Buenas Prácticas de Seguridad para la Protección de la Privacidad con Datos Abiertos

María Roxana Martínez
Universidad Argentina de la Empresa, **UADE**
mariarmartinez@uade.edu.ar
CABA, Buenos Aires, Argentina

Jorge Iván Pincay-Ponce
Universidad Laica Eloy Alfaro de Manabí, **ULEAM**
Jorge.pincay@uleam.edu.ec
Manta, Manabí, Ecuador

DOI: https://doi.org/10.56124/encriptar.v7i14.010

Resumen

El tratamiento de los datos abiertos públicos es un tema que cada vez se encuentra más auge, ya que permite incentivar las iniciativas de transparencia en entidades gubernamentales, como así también en diversas empresas privadas. Este nuevo paradigma tiene como uno de sus ejes centrales, el tratamiento de los datos abiertos para que puedan ser manipulados mediante técnicas específicas con software y servicios que permiten el almacenamiento de estos en otras bases de datos para su utilización. Esto representa una gran ventaja en aspectos de transparencia en el contexto de Gobierno Abierto, sin embargo, esta apertura de datos expone diversos desafíos en cuanto a la privacidad y seguridad, debido a que puede poner en riesgo la privacidad de los ciudadanos en caso de que no se implementen medidas adecuadas.

El objetivo de este trabajo es presentar un relevamiento sobre el estado de situación en este contexto, por lo que, para ello, se analizaron algunos casos de estudios y ejemplos prácticos de organizaciones, con el fin de trabajar en las falencias y problemáticas en lo que respecta a la privacidad y seguridad en el tratamiento de los datos abiertos públicos. Como siguiente punto, se trabajó en una propuesta de una serie de buenas prácticas y políticas para brindar una adecuada protección de la confidencialidad de datos. Finalmente, se analiza que utilizar estas prácticas, no solo podrá mejorar la protección de datos disponibles, sino que también, permitirá fortalecer la confianza pública en este tipo de iniciativas.

Palabras clave: datos abiertos; seguridad; protección de datos; derecho a la privacidad.

Best Security Practices for Protecting Privacy with Open Data

ABSTRACT

The treatment of public open data is a topic that is becoming more and more popular, since it allows encouraging transparency initiatives in governmental entities, as well as in several private companies. This new paradigm has, as one of its central points, the treatment of open data so that they can be manipulated by means of specific techniques with software and services that allow their storage in other databases for their use. This represents a great advantage in terms of transparency in the context of Open Government, however, this data openness exposes several challenges in terms of privacy and security, because it can jeopardize the privacy of citizens if appropriate measures are not implemented.

The objective of this paper is to present an analysis of the state of the art in this context, so, for this purpose, some case studies and practical examples of organizations were analyzed, in order to work on the shortcomings and problems regarding privacy and security in the treatment of public open data. As a next point, we worked on a proposal for a series of good practices and policies to provide adequate protection of data confidentiality. Finally, it was analyzed that the use of these practices could not only improve the protection of available data, but also allow strengthening public confidence in these types of initiatives.

Keywords: open data; security; data protection; right to privacy.

1. Introducción

Hoy por hoy los datos abiertos y públicos se han convertido en una de las fuentes más valiosas para el análisis de datos gubernamentales. Esto de alguna manera permite fomentar la transparencia en un contexto de Gobierno de datos junto a la innovación y como así también al desarrollo de los ciudadanos en un país. El concepto de datos públicos implica que se encuentran disponibles en sitios web, por lo que pueden ser accedidos por cualquier usuario. Estas fuentes de datos son gestionadas y publicadas por entes gubernamentales que autorizan la publicación y acceso a cualquier persona. Por otra parte, esto conlleva hacia una dirección de poder trabajar

