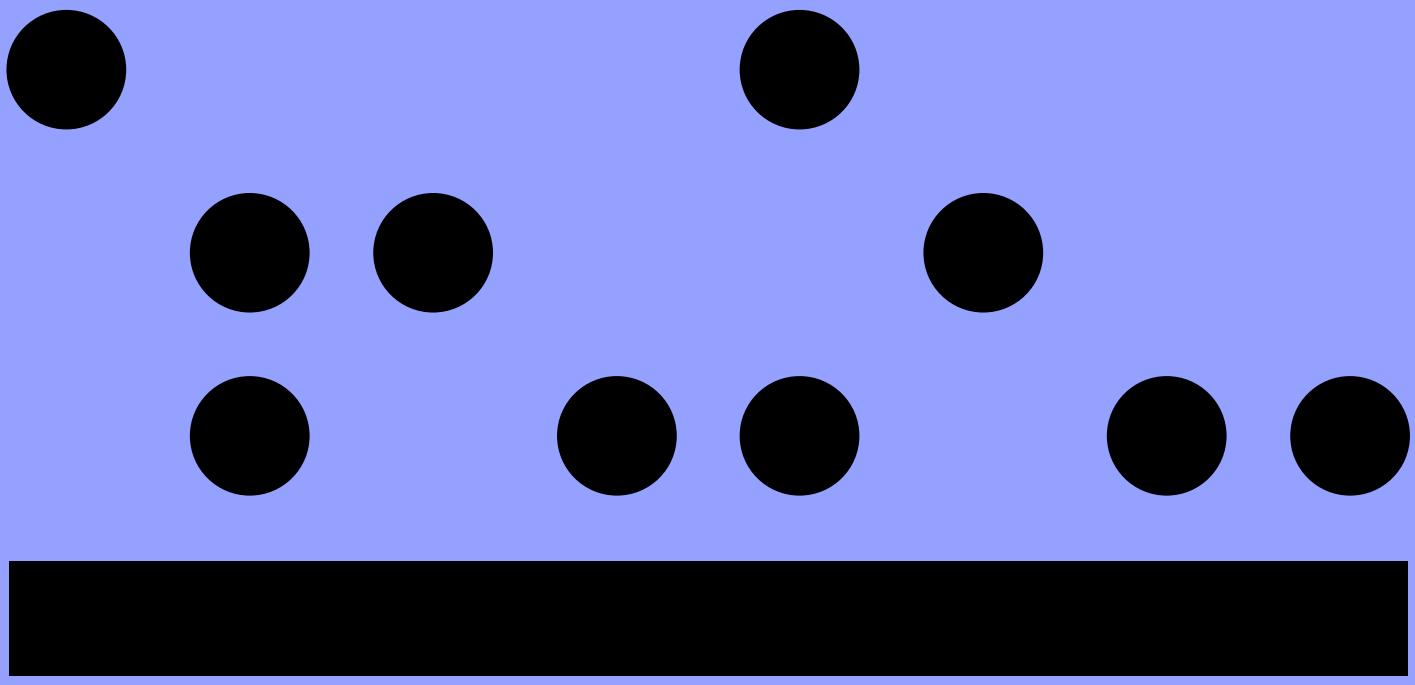
Guía práctica para la clasificación de datos



Datos

Mariana Kunst
Paula Luvini
Juan Manuel Dias

Febrero 2024

fundar

Guía práctica para la clasificación de datos

Mariana Kunst
Paula Luvini
Juan Manuel Dias

- Generar riqueza
- Promover el bienestar
- Transformar el Estado

Sobre Fundar

Fundar es un centro de estudios y diseño de políticas públicas que promueve una agenda de desarrollo sustentable e inclusivo para la Argentina. Para enriquecer el debate público es necesario tener un debate interno: por ello lo promovemos en el proceso de elaboración de cualquiera de nuestros documentos. Confiamos en que cada trabajo que publicamos expresa algo de lo que deseamos proyectar y construir para nuestro país. Fundar no es un logo: es una firma.

Nos dedicamos al estudio e investigación de políticas públicas sobre la base de evidencia. Como parte de nuestra política de promover la transparencia y promoción de la discusión pública, disponibilizamos los datos utilizados para nuestros análisis, para que cualquier persona que lo desee pueda replicar los análisis realizados y generar nuevas investigaciones.

Creemos que el lenguaje es un territorio de disputa política y cultural. Por ello, sugerimos que se tengan en cuenta algunos recursos para evitar sesgos excluyentes en el discurso. No imponemos ningún uso en particular ni establecemos ninguna actitud normativa. Entendemos que el lenguaje inclusivo es una forma de ampliar el repertorio lingüístico, es decir, una herramienta para que cada persona encuentre la forma más adecuada de expresar sus ideas.

Trabajamos en tres misiones estratégicas para alcanzar el desarrollo inclusivo y sustentable de la Argentina:

Generar riqueza. La Argentina tiene el potencial de crecer y de elegir cómo hacerlo. Sin crecimiento, no hay horizonte de desarrollo, ni protección social sustentable, ni transformación del Estado. Por eso, nuestra misión es hacer aportes que definan cuál es la mejor manera de crecer para que la Argentina del siglo XXI pueda responder a esos desafíos.

Promover el bienestar. El Estado de Bienestar argentino ha sido un modelo de protección e inclusión social. Nuestra misión es preservar y actualizar ese legado, a través del diseño de políticas públicas inclusivas que sean sustentables. Proteger e incluir a futuro es la mejor manera de reivindicar el espíritu de movilidad social que define a nuestra sociedad.

Transformar el Estado. La mejora de las capacidades estatales es imprescindible para las transformaciones que la Argentina necesita en el camino al desarrollo. Nuestra misión es afrontar la tarea en algunos aspectos fundamentales: el gobierno de datos, el diseño de una nueva gobernanza estatal y la articulación de un derecho administrativo para el siglo XXI.

Cita sugerida

Kunst, M.; Luvini, P. y Dias, J. M. (2025). Guía práctica para la clasificación de datos. Fundar.

Licencias

Agradecimientos

El equipo autoral quiere agradecer a Natalia Aquilino y la Red de Daterxs.

Índice

Guía práctica para la clasificación de datos

fundar

Introducción

¿Por qué es importante promover la gestión de datos en el Estado?

En una persona, la inteligencia se manifiesta en el saber, en la memoria y en el razonamiento. En un Estado también. Un **Estado inteligente** (2023) es aquel que conoce qué datos tiene, los cuida y los utiliza para brindar políticas públicas de calidad. Argentina avanzó significativamente en este sentido: cuenta con estándares y capacidades instaladas en temas clave como la digitalización y automatización de trámites y procesos internos. También consolidó una agenda en materia de políticas de gobierno abierto.

Sin embargo, queda mucho por hacer en términos de gestión de datos. En términos de la oferta de datos, el Estado tiene una gran deuda consigo mismo al no tener ordenados y catalogados la totalidad de los datos que genera ,y además no compartirlos internamente con asiduidad. Muchos organismos públicos capturan y administran datos propios con tecnologías e infraestructuras diversas. Esto genera un panorama heterogéneo que dificulta la comparación, el intercambio y la integración de datos para generar información útil. Como consecuencia, la información no se explota en todo su potencial y una gobernanza de datos difusa impide capitalizar experiencias positivas. En la actualidad, incluso, hay datos que no se comparten cuando bajo determinadas condiciones y a través de un proceso adecuado deberían compartirse.

La clasificación de datos contribuye a mejorar la gestión de la información y con eso incrementar el intercambio de datos entre oficinas del gobierno. Al hacer más eficiente la gestión de la información, mitiga riesgos y contribuye a garantizar el cumplimiento de leyes y regulaciones. Además, proporciona una base para el desarrollo de estrategias de seguridad de la información y promueve una cultura de conciencia y responsabilidad en el manejo de datos.

