Unidad N° 6

CALIDAD EN BASES DE DATOS

Bases de Datos Aplicada

Universidad Nacional
de La Matanza

DIIT
Departamento de Ingeniería e
Investigaciones Tecnológicas

Temario

Ley nacional de protección de datos personales.
General Data Protection Regulation (GDPR).
Modelo de Calidad de datos (ISO/IEC 25012).

Conocimiento Adquirido

Ley nacional de protección de datos personales: categorías de datos, marco regulatorio, sanciones
General Data Protection Regulation (GDPR): : categorías de datos, marco regulatorio, sanciones
Modelo de Calidad de datos (ISO/IEC 25012).

Universidad Nacional de La Matanza

DIIT

Departamento de Ingeniería e Investigaciones Tecnológicas

Pre Requisitos

Principio del mínimo privilegio.
Clasificación de usuarios.
Autenticación y directivas de contraseñas.
Estructura de permisos.
Data Control Language (DCL).
Configuración mediante propietarios y roles

Universidad Nacional
de La Matanza

DIIT

Departamento de Ingeniería e
Investigaciones Tecnológicas

Calidad significa hacer las cosas bien, incluso cuando nadie te está mirando

Henry Ford

DIIT

Departamento de Ingeniería e Investigaciones Tecnológicas

Universidad Nacional de La Matanza

Ley nacional de protección de datos personales

Ley 25.326

- Sancionada: Octubre 4 de 2000.

- La ley de protección de datos personales o hábeas data te protege si tus datos de identidad, de salud o de crédito son usados sin tu consentimiento.

- La Dirección Nacional de Protección de Datos Personales (PDP) es el órgano de aplicación de la ley de protección de datos personales (ley 25.326) del gobierno de la República Argentina.

- La PDP depende de la Agencia de Acceso a la Información Pública

Ley nacional de protección de datos personales

Ley 25.326: sobre qué datos hace referencia?

Datos personales

Son toda información que se relaciona con vos y puede identificarte, por ejemplo: DNI, dirección, teléfono, situación crediticia, imagen/video

Datos sensibles

Los datos sensibles son aquellos que revelan tu origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a tu salud o a tu vida sexual.

Se trata de datos personales especialmente protegidos, por eso nadie puede obligarte a brindarlos.

Ley nacional de protección de datos personales

ARTICULO 4° — (Calidad de los datos).

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Ley nacional de protección de datos personales

ARTICULO 5° — (Consentimiento)

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.

2. No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

Ley nacional de protección de datos personales

ARTICULO 6° — (Información).

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;

c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;

d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Ley nacional de protección de datos personales

ARTICULO 7° — (Categoría de datos)

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

Ley nacional de protección de datos personales

ARTICULO 9° — (Seguridad de los datos).

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Ley nacional de protección de datos personales

ARTICULO 31. — (Sanciones administrativas).

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

Ley nacional de protección de datos personales

ARTICULO 32. — (Sanciones penales).

1. Incorpórase como artículo 117 bis del Código Penal, el siguiente:

'1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena'.

2. Incorpórase como artículo 157 bis del Código Penal el siguiente:

'Será reprimido con la pena de prisión de un mes a dos años el que:

1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años'.

Ley nacional de protección de datos personales

Registro de base de datos privada

- Los archivos y bases de datos privados destinados a dar informes deben estar inscriptos en el Registro Nacional de Bases de Datos Personales.

- https://www.argentina.gob.ar/aaip/datospersonales/tramites

General Data Protection Regulation (GDPR)

- Es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos en la UE y el Espacio Económico Europeo (EEE).
- Aborda la transferencia de datos personales fuera de la UE y de las zonas del EEE. Entró en vigor el 24/05/2016 y fue de aplicación el 25/05/2018
- Se aplica a cualquier empresa -independientemente de su ubicación y de la ciudadanía o residencia de los interesados- que procese información personal de personas dentro del EEE.
- El objetivo principal del RGPD es mejorar el control y los derechos de las personas sobre sus datos personales y simplificar el entorno normativo para los negocios internacionales
- Las multas por el no cumplimiento del RGPD pueden llegar a los 20 millones de euros.