con datos abiertos públicos. Los datos abiertos se encuentran disponibles en repositorios en los que más allá de ser datos públicos, estos se encuentran en formatos determinados que permiten interoperar entre distintos softwares como así también disponibilizarlos en distintos motores de bases de datos. Algunos de estos formatos abiertos que permiten el tratamiento técnico con los mismos son: XML, JSON, CSV entre otros. Estos datos al estar disponibles para cualquier persona permiten que se puedan desarrollar nuevas aplicaciones como así también llevar a cabo un análisis profundo sobre las políticas públicas y así, lograr encontrar beneficios para la ciudadanía. Si bien todos estos son aspectos importantes, cabe mencionar que la apertura de datos plantea desafíos en aspectos de privacidad y seguridad, ya que se puede contar con repositorios de datos abiertos que tengan información sensible la cual podría ser expuesta en forma pública y ser utilizada de manera indebida. "*En estos tiempos, los datos son un recurso indispensable para cualquier actividad de gestión pública, por lo que es necesario mantenerlos actualizados, claros y completos. Si bien se puede determinar que cada vez son más los gobiernos que se embarcan en este nuevo paradigma de concepto de datos abiertos, todavía falta un largo camino por recorrer*" [1].

Dentro de lo que es el contexto de la privacidad, es importante indicar que es un derecho fundamental que debe ser protegido e incluso en contextos donde la información o datos pueden ser de acceso público es necesario tomar medidas y precauciones con respecto a la disponibilidad de estos. A medida que la vida de las personas se conduce cada vez más al entorno digital, crece la preocupación sobre cómo las empresas privadas y las agencias gubernamentales manejan y almacenan datos confidenciales. Estas preocupaciones han impulsado la solicitud de leyes de privacidad de datos por parte de las legislaturas estatales [2].

Los datos sensibles pueden incluir información personal sobre la identificación por parte de un ciudadano, por lo que esto requiere de un manejo

muy cuidadoso, para evitar que estos datos sean divulgados y no comprometer así, la seguridad de una persona. "*En este contexto, las Administraciones Públicas deben tener en cuenta las normativas de protección de datos al publicar información. Es fundamental que los datos personales no se divulguen de manera que puedan identificar a las personas involucradas sin su consentimiento o sin una base legal adecuada. Esto se aplica a categorías especiales de datos, como aquellos relacionados con la salud, la vida sexual, la afiliación sindical, entre otros*" [3]. Es por este mismo motivo que es fundamental desarrollar estrategias que permitan apuntar a los beneficios de los datos abiertos, sin comprometer la privacidad de las personas, es decir, que esta tarea implica el análisis, desarrollo e implementación de medidas de seguridad para que sean robustas, junto a un conjunto de técnicas de anonimización, en conjunto con criterios de Marcos legales que regulan tanto el acceso, como el uso de estos datos disponibles públicamente. Cabe mencionar que, "*los gobiernos deben asegurar la confiabilidad de los datos y propiciar espacios de colaboración donde se habilite la generación de valor público, garantizando la confidencialidad de datos personales. Es importante notar que para que los datos abiertos puedan generar valor, se necesita avanzar en la estandarización de la calidad, en la accesibilidad y la publicación en formatos fáciles de usar*" [4].

1.1. Importancia de la seguridad de los datos

Dentro de lo que es el contexto de datos abiertos públicos se presenta un gran desafío que es el tratamiento de la seguridad para proteger tanto la integridad, como la confidencialidad de la información en aspectos de transparencia y el acceso al dato público. En un entorno donde los datos pueden ser publicados en diversas páginas web pertenecientes y autorizadas por distintos entes gubernamentales o empresas privadas, las medidas de seguridad son esenciales para evitar el uso y publicación de datos sensibles,

y así, garantizar que la privacidad de las personas no se vea comprometida con esta práctica. "*El objetivo final de la estrategia no es solo proteger datos, sino también garantizar mayor calidad en su producción y recolección y permitir una gestión eficaz y eficiente de ellos bajo estrictos principios de privacidad, seguridad y confidencialidad, para tomar mejores decisiones y formular mejores políticas que beneficien a la salud de la población, con una reducción de la probabilidad de un mal uso de esos datos y el daño que ese uso inadecuado puede causar*" [5].

Poder lograr metodologías de trabajo en las que se expongan datos teniendo niveles de seguridad adecuados como, por ejemplo, la anonimización de datos y la gestión segura de los accesos, podría ser crucial para mantener la confianza de los ciudadanos y así cumplir con las normativas de Protección de Datos. Es importante enfocar en normativas y políticas, ya que deben ser diseñadas como complemento para garantizar cuestiones metodológicas, confidencialidad y la ética de los usuarios de la solución [6]. Algunas técnicas complementarias, pueden ser la encriptación y controles de accesos adecuados. Básicamente, la confianza de los usuarios en los sistemas de software que trabajan con estos datos depende en gran medida, de las estrategias de protección de esta información para lograr un ambiente seguro.

