- Proteger los derechos de las partes interesadas y mejorar la fiabilidad del ecosistema de datos.
- Fomentar la coherencia de los marcos de gobernanza de datos entre sectores y países.

OECD
BETTER POLICIES FOR BETTER LIVES

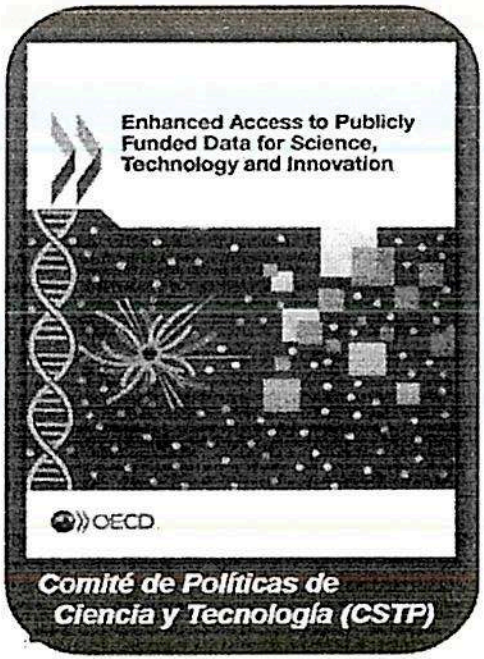
Texto completo: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463

Recomendación para la mejora en el acceso e intercambio de datos en los instrumentos legales de la OCDE sobre gobernanza de datos

El trabajo referente a la EASD aprovecha los conocimientos de varios interesados en la OCDE



Comité de Política de la Economía Digital (CDEP) y Gobernanza de Datos y Privacidad (DGP)



Comité de Políticas de Ciencia y Tecnología (CSTP)

Comité de Gobernanza Pública (PGC)/líderes electrónicos

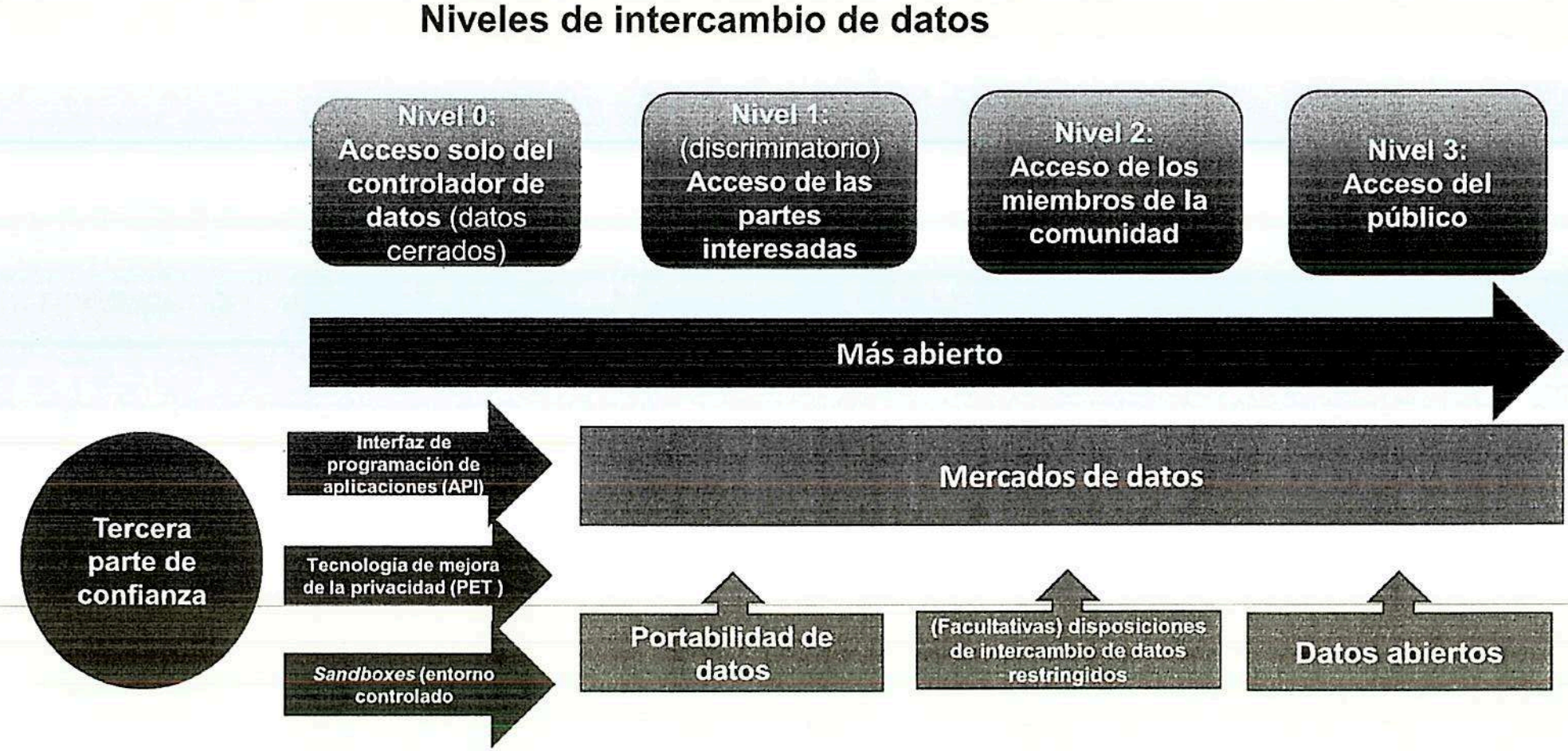
Grupo Directivo Conjunto (JSG)

cho Grupo está compuesto por más de 90 especialistas, incluyendo representantes de más de 30 economías miembros y asociadas a l CDE, así como el Comité Consultivo Empresarial e Industrial (BIAC) (negocios en la OCDE), Comité Consultivo Sindical (TUAC) (sindicato onsejo Consultivo de la Sociedad Civil sobre la Sociedad de la Información (CSISAC) (sociedad civil) y Comité Asesor Técnico d ternet (ITAC) (comunidad técnica de Internet).