En términos de la demanda de datos, ordenar su ciclo de vida es crucial para responder a las cada vez mayores demandas de la ciudadanía en torno a datos, particularmente en las etapas iniciales de generación, captura y clasificación de datos. En los últimos años, la concientización respecto a su valor para la toma de decisiones informadas ha avanzado considerablemente. La sociedad civil demanda cada vez más acceso y apertura de mayor cantidad de datos. Sin una política de gestión de datos que incluya a la clasificación como un pilar fundamental, la apertura de datos se torna menos escalable. También tomó relevancia la discusión en torno al resguardo de datos personales. La sociedad civil está cada vez más interesada en saber qué uso se le da a sus datos. Hay más episodios de vulneración, como por ejemplo las filtraciones de datos. Contar con prácticas y políticas para determinar los tipos de datos, qué normativas los regulan y bajo qué condiciones pueden ser utilizados es esencial para mejorar la confianza de la ciudadanía en sus gobiernos.

> La clasificación de datos es una práctica administrativa necesaria para la gestión de la información y también es un paso fundamental para la protección de los derechos de las personas, en particular, el derecho a la información.

Proceso de clasificación ↓

En un mundo donde la información se convirtió en un recurso fundamental, la manera en que clasificamos y protegemos los datos tiene implicaciones directas sobre la transparencia de las políticas públicas y la privacidad de las personas. Gestionar correctamente los datos y contar con catálogos y clasificaciones ordenadas no sólo facilita su apertura y protección, sino que también promueve la participación informada de la sociedad y la toma de decisiones fundamentadas en el Estado.

Acerca de esta guía

Objetivo: El presente documento tiene como objetivo contribuir a la generación de una guía para la clasificación de datos en el sector público. Busca ayudar a determinar qué datos pueden ser compartidos e intercambiados una vez que son clasificados. Pretende ser una herramienta útil para mejorar los procesos de clasificación de datos y promover mejores prácticas en materia de seguridad y apertura de la información en entornos gubernamentales nacionales, provinciales o municipales.

Qué vas a encontrar en esta guía: un paso a paso detallado de cómo clasificar los datos. El proceso abarca desde la creación de políticas de clasificación hasta la identificación, etiquetado, protección y monitoreo de los datos. Repasamos normativas que regulan el uso y la protección de datos. Analizamos cómo distintos países abordaron la clasificación de datos. Nos enfocamos en la realidad argentina, mostrando cómo se lleva a cabo la clasificación de datos en nuestro contexto. Para poner en práctica toda esta información, ofrecemos ejemplos concretos como el Registro Nacional de las Personas (RENAPER) y el programa de la Prestación Alimentar, ilustrando cómo se aplica la clasificación de datos en situaciones reales

Destinatarios: La guía está dirigida principalmente a las áreas técnicas de organismos públicos que tienen responsabilidad sobre los datos y aquellas personas que ocupan puestos decisores en la gestión de datos.

Proceso de clasificación

¿Qué es la clasificación de datos y por qué es importante?

La clasificación de datos es una práctica administrativa necesaria para la gestión de la información. Establece procedimientos específicos sobre cómo deben tratarse los datos, quién puede procesarlos, a dónde transferirse o dónde deben almacenarse.

Si bien existen distintos modelos de clasificación, todos tienen en común la generación de etiquetas en función de distintas características de los datos. Algunos de los aspectos que se suelen tener en cuenta al momento de clasificar son el contenido de la información (para poder definir el contexto de aplicación y área del marco normativo), el tipo de dato (estructurado, semiestructurado, no estructurado) y el riesgo asociado a los datos (para poder aplicar el nivel de protección adecuado). Estos aspectos pueden variar según las necesidades de cada organización pero el proceso de clasificación siempre debe ser transparente, de fácil acceso y coherente tanto para los miembros de la organización como para los externos.

Al establecer niveles de criticidad para diferentes tipos de datos, se pueden implementar medidas adecuadas de seguridad, privacidad, intercambio y apertura. Esto asegura que la información esté debidamente resguardada y garantiza que la información pública se maneje de manera ética y responsable.

Proceso de clasificación

¿Por qué clasificar?

Box 1

Beneficios de la clasificación de datos

- Permite estructurar los datos de manera coherente, facilitando su búsqueda y recuperación cuando sea necesario.
- Permite aplicar niveles de acceso y medidas de seguridad para proteger la información contra accesos no autorizados.
- Al identificar y proteger la información, ayuda a cumplir con las regulaciones de protección de datos.
- Mejora la eficiencia en la gestión de datos. Permite dar respuestas más rápidas y efectivas que pueden traducirse en ahorro de tiempo y recursos tanto para el funcionamiento interno del Estado como para la ciudadanía.
- Proporciona una base sólida para el intercambio de datos entre organizaciones y para la apertura de datos a la ciudadanía.

Riesgos asociados a una clasificación de datos inadecuada

- Puede resultar en la pérdida de datos.
- Una clasificación excesivamente rigurosa puede burocratizar el acceso a los datos, ralentizando procesos administrativos y toma de decisiones.
- Puede hacer que no se protejan correctamente los datos. Aumenta el riesgo de violación de la privacidad de las personas y puede generar pérdida de confianza en los datos públicos.
- Puede facilitar el acceso no autorizado a los datos aumentando el riesgo de ciberataques.

¿Cómo clasificar? Paso a paso para la clasificación de datos

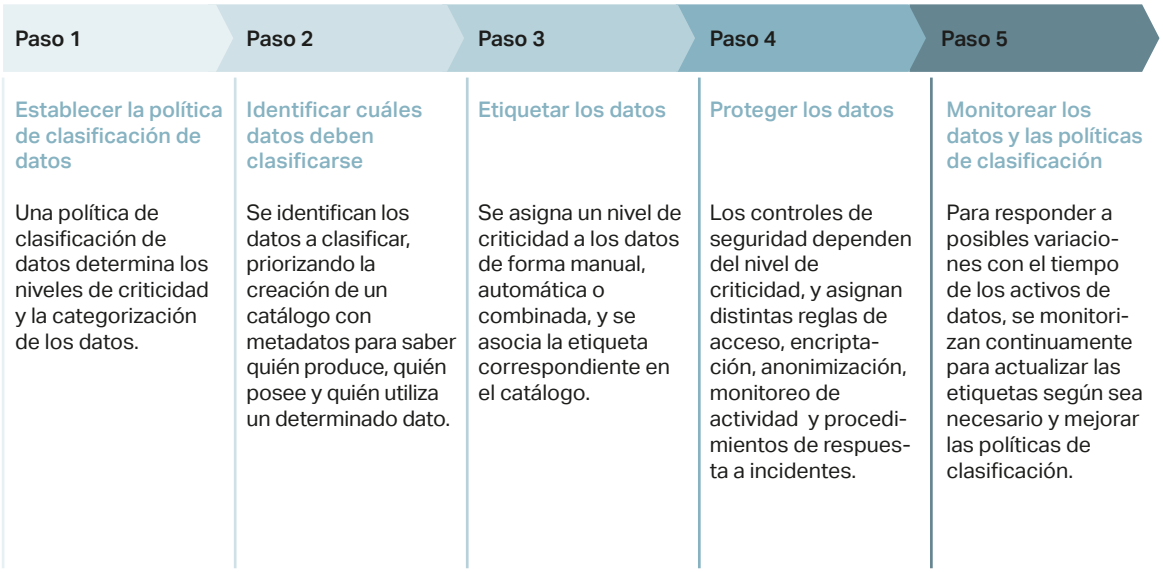
Existen estándares internacionales para desarrollar procesos de clasificación de datos. Los más reconocidos son elaborados por la Organización Internacional de Normalización (ISO, por sus siglas en inglés) (2022) y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) (2023). Nuestro documento presenta un enfoque de cinco pasos para el proceso de clasificación de datos, con base en los estándares del NIST. Este enfoque usa el término "activo de datos" para referirse a un recurso basado en información que puede ser una base de datos, un documento, una página web o un servicio (Newhouse *et al.*, 2023).

Para implementar procesos de clasificación de datos es necesario que dentro de la organización exista una estructura con capacidades para ponerla en práctica. Para evaluar la estructura, los roles y responsabilidades dentro de la organización es necesario realizar un diagnóstico previo a la clasificación. Implica realizar una evaluación de las capacidades de la organización para identificar necesidades y áreas de mejora. Así, se va a tener una visión más clara de qué información es procesada y quienes son sus responsables. Se puede diagnosticar a través de una evaluación de madurez de datos como la desarrollada por Dias *et al.* (2024a). Como resultado, las organizaciones conocen con qué capacidades cuentan para la gestión de datos e identifican áreas de mejora, como podrían ser la clasificación y protección de la información.