Finalmente, otro punto necesario es un marco legal mucho más desarrollado, a través de resoluciones, leyes y normativas en los distintos países, con el fin de equilibrar la apertura de los datos, con la protección de la privacidad en una sociedad digital con el resguardo del gobierno.

1.2. Antecedentes del estudio

El interés por el enfoque de los datos abiertos ha crecido exponencialmente en los últimos años, esto fue impulsado debido a una propuesta en el contexto de transparencia para Gobierno Abierto. Este crecimiento también viene acompañado por la preocupación de conocer cómo

hay que proteger la privacidad de las personas. Existen varios estudios que han trabajado sobre la implementación de políticas de seguridad, privacidad en el manejo de datos abiertos, y hacen especial foco, en la necesidad de un equilibrio entre la apertura y la protección de información sensible.

Algunos de estos trabajos presentan una serie de directrices sobre cómo gestionar la privacidad de datos abiertos [7], otros trabajos fundamentan directrices de Protección de Datos, como por ejemplo el trabajo realizado por la Unión Europea [8], como así también, propuestas de guías de buenas prácticas sobre la privacidad y datos abiertos por parte de un estudio realizado por el Gobierno del Reino Unido [9]. Otro enfoque de mejores prácticas son las recomendaciones brindadas sobre privacidad y seguridad en la gestión de datos abiertos por parte del Gobierno de Australia [10].

1.3. Objetivo y aportes

El aporte principal de este trabajo es identificar y analizar buenas prácticas de seguridad para la protección de la privacidad de datos en el contexto de gobierno abierto, es decir en el enfoque de las fuentes de datos abiertas. Este estudio aporta una guía para el tratamiento de los desafíos que surgen en la gestión de la apertura de datos públicos como así también, tener en cuenta algunas técnicas para la protección de la privacidad. Estas buenas prácticas se esperan que sean adoptadas por los gobiernos organizaciones y partes involucradas como los ciudadanos de un país, ayudando de esta manera a implementar estrategias eficientes de seguridad que permitan brindar grandes beneficios en la utilización de datos abiertos sin comprometer la privacidad de las personas. Se espera potenciar las políticas y prácticas en el contexto de transparencia para proteger la información de las personas.

2. Metodología

2.1. Diseño del estudio

En lo que respecta al diseño de la investigación para este trabajo, se basa en un enfoque que combina un análisis comparativo entre distintos trabajos relevados en la sección anterior, como así también casos de estudio en diferentes entes gubernamentales que aplicaron distintas técnicas para poder realizar mitigaciones en aspectos de privacidad y confidencialidad de datos abiertos. Este análisis permitió identificar patrones comunes y prácticas es que son fundamentales a la hora de gestionar datos abiertos.

Finalmente se realizó un análisis cualitativo de políticas y regulaciones relacionadas con los datos abiertos en distintos entes gubernamentales de todo El Mundo, obteniendo así los aspectos más relevantes en el tratamiento de temas de privacidad y seguridad, con el fin de evaluar una correcta efectividad en la protección de la información sensible.

2.2. Recolección de datos

Para la recolección de datos se llevó a cabo un estudio de los diversos documentos que se encuentran en distintos sitios web gubernamentales que pertenecen a varios países del mundo. El análisis de estos documentos implicó el estudio de informes gubernamentales como así también, políticas de datos abiertos y regulaciones fundamentales que mantienen disponibles los gobiernos a nivel internacional. Otro de los puntos que se tuvo en cuenta para la recolección de datos fueron las entrevistas con expertos y profesionales en el campo de datos abiertos, la seguridad de la información y la privacidad. Estas opiniones con expertos se recolectaron de diversos foros webs de acceso público. El aporte fundamental en la recopilación de datos también tuvo relación en lo que respecta a la revisión de políticas de datos abiertos, leyes, y normativas que abarcan la seguridad y la privacidad, tomando como buena

práctica, aspectos para tener en cuenta en la implementación.

Las técnicas de recolección de datos utilizadas fueron:

- Revisión documental: Análisis de políticas de datos abiertos y regulaciones, como así también, relevamiento de documentos y normativas gubernamentales y políticos.
- Análisis de contenidos: Interpretación de los documentos estudiando, como así también, foros oficiales de distintas participaciones. Básicamente, opiniones de expertos en las que se analizaron debates en foros en línea.