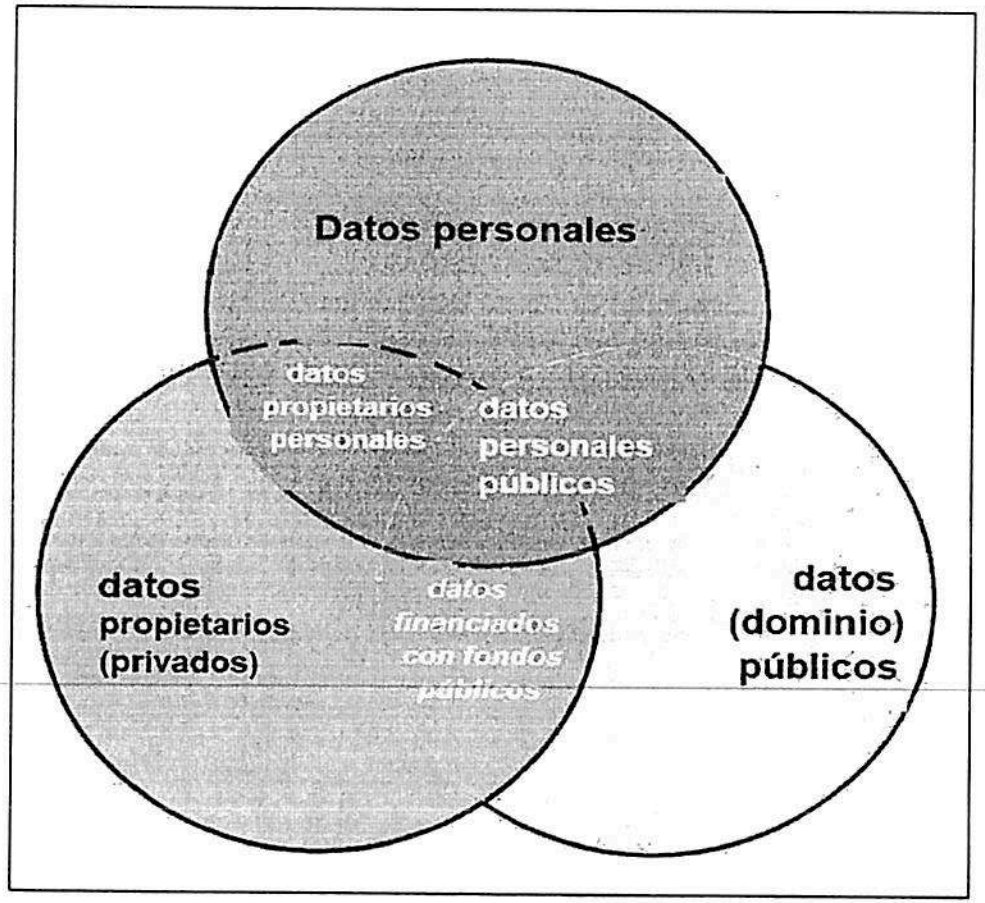
Para mayor información sobre nuestro trabajo, sírvase ingresar al siguiente enlace https://oe.cd/easd21

Recomendaciones del Consejo de la OCDE sobre la mejora en el acceso e intercambio de datos

Solución potencial: Aprovechar la continuidad de niveles del intercambio de datos



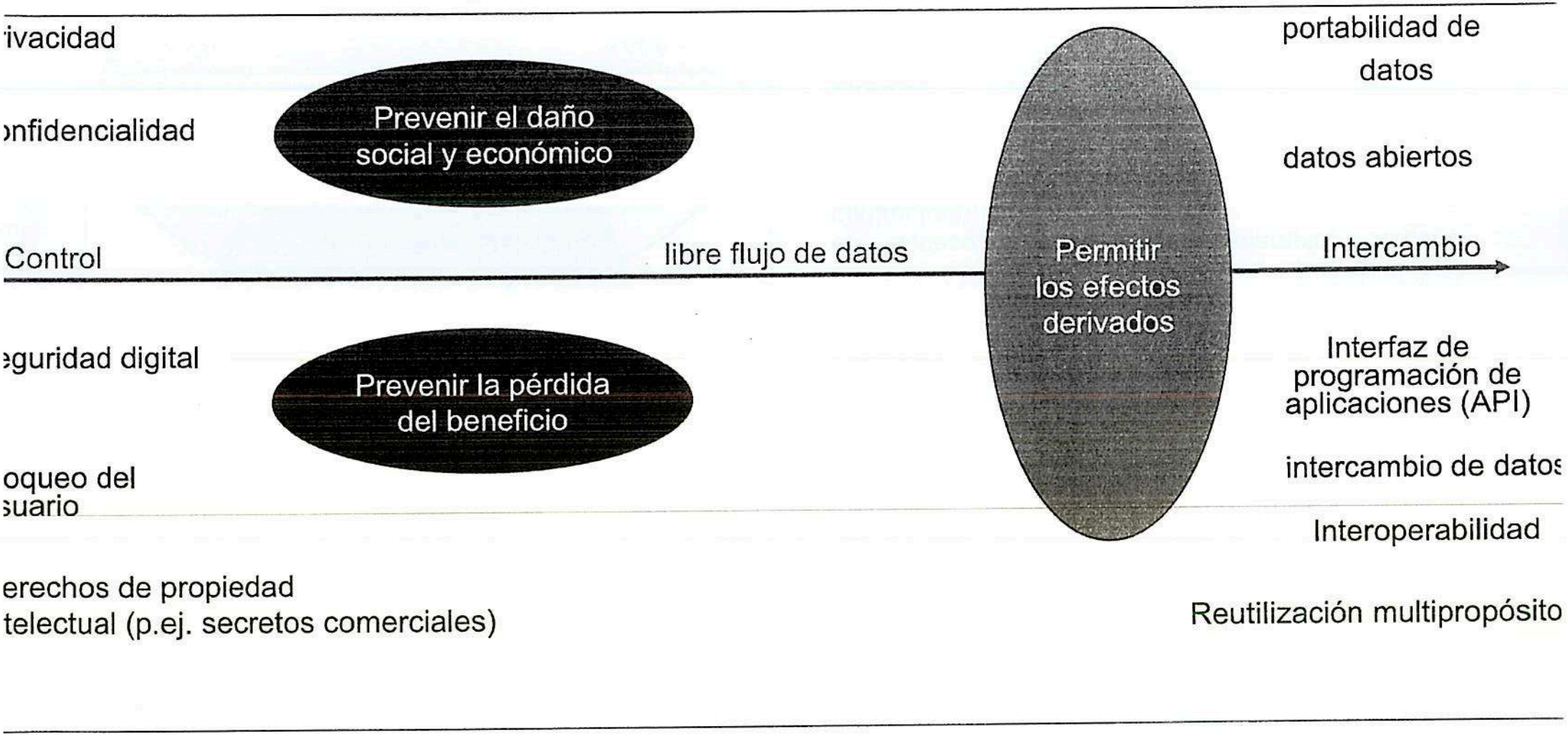
Dilema clave 2: la superposición de derechos e intereses (conflictivos) en los datos



- ***Dominio personal*** abarca todos los datos «relacionados con una persona identificada o identificable» (datos personales) respecto de los cuales los interesados tienen un interés privado;
- ***Dominio propietario*** abarca todos los *datos propietarios* que suelen estar protegidos por derecho de propiedad intelectual (DPI) (p. ej., derechos de autor y secretos comerciales) o por otros derechos de acceso y control (por ejemplo, derecho contractual);
- ***Dominio público*** abarca todos los datos que no están protegidos por DPI y que, por tanto, pertenecen al «dominio público» o **son de interés público**.