General Data Protection Regulation (GDPR)

¿Cuándo se aplica el Reglamento general de protección de datos (RGPD)?

El RGPD no se aplica cuando:

- el interesado ha fallecido
- el interesado es una persona jurídica
- el tratamiento de datos es efectuado por una persona que actúa con fines ajenos a sus actividades comerciales, empresariales o profesionales

General Data Protection Regulation (GDPR)

¿Qué son los datos personales?

Los datos personales son cualquier información relacionada con una persona identificada o identificable, también denominada " **el interesado**". Ejemplos de datos personales:

- nombre y apellidos
- dirección
- número de documento de identidad/pasaporte
- ingresos
- perfil cultural
- dirección de protocolo internet (IP)
- datos en poder de hospitales o médicos (que identifican únicamente a una persona con fines sanitarios).

General Data Protection Regulation (GDPR)

Categorías especiales de datos

No se pueden tratar datos personales sobre:

- origen racial o étnico
- orientación sexual
- opiniones políticas
- convicciones religiosas o filosóficas
- afiliación sindical
- datos genéticos, biométricos o sanitarios, salvo en casos específicos (por ejemplo, cuando se da un consentimiento explícito o cuando el tratamiento es necesario por razones de interés público esencial, sobre la base del Derecho nacional o de la UE)
- condenas e infracciones penales, a menos que lo autorice el Derecho nacional o de la UE.

General Data Protection Regulation (GDPR)

Transferencia de datos fuera de la UE

Cuando los datos personales se transfieran fuera de la UE, la protección ofrecida por el RGPD acompañará a los datos. Eso significa que si los datos se exportan al extranjero, la empresa debe garantizar que se cumpla una de las siguientes condiciones:

- La protección de datos del país no miembro de la UE se considera adecuada.
- La empresa toma las medidas necesarias para proporcionar las oportunas salvaguardias, como la inclusión de cláusulas específicas en el contrato celebrado con el importador no europeo de los datos personales.
- La empresa se basa en motivos específicos para la transferencia (excepciones), como el consentimiento del interesado.

Modelo de Calidad de datos (ISO/IEC 25012)

- ISO son las siglas en inglés International Organization for Standardization.
- Se dedica a la creación de normas o estándares para asegurar la calidad, seguridad y eficiencia de productos y servicios

- El modelo de Calidad de Datos (ISO/IEC 25012) representa los cimientos sobre los cuales se construye un sistema para la evaluación de un producto de datos

- La Calidad del Producto de Datos se puede entender como el grado en que los datos satisfacen los requisitos definidos por la organización a la que pertenece el producto

Modelo de Calidad de datos (ISO/IEC 25012)

Las características de Calidad de Datos están clasificadas en dos grandes categorías:

