Los principios TRUST en los repositorios digitales

Este trabajo es una traducción del trabajo:

Dawei Lin [1] ✉, Jonathan Crabtree [2], Ingrid Dillo [3], Robert R. Downs [4], Rorie Edmunds[5],David Giaretta [6], Marisa De Giusti [7], Hervé L'Hours [8], Wim Hugo [9], Reyna Jenkyns [10], Varsha Khodiyar [11], Maryann E. Martone [12], Mustapha Mokrane [3], Vivek Navale [13],Jonathan Petters [14], Barbara Sierman [15], Dina V. Sokolova [16], Martina Stockhause [17] &John Westbrook [18]. The TRUST Principles for digital repositories. *Sci Data* **7,** 144 (2020). https://doi.org/10.1038/s41597-020-0486-7

La presente traducción ha sido realizada por Marisa De Giusti

Con la adopción cada vez más generalizada de las TICs en nuestra sociedad, dependemos cada vez más de los datos digitales y de los repositorios que brindan acceso a ese tipo de recursos y nos permiten utilizarlos.

Los repositorios deben ganarse la confianza de las comunidades a las que pretenden brindar servicios y demostrar que son confiables y capaces de administrar adecuadamente los datos que contienen.

Tras un debate público que se prolongó durante un año y en función del consenso actual de la comunidad[1], varias partes interesadas, que representan diversos segmentos de la comunidad de los repositorios digitales, han colaborado para desarrollar y avalar un conjunto de principios rectores, para demostrar que el repositorio digital es confiable. Estos principios abarcan la Transparencia, la Responsabilidad, el Foco en el Usuario, la Sostenibilidad y la Tecnología, y presentan un marco común para facilitar el debate y la implementación de las mejores prácticas en cuanto a preservación digital en beneficio de todas las partes interesadas.

[11]Division of Allergy, Immunology, and Transplantation, National Institute of Allergy and Infectious Diseases, National Institutes of Health, Maryland, USA. [2]HW Odum Institute for Research in Social Science, University of North Carolina at Chapel Hill, North Carolina, USA. [3]Data Archiving and Networked Services (DANS), The Hague, The Netherlands. [4]Center for International Earth Science Information Network (CIE SIN), The Earth Institute, Columbia University, New York, USA. [5]World Data System of the International Science Council (WDS), WDS International Programme Office, Tokyo, Japan. [6]PTAB Ltd, Dorset, UK. [7]Universidad Nacional de La Plata, Comisión de Investigaciones Científicas de la Provincia de Buenos Aires, La Plata, Argentina. [8]UK Data Archive, UK Data Service, University of Essex, Colchester, UK. [9]South African Environmental Observation Network, Cape Town, South Africa. [10]Ocean Networks Canada, University of Victoria, Victoria, Canada. [11]Springer Nature, London, UK. [12]University of California, San Diego,California, USA and SciCrunch Inc., San Diego, USA. [13]Center for Information Technology, National Institutes of Health, Maryland, USA. [14]Data Services, University Libraries, Virginia Tech, Virginia, USA. [15]KB National Library of the Netherlands, The Hague, The Netherlands. [16]University Libraries, Columbia University, New York, USA. [17]German Climate Computing Center (DKRZ), Hamburg, Germany. [18]RCSB, Protein Data Bank, Rutgers, The State University of New Jersey, Institute for Quantitative Biomedicine at Rutgers, New Jersey, USA. ✉e-mail: dawei.lin@nih.gov

Contexto e historia

Durante más de sesenta años, la administración y la preservación de los datos digitales han sido fundamentales para las instituciones académicas, tales como las bibliotecas, los archivos y repositorios de dominio[2] que colaboran con numerosas partes interesadas, entre ellas investigadores, financiadores, infraestructura y prestadores de servicios.

La gestión de los datos científicos llama cada vez más la atención dentro y fuera de la comunidad científica, particularmente en el discurso contemporáneo de la ciencia abierta.