OCDE (2019), «Enhancing Access to Data and Sharing of Data: Reconciling Rosks and Benefits for Data Re-Use across Societies».

Dilema clave 1: Conseguir el equilibrio adecuado entre el «intercambio» y el «control»



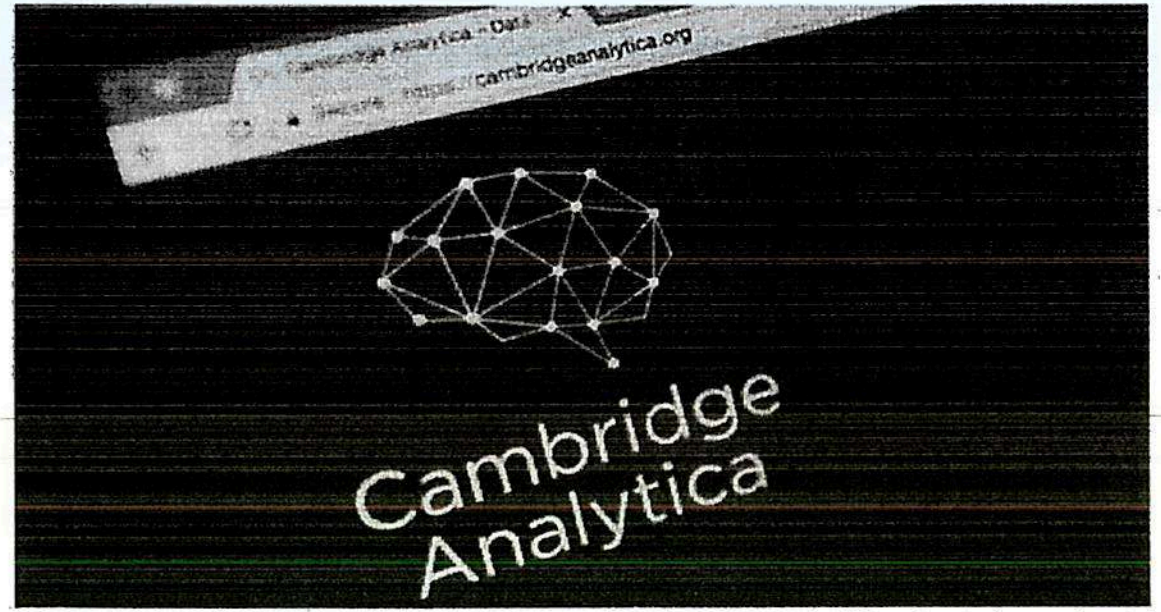
Tensión entre datos abiertos y control

os datos abiertos pueden socavar la capacidad de los titulares de los datos (colectores e datos) y de los interesados para controlar la forma en que se reutilizan «sus» datos.

Cambridge Analytica

Cambridge Analytica engañó a usuarios de Facebook, sostiene la Comisión Federal de Comercio (FTC)

Empresa se involucró en prácticas engañosas con los datos de los votantes para definir sus perfiles políticos y convertirlos en objetivos de campaña, en relación con el marco del Escudo de Privacidad UE-EE.UU.



▲ La investigación de la FTC se desencadenó ante las denuncias de que Facebook violó un decreto de acuerdo extrajudicial del 2012, al compartir indebidamente información de 87 millones de usuarios con Cambridge Analytica Fotografía Alamy Stock Foto

Los datos pueden acabar siendo reutilizados contra

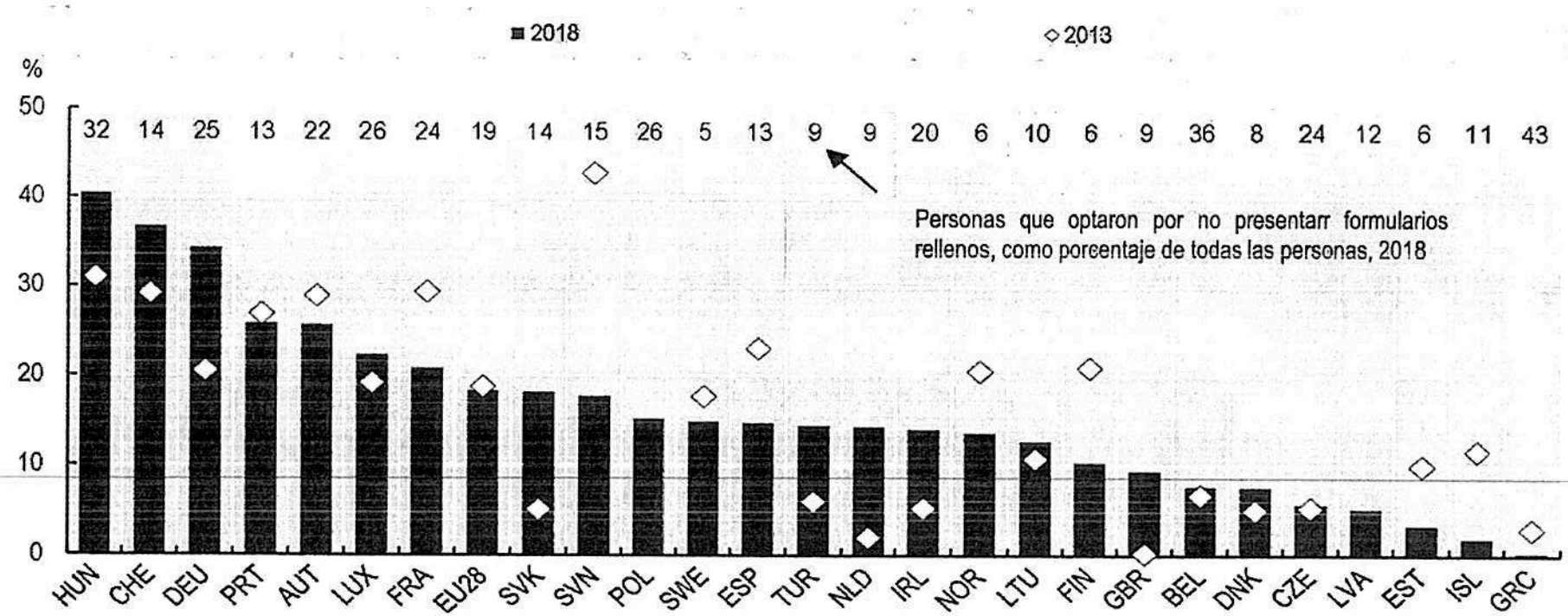
- las expectativas de los usuarios, y
- los términos y condiciones acordados por el titular de los datos.