Proceso de clasificación

Paso a paso para la clasificación de datos

Diagrama 1



Fuente: Fundar con base en Newhouse *et al.* (2023).

Paso 1. Establecer la política de clasificación de datos

La política de clasificación de datos tiene como objetivo favorecer el intercambio y la apertura de información garantizando un nivel adecuado de protección. Proporciona una base para el desarrollo de estrategias de seguridad de la información y promueve una cultura de conciencia y responsabilidad en el manejo de datos abiertos. La política de clasificación de datos debe permitir establecer un lenguaje común que haga más fácil el trabajo con datos. De esta forma, contribuye a la gestión de los datos al mejorar la forma de ordenarlos.

> La política de clasificación de datos abarca dos dimensiones: los niveles de criticidad y la categorización de los datos.

1.1. Definir niveles de criticidad de los datos

Los niveles de criticidad se establecen en base a criterios definidos por un esquema de clasificación. Los esquemas más usados suelen guiarse por criterios de seguridad de la información. La cantidad de niveles y los criterios para definirlos dependen de cada organización. En general, las guías recomiendan que se establezcan entre tres y cinco niveles.

La precisión de un esquema de clasificación de datos determina la eficacia de las políticas de protección que luego pueden implementarse. El NIST señala que un aspecto importante es el equilibrio entre un esquema de clasificación de datos riguroso y las capacidades de la organización para implementarlo. La cantidad óptima de niveles de criticidad debe encontrar un equilibrio entre un esquema demasiado complejo y uno excesivamente simple. Un esquema demasiado complejo para las posibilidades de una organización puede hacer que no sea puesto en práctica pero un esquema demasiado simple puede llevar a una clasificación insuficiente (Newhouse *et al.* 2023).

Esta guía contempla la legislación argentina existente y propone tres niveles de criticidad: criticidad baja, media y alta, considerando los criterios de confidencialidad, integridad y disponibilidad. Para ver cómo establecer los niveles ir a Tres conceptos clave para pensar los niveles de criticidad.

1.2. Categorizar los datos

Las categorías de datos son una representación que permite organizarlos de manera jerárquica. Puede haber categorías principales y subcategorías. Cada nivel de la jerarquía desglosa más la información. Por ejemplo, una categoría puede ser "datos sensibles" y una subcategoría "datos de salud". Las categorías agrupan datos con características similares. Deben estar bien definidas utilizando nombres claros de acuerdo con determinados criterios como su naturaleza, su tipo, su finalidad, su sensibilidad o el nivel de riesgo asociado a su divulgación indebida. El objetivo de las categorías es facilitar la búsqueda y el uso de los datos dentro de la organización.

Algunos ejemplos de categorías de datos son los datos personales, de salud, financieros, de investigación, datos administrativos, sensibles y datos de organizaciones. En esta guía desarrollamos ejemplos de datos personales y datos organizacionales en Argentina. Para ver cómo definir las categorías de datos ir a Categorización de datos.

Paso 2. Identificar cuáles datos deben clasificarse

Una vez definida la política de clasificación de datos el siguiente paso es identificar cuáles datos deben clasificarse. Según el enfoque del NIST, la clasificación es necesaria cuando se crean datos, cuando se descubren datos que ya existían pero no estaban clasificados y cuando se importan datos de otra organización o dependencia.

Para asegurar una gestión y protección efectiva de los datos, es necesario clasificarlos en cuanto se crean, descubren o importan. En el caso de la importación de datos de otras organizaciones, debería conservarse la clasificación de datos de la organización de origen para garantizar que se cumplan los compromisos asociados a los datos de las organizaciones externas. Este paso debería permitir mantener la información de clasificación original y en el caso de que sea necesario, incorporar clasificaciones adicionales de la organización importadora. También puede pasar que los datos importados tengan que ser reclasificados si el acto de compartirlos con otra organización introduce requisitos que cambian las necesidades de clasificación (Newhouse *et al.*, 2023).

Para identificar dónde están los datos que deben clasificarse y ordenarse, es fundamental hacer un catálogo de los datos de la organización. Un inventario de datos debe incluir metadatos para saber quién produce, quién posee y quién utiliza determinado dato así como información sobre las fuentes, los tipos de datos, formatos, calidad y almacenamiento. Para la creación y mantenimiento del catálogo, se deben elegir herramientas adecuadas que aseguren que sea fácil de navegar y utilizar para los usuarios finales. Es recomendable que las dependencias actualicen el catálogo de manera continua a medida que se crean nuevos activos de datos.

Paso 3. Etiquetar los datos

Una vez que se identifican los activos de datos, se debe determinar qué nivel de criticidad les corresponde. Esta tarea puede ser manual, automática o una combinación de ambas. La clasificación manual es la intervención humana para clasificar datos. Especialmente necesaria en la validación y en los casos en los cuales no es posible hacer una clasificación automática. La clasificación automática puede estar basada en el análisis de metadatos o en el análisis del contenido (por ejemplo: OCR, búsqueda de palabras clave, herramientas de aprendizaje automático para buscar patrones en los datos, etc.). Cuando se trata de activos de datos no estructurados (por ejemplo un documento en formato pdf), donde no existe un modelo de datos o es informal, es necesario usar una combinación de enfoques para clasificarlos. Dependiendo qué aspectos de los activos de datos se hayan definido en la política de clasificación (tipo de dato, contenido, riesgo asociado, etc.) será conveniente una u otra forma de implementarla. Según el NIST, el ejercicio de clasificación solo en pocos casos puede estar totalmente automatizado, por lo general requerirá intervención manual (Newhouse *et al.*, 2023).

Al determinar las clasificaciones (manual o automáticamente) se asocian las etiquetas correspondientes. El etiquetado es el proceso mediante el cual las etiquetas de clasificación se asocian con un conjunto de datos en el catálogo de datos: la etiqueta de clasificación se convierte en un atributo de los metadatos. Un activo de datos puede tener más de una etiqueta. Según el NIST, uno de los principales desafíos en la clasificación de activos de datos son los que tienen secciones que requieren distintas etiquetas de clasificación (Newhouse *et al.*, 2023).

Para ver ejemplos de etiquetado de datos ir a La clasificación de datos en la práctica.

Paso 4. Proteger los datos

La protección de los activos de datos establece un nivel adecuado de controles en función de su clasificación. Incluye reglas de acceso, encriptación, anonimización, monitoreo de actividad y procedimientos de respuesta a incidentes (Luvini, 2022; López *et al.*, 2023; Luvini *et al.*, 2024).

Cada nivel de criticidad debe estar asociado a un conjunto de controles de seguridad acordes a las necesidades de protección. La protección estará basada en el riesgo asociado para la organización. Puede incluir riesgos como el acceso no autorizado a información confidencial (defensa, seguridad nacional), la pérdida o alteración de datos críticos, y las posibles sanciones legales por incumplimiento de normativas de protección de datos. Para las personas físicas, el riesgo se refiere a la posibilidad de que su información personal sea utilizada de manera indebida, lo que podría llevar a situaciones como el robo de identidad, el fraude, o la violación de su privacidad.

La protección de los datos está determinada por las restricciones de acceso establecidas en la organización y por el marco normativo vigente. Es esencial que las medidas de protección tomadas estén alineadas con las leyes y regulaciones de protección de datos de los países que se vean afectados.

Para revisar la normativa vigente sobre protección de datos personales ir al apartado de marco normativo. Para revisar la normativa vigente sobre protección de datos organizacionales ir al apartado de marco normativo.

Los niveles de la clasificación

↓

Paso 5. Monitorear los datos y las políticas de clasificación

El último paso es el monitoreo. Las características de los activos de datos pueden variar con el tiempo por lo que, después de la clasificación, los datos deben ser monitoreados de forma continua para identificar cualquier cambio que pueda requerir la actualización de sus etiquetas. El método de monitoreo también puede ser manual o automático y va a depender principalmente de si los datos son estructurados, semiestructurados o no estructurados. Este paso puede incluir supervisión, asesoramiento, revisión y mejora continua de las decisiones de clasificación.