Ha comenzado a lograrse un consenso sobre las "buenas" prácticas en la gestión de datos, pero todavía no se han implementado lo suficiente en algunos dominios científicos.

Los principios de datos FAIR[3] destacan la necesidad de adoptar las buenas prácticas y de las características esenciales de los objetos de datos para asegurarse de que los datos se puedan volver a utilizar, ya sea por parte de seres humanos o de máquinas, para ello deben ser: **F**indable (Encontrables), **A**ccesible (Accesibles), **I**nteroperable (Interoperables) y **R**eusable (Reutilizables).

Sin embargo, para asegurar que los datos sean "FAIR" sin comprometer su conservación a lo largo del tiempo, es necesario disponer de repositorios digitales confiables (trustworthy digital repositories, TDR) provistos de administración y organización sostenible, infraestructura confiable y políticas comprensibles que sustenten las prácticas acordadas por toda la comunidad.

Los TDR, con su claro propósito de preservar activamente los datos en respuesta a los cambios tanto en la tecnología como en los requisitos de las partes interesadas, desempeñan una función importante a la hora de asegurar el mantenimiento del valor de los datos.

Se mantienen en una posición de confianza por parte de sus usuarios, ya que aceptan la responsabilidad de la administración de los datos. Para cumplir esta función, los TDR deben demostrar una capacidad fundamental y duradera.

Es necesario asegurar que las comunidades a las que sirven puedan acceder y volver a utilizar los datos a lo largo del tiempo.

Cuadro 1 Los principios TRUST

Principio	**Pautas para los repositorios**
Transparencia	Ser transparente sobre los servicios de repositorio específicos y las tenencias de datos[2], las cuales se puedan verificar mediante evidencia de acceso público.
Responsabilidad	Ser responsable de garantizar la autenticidad e integridad de las tenencias

[2] El término utilizado en la versión en inglés es “data holdings” el cual se ha preferido a “data collection” para remarcar que es la totalidad de los datos más allá de cualquier agrupamiento elegido. En este trabajo se traducirá indistintamente como “tenencias ó existencias de datos”.

	de datos, así como la confiabilidad y permanencia del servicio.
Foco en el Usuario	Garantizar que se cumplan las normas y expectativas de las comunidades de usuarios en cuanto a la gestión de los datos
Sostenibilidad	Mantener los servicios y conservar las existencias de datos a largo plazo.
Tecnología	Brindar infraestructura y capacidades para prestar servicios seguros, duraderos y confiables.

Los TDR facilitan la selección y preservación de las tenencias de datos con diversos niveles de capacidad de reutilización.

En ciertos casos, incluso los datos de baja calidad, que no puedan mejorarse o hacerse más interoperables, aún puede conservar un alto valor para su comunidad de usuarios y, por lo tanto, requerir una administración confiable. Un TDR debe identificar y tratar de cumplir con los criterios aceptados por la comunidad y comunicar el nivel alcanzado de calidad de los datos. El modelo de referencia del Open Archival Information System (OAIS)[4] brinda recomendaciones sobre la configuración de archivos para asegurar la preservación a largo plazo y el acceso a la información (en particular, de la información digital) y la creación de paquetes de preservación. OAIS ofrece un marco coherente e integral de principios y terminología para facilitar la gestión de los sistemas de información de archivo.

Sin embargo, el hecho de cumplir con el modelo de referencia OAIS no garantiza la confiabilidad.

Con el fin de evaluar la confiabilidad, deben tratarse otros elementos adicionales del repositorio, incluyendo, la administración, los recursos y la seguridad adecuados.

Además, dado que OAIS es un modelo abstracto y no establece una guía de implementación detallada, hay diversas interpretaciones e implementaciones que requieren mecanismos de auditoría y certificación, tal como se reconoce en el informe de 1996, Preserving Digital Information[5].

Los autores del informe recomendaron que "los repositorios que afirman cumplir una función de archivo deben estar en condiciones de demostrar que son quienes dicen ser, cumpliendo o superando las disposiciones de las normas y criterios de un programa administrado independientemente para la certificación de archivo".