➢ Pérdida de control de los datos

reocupación por privacidad y seguridad suele ser una de las principales causas para no tilizar los servicios digitales

Personas que no presentaron formularios oficiales en línea debido a preocupaciones por la privacidad y seguridad, 2018

Porcentaje de personas que optaron por no presentar formularios oficiales en línea

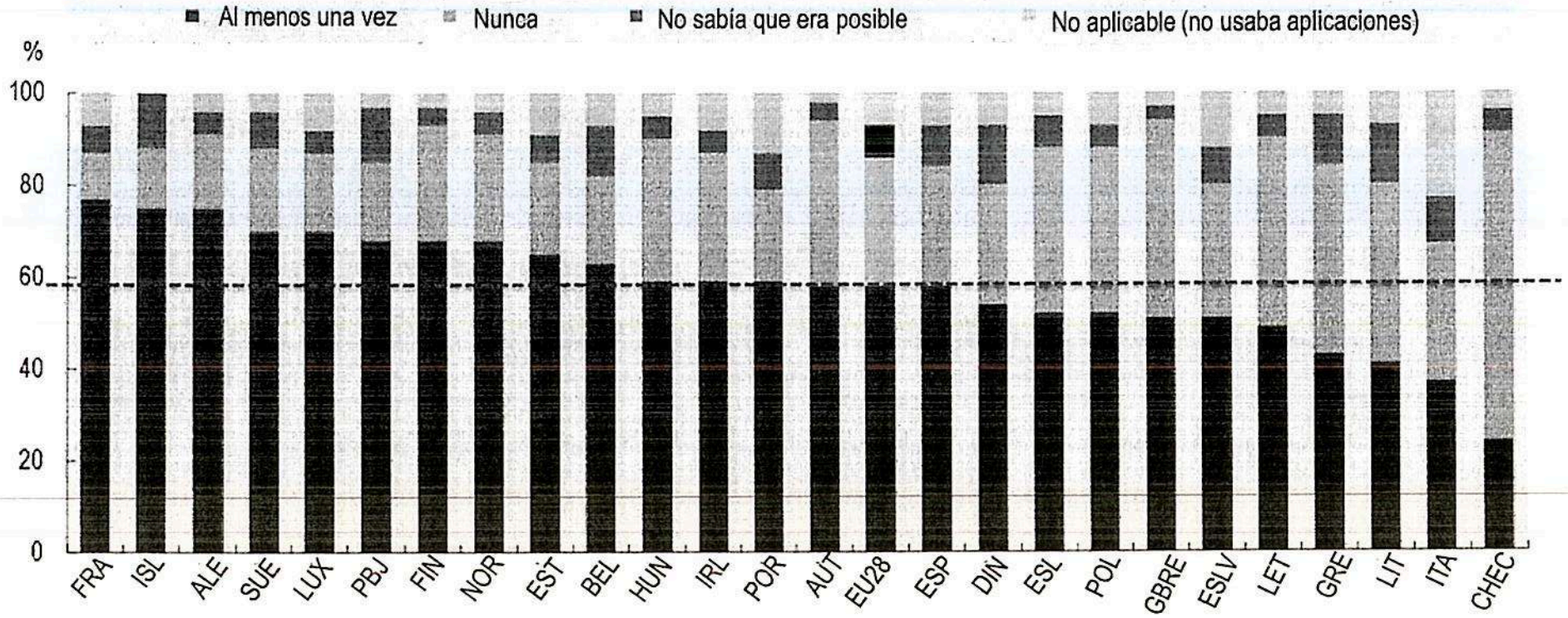


OECD (2019), *Measurin g the Di gital Transformation,* OECD Publishing, Pa ris, https://doi.org/10.1787/86a789d9-en, basado en Eurostat, Digital Economy and Society Statistics, Base de datos integral. Respecto a Suiza, los datos corresponden al 2014 y 2017.

isposición de las personas para compartir datos varía considerablemente entre países

Personas que restringieron o rechazaron el acceso a sus datos personales al utilizar o instalar una aplicación en un *smartphone*, 2018

Porcentaje de personas que utilizan un smartphone con fines privados



OECD {2019), *Measuring the Digital Transformation: A Roadmap far the Future,* OECD Publishing, Paris, https://doi.org/10.1787/62ff8236-en ,basado en Eurostat Digital Economy and Society Statistics

as violaciones a la seguridad digital varían considerablemente según el sector

Prevalencia y tipo de incidentes contra la seguridad digital por industria, 2019

Número de incidentes y porcentaje del total de incidentes (%)

	Intensidad digital	Prevalencia de riesgos seguridad digital		Actores (%)	Principales datos comprometidos (%)					
		Incidentes	Violaciones	Ataques externos	Datos personales	Credenciales	Datos internos	Datos de pagos	Datos bancarios	Datos médicos
Servicios profesionales, científicos y técnicos	Alta	7 463	326	75%	75%	45%				
Administración pública	Medio alta	6 843	346	59%	51%	33%				
Serv. de información	Alta	5 741	360	67%	69%	41%	16%			
Finanzas y seguro	Alta	1 509	448	64%	77%	35%			32%	
Ind. manufacturera	Medio baja a alta	922	381	75%	49%	55%		20%		
Servicios educativos	Medio baja	819	228	67%	75%	30%	13%			
Atención médica	Medio baja	798	521	51%	77%	18%				67%
Comercio minorista	Medio alta	287	146	75%	49%	27%		47%		
Arte, entretenimiento y recreación	Medio alta	194	98	67%	84%			25%		31%
Minería, ind. extractiva y servicios públicos	Baja	194	43	75%	41%	41%	19%			
Alojamiento y alimentación	Baja	125	92	79%	44%	14%		68%		
Transporte y almacenamiento	Baja	112	67	68%	64%	34%				
Otros servicios	Baja a alta	107	66	68%	81%	36%				
Construcción	Baja	37	25	95%	N/A	N/A				
Bienes raíces	Baja	37	33	73%	83%	40%	43%			