Los niveles de la clasificación

Tres conceptos clave para pensar los niveles de criticidad

Si bien los esquemas de clasificación de datos cambian de acuerdo con el país, la mayoría se basa en la tríada CIA, por los términos **Confidencialidad, Integridad y Accesibilidad** (Walkowski, 2019). Estos son los tres principios fundamentales de la seguridad de la información a partir de los cuales se evalúa el control de seguridad que deberá tener un activo de datos.

Principios de Seguridad de la Información

Tabla 1

Principios de seguridad	**Confidencialidad**	**Integridad**	**Accesibilidad**
Definición	Implica todas aquellas acciones hechas para mantener datos privados o secretos, controlando con fines determinados el acceso a personas y/u organizaciones específicas.	Asegura que los datos no hayan sido alterados, garantizando su confiabilidad.	Garantiza el acceso irrestricto a los datos o sistemas de información a todos aquellos usuarios autorizados.
Aplicación	Evaluación del nivel de acceso a la información de una oficina o un funcionario. Puede haber accesos diferenciados.	Garantía del seguimiento de los cambios que sufra la información y la afirmación al usuario de que lo que está consultando es verídico y no ha sido alterado.	Ininterrupción en el acceso a la información.

Fuente: Fundar, con base en Walkowski (2019).

Los esquemas de clasificación que están basados en estos términos estiman tres niveles de criticidad para los datos, que son el resultado de la combinación de los valores asignados al impacto potencial de la pérdida de confidencialidad, integridad y disponibilidad. Es decir, a cada uno de estos tres principios se asocia un número que representa el nivel de criticidad del 0 al 3.

Los niveles de la clasificación

Experiencias de clasificación de datos

En el mundo

Son muchos los países del mundo que adoptaron estos esquemas para la clasificación de activos de datos. La forma en que se reglamentan los mismos difiere y se adapta según la institucionalidad de cada país.

En **Brasil**, el intercambio de datos se establece en tres niveles de confidencialidad. Aunque menciona la accesibilidad e integridad como características de los datos, estas no forman parte específica de las reglas de clasificación de datos.

En **Reino Unido** se sigue un lineamiento similar. El sistema de clasificación de activos destaca la confidencialidad, además de otras consideraciones.

En **Estados Unidos** la E-Government Act le asigna al NIST la responsabilidad de desarrollar estándares y guías para clasificar la información según su riesgo, con el objetivo de proteger la confidencialidad, integridad y disponibilidad de los datos. La ley define tres niveles de criticidad (baja, moderada y alta) según la gravedad de la pérdida de cualquiera de estos tres aspectos de seguridad. Asimismo, la clasificación de los sistemas de información, es decir de aquellos casos que no se trate de bases de datos aisladas sino más bien relacionadas, se considerarán a los valores más altos de impacto identificados en cada una de las bases.

En **Australia** también se utiliza la tríada para clasificar los activos, con niveles similares a los de Estados Unidos.

En Argentina

Si bien en Argentina las políticas de datos están alineadas con los criterios internacionales aplicados en otros países, no existe una asignación clara de funciones respecto a qué organismo debería encargarse de clasificar los datos o de establecer lineamientos sobre cómo hacerlo en cada entidad. Tampoco existe la asignación de responsabilidades mediante la creación de figuras, como el DPO (*Data Protection Officer*), como en el caso de Brasil. Aunque existen normas que abordan el tema, aún faltan directrices claras para su aplicación.

En Argentina, la Disposición 1/2015 de la Oficina Nacional de Tecnologías de Información (ONTI) establece tres niveles de criticidad a partir de la combinación de los valores asignados a cada uno de los principios de confidencialidad, integridad y disponibilidad. Cada principio va a ser analizado según establece la metodología expuesta en la tabla 2, asignando a cada conjunto de datos un valor entre 0 y 3. Luego, dependiendo de qué valores fueron asignados, cada activo va a tener un nivel de criticidad:

- **Criticidad baja:** ninguno de los valores asignados superan el 1.
- **Criticidad media:** alguno de los valores asignados es 2.
- **Criticidad alta:** alguno de los valores asignados es 3.

Los niveles de la clasificación

Metodología para evaluar un activo de datos según los principios de seguridad de la información

Principio / Valor	Confidencialidad	Integridad	Disponibilidad
0	"Información pública: puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del organismo o no."	"Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del organismo."	"Información cuya inaccesibilidad no afecta la operatoria del organismo."
1	"Información reservada/ de uso interno: que puede ser conocida y utilizada por todos los empleados del organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el organismo, el Sector Público Nacional o terceros."	"Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el organismo, el Sector Público Nacional o terceros."	"Información cuya inaccesibilidad permanente durante (plazo no menor a una semana) podría ocasionar pérdidas significativas para el organismo, el Sector Público Nacional o terceros."
2	"Información reservada-confidencial: que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al organismo, al Sector Público Nacional o a terceros."	"Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el organismo, el Sector Público Nacional o terceros."	"Información cuya inaccesibilidad permanente durante (plazo no menor a un día) podría ocasionar pérdidas significativas al organismo, al Sector Público Nacional o a terceros."
3	"Información reservada-secreta: que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del organismo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros."	"Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al organismo, al Sector Público Nacional o a terceros."	"Información cuya inaccesibilidad permanente durante (plazo no menor a una hora) podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros."

Tabla 2

Fuente: Fundar, con base en citas textuales de la Disposición 1/2015, Oficina Nacional De Tecnologías De Información (ONTI).

A partir de los valores asignados a los principios de confidencialidad, integridad y disponibilidad, cada activo de datos recibe como resultado un nivel de criticidad que corresponde al valor más alto de los tres. Como puede verse en el ejemplo a continuación:

Los niveles de la clasificación

Ejemplos de niveles de criticidad

Tabla 3

Confidencialidad	Integridad	Disponibilidad	Nivel de criticidad
1	0	1	Baja
0	2	1	Media
3	2	2	Alta

Fuente: Fundar.

Box 2

Legislación argentina sobre clasificación de los datos

El Estado nacional cuenta con legislación relevante sobre clasificación de datos. Un antecedente es la Resolución Nº 2979/2013 del Registro Nacional de las Personas (RENAPER) que toma el artículo 1º de la Decisión Administrativa Nº 669/2004 de la Jefatura de Gabinete de Ministros que establece que los organismos del Sector Público Nacional deberán dictar o adecuar sus políticas de seguridad de la información. En 2005, se aprobó en el contexto del Plan Nacional de Gobierno Electrónico y Planes Sectoriales de los Organismos de la Administración Pública Nacional, el Decreto N° 378/2005 del Poder Ejecutivo Nacional que establecía lineamientos de clasificación de datos. Este decreto se incorporó y actualizó posteriormente a la Disposición 1/2015, que también incluía el contenido de otras disposiciones y resoluciones. Tanto el decreto original como la Disposición fueron impulsados por la Oficina Nacional de Tecnologías de Información (ONTI).

El siguiente cuadro contiene ejemplos de clasificación de bases de datos de distintas dependencias del Estado argentino.

Tabla 4

Ejemplos de clasificación de bases de datos de distintas dependencias del Estado argentino

Tabla 4

Nivel de criticidad	Ejemplo
Criticidad baja	• Información agregada sobre beneficios y programas de la ANSES. • Información sobre presupuesto ejecutado por Ministerio o programas generales del gobierno del Ministerio de Economía. • Listado de nombre y DNI de beneficiarios de programas culturales como Becas Creación del Fondo Nacional de las Artes del ex Ministerio de Cultura. • Padrón electoral de la Dirección Nacional Electoral.
Criticidad media	• Datos personales - biométricos del proceso Certificado de Pre-identificación (CPI) del RENAPER. • Datos personales-financieros sobre beneficiarios del programa Prestación Alimentar del Ministerio de Capital Humano de la Nación. • Información sobre programas de salud pública, estadísticas de enfermedades y registros de vacunación del Ministerio de Salud. • Datos sobre estudiantes, docentes y programas educativos del Ministerio de Capital Humano. • Datos personales y financieros sobre beneficiarios de la Asignación Universal por Hijo, Asignación por embarazo de la ANSES.
Criticidad alta	• Información sobre Defensa Nacional y seguridad interior de la Nación de la Agencia Federal de Inteligencia reguladas por la **Ley N° 25520/2001** de Inteligencia Nacional. • Información sobre la prevención, investigación y combate de delitos federales y complejos de la Policía Federal Argentina. Se trata de información exceptuada en la **Ley N° 27275/2016** de Acceso a la Información Pública (Art. 8). • Información de inteligencia financiera sobre lavado de activos de la Unidad de Información Financiera (UIF).