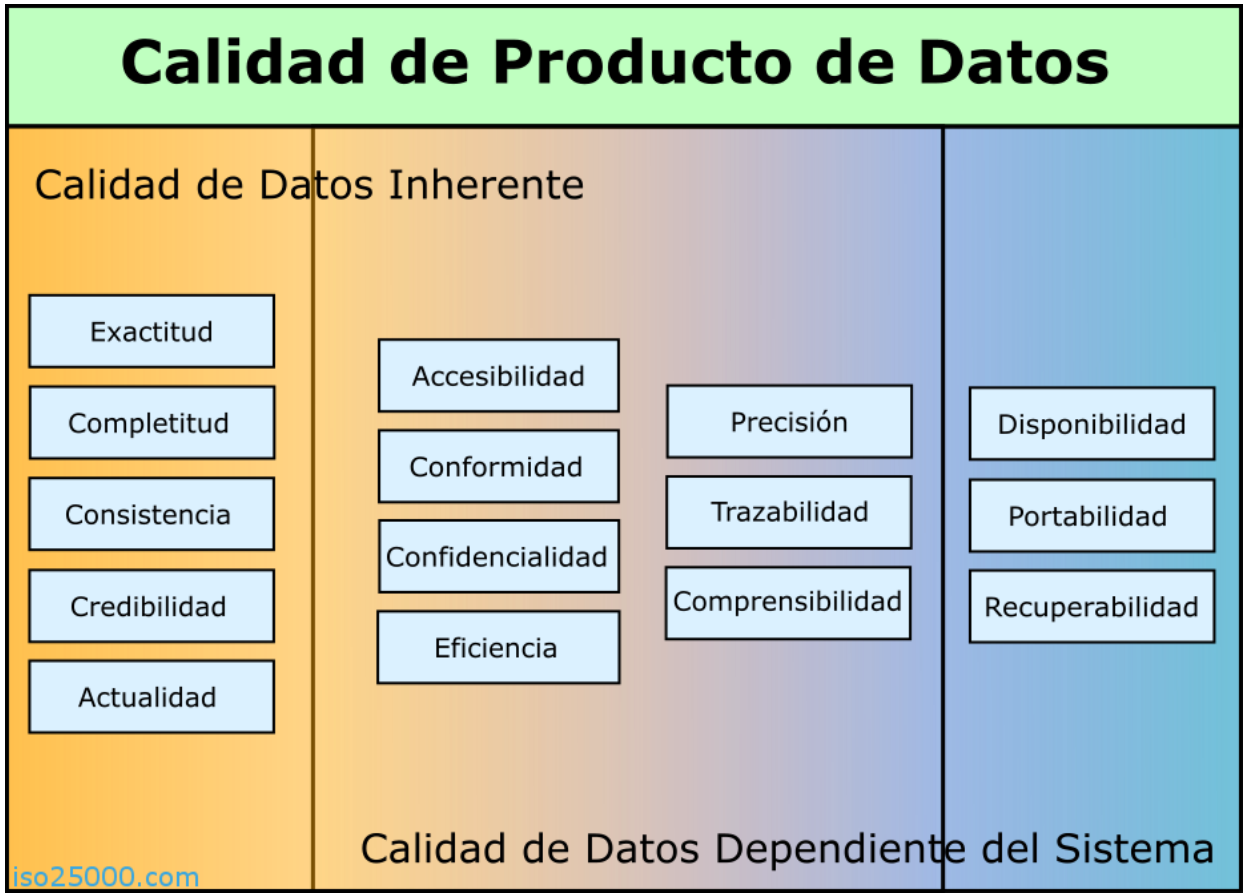
- Calidad de Datos Inherente: Se refiere al grado con el que las características de calidad de los datos tienen el potencial intrínseco para satisfacer las necesidades establecidas y necesarias cuando los datos son utilizados bajo condiciones específicas. Desde el punto de vista inherente, la Calidad de Datos se refiere a los mismos datos, en particular a:
  - Valores de dominios de datos y posibles restricciones (e.g., Reglas de Negocio gobernando la calidad requerida por las características en una aplicación dada).
  - Relaciones entre valores de datos (e.g., Consistencia).
  - Metadatos.

- Calidad de Datos Dependiente del Sistema: Se refiere al grado con el que la Calidad de Datos es alcanzada y preservada a través de un sistema informático cuando los datos son utilizados bajo condiciones específicas.

  Desde el punto de vista dependiente del sistema, la Calidad de Datos depende del dominio tecnológico en el que los datos se utilizan, y se alcanza mediante las capacidades de los componentes del sistema informático tales como: dispositivos hardware (e.g., Respaldo Software para alcanzar la Recuperabilidad), y otro software (e.g., Herramientas de migración para alcanzar la Portabilidad).