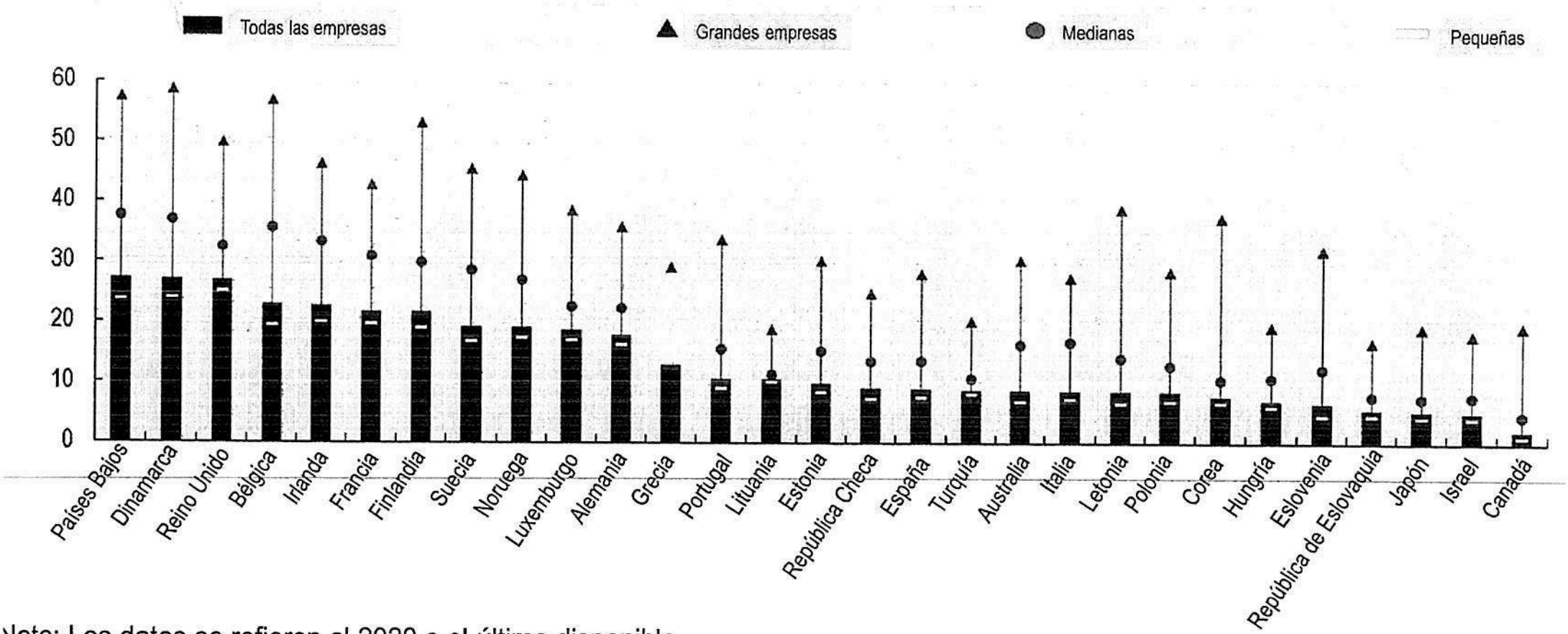
Nota: La intensidad digital corresponde a una taxonomía de sectores intensivos en tecnología digital que da cuenta de algunas de las facetas clave de la transformación digital. Los indicadores utilizados para clasificar 36 sectores definidos según la clasificación industrial estándar internacional de actividades económicas (CIIU revisión 4) durante el periodo 2013-2015 son: porcentaje de inversión en TIC tangibles e intangibles (es decir, software); porcentaje de compras de bienes y servicios intermedios de TIC; el stock de robots por cada cientos de empleados; porcentaje de especialistas en TIC en el empleo total, y porcentaje del volumen de negocio de las ventas en línea.

Fuente: OCDE (2021), OECD *Studies on SMEs and Entrepreneurship*, OECD Publishing, París, basado en (Verizon, 2020; Calvino *et al.*, 2018).

RIESGOS DE LOS DATOS ABIERTOS

.pero las PYMES están a la zaga

Uso de la analítica de macro datos por tamaño de empresa como porcentaje de empresas, 2020



Nota: Los datos se refieren al 2020 o el último disponible

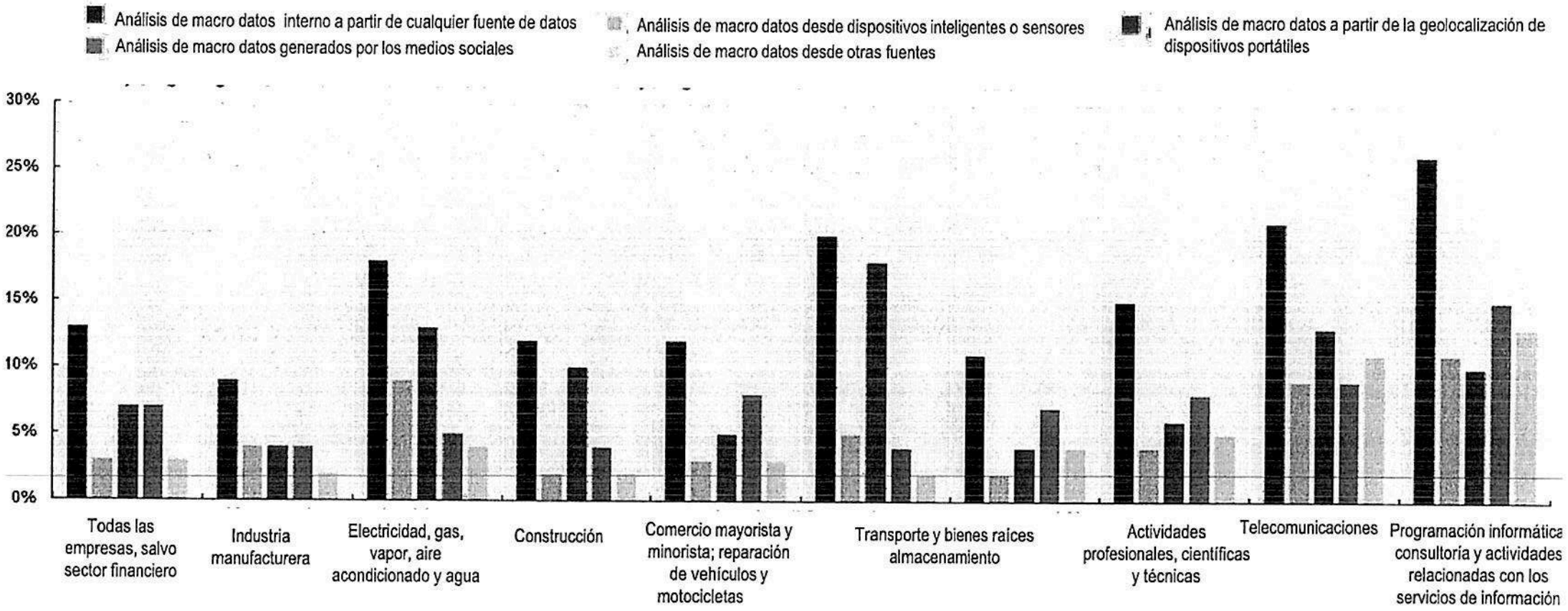
Fuente: OCDE (2022) Base de datos de acceso y uso de las TIC por base de datos de las empresas, http://oe.cd/bus

. con efectos positivos en la innovación y productividad

- Las empresas que realizan análisis de macro datos tienen más probabilidades de innovar en productos y procesos.
  - Las empresas de servicios suecas que realizan análisis de macro datos a partir de la geolocalización de dispositivos portátiles son ~25°/o más propensas a innovar sus servicios (OCDE, 2021)
- La adopción de activos relacionados con macro datos se asocia a una mejora en la media de productividad de las empresas del 3%-7%.