Fuente: Fundar.

Categorización de datos

Los niveles de criticidad de datos permiten tener una mayor organización y conocimiento de los datos con los que se cuenta, así como también detallar la criticidad de cada una de las variables. Por ejemplo, conocer que hay datos de criticidad media permite entender que no pueden compartirse sin restricciones al público, pero que potencialmente podrían compartirse a usuarios internos que tengan ciertos permisos y accesos.

Categorización de datos

Categorizar los datos permite identificarlos y entender fácilmente su jerarquía y vínculo en relación a otros datos. El objetivo de las categorías es facilitar la búsqueda y el uso de los datos dentro de la organización. La granularidad de las categorías y subcategorías puede variar. Un proceso de clasificación debe permitir relacionar de forma organizada las categorías de los datos con los **niveles de criticidad**.

Algunos ejemplos de categorías de datos son los datos personales, de salud, financieros, de investigación, datos administrativos, sensibles y datos de organizaciones. Las categorías se pueden construir en base a distintos criterios como su naturaleza, su tipo, su finalidad, su sensibilidad o el nivel de riesgo asociado a su divulgación indebida. Lo importante es que siempre sean nombres claros.

> Al identificar las categorías de datos se puede establecer con más precisión el nivel de criticidad asociado al impacto potencial de la pérdida de confidencialidad, integridad y disponibilidad.

Ejemplos de niveles de criticidad y categorías de clasificación

Tabla 5

Categoría	Confidencialidad	Integridad	Disponibilidad	Criticidad
Información administrativa	1	1	1	Baja
Información pública	0	2	2	Media
Información de investigación	3	2	2	Alta

Fuente: Fundar, con base en Newhouse *et al.* (2023).

Tomar la legislación existente y traducirla en buenas prácticas contribuye a una implementación efectiva de las categorías de datos, facilitando su aplicación en distintos contextos y sectores. En esta guía desarrollamos ejemplos de categorías de datos personales y de organizaciones pero se pueden establecer otros tipos de categorías según la conveniencia y las prioridades de cada organización.

Datos personales

Los datos personales son una categoría referida a cualquier tipo de información relacionada con una persona física (como el nombre y DNI). En Argentina la Ley N° 25326/2000 de Protección de Datos Personales establece un marco legal para protegerlos. A partir de esta ley se pueden definir otras categorías de información como **datos públicos, datos personales, datos sensibles y datos confidenciales.** Una categorización simple podría sólo tener en cuenta las categorías mencionadas y, luego, una más compleja puede agregar subcategorías (ver tabla 6). Por ejemplo, la Guía de Clasificación de Datos del Gobierno de la Ciudad de Buenos Aires utiliza esta categorización en su guía para la clasificación de datos.

Categorización de datos

Al asignar a cada una de las categorías de datos personales los distintos niveles de criticidad del esquema de clasificación, se puede ver que en un extremo el nivel más bajo de criticidad coincide con los datos públicos y en el otro extremo los datos confidenciales tienen el nivel de criticidad más alto.

Propuesta de categorización y niveles para la clasificación de datos personales en Argentina

Tabla 6

Categoría		Subcategoría		Nivel de criticidad
Datos públicos	Información contenida en documentos oficiales accesibles al público, como acuerdos, directivas, resoluciones, expedientes, informes, actas, contratos, convenios, estadísticas, etc. Estos datos son generados y mantenidos por organismos públicos y están disponibles para cualquier ciudadano.	Datos de acceso público irrestricto	Información publicada en boletines oficiales, medios de comunicación escritos, guías telefónicas, listas de profesionales, etc. Estos datos están disponibles sin restricciones y pueden ser utilizados por cualquier persona.	Baja
		Datos anónimos	Información tratada de manera que no pueda asociarse a una persona identificada o identificable, asegurando que no se pueda revertir el proceso de anonimización. Este tipo de datos es crucial para investigaciones y análisis que no requieren la identificación personal de los individuos.	Baja
Datos personales	Toda información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.	Datos administrativos	Información personal utilizada en la identificación y gestión de trámites: nombre, DNI, CUIT, domicilio, correo electrónico personal, fecha de nacimiento, género, patrimonio, trayectoria académica, laboral o profesional.	Baja

Tabla 6

Categorización de datos

Tabla 6

Categoría		Subcategoría		Nivel de criticidad
Datos sensibles	Datos personales que puedan revelar aspectos como: origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical u opiniones políticas; datos relativos a la salud, discapacidad; datos referidos a la preferencia u orientación sexual; datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona humana.	Datos de características físicas, genéticas o biométricas	Datos genéticos o biométricos (huellas dactilares, reconocimiento facial) que pueden identificar de manera única a una persona.	Media
		Datos de salud	Información médica y sanitaria, cuyo tratamiento está restringido por ley y requiere el consentimiento del titular. Incluye detalles sobre enfermedades, tratamientos médicos y cualquier información que pueda identificar el estado de salud de una persona. De hacerse públicos estos datos, las personas podrían ser discriminadas por condiciones médicas, por ejemplo al ser rechazadas y aisladas por las mismas en el entorno laboral.	Media
		Datos financieros	Información relacionada con la situación económica y bancaria de una persona, protegida por el secreto bancario y fiscal. Incluye datos sobre cuentas bancarias, ingresos, deudas y cualquier otra información financiera personal. La situación económica de una persona podría ser un motivo de discriminación por parte de sus pares o de estigma, ya sea por el monto de sus ingresos o el estado de sus deudas y créditos, razón por la que estos datos deben ser resguardados.	Media
		Datos de opiniones personales o afiliaciones	Información sobre opiniones políticas, convicciones religiosas o morales, y afiliación sindical. Estos datos pueden ser utilizados para discriminar o estigmatizar a una persona, o mismo ser utilizados por empresas con fines comerciales sin el consentimiento del individuo y, por lo tanto, requieren una protección especial.	Media
Datos confidenciales	Información que requiere protección especial debido a su naturaleza y al impacto que su divulgación indebida podría tener.	Datos de inteligencia	Información recolectada por fuerzas armadas, de seguridad, policiales o de inteligencia, necesaria para el cumplimiento de misiones legales específicas. Estos datos son esenciales para la seguridad nacional y la prevención del delito.	Alta
		Datos fiscales	Información presentada por los contribuyentes ante organismos fiscales, protegida por el secreto fiscal con algunas excepciones legales. Incluye declaraciones de impuestos, patrimonios y otras informaciones financieras.	Alta
		Datos de niñez y adolescencia	Información de menores de edad, que debe protegerse prioritariamente conforme al "interés superior del niño". Incluye datos personales y sensibles de niños y adolescentes, asegurando su privacidad y seguridad.	Alta

Fuente: Fundar, con base en Resolución Nº 2979/2013, Ley 25326/2000 y Guía de Evaluación de Impacto en la Protección de Datos.

Categorización de datos

Normativas que regulan el uso de datos personales

En Argentina la Ley N° 25326/2000 de Protección de Datos Personales reconoce que los datos personales no pueden ser utilizados ni registrados sin el consentimiento de las personas. También el derecho a las personas a pedir qué datos personales se encuentran registrados en bancos públicos o privados y la supresión, corrección y confidencialidad de los mismos. La autoridad de aplicación de esta ley es la Agencia de Acceso a la Información Pública (AAIP), un ente autárquico que funciona bajo la Jefatura de Gabinete de Ministros.

En 2020, la AAIP presentó el borrador de un anteproyecto de ley para actualizar la Ley N° 25326/2000. El proyecto está alineado con estándares internacionales de protección de datos, tomando como referencia a la General Data Protection Regulation (GDPR) y al Convenio 108 del Consejo de Europa , la Ley General de Protección de Datos Personales (LGPD) brasileña, la Ley Orgánica de Protección de Datos Personales de Ecuador, entre otros documentos. El proyecto incorpora figuras de la GDPR como el delegado de protección de datos y la obligación al responsable de los datos de informar de la ocurrencia de incidentes de seguridad a la autoridad de aplicación. En junio de 2023, el Poder Ejecutivo envió al Congreso Nacional el nuevo proyecto de ley incorporando aportes recibidos durante las consultas públicas que tuvieron lugar en 2022.