La confiabilidad se demuestra con evidencia, la cual depende de la transparencia, y por lo tanto, los repositorios deben presentar evidencia transparente, honesta y verificable, que avale su práctica.

De esta manera, las partes interesadas podrán confiar en que los repositorios aseguran la integridad, autenticidad, precisión, confiabilidad y accesibilidad de los datos durante períodos prolongados.

La confiabilidad no es un logro extraordinario y puntual; no se puede dar por sentada sin auditorías y certificación periódicas.

La certificación es una herramienta objetiva e importante para afianzar la confianza de las diversas partes interesadas de un repositorio.

Para evaluar y mejorar la calidad de sus prácticas profesionales, los repositorios se basan en una serie de normas internacionales de certificación que abarcan la certificación básica, ampliada o formal.
Estos estándares, entre ellos, CoreTrustSeal[6], DIN31644/NESTOR[7] e ISO16363[8], se centran en cuatro áreas principales de evaluación: organización, gestión de objetos digitales, infraestructura técnica y gestión de los riesgos de seguridad.
Los estándares varían en cuanto al número y la complejidad de sus requisitos, y la intensidad de las evaluaciones puede ir desde la revisión por pares de una autoevaluación, hasta una visita personal a las instalaciones por parte de un equipo de auditoría externa.
La elección del mecanismo de certificación depende de la necesidad, disposición y capacidad del repositorio para invertir en una mayor profesionalización y confiabilidad.
La adopción de los requisitos para los repositorios de datos confiables de CoreTrustSeal por parte de muchos repositorios de datos es un ejemplo de las medidas tomadas para mejorar el servicio y garantizar que sus capacidades logren las propiedades descritas por los Principios TRUST[6].
Muchos repositorios de datos han recibido la certificación CoreTrustSeal y se han convertido en miembros del International Science Council's World Data System (WDS).
El logro de la certificación y la realización de auditorías por parte de muchos repositorios digitales demuestran la voluntad de que los repositorios sean percibidos como confiables.
Los administradores de repositorios y sus equipos son la audiencia principal del modelo de referencia OAIS actual y los mecanismos de certificación de confiabilidad mencionados anteriormente.
Sin embargo, en un contexto de "ciencia abierta", esperamos que una audiencia más amplia, que abarque a los financiadores y a los usuarios del repositorio, pueda aprovechar los beneficios del marco creado por los Principios TRUST, habida cuenta de la creciente atención suscitada por la administración de los datos científicos (Cuadro 1).

Transparencia

Para seleccionar el repositorio más apropiado para un caso de uso particular, todos los potenciales usuarios pueden beneficiarse de poder encontrar y acceder fácilmente a la información sobre el alcance, la comunidad de usuarios a la que se dirige, las políticas y las capacidades del repositorio de datos.
La transparencia en estas áreas ofrece la oportunidad de conocer el repositorio y considerar su idoneidad para los requisitos específicos de los usuarios, incluyendo el depósito de los datos, la preservación de los datos y el descubrimiento de los datos.
Para cumplir con este principio, los repositorios deben garantizar que, como mínimo, la declaración de misión y el alcance del repositorio se hayan establecido con claridad.
Asimismo, se deben declarar con transparencia los siguientes aspectos:
• Términos de uso, tanto del repositorio como de las existencias de datos.
• Tiempo mínimo de conservación digital de las existencias de datos.
• Cualquier característica o servicio adicional pertinente, por ejemplo, la capacidad de administrar con responsabilidad los datos confidenciales.

Comunicar claramente las políticas del repositorio y en particular, los términos de uso de las tenencias de datos, sirve para informar a los usuarios sobre cualquier limitación que pueda restringir el uso de los datos o el repositorio.
Del mismo modo, ser capaz de evaluar si un repositorio puede manejar datos confidenciales con responsabilidad también puede ayudar al usuario a decidir si quiere o no utilizar los servicios de datos disponibles.