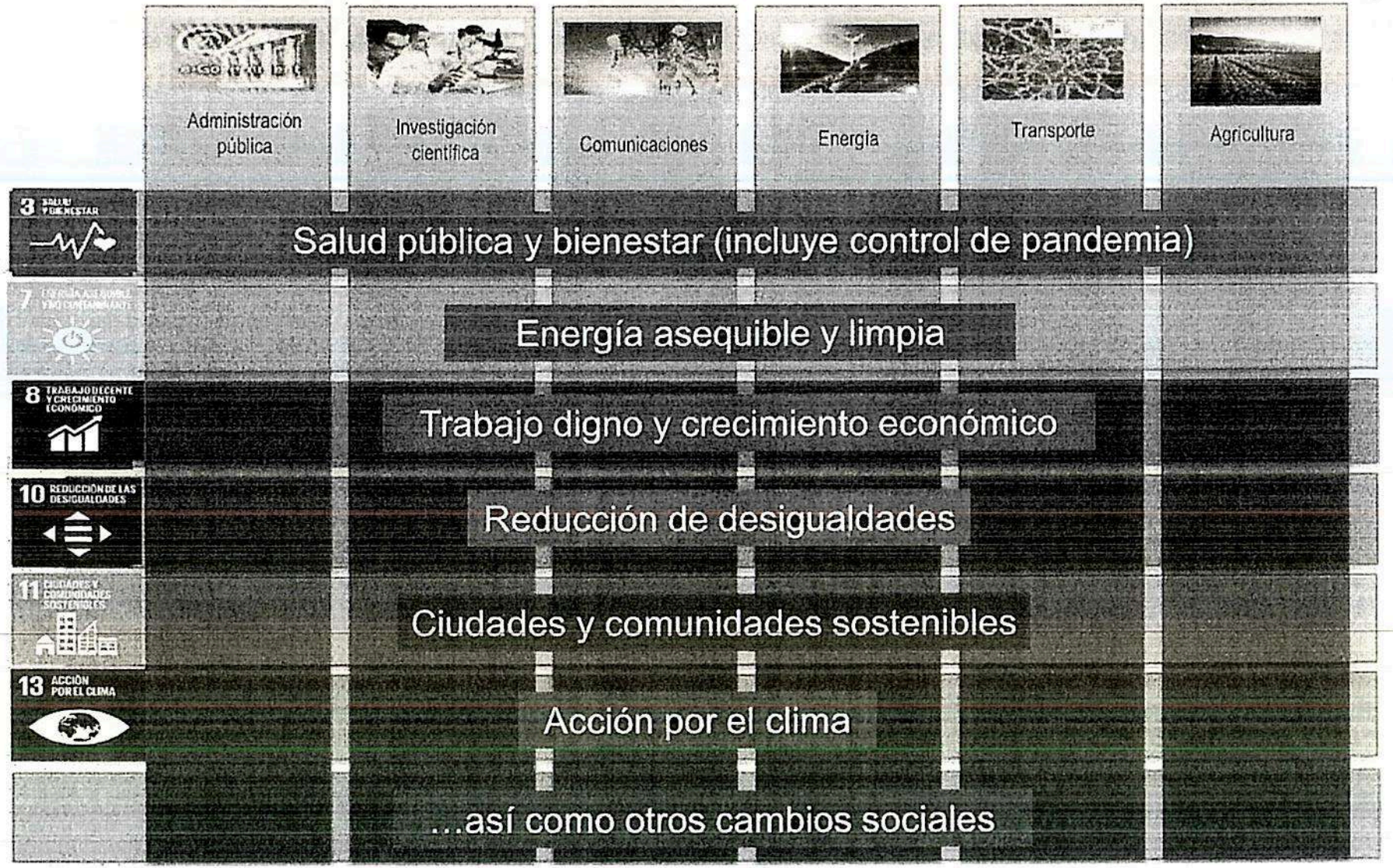
as empresas usan datos de todo tipo…

Porcentaje de empresas de la UE27 que realizan análisis de macro datos por sectores y fuentes de datos, 2020



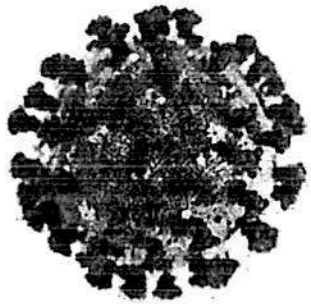
Fuente: Eurostat (2022), Base de datos de uso de TIC en empresas

so de datos puede adelantar los objetivos de desarrollo sostenible



cceso e intercambio de datos oportunos, seguros y confiables es fundamental para grar respuestas e investigación efectivas al COVID-19

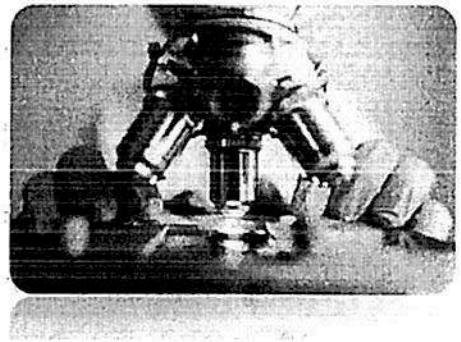
Comprender y controlar la difusión del virus



Mejorar la capacidad de los sistemas de atención de salud

Evaluar la eficacia de las políticas

Promover la investigación y desarrollo de vacunas y medicamentos



Para mayor información, véase los siguientes enlaces:

- Ensuring data privacy as we battle COVID-19
- Open data in action: Initiatives during the initial stage of the COVID-19 pandemic
- Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics
- Why open science is critical to combatting COVID-19
- The Covid-19 crisis: A catalyst for government transformation?