3. Resultados

3.1. Estudio de Casos

En esta sección se presenta el análisis comparativo de los estudios de casos relevados sobre algunas de las estrategias y políticas que fueron implementando diferentes gobiernos e instituciones para poder trabajar sobre el foco de confidencialidad, seguridad, y privacidad de los datos.

A continuación, se muestra la Tabla 1, con un relevamiento de las técnicas más relevantes discriminados por países, política de datos abiertos que empleó dicho país, un enfoque en la protección de la privacidad, qué tipo de aspecto a nivel tecnología utilizaron, y cuál fue la evaluación de impacto en aspectos de privacidad.

Tabla 1. Análisis comparativo sobre estudios de casos gubernamentales.

País	Política de datos abiertos	Enfoque de protección de la privacidad	Tecnologías	Evaluación de impacto de privacidad
Reino Unido	políticas de implementación robustas con foco en transparencia	anonimización de datos evaluación; previa de riesgos	herramientas de anonimización	implementación en forma obligatoria

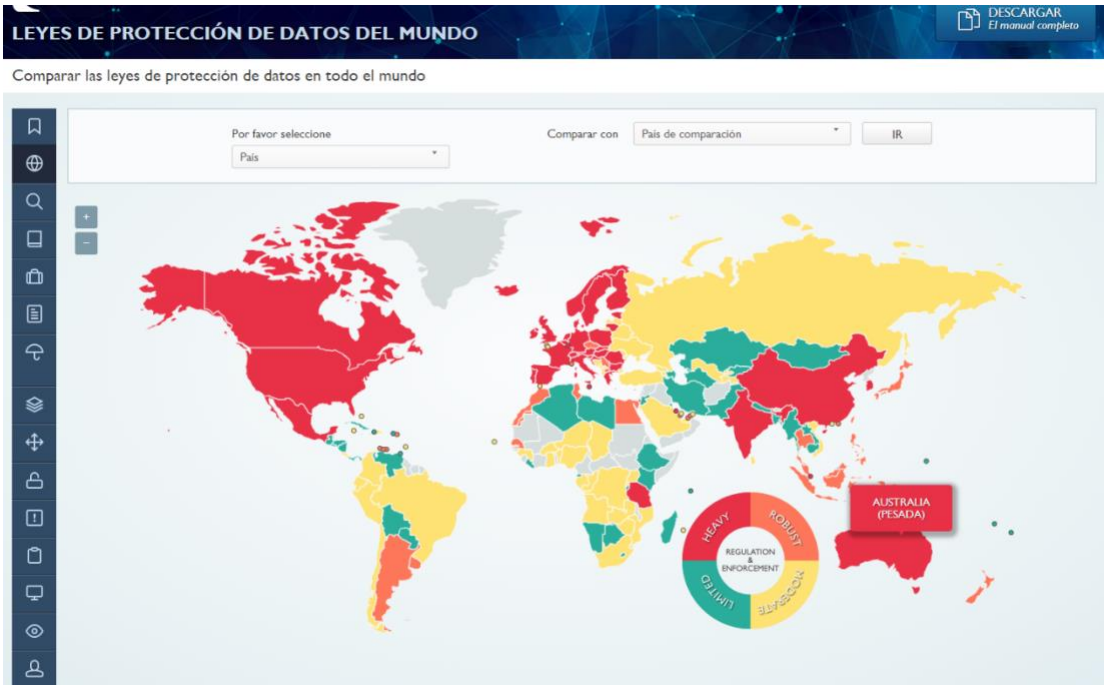
País	Política de datos abiertos	Enfoque de protección de la privacidad	Tecnologías	Evaluación de impacto de privacidad
Estados Unidos	enfoque descentralizado en datos abiertos	políticas de privacidad	encriptación y sistemas de control de acceso	implementación variable
Canadá	gobernanza con privacidad por diseño	evaluación continua de privacidad; adaptación de políticas gubernamentales	softwares de gestión de privacidad	revisión periódica
Australia	políticas de datos abiertos	enfoque en la minimización de datos	encriptación avanzada de datos	evaluación limitada
Alemania	Normativas, regulaciones y enfoque estructurado	leyes de privacidad y Protección de Datos	herramientas de encriptación y gestión de acceso	evaluaciones periódicas
México	estrategias enfocadas a la transparencia	anonimización de datos y cumplimiento con leyes de privacidad	sistema de anonimización y encriptación	testeos de nuevas propuestas
Ecuador	estrategias de datos abiertos	ley de protección de datos personales	Anonimización y encriptación básica	recomendada pero no obligatoria
Brasil	varias iniciativas de datos abiertos	Ley General de Protección de Datos	herramientas de anonimización y encriptación	bajo impacto en evaluación
Argentina	políticas de datos abiertos y acceso público	minimización de datos personales y anonimización	herramientas básicas de encriptación	recomendada pero no obligatoria
Japón	políticas nacionales	fuerte regulación de privacidad	sistemas de seguridad cibernética avanzadas	recomendada pero no obligatoria