Responsabilidad
Los repositorios confiables asumen la responsabilidad de administrar correctamente sus datos y prestar servicios a su comunidad de usuarios.
La responsabilidad queda demostrada por el hecho de:
• Cumplir con las normas de metadatos y selección de la comunidad designada, además de administrar las tenencias de datos, por ejemplo, la validación técnica, documentación, control de calidad, protección de autenticidad y permanencia a largo plazo.
• Prestar servicios de datos, por ejemplo, interfaces de portal y máquina, descarga de datos o procesamiento a nivel del servidor.
• Gestionar los derechos de propiedad intelectual de los productores de datos, la protección de los recursos de información confidencial, y la seguridad del sistema y su contenido.
Los usuarios del repositorio deben tener la confianza de que a los depositantes de los datos se les solicita que proporcionen todos los metadatos que cumplan con las normas de la comunidad, ya que esto mejora en gran medida la capacidad de descubrimiento de los datos y su utilidad.
El saber que un repositorio verifica la integridad de los datos y metadatos disponibles asegura a los eventuales usuarios que las existencias de datos tienen más probabilidades de ser interoperables con otros conjuntos de datos relevantes.
Tanto los depositantes como los usuarios deben tener la confianza de que los datos seguirán siendo accesibles a lo largo del tiempo y, por lo tanto, pueden ser siempre citados y mencionados en las referencias de otras publicaciones académicas.
La responsabilidad puede aclararse a través de ciertos medios legales (derecho a preservar) o puede tomar la forma del cumplimiento voluntario con alguna norma (estándares/normas éticas).

Foco en el usuario
Un repositorio confiable debe estar abocado a servir a la comunidad de usuarios a la que se dirige.
Cada comunidad de usuarios probablemente tenga expectativas diferentes respecto de los repositorios de su comunidad, en parte según el grado de madurez de la comunidad, en cuanto a la gestión y el intercambio de datos.
El repositorio confiable se inserta en las prácticas de datos de la comunidad de usuarios a la que se dirige y así puede responder a los requisitos cambiantes de la comunidad.
Adoptamos una visión amplia en cuanto a la "comunidad de usuarios" ya que puede incluir a usuarios que depositan o acceden a los datos, a procesos informáticos que los consumen y a las partes interesadas indirectas, como por ejemplo, los financiadores, editores de revistas y otros socios institucionales o ciudadanos.

El uso y la reutilización de los datos de la investigación es una parte integral del proceso científico y, por lo tanto, los repositorios confiables deberían ayudar a los usuarios de su comunidad a encontrar, explorar y comprender sus datos con respecto al potencial de reutilización.
Los repositorios tienen un papel fundamental en la aplicación y el cumplimiento de las normas y estándares de la comunidad de usuarios a la que se dirigen, dado que este cumplimiento facilita la interoperabilidad y la reutilización de los datos.
Las normas de datos que los repositorios confiables deberían hacer cumplir abarcan los esquemas de metadatos, formatos de archivos de datos, vocabularios controlados, ontologías y demás semánticas en caso de existir en la comunidad de usuarios.
Un repositorio confiable puede demostrar la adhesión a este principio de las siguientes formas:
• Implementar métricas de datos relevantes y ponerlas a disposición de los usuarios.
• Proporcionar (o contribuir a) catálogos comunitarios para facilitar el descubrimiento de datos.
• Monitorear e identificar las expectativas cambiantes de la comunidad y responder según sea necesario para cumplir con esas necesidades cambiantes.

Sostenibilidad
Asegurar la sostenibilidad de un repositorio confiable es necesario para garantizar el acceso constante a un valioso conjunto de datos para comunidades de usuarios actuales y futuras.
El acceso continuo a los datos depende de la capacidad del repositorio para prestar servicios a lo largo del tiempo y responder con servicios nuevos o perfeccionados en función de los cambios en los requisitos de la comunidad
Un repositorio confiable puede demostrar la sostenibilidad de sus conjuntos de datos de la siguiente manera:
• Con una planificación suficiente para la mitigación de riesgos, la continuidad del negocio, la recuperación ante desastres y la sucesión.
• Asegurando la financiación para permitir el uso continuo y mantener las propiedades deseables de los recursos de datos que el repositorio se ha comprometido a preservar y difundir.
• Gestión sostenible de los datos para garantizar su preservación a largo plazo de forma que se mantengan localizables, accesibles y usables en el futuro.