os datos son un recurso infraestructural con amplios beneficios derivados

Los datos son:

1. Bienes de capital
   - Los datos pueden reutilizarse como insumo de producción
2. Bienes de uso general
   - Los mismos datos pueden ser insumos para múltiples fines
3. Bienes no rivales
   - Los datos pueden reutilizarse sin que disminuya su valor potencial para terceros

➢ **Datos abiertos (p.ej. acceso, intercambio y reutilización) pueden maximizar el valor**

BENEFICIOS ECONÓMICOS Y SOCIALES DE LOS DATOS ABIERTOS

structura y narrativa de la presentación

Datos abiertos conllevan pérdida de control sobre los datos, lo que aumenta el riesgo de violaciones a los derechos y otros intereses, que a su vez socaban la confianza en el ecosistema de datos

Sería necesario algunas restricciones a los datos abiertos para controlar riesgos, si bien algunas pueden reprimir la innovación y los beneficios económicos, y sociales de los datos

Se requieren enfoques más equilibrados y estratégicos para maximizar los beneficios de los datos abiertos, a la vez que se mejora la confianza en el sistema económico de datos

Red Parlamentaria Global de la OCDE. Construir un futuro digital seguro e inclusivo en un mundo post-COVID
Saeima de la República de Letonia
1 de julio del 2022

MEJORA EN EL ACCESO E INTERCAMBIO DE DATOS (EASD)

- Presentación de la Recomendación del Consejo de la OCDE repecto a la EASD
- [OCDE/JURÍDICO/0463]

Christian Reimsbach-Kounatze (STI/DEP.)

Documento traducido por la Biblioteca del Congreso, con fines meramente informativos. Como es usual, el documento original puede estar sujeto a derechos de autor.

16:30 – 18:00 **Ciberseguridad y seguridad digital: gestionar los riesgos y enfrentar las vulnerabilidades**

Christian Reimsbach-Kounatze, *Economista, Analista de Políticas, Gobernanza de Datos y Privacidad-Seguridad en la Economía Digital, División de Políticas de Economía Digital, Dirección de Ciencia, Tecnología e Innovación, OCDE*

A medida que se acelera la transformación digital, nuestras economías y sociedades se vuelven cada vez más vulnerables a los ciberataques que pueden dañar los activos, la reputación y competitividad de las organizaciones. Estos ataques incluso pueden ocasionar el cierre de empresas y, con el desarrollo del Internet de las cosas (IoT), amenazan la seguridad de las personas. El surgimiento del cibersecuestro de datos es el más reciente ejemplo de esta tendencia, que afecta a los operadores de actividades cruciales como distribución de gas y atención sanitaria.

Esta sesión destaca ***cómo fortalecer la seguridad y la confianza, sin limitar los beneficios de la transformación digital y su posibilidad de incrementar el bienestar, la innovación y el crecimiento****. La sesión se centra en los aspectos económicos y sociales de la ciberseguridad, en oposición a los aspectos puramente técnicos que están relacionados directamente con la aplicación del derecho penal o la seguridad nacional. En particular, resalta la importancia de la* ***gestión de riesgos de la seguridad digital como característica fundamental del planteamiento de OCDE para la seguridad digital,*** *orientado en (i) mejorar la seguridad de los productos y servicios, y (ii) fomentar el tratamiento de las vulnerabilidades.*

Desde la perspectiva de Letonia

Kristians Teters, *CERT.LV – Instituto de Respuesta a incidentes de seguridad de las tecnologías de la información de la República de Letonia*

Comentarista: ***Luis Jesús Uribe-Etxebarría****, Miembro del Parlamento, España*

18:00 – 18:15 **Observaciones finales y próximos pasos**

a la vez que protegen los derechos de los individuos y las organizaciones. Esta sesión resalta las oportunidades y retos del acceso a los datos y el intercambio de estos, así como en qué medida la Recomendación de la OCDE sobre la EASD puede ayudar a los gobiernos a desarrollar ***políticas públicas y marcos de gobernanza de datos coherentes****, a fin de destrabar los beneficios potenciales de los datos entre los sectores y países.*

Comentarista especial. Desde la perspectiva de Letonia
Jekaterina Macuka, *Directora, Data State Inspectorate [Inspectoría de Datos del Estado] (Letonia)*

Otros comentaristas:
Mattia Fantinati, *Miembro del Parlamento, Italia*
Lukas Savickas, *Miembro del Parlamento, Lituania*

11:00 - 11:30 Pausa café

11:30 - 13:00 **Gobernar y legislar en la era digital**
Perspectiva del Parlamento Europeo
Alexandra Geese*, Miembro del Parlamento Europeo*
Andreas Schwab*, Miembro del Parlamento Europeo*
Comentarista ***Fadli Zon****, Miembro del Parlamento, Indonesia*

13:00 - 13:15 Foto grupal

13:15 - 14:30 Almuerzo

14:30 - 16:30 **Combatir la desinformación digital: visión desde el Frente Oriental**
Janis Karlsbergs, *Director de Publicaciones y Políticas, Centro de Excelencia de Comunicaciones Estratégicas de la OTAN*
Molly Lesher*, Analista sénior de Políticas Públicas,* ***Going digital*** *[Hacia lo digital], División de Políticas de Economía Digital, Dirección de Ciencia, Tecnología e Innovación, OCDE*

Herramienta: Disentangling untruths online: Creators, spreaders and how to stop them [Desenmarañar las falsedades en línea: Creadores, difusores y cómo detenerlos]
Podcast: Disinformation and its discontents [Desinformación y sus descontentos]

Comentaristas:
Eun A Her; *Miembro del Parlamento, Corea*
Anke Domscheit-Berg; *Miembro del Parlamento, Alemania*
Darren Jones; *Miembro del Parlamento, Reino Unido*

cómo construir una gobernanza robusta a fin de apoyar la transformación digital y comentará los aspectos fundamentales que necesitan ser abordados para construir un futuro seguro e inclusivo.

