



Gobierno Digital



¿Qué puedo publicar?

Privacidad, seguridad y confidencialidad

UN PROYECTO DE:



Red Ciudadana

www.redciudadana.org





Introducción a la Publicación de Datos Abiertos

Objetivo del Manual

Este manual tiene como propósito ayudar a los funcionarios públicos a identificar qué datos pueden ser publicados de manera abierta, respetando normas de privacidad, seguridad y confidencialidad. A través de esta guía, los usuarios podrán comprender los principios y buenas prácticas necesarias para determinar los datos aptos para la publicación y evitar riesgos legales o éticos.

Importancia de Publicar Datos Abiertos

La apertura de datos es fundamental para mejorar la transparencia, rendición de cuentas y participación ciudadana. Al compartir información de interés público, las instituciones fomentan la confianza y facilitan la creación de soluciones innovadoras para desafíos sociales. Sin embargo, es esencial que los datos publicados sean seleccionados cuidadosamente, asegurando el cumplimiento de regulaciones de privacidad y protección de datos personales.

Principios Fundamentales para la Publicación de Datos



Transparencia y Acceso Equitativo

La transparencia es uno de los principios más importantes en la publicación de datos abiertos. Los datos deben ser accesibles para todos los ciudadanos, sin barreras de acceso ni restricciones de uso, a menos que existan razones legítimas para restringir su difusión.



Seguridad y Privacidad

La protección de la privacidad y la seguridad de la información es esencial. Los datos que contengan información sensible o personal deben ser anonimizados o excluidos de la publicación. La apertura de datos no debe poner en riesgo la seguridad de los ciudadanos o de la nación.



Relevancia y Valor Público

Los datos publicados deben tener un propósito claro y aportar valor a la ciudadanía. Esto incluye datos que apoyen la investigación, faciliten la toma de decisiones informadas y fomenten la creación de servicios y productos innovadores.



Interoperabilidad y Estándares

Los datos deben publicarse en formatos estándar y abiertos para asegurar su reutilización y compatibilidad con otros conjuntos de datos, promoviendo un ecosistema de datos accesible y aprovechable a nivel nacional e internacional.

Clasificación de los Tipos de Datos



1. Datos Públicos

Son aquellos datos que se encuentran en el dominio público y no presentan riesgos para la privacidad ni la seguridad. Estos datos incluyen información estadística, reportes de desempeño, indicadores económicos y sociales, y datos sobre servicios públicos.

Ejemplos de datos públicos:

- ▶ Estadísticas sobre educación y salud.
- ▶ Información sobre obras y proyectos de infraestructura.
- ▶ Datos demográficos agregados, como censos y encuestas.
- ▶ Indicadores económicos, como tasas de empleo, PIB, y comercio.



2. Datos Sensibles

Los datos sensibles contienen información que podría poner en riesgo la privacidad o seguridad de las personas si se divulgan sin precauciones. Antes de publicar estos datos, es esencial realizar un proceso de anonimización y aplicar medidas de seguridad adecuadas.

Ejemplos de datos sensibles:

- ▶ Registros de salud con detalles personales.
- ▶ Datos sobre minorías étnicas y religiosas.
- ▶ Información sobre servicios de emergencia y fuerzas de seguridad



3. Datos Personales y Privados

Incluyen toda información relacionada con una persona identificable, como su nombre, dirección, número de identificación y otros detalles específicos. Estos datos no deben ser publicados abiertamente sin el consentimiento explícito del individuo o una evaluación cuidadosa de los riesgos y beneficios.

Ejemplos de datos personales:

- ▶ Números de seguridad social.
- ▶ Historial médico personal.
- ▶ Datos de contacto privado.

Guía para la Selección de Datos Publicables



Identificación de Datos de Alto Valor Público

Para priorizar la publicación, es útil identificar los datos de mayor valor público, es decir, aquellos que ofrecen un beneficio social significativo. Algunos criterios para evaluar el valor público incluyen:

- ▶ **Demanda de la ciudadanía:** Datos que sean frecuentemente solicitados por ciudadanos, académicos o empresas.
- ▶ **Impacto en políticas públicas:** Datos que puedan mejorar el diseño o implementación de políticas.
- ▶ **Relevancia para la transparencia y la rendición de cuentas:** Información que permita a los ciudadanos evaluar el desempeño y uso de recursos de la institución.



Análisis de Riesgo

Antes de publicar cualquier conjunto de datos, es esencial realizar un análisis de riesgo que considere la sensibilidad de la información y el posible impacto de su divulgación. Algunas preguntas clave para el análisis incluyen:

- ▶ ¿Este conjunto de datos contiene información personal?
- ▶ ¿Podría la publicación de estos datos afectar la seguridad de la nación o de algún grupo específico?
- ▶ ¿Existen regulaciones o leyes que limiten la publicación de este tipo de datos?



Categorización de los Datos Según el Nivel de Sensibilidad

Una buena práctica es clasificar los datos en categorías según su nivel de sensibilidad:

- ▶ **Datos de acceso libre:** Datos que pueden ser publicados sin restricciones.
- ▶ **Datos de acceso restringido:** Datos que requieren anonimización o protección adicional antes de ser publicados.
- ▶ **Datos confidenciales:** Información que no debe ser publicada debido a su alto nivel de sensibilidad o riesgo.

Herramientas para la Anonimización de Datos



Técnicas de Anonimización

La anonimización permite eliminar la información personal de un conjunto de datos para reducir el riesgo de identificar a individuos específicos. Las técnicas de anonimización incluyen:

- **Generalización:** Agrupar datos específicos en categorías amplias (por ejemplo, cambiar la edad exacta a un rango de edad).
- **Enmascaramiento:** Ocultar datos específicos que podrían permitir la identificación directa.
- **Perturbación:** Alterar ligeramente los datos para dificultar la identificación de personas o entidades.