Tecnología
Un repositorio depende de la interacción de las personas, los procesos y las tecnologías para garantizar la seguridad, permanencia y servicios confiables.
Sus actividades y funciones están respaldadas por herramientas de software, hardware y servicios técnicos.
Juntas, estas herramientas facilitan la ejecución de los Principios TRUST.
Un repositorio confiable puede demostrar la idoneidad de sus capacidades tecnológicas de las siguientes maneras:
• Implementar estándares, herramientas y tecnologías relevantes y apropiadas para la gestión y curación de los datos.

• Tener planes y mecanismos para prevenir, detectar y responder a las amenazas de seguridad física o virtual.

Repercusión de los Principios TRUST

Los Principios TRUST en su formulación abstracta y no técnica facilitan la comunicación y, por lo tanto, atañen a las partes interesadas tanto dentro como fuera de la comunidad de usuarios de los datos.
Cuando los repositorios de datos, los financiadores y los creadores de los datos adoptan los Principios FAIR e implementan los Principios TRUST, los usuarios del repositorio se benefician directamente, gracias a la permanencia y la mejora de las capacidades que permiten un uso más eficiente y eficaz de los datos.
Juntas, las partes interesadas en los Principios TRUST contribuyen a un cambio cultural en la investigación, en pos de un ecosistema de datos e información que ha venido evolucionando durante la era de la información, pero ha sido una parte esencial del proceso científico durante siglos.
Varios estudios han revelado que la transparencia se asocia con la confianza en los repositorios digitales[9].
Por ejemplo, para los usuarios de datos de video, “la transparencia de las prácticas de un repositorio, y en especial, las prácticas de selección de datos, son importantes para generar confianza"[10].
Al estudiar las percepciones del personal del repositorio de datos sobre la certificación del repositorio, Donaldson, et al. et al.[11], encontraron que el proceso de adquisición de la certificación contribuyó a la transparencia de su repositorio, entre otros beneficios.
El modelo de referencia OAIS describe las responsabilidades de los sistemas de información archivística que son responsables de administrar recursos de información.
Al describir los desafíos de la administración eficaz de los datos, Peng et al.[12] declararon lo siguiente: "Definir los roles y las responsabilidades en cada nivel de administración y cada etapa de la vida útil de los productos de datos ayudará a superar este desafío".
Además, al relevar las prácticas de datos de investigación en toda la vida útil de los datos, Kowalczyk[13] informó que “la probabilidad de mantener la gestión de datos a largo plazo de las colecciones de investigación es baja cuando la responsabilidad permanente recae en un investigador individual o estudiante graduado".
Al estudiar cómo las experiencias de los usuarios influyeron en sus percepciones de confianza en los repositorios de datos, Yoon[14] encontró que "el conocimiento de los usuarios sobre los roles o funciones de los repositorios puede ser un factor determinante a la hora de generar confianza en los usuarios".
Los usuarios a menudo confían en los repositorios en función de sus propias experiencias, prácticas y en la reputación del repositorio, así como en función de las experiencias de otros miembros de la comunidad[9,14,15].
La confianza de los usuarios en los datos también se asocia con su confianza en el archivo desde el que se obtuvo el contenido[16].
El informe de un estudio sobre la sostenibilidad de los repositorios digitales realizado por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) concluyó que "los repositorios de datos de investigación son una parte fundamental de la

infraestructura para la ciencia abierta" [y que] "es importante para garantizar la sostenibilidad de los repositorios de datos de investigación"[17].