Panel parlamentario
Moderador: ***Vjaceslavs Dombrovskis,*** *Presidente de la Comisión de Desarrollo Sostenible, Saeima de la República de Letonia.*

- ***Liam Byrne****, Miembro del Parlamento, Reino Unido*
- ***Anke Domscheit-Berg****, Miembro del Parlameno, Alemania*
- ***Christopher Frassa****, Miembro del Parlamento, Francia.*
- ***Konstantinos Karagounis,*** *Miembro del Parlamento, Grecia*
- ***Irine Yusiana Roba Putri,*** *Miembro del Parlamento, Indonesia*
- ***Lukas Savickas,*** *Miembro del Parlamento, Lituania*

20:00 Recepción
Museo Nacional de Arte de Letonia
Jana Rozentala laukums 1, Riga

Viernes 1 de julio del 2022

09:00 - 09:30 Palabras de bienvenida

- ***Ināra Mūrniece****, Presidenta de la Saeima (parlamento), Letonia*
- ***Rihards Kols,*** *Presidente, Comisión de Asuntos Exteriores, Saeima de la República de Letonia*
- ***Artūrs Toms Plešs****, Ministro de Protección Ambiental y Desarrollo Regional y responsable de la Transformación digital, Letonia*
- ***Anthony Gooch,*** *Presidente de la Red Parlamentaria Global, OCDE*

09:30 - 11:00 **Espacios digitales seguros: gobernanza de datos para mejorar el acceso y el intercambio**
Christian Reimsbach-Kounatze*, Economista, Analista de Políticas, Gobernanza de Datos y Privacidad-Seguridad en la Economía Digital, División de Políticas de Economía Digital, Dirección de Ciencia, Tecnología e Innovación, OCDE*

Aprobada en octubre del 2021, la Recomendación de la OCDE sobre la mejora del acceso y el intercambio de datos (EASD) es el ***primer acuerdo internacional sobre un conjunto de principios y directivas de políticas públicas*** *sobre cómo los gobiernos pueden maximizar los beneficios transectoriales de* ***todos los tipos de datos***

PROGRAMA

Reunión itinerante de la Red Parlamentaria Global de OCDE

el 30 junio y 1 julio del 2022

Saeima de la República de Letonia

Jēkaba iela 11, Rīga

Sírvase tener en cuenta que los horarios del programa relejan el horario de Letonia (hora de Riga - EEST

«Construir un futuro digital seguro e inclusivo en un mundo post-COVID»

Jueves 30 de junio del 2022

16:30 Café de bienvenida

17:00 - 19:00 **Taller parlamentario – Hacia una respuesta a los desafíos de la transformación digital en los procesos democráticos**
Discurso inaugural: ***Rihards Kols,*** *Presidente de la Comisión de Asuntos Exteriores, Saeima, Parlamento de la República de Letonia.*

Puesta en contexto: ***Barbara Ubaldi****. Jefe de la Unidad de Datos y Gobierno Digital. División de Gobierno Abierto e Innovador. Dirección de Gobernanza Pública, OCDE.*

La transformación digital ha cambiado radicalmente los mecanismos tradicionales de la democracia. El uso de las tecnologías y datos digitales ha empoderado a los ciudadanos con nuevas herramientas a fin de que tomen parte en las prácticas democráticas y tengan una participación política más amplia. Sin embargo, la digitalización rápida también presenta retos que debilitan los procesos democráticos como la protección de los derechos fundamentales; ha desestabilizado los ecosistemas de información y la intermediación democrática. En la era digital, la nueva forma de gobernar y legislar requiere enfrentar estos desafíos. En la presentación de este escenario, la OCDE expondrá

Lima, 14 de julio de 2022

Oficio 265-2021-2022-AB-DIDP-DGP/CR

Señor
GABRIEL DUARTE RODRIGUEZ
Jefe (e) del Departamento de Investigación y Documentación Parlamentaria
Presente.-

Asunto: Traducción de documentos, del inglés al español, referidos a la Reunión Itinerante de la Red Parlamentaria Global de la OCDE

Referencia: Memorando N° 026-2021-2022-/CESIP-OCDE-CR (RU 895207)

De mi consideración:

Tengo el agrado de dirigirme a usted para expresarle mi cordial saludo y, a la vez, en atención al documento de la referencia, referido a la solicitud de traducción de documentos, del inglés al español, de la Reunión Itinerante de la Red Parlamentaria Global de la OCDE, remitirle adjunto al presente la traducción, del inglés al español, en formato pdf, de los documentos antes mencionados.

Sin otro particular aprovecho la oportunidad para hacerle llegar los sentimientos de mi estima personal.

Atentamente,

FIRMA DIGITAL

Firmado digitalmente por: CEVALLOS SCUDIN Jose Antonio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 14/07/2022 20:03:38-0500

Se adj.: lo indicado

RU 900532

Lima, 15 de julio de 2022

Registro Único 899085

CONGRESO DE LA REPÚBLICA
RECIBIDO
15 JUL 2022
Hora: 2:32 pm
Fecha:
DIRECCIÓN GENERAL PARLAMENTARIA

OFICIO 400-2021-2022-DIDP-DGP-CR

Señor
JAVIER ADOLFO ÁNGELES ILLMANN
Director General Parlamentario
Congreso de la República

Asunto: Traducción de documentos, del inglés al español, referidos a la Reunión Itinerante de la Red Parlamentaria Global de la OCDE

Referencia: Memorando 026-2021-2022-/CESIP-OCDE-CR (RU 895207)

Es grato dirigirme a usted para saludarlo cordialmente y en atención al asunto y documento de la referencia, remitirle el Oficio 265-2021-2022-AB-DIDP-DGP/CR (Registro Único 900532) del jefe del Área de Biblioteca, con la traducción del inglés al español de los documentos referidos a la *Reunión Itinerante de la Red Parlamentaria Global de la OCDE*, solicitada por la presidencia de la Comisión Especial de Seguimiento de la Incorporación del Perú a la Organización para la Cooperación y el Desarrollo Económicos (CESIP – OCDE).

Válgome de la ocasión para expresarle las seguridades de mi consideración y estima.

Atentamente,

FIRMA DIGITAL

Firmado digitalmente por: DUARTE RODRIGUEZ Juan Gabriel FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 15/07/2022 13:48:36-0500

Adj.: Lo indicado.

C. c: Área de Biblioteca.

JGDR/rila.

Lima, 15 de julio de 2022

OFICIO Nº 1082-895207-3-2021-2022-DGP-OM-CR

Señor congresista
Luis Gustavo Cordero Jon Tay
Presidente de la Comisión Especial de Seguimiento de la incorporación del Perú a la Organización para la Cooperación y el Desarrollo Económico (CESIP-OCDE)
Presente. -

Ref.: Memorando Nº 026-2021-2022/CESIP-OCDE-CR (RU-895207)

Me dirijo a usted, por encargo del Oficial Mayor del Congreso de la República, en atención al documento y proveído de la referencia, para hacerle llegar el Oficio 400-2021-2022-DIDP-DGP-CR suscrito por el jefe (e) del Departamento de Investigación y Documentación Parlamentaria, mediante el cual remite la traducción del inglés al español requeridos.

Sea propicia la ocasión para expresarle los sentimientos de mi consideración.

Atentamente,

Javier Ángeles Illmann
Director General Parlamentario
Congreso de la República

RU-901160