A su vez, la Ley N° 27275/2016 de Derecho de Acceso a la Información Pública define el concepto de presunción de publicidad: "toda la información en poder del Estado se presume pública, salvo las excepciones previstas en esta ley[1]". Es decir, la información con la que cuenta el Estado debería ser pública irrestrictamente, a no ser que se indique de alguna manera lo contrario. La ley también lo exige en el principio de transparencia y máxima divulgación: "Toda la información en poder, custodia o bajo control del sujeto obligado debe ser accesible para todas las personas. El acceso a la información pública sólo puede ser limitado cuando concurra alguna de las excepciones previstas en esta ley". Estos principios garantizan el libre acceso a la información del Estado argentino, limitándose solo en casos excepcionales, donde las normas vigentes[2] en materia datos así lo establezcan.

Box 3

Protección de datos personales en la Unión Europea

La Unión Europea es la región con la regulación más avanzada de protección de datos personales. En 1981 los miembros del Consejo de Europa firmaron el Convenio N°108 para garantizar a las personas de los países firmantes el respeto de sus derechos y libertades fundamentales y a los datos que afectan la vida privada. En 2016, se sancionó la General Data Protection Regulation (GDPR), para regular cómo los datos personales son utilizados y transferidos. Esta regulación determina los derechos de los individuos y las obligaciones de quienes utilizan sus datos. Además de nombres, correos electrónicos o teléfonos de las personas, la GDPR también considera datos personales a las cookies de un sitio web que extraen información sobre la identidad. Todo procesamiento de datos personales requiere el consentimiento explícito de los sujetos, que puede ser retirado en cualquier momento. La regulación europea destaca por ser extensiva en su alcance[3] y exigente en las multas para quienes incumplen la normativa. La ley también define varias figuras en la gestión de datos, dentro de las que se destaca el Data Protection Officer (DPO).

Box 3

1 Las excepciones contempladas en esta ley se precisan en sus decretos reglamentarios (Decreto N° 206/2017 y sus modificaciones, incluyendo el Decreto N° 780/2024)

2 Ley N°25326/2000 de protección de datos personales, Ley N° 17622/1968 del Sistema Estadístico y Ley N° 11683/1933 de Procedimiento Fiscal.

3 Comprende a todos los ciudadanos o residentes de la Unión Europea aún cuando la compañía que tenga la información o la utilice no esté en ninguno de los países del grupo.

Box 3

La GDPR se convirtió en un modelo de regulación y fue tomada de referencia por varios países. Se destaca el Reino Unido, que se rige actualmente por el *Data Protection Act 2018* y por la UK GDPR, una adaptación de la ley europea. En términos prácticos, hay pocas diferencias entre la GDPR original y aquella sancionada por el Reino Unido. En este país, la oficina del *Information Commissioner's Office (ICO)* tiene a cargo la difusión de manuales y de guías para respetar los marcos regulatorios a la hora de compartir datos personales. Dentro de estas guías se destaca la aclaración de que la UK GDPR sólo considera y protege a los datos personales: todos aquellos datos donde ningún individuo pueda ser identificado se rige por fuera de esta regulación.

Brasil es otro caso de país que tomó la norma europea para sancionar la ley Nº 13709/2018 General de Protección de Datos Personales (LGPD). La LGPD instituyó a la Autoridad Nacional de Protección de Datos (ANPD) como ente regulador del uso de datos personales.

Datos de organizaciones

Los datos de organizaciones son una categoría referida a información relacionada con las personas jurídicas, ya sean empresas u organizaciones (privadas, públicas, mixtas o sin fines de lucro). En Argentina, hay varias leyes que protegen los datos de personas jurídicas, dentro de las cuales se destacan la Ley N° 11683/1933 de Secreto Fiscal y la Ley N° 17622/1968 de Secreto Estadístico.

Entrando en detalle a los tipos de datos y a las categorías en que se agrupan, podemos mencionar los datos de facturación de las empresas, datos de cantidad de personas empleadas de cada persona jurídica y datos de su intercambio y comercio —por ejemplo, de exportaciones—. La Tabla 7 incluye algunos ejemplos de categorizaciones y niveles para la clasificación de datos organizacionales.

Propuesta de categorización y niveles para la clasificación de datos de organizaciones en Argentina

Tabla 7

La clasificación de datos en la práctica

Categorías		Subcategorías		Criticidad
Datos de organizaciones privadas	Información referida al funcionamiento de las personas jurídicas, ya sean empresas u otro tipo de organizaciones. Esto incluye información sobre su funcionamiento, su facturación y sus ingresos.	Datos de empleo	Datos de empleo públicos, agregados por CLAE a 6 dígitos a nivel de departamento.	Baja
		Datos de exportaciones	Información de exportaciones agregada por producto a nivel Nomenclatura Común de Mercosur (NCM) del sistema armonizado o categorizaciones similares que permitan una amplia desagregación de los montos FOB.	Media
			Información de exportaciones al máximo nivel de desagregación y por CUIT de la empresa exportadora.	Alta
Datos de organizaciones del estado	Información referida al funcionamiento de los servicios brindados en establecimientos públicos	Datos de recursos y servicios de salud	Datos sobre la disponibilidad y funcionamiento de los establecimientos de salud (hospitales, centros de salud, etc.).	Media
		Datos sobre cobertura y utilización de los servicios	Datos sobre el acceso a servicios de salud, el uso de instalaciones y el gasto en salud.	Media

Fuente: Fundar.

Normativas que regulan el uso de datos de organizaciones

Así como los datos personales deben ser protegidos para evitar las reidentificaciones, las personas jurídicas —empresas, y diversas organizaciones— también tienen el derecho a que no se divulguen ciertas informaciones sobre ellos. En Argentina entre las regulaciones que garantizan la protección de datos críticos para las personas jurídicas encontramos la Ley N° 17622/1968 del Sistema Estadístico, donde se define el secreto estadístico (en su artículo 10), y la Ley N° 11683/1933 de Procedimientos Fiscales, donde se establece el secreto fiscal.

Este marco normativo es el que determina que haya datos protegidos y que no se publiquen con un gran nivel de apertura. Por ejemplo, en las publicaciones de Comercio Exterior de bienes realizadas por el Instituto Nacional de Estadísticas y Censos (INDEC) hay productos que no presentan valor exportado por la aplicación del secreto estadístico. Esto sucede cuando en determinada posición arancelaria no hay suficientes operadores, por lo que publicar el monto FOB dejaría inferir con facilidad cuánto exportó una empresa en particular- En esos casos, no se publica con la mayor desagregación disponible a la exportación medida en FOB.". Sucede en casos como material de transporte terrestre —partes y piezas de vehículos y tractores— y en algunas pieles y cueros —de bovino y equino y de reptil—.

Existen otro tipo de datos de organizaciones que no comprometen el secreto comercial o patrimonial pero son importantes para la planificación y gestión pública. Un ejemplo de esto es la información sobre los establecimientos de salud del Estado (a nivel provincial, nacional o municipal). En Argentina, el Sistema Estadístico de Salud (SES), coordinado por la Dirección de Estadística e Información de Salud (DEIS) del Ministerio de Salud, recopila datos sobre infraestructura y desempeño de los servicios de salud. Como muestra la Tabla 7, aunque esta información es de acceso público y no está sujeta a restricciones de confidencialidad, su criticidad es media en términos de integridad y disponibilidad. Esto se debe a que los datos son fundamentales para la planificación y evaluación de políticas públicas, por ejemplo, en situaciones como la pandemia de COVID-19, donde la disponibilidad y precisión de estos datos sirvieron para una gestión eficiente de los recursos de salud. Por lo tanto, si bien la confidencialidad es baja, se necesita asegurar que los datos estén siempre disponibles y correctamente preservados para evitar interrupciones en la planificación de los recursos del sistema de salud.