Pruebas de Reidentificación

Para verificar la efectividad de la anonimización, es recomendable realizar pruebas de reidentificación. Estas pruebas simulan intentos de identificar individuos en los datos anonimizados, permitiendo ajustar las medidas de seguridad según los resultados.



Herramientas de Software para Anonimización

Existen herramientas y software especializados que facilitan el proceso de anonimización, como:

- **ARX:** Un software que permite realizar múltiples técnicas de anonimización y medir el riesgo de reidentificación.
- **sdcMicro:** Paquete de R diseñado para la anonimización de datos sensibles en encuestas.

Ejemplos de Datos para Publicación Segura



Datos Geográficos y de Infraestructura

Los datos sobre infraestructura y geografía suelen ser de alto valor para la ciudadanía, ya que proporcionan información sobre la disponibilidad y calidad de los servicios en diferentes regiones.

Ejemplos de datos públicos:

- ▶ Mapas de áreas urbanas y rurales.
- ▶ Datos sobre redes de transporte público.
- ▶ Ubicación y capacidad de infraestructuras educativas y de salud.



Datos Económicos y Sociales Agregados

Los datos sobre economía, empleo, salud y educación proporcionan información valiosa sin poner en riesgo la privacidad cuando están en formato agregado.

Ejemplos seguros de datos

- ▶ Tasa de desempleo, PIB, y estadísticas de crecimiento.
- ▶ Datos sobre el sistema educativo, como tasas de graduación.
- ▶ Información sobre acceso a servicios de salud, sin datos individuales.



Datos de Proyectos y Presupuesto

Publicar datos sobre el presupuesto y el uso de recursos en proyectos específicos fomenta la transparencia y la rendición de cuentas.

Ejemplos seguros de datos

- ▶ Presupuesto de proyectos de infraestructura.
- ▶ Ejecución de programas de ayuda social.
- ▶ Evaluaciones de impacto de programas de gobierno.

Regulaciones y Normativas sobre la Publicación de Datos



Leyes de Protección de Datos Personales

Es fundamental cumplir con las leyes nacionales e internacionales de protección de datos personales, que establecen límites y condiciones para la divulgación de información personal. Ejemplos de leyes incluyen:

- ▶ **Ley General de Protección de Datos Personales:** Que regula el tratamiento de información personal en varios países de Latinoamérica.
- ▶ **Reglamento General de Protección de Datos (GDPR)** de la Unión Europea, aplicable a instituciones que manejan datos de ciudadanos europeos.



Normativas Internacionales de Datos Abiertos

Existen estándares y principios internacionales que orientan la publicación segura de datos abiertos, como la **Carta Internacional de Datos Abiertos**. Estos lineamientos fomentan la transparencia y el acceso a la información, al tiempo que protegen la privacidad de los ciudadanos.



Políticas Internas de la Institución

Las instituciones deben desarrollar políticas internas para guiar a sus funcionarios en la publicación de datos, abordando aspectos como:

- ▶ Procesos de revisión y aprobación de datos para publicación.
- ▶ Protocolos de seguridad y anonimización.
- ▶ Responsabilidades y roles para el cumplimiento de las normativas.

Pasos para Publicar Datos de Forma Segura



1. Evaluación de la Información para Publicación

El primer paso es revisar el contenido del conjunto de datos y clasificarlo según su nivel de sensibilidad. Esta evaluación debe incluir la consulta de regulaciones legales y políticas internas.



2. Anonimización de Datos Sensibles

Si los datos contienen información personal o sensible, se deben aplicar técnicas de anonimización para proteger la identidad y privacidad de los individuos.



3. Creación de Metadatos y Documentación

Los datos deben estar acompañados de metadatos que proporcionen contexto sobre el origen, la periodicidad, y las condiciones de uso. La documentación adicional facilita la interpretación y el uso correcto de los datos.



4. Publicación y Monitoreo

Una vez que los datos están anonimizados y documentados, se publican en una plataforma de acceso público. Es importante monitorear el uso de los datos para detectar posibles riesgos o problemas de seguridad.

Buenas Prácticas para la Publicación Responsable de Datos

1. Revisión periódica

Es recomendable revisar y actualizar los conjuntos de datos regularmente para asegurar su precisión y relevancia.

2. Consulta con expertos

Involucrar a expertos en privacidad y seguridad de datos para asesorar en la publicación y manejo de datos sensibles.

3. Promoción de la cultura de datos abiertos

Capacitar al personal sobre la importancia de los datos abiertos y las mejores prácticas para su publicación, promoviendo una cultura de transparencia.

4. Comunicación clara con los usuarios

Proporcionar orientación clara a los usuarios sobre el uso y limitaciones de los datos, asegurando una comprensión adecuada de su alcance y propósito.



Conclusión

El proceso de publicar datos abiertos de manera segura es una responsabilidad que implica tanto compromiso con la transparencia como respeto por la privacidad y la seguridad de la información. Este manual establece lineamientos claros para que los funcionarios puedan decidir qué datos pueden publicarse sin riesgo, garantizando que la apertura de datos genere valor social y fortalezca la confianza en las instituciones públicas. La implementación de estas recomendaciones permitirá que las instituciones avancen en la construcción de una cultura de datos abiertos responsable, que beneficie tanto a la administración pública como a la ciudadanía.



Gobierno Digital

www.redciudadana.org