La importancia de la sostenibilidad de la infraestructura de los datos de investigación ha quedado clara a partir de ciertos estudios que describen las necesidades de los arqueólogos[9,18]. En ausencia de estrategias de sostenibilidad y planes de continuidad eficaces, los repositorios de datos y con ello sus existencias, podrían desaparecer, como ha acontecido con muchas bases de datos biológicas[19].

Irónicamente, York et al.[20] observaron que "a pesar de la gran cantidad de repositorios de datos, iniciativas de administración y políticas en todo el sector de los datos de investigación, sabemos relativamente poco acerca de la cantidad total, las características o la sostenibilidad de los datos de investigación coordinados".

La adopción de capacidades tecnológicas se debe complementar en conjunto con las capacidades de organización y gestión que facilitan el uso continuo de las existencias de un repositorio de datos[10,21].

Al describir la necesidad de ganarse la confianza del público en los datos médicos, Van Staa et al.[22] subrayaron la importancia de "combinar nuevas tecnologías con responsabilidad clara, operaciones transparentes y confianza pública" y señalaron que "la administración de datos no tiene que ver únicamente con la seguridad física y digital, sino que la capacitación del personal, los procedimientos operativos estándar, y las habilidades y actitudes del personal también son importantes"[22].

Conclusiones

Los Principios TRUST constituyen una ayuda mnemotécnica para recordarles a las partes interesadas de un repositorio de datos la necesidad de desarrollar y mantener una infraestructura que garantice la administración permanente de los datos y facilite el uso de sus tenencias de datos en el futuro.

Sin embargo, los Principios TRUST no son un fin en sí mismos, sino un medio para agilizar la comunicación con todas las partes interesadas, a modo de orientación para que los repositorios puedan demostrar su transparencia, responsabilidad, foco en el usuario, sostenibilidad y tecnología.

Referencias

1. RDA/WDS Certification of Digital Repositories IG. The TRUST Principles for Trustworthy Data Repositories – An Update. *Research Data Alliance (RDA)*, https://www.rd-alliance.org/trust-principles-trustworthy-data-repositories-update (2019).

2. Mokrane, M. & Parsons, M. Learning from the International Polar Year to Build the Future of Polar Data Management. *Data Sci. J.***13**, IFPDA–15 (2014).

3. Wilkinson, M. D. *et al*. The FAIR Guiding Principles for scientific data management and stewardship. *Sci. Data* **3**, 160018 (2016).

4. Consultative Committee for Space Data Systems. Reference Model for an Open Archival Information System (OAIS). Recommended Practice CCSDS 650.0-M-2. *Consultative Committee for Space Data Systems*, https://public.ccsds.org/Pubs/650x0m2.pdf (2012).

5. Waters, D. & Garrett, J. *Preserving Digital Information, Report of the Task Force on Archiving of Digital Information*. 1400 16th St.,NW, Suite 740, Washington, DC 20036-2217. 59 pp, https://www.clir.org/pubs/reports/pub63/ (1996).

6.CoreTrustSeal. CoreTrustSeal Certified Repositories. *CoreTrustSeal*, https://www.coretrustseal.org/why-certification/certifiedrepositories/ (2020).