La clasificación de datos en la práctica

Esta sección identifica ejemplos específicos de clasificación de datos en el sector público en Argentina. En primer lugar se analiza el caso de los datos del RENAPER y en segundo la Prestación Alimentar de la Secretaría de Inclusión Social del Ministerio de Desarrollo Social de la Nación[4]. En ambos ejemplos se aplica un esquema de clasificación evaluando algunos casos hipotéticos de los datos de estos programas.

Caso 1: Certificado de Pre-identificación (CPI) del Registro Nacional de las Personas (RENAPER)

El CPI es un instrumento con carácter de declaración jurada que permite el registro de datos de los nacidos en Argentina que nunca tuvieron DNI. De este modo, las personas pueden gestionar el acceso a sus derechos básicos, mientras inician o continúan el trámite de obtención de la partida de nacimiento y posteriormente de su DNI.

---

4 Los datos del programa Alimentar fueron procesados y publicados en el portal de datos abiertos durante el periodo en que las tareas de desarrollo social estaban bajo la jurisdicción del Ministerio de Desarrollo Social. Actualmente el programa está en la órbita del Ministerio de Capital Humano.

La clasificación de datos en la práctica

La Resolución Nº 2979/2013 del RENAPER representa un precedente importante en la clasificación de datos en Argentina. A través de ella, el RENAPER establece los lineamientos para clasificar sus activos de datos. La clasificación de la información se realizó en dos categorías principales: datos personales sensibles y datos organizacionales sensibles. Los datos personales sensibles incluyen información de carácter personal como origen racial o étnico, ideología, creencias religiosas o filosóficas, afiliación sindical, salud y vida sexual. Estos datos requieren protección debido a su naturaleza privada y el riesgo potencial de abuso o discriminación. Los datos sensibles organizacionales se refieren a información propia de la organización, cuya difusión pública podría aumentar el riesgo de amenazas a la información. Esto incluye información interna, planes estratégicos y datos financieros, entre otros. A continuación se presenta un ejemplo de clasificación de los datos solicitados en el proceso del CPI.

Descripción de los datos incluídos en la base de datos del CPI RENAPER

Tabla 8

Categoría	Subcategoría	Descripción	Criticidad
Datos personales	Datos biométricos	Foto y huellas	Media
	Datos administrativos	Información biográfica declarada	Baja
	Datos biométricos	Biometría facial y homonimia[5]	Media

Fuente: Fundar, con base en CPI RENAPER.

El resultado de la clasificación de la base de datos del proceso de CPI es criticidad media. La base de datos contiene variables con criticidad media y baja y, dado que su etiqueta de clasificación debe reflejar la criticidad más alta asociada a las variables garantizando así una protección adecuada, queda clasificada como de criticidad media.

Caso 2: El programa de la Prestación Alimentar

La Prestación Alimentar consiste en la transferencia monetaria para la adquisición de alimentos de la canasta básica a beneficiarios de la Asignación Universal por Hijo (AUH)[6]. Para este ejercicio, utilizamos los datos que publica el programa a través del portal de datos abiertos del gobierno nacional. Estos datos incluyen: `persona_id, sexo, edad, provincia_id, provincia, departamento_id, departamento, monto_ultima_liquidacion, periodo_desde y periodo_hasta`. La base de datos está anonimizada. El campo persona_id es un identificador que permite compartir información de personas únicas sin que se las pueda identificar directamente.

El programa maneja datos personales a gran escala, incluyendo datos sensibles de personas en situaciones de vulnerabilidad. Es importante destacar que como la base de datos está anonimizada, su criticidad es baja. Si la misma base de datos no estuviera anonimizada, sería de criticidad media, ya que la anonimización elimina la posibilidad de identificar a individuos específicos, reduciendo el riesgo asociado a la divulgación de la información.

---

5 El RENAPER realiza una búsqueda por biometría de huellas, biometría facial y homonimia, en la base de datos de personas que están registradas y cuentan con DNI. Se cruza la información con otras bases de datos donde destaca la de la Dirección Nacional de Migraciones: consulta por homonimia de la madre, en la base de datos de ingresos y egresos de puntos fronterizos al momento del nacimiento declarado del no inscripto.

6 La Prestación Alimentar es una transferencia monetaria que entrega el Estado nacional para el acceso a la canasta básica alimentaria. Está dirigido a padres con hijos de hasta 17 años de edad (inclusive) que reciben la AUH. Mujeres embarazadas a partir de los 3 meses, que cobran la asignación por embarazo. Personas con discapacidad que reciben la AUH. Madres con 7 hijos o más que perciben Pensiones No Contributivas.

La clasificación de datos en la práctica

Para enriquecer el ejemplo y tener datos de diferentes niveles de criticidad añadimos información ficticia sobre DNI, ingresos de la persona y su domicilio. Aunque estos datos adicionales no están disponibles públicamente, asumimos que el programa dispone de esta información pero con restricciones de acceso debido a su mayor nivel de criticidad. Por ejemplo, la información sobre los ingresos de las personas deberían ser de criticidad media, ya que sólo debería poder acceder personal autorizado.

Para clasificar los datos de los titulares de la Prestación Alimentar, aplicamos el esquema de clasificación basado en los criterios de confidencialidad, integridad y disponibilidad. A continuación, se detalla la clasificación propuesta para este caso. En el ejemplo, incluimos al DNI como un identificador único de la persona. Así como están los datos no podrían compartirse en el portal de Datos Abiertos ya que deberían pasar por un proceso de anonimización (para anonimizar estos datos, deberíamos usar el campo `persona_id`) .

Clasificación de datos Prestación Alimentar

Tabla 9

Categoría	Subcategoría	Campo	Criticidad
Datos personales	Datos administrativos	DNI	Media
		Sexo	Baja
		Edad	Baja
		Provincia	Baja
		Departamento	Baja
		Domicilio de la persona	Media
Datos sensibles	Datos financieros	Monto de la última liquidación	Baja
		Periodos de la primera y última liquidación	Baja
		Información de los ingresos de la persona	Media

Fuente: Fundar, con base en Datos abiertos del Ministerio de Desarrollo Social de la Nación.

Consideraciones finales

La clasificación de la base de datos del Programa Alimentar es criticidad media. Dado que la base de datos contiene variables con criticidad media y baja, la criticidad de la base de datos refleja la criticidad más alta asociada a las variables. Este criterio asegura una protección adecuada de los datos más críticos dentro de una base de datos, ya que la criticidad de una sola variable puede impactar significativamente la seguridad y el manejo de toda la base.

Al aplicar la clasificación a los datos de los titulares de la Prestación Alimentar, se observa que la mayoría de estos datos tienen una criticidad baja. Las variables que tienen una criticidad media son aquellas que no están compartidas en datos abiertos. Debido a la baja criticidad de estos datos, se pueden compartir sin necesidad de aplicar medidas estrictas de seguridad, como la provincia o la edad de una persona anonimizada si se considera que no hay un riesgo de reidentificación (Yankelevich, 2021). En otros casos, no se deben compartir para proteger la privacidad y seguridad de los titulares de los datos y para cumplir con las normativas vigentes en Argentina, como en los casos del domicilio y de los ingresos. En el caso del domicilio, tal como establece la Ley N° 25326/2000 de Protección de Datos Personales, no debe compartirse puesto que esta información personal debe ser guardada confidencialmente. En el caso de los ingresos, puede también intervenir el secreto fiscal si esta información hubiese sido obtenida mediante un intercambio con AFIP.

Consideraciones finales

Los gobiernos tienen una oportunidad de generar valor público a través de la clasificación de datos. La clasificación es una de las características técnicas necesarias para que los datos puedan ser usados, reutilizados y redistribuidos según los accesos y permisos que tenga cada organización, o inclusive ser abiertos al público con accesos en cualquier momento y en cualquier lugar. Como vimos en los ejemplos expuestos, contar con categorías y niveles de criticidad hace más sencillo compartir la información.

Para clasificar necesitamos datos y responsabilidades asignadas sobre ellos. Es muy útil contar con un marco que permita seguir el proceso de clasificación correctamente y replicar modelos aplicados por otros. La guía que se utilice debe incluir las normas relevantes y su interpretación, lo que ayudará a garantizar que los procedimientos sigan las regulaciones vigentes y mejores prácticas establecidas.