Modelo de Calidad de datos (ISO/IEC 25012)

El modelo de Calidad de Producto de Datos definido por el estándar ISO/IEC 25012 se encuentra compuesto por las 15 características que se muestran en la siguiente figura:



Modelo de Calidad de datos (ISO/IEC 25012)

Calidad de Datos Inherente

- Exactitud: Grado en el que los datos representan correctamente el verdadero valor del atributo deseado de un concepto o evento en un contexto de uso específico.
  Tiene dos principales aspectos:
  - ❑ Exactitud Sintáctica: cercanía de los valores de los datos a un conjunto de valores definidos en un dominio considerado sintácticamente correcto.
  - ❑ Exactitud Semántica: cercanía de los valores de los datos a un conjunto de valores definidos en un dominio considerado semánticamente correcto.
- Completitud: Grado en el que los datos asociados con una entidad tienen valores para todos los atributos esperados e instancias de entidades relacionadas en un contexto de uso específico.

- Consistencia: Grado en el que los datos están libres de contradicción y son coherentes con otros datos en un contexto de uso específico. Puede ser analizada en datos que se refieran tanto a una como a varias entidades comparables.

- Credibilidad: Grado en el que los datos tienen atributos que se consideran ciertos y creíbles en un contexto de uso específico. La credibilidad incluye el concepto de autenticidad (la veracidad de los orígenes de datos, atribuciones, compromisos).

- Actualidad: Grado en el que los datos tienen atributos que tienen la edad correcta en un contexto de uso específico.

Modelo de Calidad de datos (ISO/IEC 25012)

Calidad de Datos Inherente y Dependiente del Sistema:

- Accesibilidad: Grado en el que los datos pueden ser accedidos en un contexto específico, particularmente por personas que necesiten tecnologías de apoyo o una configuración especial por algún tipo de discapacidad.

- Conformidad: Grado en el que los datos tienen atributos que se adhieren a estándares, convenciones o normativas vigentes y reglas similares referentes a la calidad de datos en un contexto de uso específico.

- Confidencialidad: Grado en el que los datos tienen atributos que aseguran que los datos son sólo accedidos e interpretados por usuarios autorizados en un contexto de uso específico. La confidencialidad es un aspecto de la seguridad de la información (junto con la disponibilidad y la integridad) definida como en ISO/IEC 13335-1:2004.

Modelo de Calidad de datos (ISO/IEC 25012)

Calidad de Datos Inherente y Dependiente del Sistema:

- Eficiencia: Grado en el que los datos tienen atributos que pueden ser procesados y proporcionados con los niveles de rendimiento esperados mediante el uso de cantidades y tipos adecuados de recursos en un contexto de uso específico.

- Precisión: Grado en el que los datos tienen atributos que son exactos o proporcionan discernimiento en un contexto de uso específico.

- Trazabilidad: Grado en el que los datos tienen atributos que proporcionan un camino de acceso auditado a los datos o cualquier otro cambio realizado sobre los datos en un contexto de uso específico.

- Comprensibilidad: Grado en el que los datos tienen atributos que permiten ser leídos e interpretados por los usuarios y son expresados utilizando lenguajes, símbolos y unidades apropiados en un contexto de uso específico. Cierta información sobre la comprensibilidad puede ser expresada mediante metadatos.

Modelo de Calidad de datos (ISO/IEC 25012)

Calidad de Datos Dependiente del Sistema:

- Disponibilidad: Grado en el que los datos tienen atributos que permiten ser obtenidos por usuarios y/o aplicaciones autorizadas en un contexto de uso específico.

- Portabilidad: Grado en el que los datos tienen atributos que les permiten ser instalados, reemplazados o eliminados de un sistema a otro, preservando el nivel de calidad en un contexto de uso específico.

- Recuperabilidad: Grado en el que los datos tienen atributos que permiten mantener y preservar un nivel específico de operaciones y calidad, incluso en caso de fallos, en un contexto de uso específico.

¿Dudas?


DIIT
Departamento de Ingeniería e
Investigaciones Tecnológicas
Universidad Nacional
de La Matanza

Bibliografía

https://www.argentina.gob.ar/aaip/datospersonales
https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

https://iso25000.com/index.php/normas-iso-25000/iso-25012

DIIT
Departamento de Ingeniería e Investigaciones Tecnológicas

Universidad Nacional de La Matanza