País	Política de datos abiertos	Enfoque de protección de la privacidad	Tecnologías	Evaluación de impacto de privacidad
Francia	estrategia de apertura de datos con privacidad	regulaciones estrictas	técnicas de anonimización y control de acceso	recomendada pero no obligatoria
Suecia	transparencia y acceso a la información	fuerte enfoque en la privacidad	herramientas avanzadas de anonimización	altas recomendaciones
Colombia	iniciativas de datos abiertos	ley de Protección de Datos personales	sistemas de seguridad cibernética	altas recomendaciones

Fuente: Relevamientos de recolección de datos.

Además del cuadro comparativo con los distintos aspectos sobre política de datos, enfoque de la protección de la privacidad, y técnicas implementadas desde el concepto de herramientas de encriptación o bien gestión de accesos, como así también la evaluación de impacto de privacidad, se muestra a continuación, la Figura 1, que presenta un mapa mundial, qué muestra las regulaciones y comparativas. El sitio web de DLA Piper "*Global Data Protection Laws of the World*" [11], visualiza un análisis comparativo de las leyes de Protección de Datos a nivel mundial, reflejadas por cada uno de los países. Además, posee un filtro de búsqueda en el que los usuarios pueden seleccionar y comparar las regulaciones de diferentes países en aspectos como la autoridad de Protección de Datos, aspectos de transferencia de datos, notificaciones de infracciones e incumplimiento normativo.

Figura 1. Mapa con un análisis comparativo sobre Leyes de Protección de datos en el mundo.



Fuente: Global Data Protection Laws of the World [11] (2024).

Esta herramienta no solo se muestran las categorías en aspectos de Protección de Datos, sino que además brinda más información en comparativas entre países. Esto se ve en la Figura 2, allí se comparan dos países Ecuador y Argentina. En esta imagen se comparan aspectos que fueron seleccionados del panel de la parte izquierda de la imagen, es decir aspectos comparativos entre ambos países sobre Seguridad.

Figura 2. Análisis comparativo sobre Seguridad entre Ecuador y Argentina.

Fuente: Global Data Protection Laws of the World [11] (2024).

Esto mismo se puede observar en la Figura 3, con la diferencia que se analizan aspectos de leyes de cada país en contexto de Protección de Datos. También se pueden visualizar los números de leyes en cada uno de los países en aspectos de Protección de Datos personales, como así también, artículos específicos de la Constitución de cada país.

Figura 3. Análisis comparativo sobre Leyes entre Ecuador y Argentina.

Fuente: Global Data Protection Laws of the World [11] (2024).

Otra de las fuentes es la organización para la cooperación y desarrollo económico (OCDE) [12], que publica informes que combinan la apertura de datos con la protección de la confidencialidad y la seguridad de la información, brindando estadísticas sobre políticas de Protección de Datos en varios gobiernos.

Algunos estudios [13], mencionan principios que "*reflejan las distintas aproximaciones que prevalecen en los Estados miembros sobre los temas centrales de la protección de los datos personales, entre ellos el consentimiento, las finalidades y medios para la captación y tratamiento de estos datos, el flujo transfronterizo y la seguridad de los datos personales, la protección especial a los datos sensibles, y el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad*". Otros estudios [14] analizan buenas prácticas de gestión de datos, como, por ejemplo, gestión

de contraseñas, tratamiento de datos encriptados y medidas de seguridad para datos en la nube. Este estudio cita como "*La encriptación es el proceso que permite convertir datos a una forma o código no reconocible o legible. El uso de la encriptación permite proteger datos que son importantes o sensibles, previniendo que otros tengan acceso a ellos. Para que esto sea así, luego de ser encriptados, se debe utilizar una contraseña para tener acceso a los datos en su forma original*". Finalmente, otras investigaciones [15], hacen hincapié en la necesidad de una adecuada planificación en aspectos de seguridad informática en la implementación de un eficiente ambiente en aspectos de arquitectura de gestión de datos.