El marco para la clasificación de datos presentado en este documento puede aplicarse tanto a organizaciones que manejan información de alta criticidad como a aquellas que gestionan datos con baja criticidad. Las organizaciones que trabajan con datos confidenciales de criticidad alta probablemente conozcan mejor las restricciones para compartirlos. Sin embargo, las organizaciones con datos de menor criticidad pueden no estar tan familiarizadas con sus necesidades de clasificación. Esta guía les ayudará a identificar y organizar sus datos facilitando el proceso de clasificación.

No es necesario hacerlo de forma automatizada, puede lograrse con herramientas simples sin necesidad de un software sofisticado. Lo que realmente mejora la gestión de los datos es conocerlos y aumentar el compromiso con ellos. Para ello es importante dejar documentados los procedimientos realizados, ya sean manuales, automatizados o una combinación de ambos y declarar e informar a otros sobre las acciones realizadas en la clasificación de datos. Además, es necesario explicitar los estándares aplicados para posibles desarrollos de planes de seguridad u otras gestiones. La clasificación puede ser un proceso gradual que se vaya complejizando con el tiempo. Al comienzo se pueden establecer pocas categorías e ir agregando más con la experiencia. Desde el inicio, los criterios formulados en la política de clasificación deben ser claros para todas las personas involucradas y deben monitorearse ya que la criticidad de la información puede variar con el tiempo.

> Para una implementación efectiva es fundamental que exista voluntad política de las autoridades responsables.

Consideraciones finales

Si bien en esta guía se presentó el enfoque de clasificación basado en la seguridad de los datos según la tríada CIA (Confidencialidad, Integridad y Disponibilidad), también es importante explorar enfoques más amplios. En un mundo donde los datos son un recurso cada vez más estratégico, debemos considerar otras dimensiones de los datos como su valor social, contextual y estratégico. Tenemos que comprender que los datos adquieren diferentes significados y usos según el contexto en el que se manejan y tratarlos como recursos cuyo valor se incrementa cuando se comparte. La clasificación de los datos debe ser una herramienta no sólo para asegurar su protección, sino también para maximizar su valor en función de su impacto social y su potencial para ser reutilizados en la planificación de las políticas públicas.

Aplicar este tipo de metodologías es un paso necesario para compartir datos que de otro modo podrían quedar aislados. Sin una clasificación adecuada, la presencia de información puede llevar a restringir el acceso a toda la base de datos, lo cual sería un error que limitaría el potencial del uso de la información.

Bibliografía

• Amazon Web Services (2024). Data classification (AWS Whitepaper).

• Australian Government, Department of Home Affairs (2023). Protective Security Policy Framework.

• Banco Mundial (2021). Global Data Regulation Diagnostic Survey Dataset 2021 [Dataset]. World Bank, Development Data Group.

• Coyle, D. (2022). Socializing data. Daedalus, 151(2), 348-359.

• Data Protection Act (2018). UK's implementation of the GDPR.

• Dias, J. M., Kunst, M. y Juara, J. G. (2024a). Matriz de madurez en datos. Fundar.

• Agencia de Acceso a la Información Pública (2020). Guía de Evaluación de Impacto en la Protección de Datos.

• Jefatura de Gabinete de Ministros (2004). Decisión Administrativa N° 669/2004. Argentina.

• Congreso de la República Argentina (2016). Ley de Derecho de Acceso a la Información Pública, Ley N° 27275/2016 (2016). Argentina.

• Congreso de la República Argentina (2000). Ley de Protección de Datos Personales, Ley N° 25326/2000. Argentina.

• López, S., Alonso Alemany, L., Dias, J.M., Ación, L. y Xhardez, V. (2023). Guía práctica para la protección de datos personales en salud. Fundar.

• Luvini, P., Anand, A., Kunst, M., Dammalapati, S. (2024) Towards a Framework of Data Protection for Open Data. T20 Brasil 2024

• Luvini, P., Dias, J. M., Kunst, M., Ruiz Nicolini, J. P. y Yankelevich, D. (2023). Hacia un Estado Inteligente: una estrategia de datos para la Administración Pública Nacional. Fundar.

• Luvini, Paula (2022). Guía práctica para la protección de datos. Fundar.

• Microsoft (2024). Creación de un marco de clasificación de datos bien diseñado.

• Ministerio de Desarrollo Social de la Nación. (2016). Datos correspondientes a los titulares de la Prestación Alimentar en el marco del Plan Argentina Contra el Hambre.

• Newhouse, W., Souppaya, M., Kent, J, Sandlin, K. y Scarfone, K. (2023). Data Classification Concepts and Considerations for Improving Data Protection. National Institute of Standards and Technology, Gaithersburg, MD, NIST Interagency Report (IR) 8496.

• Organización de los Estados Americanos (2019). Clasificación de datos.

• Organización Internacional de Normalización (2013). (ISO) 27001, Requisitos para los sistemas de gestión de seguridad de la información.

• Poder Ejecutivo Nacional. (2005). Plan Nacional de Gobierno Electrónico y Planes Sectoriales de los Organismos de la Administración Pública Nacional. Decreto N° 378. Argentina.

• RENAPER (2021). Política de Protección de Datos Personales.

• Registro Nacional de las Personas. (2013). Resolución N° 2979/2013. Argentina.

• Ruiz Nicolini, J. P., Kunst, M. y Dias, J. M. (2024). Usos inteligentes de datos en el Estado. Fundar.

• Stine, K. M., Kissel, R., Barker, W. C., Lee, A., Fahlsing, J. y Gulick, J. (2008). SP 800-60 Rev. 1. Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories; Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. National Institute of Standards & Technology.

• Unión Europea (2016). General Data Protection Regulation (GDPR)

• Walkowksi, D. (2019). ¿Qué es la tríada CIA? Computerweekly.

• Yankelevich, Daniel (2021). Anónimos pero no tanto: cómo hacer una gestión de datos eficiente sin poner en riesgo la privacidad. Fundar.

Acerca del equipo autoral

Mariana Kunst

Coordinadora de Datos de Fundar

Licenciada en Economía y magíster en Métodos Cuantitativos para la Gestión y Análisis de Datos por la Universidad de Buenos Aires. Se desempeñó como coordinadora del Sistema de Información Cultural de la Argentina (SInCA) y como asesora en programas vinculados a las industrias culturales y análisis de información en el Ministerio de Cultura de la Nación. Realizó tareas de investigación relacionadas con empresas y organizaciones del sector cultural desde la Historia Económica. Actualmente es docente en la Universidad de Buenos Aires.

Paula Luvini

Investigadora de Datos de Fundar

Licenciada en Economía por la Universidad de Buenos Aires y Magíster en Ciencia de Datos por la Universidad de San Andrés. Se desempeñó como analista técnica en el Instituto Nacional de Estadísticas y Censos (INDEC) y como analista econométrica en el sector privado. Ha realizado asistencias en investigaciones de Data Science aplicadas a problemas sociales. Actualmente dicta clases de grado en la Facultad de Ciencias Económicas de la UBA.

Juan Manuel Dias

Científico de Datos de Fundar

Licenciado en Sociología por la UBA y maestrando en Estadística de la UNTREF. Es egresado de la carrera de ciencia de datos de la EANT y de la Diplomatura de Ciencias Sociales Computacionales de la UNSAM. Trabajó en investigaciones de mercado y de opinión pública en el sector privado y tiene una amplia experiencia en la administración pública, en las áreas de evaluación de políticas e innovación de procesos vinculados a la captación y análisis de información. Actualmente es docente de estadística en la UNPAZ.

Equipo Fundar

Dirección ejecutiva: Martín Reydó

Dirección de proyectos: Lucía Álvarez

Coordinación editorial: Gonzalo Fernández Rozas

Revisión institucional: Marcelo Mangini

Corrección/Edición: Juan Abadi

Diseño: Micaela Nanni

Edición de gráficos: Maia Persico

Kunst, Mariana
Guía práctica para clasificación de datos / Mariana Kunst ; Paula Luvini ; Juan Manuel Dias. - 1a ed. - Ciudad Autónoma de Buenos Aires : Fundar , 2025.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-631-6610-40-9

1. Elaboración de Datos. 2. Recopilación de Datos. 3. Protección de Datos. I. Luvini, Paula II. Dias, Juan Manuel III. Título
CDD 005.8

ISBN 978-631-6610-40-9

www.fund.ar info@fund.ar