7. Harmsen, H. *et al*. Explanatory notes on the Nestor seal for trustworthy digital archives. *Nestor Certification Working Group*, http://nbn-resolving.de/urn:nbn:de:0008-2013100901 (2013).
8. Audit and Certification of Trustworthy Digital Repositories. ISO 16363/CCSDS 652.0-M-1, https://public.ccsds.org/Pubs/652x0m1.pdf (2011).
9. Yakel, E., Faniel, I. M., Kriesberg, A. & Yoon, A. Trust in Digital Repositories. *Int. J. Digit. Curation* **8**, 143–156 (2013).
10. Frank, R. D., Chen, Z., Crawford, E., Suzuka, K. & Yakel, E. Trust in qualitative data repositories. In *Proceedings of the Association for Information Science and Technology* **54** 102–111 Association for Information Science and Technology (2017).
11. Donaldson, D. R., Dillo, I., Downs, R. & Ramdeen, S. The Perceived Value of Acquiring Data Seals of Approval. *Int. J. Digit. Curation* **12**, 130–151 (2017).
12. Peng, G. *et al*. A Conceptual Enterprise Framework for Managing Scientific Data Stewardship. *Data Sci. J.* **17**, 15 (2018).
13. Kowalczyk, S. T. Modelling the Research Data Lifecycle. *Int. J. Digit. Curation* **12**, 331–361 (2017).
14. Yoon, A. End users' trust in data repositories: definition and influences on trust development. *Arch. Sci.* **14**, 17–34 (2014).
15. Downs, R. & Chen, R. Organizational needs for managing and preserving geospatial data and related electronic records. *Data Sci. J.***4**, 255–271 (2006).
16. Donaldson, D. R. Trust in Archives–Trust in Digital Archival Content Framework. *Archivaria* **88**, 50–83 (2019).
17. OECD. *Business models for sustainable research data repositories*. **58**, https://doi.org/10.1787/302b12bb-en (2017).
18. Williams, J. P. & Williams, R. D. Information science and North American archaeology: examining the potential for collaboration.*Inf. Res*. **24**, paper 820. Retrieved from, http://InformationR.net/ir/24-2/paper820.html (Archived by WebCite® at, http://www.Webcitation.Org/78mnvhrti) (2019).
19. Attwood, T. K., Agit, B. & Ellis, L. B. M. Longevity of Biological Databases. *EMBnet. journal* **21**, 803 (2015).
20. York, J., Gutmann, M. & Berman, F. What Do We Know about the Stewardship Gap. *Data Sci. J.* **17**, 19 (2018).
21. Corrado, E. M. Repositories, Trust, and the CoreTrustSeal. *Tech. Serv. Q.* **36**, 61–72 (2019).
22. Staa, T.-P., van, Goldacre, B., Buchan, I. & Smeeth, L. Big health data: the need to earn public trust. *BMJ* **354**, i3636 (2016).

Agradecimientos

Los autores quisieran manifestar su aprecio por las sugerencias para mejorar este trabajo ofrecidas por los miembros de CoreTrustSeal Standards and Certification Board, cuyo aporte no se efectuó en calidad de autores, por los participantes de la 13.ª Sesión Plenaria de Research Data Alliance, "Build TRUST to be FAIR - Emerging Needs of Certification in Life Sciences, Geosciences and Humanities", convocada por el RDA/WDS Certification of Digital Repositories Interest Group, y por participantes del Taller de NIH, "Trustworthy Data Repositories for Biomedical Sciences" (Taller de NIH, 2019) patrocinado por NIH Office of Data Science Strategy, que fue la primera oportunidad en el que se utilizó el marco TRUST para tratar el tema de los repositorios de datos confiables.

Agradecemos las interesantes conversaciones que mantuvimos con Shelley Stall, Robert S. Chen, Mark Conrad, Peter Doorn, Eliane Fankhauser, Elizabeth Hull, Siri Jodha Singh Khalsa, Micky Lindlar, Limor Peer, Philipp Conzett y Rachel Drysdale.
Nos gustaría agradecer a Anupama Gururaj por haber revisado este artículo.

Conflicto de intereses

V.K.K. trabaja para Springer Nature, editores de Scientific Data.
Hasta febrero de 2020, VKK mantuvo una posición editorial en Scientific Data.
Los autores declaran que V.K.K. no participó en el proceso editorial y el arbitraje de este manuscrito.
Varios de los autores participan en las normas e iniciativas de certificación tratadas en el manuscrito, en particular, D.L., J.C., I.D., R.R.D., R.E., H.L.H., W.H., R.J. y M.M., quienes integran la CoreTrustSeal Standards and Certification Board y DG, quien es miembro de Primary Trustworthy Digital Repository Authorization Body (PTAB).
El resto de autores declaran no tener ningún conflicto de intereses.

Información complementaria

La correspondencia y la solicitud de materiales se deben dirigir a D.L.