3.2. Interpretación de los Resultados

A raíz de los resultados obtenidos en base a los estudios de casos, sitios web gubernamentales, documentos, y demás aspectos que se tuvieron en cuenta en la sección anterior, se puede analizar que existe un enfoque equilibrado entre la transparencia y privacidad en el manejo de datos abiertos a nivel mundial. Por ejemplo, la utilización de herramientas como las evaluaciones de impacto de la privacidad (PIA), cada vez están más en auge, debido a que cada país puede indicar el índice de privacidad de datos en el conjunto de datos abiertos disponibles. Por otra parte, se recomendaron enfoques de principios sobre la privacidad en base al diseño con el fin de proteger la privacidad sin restringir el acceso a los datos.

Otro de los puntos sobresalientes es el conocimiento sobre el marco teórico, en el que fortalece nuevas oportunidades para mejorar tanto la seguridad como la transparencia en el manejo de datos abiertos, ya que estas van de la mano con la evolución de distintas tecnologías que pueden ser utilizadas en las políticas de datos abiertos para poder adaptarse e incorporar estos avances, por ejemplo: la utilización de blockchain o bien inteligencia artificial. Además, los casos de estudios también enfocan que la mayoría de

los gobiernos e instituciones reconocen la importancia de la privacidad como así también la implementación de políticas, por lo que hoy por hoy siguen trabajando en adquirir nuevos conocimientos y estrategias para adaptarse a los cambios tecnológicos, legales y contextuales. Esto confirma la gran necesidad de un marco de trabajo dinámico y adaptable en el que aún todavía queda un largo camino.

4. Hallazgos y recomendaciones específicas

En esta sección se presentan algunas recomendaciones propuestas que pueden mejorar la protección de la privacidad de los datos abiertos sin comprometer la transparencia, ni la exposición de datos sensibles que pueden comprometer a las personas de dichos datos.

- ***Aplicar técnicas de anonimización:*** esto consiste en asegurarse de que los datos personales sean irreversiblemente anonimizados, con el fin de que no puedan ser utilizados para identificar a personas específicas. Por ejemplo, se incluyen técnicas como la agregación y la eliminación de identificadores directos. En lo que respecta de un ejemplo puntual, existen procesos de anonimización, algunas de estas técnicas es la eliminación de identificadores directos, por ejemplo, se eliminan datos de pacientes en un hospital, como ser: nombres, número de obra social, números de teléfonos, entre otros. En aspectos de agregación, se podrían incorporar rangos de fechas en lugar de utilizar una fecha exacta. Por ejemplo, no se brinda la fecha de nacimiento, pero sí se brinda un rango específico, de 30 a 40 años.
- ***Eliminación de datos sensibles*** directamente en el set de datos que se presentan. Es decir, se excluyen o bien se agregan otros

datos para reducir el riesgo de identificación.

- ***Desidentificación***: este tipo de método permite eliminar o enmascarar identificadores personales, como, por ejemplo: direcciones, nombres o bien correos electrónicos que puedan utilizarse para la identificación indirecta de una persona.
- ***Políticas sobre el acceso y uso de datos***: existen diversos dos países que presentan políticas claras en sus sitios web gubernamentales, y además brindan guías de buenas prácticas para poder implementarlas. Otros países también presentan sistemas de autenticación y autorización para el control de acceso a estos datos que son un tanto más confidencial.
- ***Controles de seguridad:*** se puede utilizar la Protección de Datos a través de cifrados o bien técnicas de Protección de Datos de encriptación, en el que el dato permanece almacenado de manera en cubierta. Para esta técnica se implementan métodos de encriptación y descripción con algoritmos específicos de seguridad que son robustos.
- ***Capacitaciones en gestión de datos:*** uno de los puntos fundamentales en todo este nuevo paradigma es poder ofrecer por parte de los distintos gobiernos como así también empresas o instituciones, programas de formación y capacitación continua para comprender el alcance y buenas prácticas en la gestión de datos abiertos, y, además, comprender metodologías específicas en privacidad, seguridad y transparencia.
- ***Eventos:*** otro foco fundamental es la concientización a los ciudadanos sobre la importancia de la seguridad de los datos como así también la confidencialidad de estos. Diversas instituciones podrían ofrecer eventos en forma nacional o

internacional.

5. Conclusiones

Este trabajo presentó grandes desafíos de relevamiento, ya que actualmente existen muchos países de los distintos continentes que participan en aspectos de gobierno abierto en el contexto de transparencia mediante la utilización de datos abiertos. Se ha analizado la articulación de la apertura de datos abiertos y la protección de la privacidad de estos, teniendo en cuenta las estrategias más efectivas para aplicar los principios fundamentales de acceso a la información a las personas. Este derecho ganado y otorgado por los distintos gobiernos a los ciudadanos, implica utilizar los datos abiertos públicos a conciencia, por lo que este estudio realizó una propuesta de buenas prácticas sobre la implementación de medidas de anonimización, agregación de datos, como así también, técnicas de encriptación para que puedan ser utilizados de manera eficiente sin comprometer la privacidad de una persona.

Los resultados obtenidos muestran que los gobiernos como así también instituciones, van adoptando a lo largo del tiempo un enfoque más proactivo en la protección de la confidencialidad para mejorar la confianza pública, y, además, concientización de la importancia del acceso a este tipo de datos.

Más allá de cualquier propuesta de recomendación de buenas prácticas, es fundamental y crucial tener el apoyo de los gobiernos y organismos que desarrollan y adopten políticas públicas y claras para todos los ciudadanos. El desarrollo de procedimientos y normas para la gestión de datos abiertos permite garantizar que se utilizarán medidas de protección de la privacidad que estén alineadas con nuevas tecnologías, y también comprobadas y verificadas.

6. Referencias

[1] Martínez, M. R. (2022). *Métricas de calidad para validar los conjuntos de datos abiertos públicos gubernamentales* (Doctoral dissertation, Universidad Nacional de La Plata).

[2] James Madison Institute (2024). *The promise and perils of data privacy in Florida*. Disponible en: https://jamesmadison.org/the-promise-and-perils-of-data-privacy-in-florida/

[3] Balladares, C. P. M. (2023). Transparencia, Protección de Datos, Open Data y perspectiva del Portal de Datos Abiertos de Canarias. *Revista Canaria de Administración Pública*, (2), 184-242.

[4] Muente-Kunigami, A., & Serale, F. (2018). Los datos abiertos en América Latina y el Caribe.

[5] Marti, M., Mejía, F., Cosio, G. D., & Faba, G. (2018). Estrategia para la gobernanza de datos abiertos de salud: un cambio de paradigma en los sistemas de información. *Revista Panamericana de Salud Pública*, 41, e27.

[6] Ruvalcaba, E. A. (2016). Participación ciudadana en la era del Open Government. Una mirada desde las publicaciones científicas. PAAKAT: *Revista de Tecnología y Sociedad*, 6(11).

[7] Data.gov (2024). *The Home of the U.S. Government's Open Data*. Disponible en: https://data.gov/

[8] European Data Protection Supervisor (2024). *European Data Protection Supervisor*. Disponible en: https://www.edps.europa.eu/_en

[9] Information Commissioner's Office (ICO) (2024). *The ICO exists to empower you through information*. Disponible en: https://ico.org.uk/

[10] Office of the Australian Information Commissioner (OAIC) (2024). *We're the independent national regulator for privacy and freedom of information*. Disponible en: https://www.oaic.gov.au/

[11] DLA (2024). Global Data Protection Laws of the World. Disponible en: https://www.dlapiperdataprotection.com/

[12] OECD (2024). Data:Trusted statistics supporting evidence-based policy. Disponible en: https://www.oecd.org/en/data.html

[13] OEA (2021). Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Disponible en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

[14] CEPAL (2024). Gestión de datos de investigación. Disponible en: https://biblioguias.cepal.org/c.php?g=495473&p=4398100

[15] Jefatura de Gabinete de Ministros Argentina (2020). Disponible en: https://www.argentina.gob.ar/sites/default/files/recomendaciones_y_buenas_practicas_dnmsc_0.pdf