



UNIVERSIDAD TECNOLÓGICA DE PANAMÁ  
CENTRO REGIONAL DE CHIRIQUÍ  
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES



**CARRERA:**  
LICENCIATURA EN DESARROLLO Y GESTION DE SOFTWARE

# ÉTICA, PRIVACIDAD Y PROTECCIÓN DE DATOS EN LAS BASES DE DATOS

**ASIGNATURA:**  
BASE DE DATOS I

**DOCENTE:**  
MARLENIS A. PIMENTEL M.

**ESTUDIANTES:**  
ABDIEL CASTILLO 4-804-773  
CARLOS MONTENEGRO 4-841-2441  
YUREM JORDAN 4-843-2034  
JEISON PALACIO 4-843-856  
KHALED MOJICA 8-1013-948

**II SEMESTRE 2026**

**FECHA:**  
2/10/2026





# Ética, privacidad y protección de datos en las bases de datos

# Introducción

**En la actualidad, las bases de datos son fundamentales para almacenar, organizar y gestionar grandes cantidades de información. Empresas, universidades, hospitales, bancos y otras organizaciones utilizan datos para realizar sus actividades y tomar decisiones.**

# Concepto de privacidad de datos

¿Qué es la privacidad de datos?

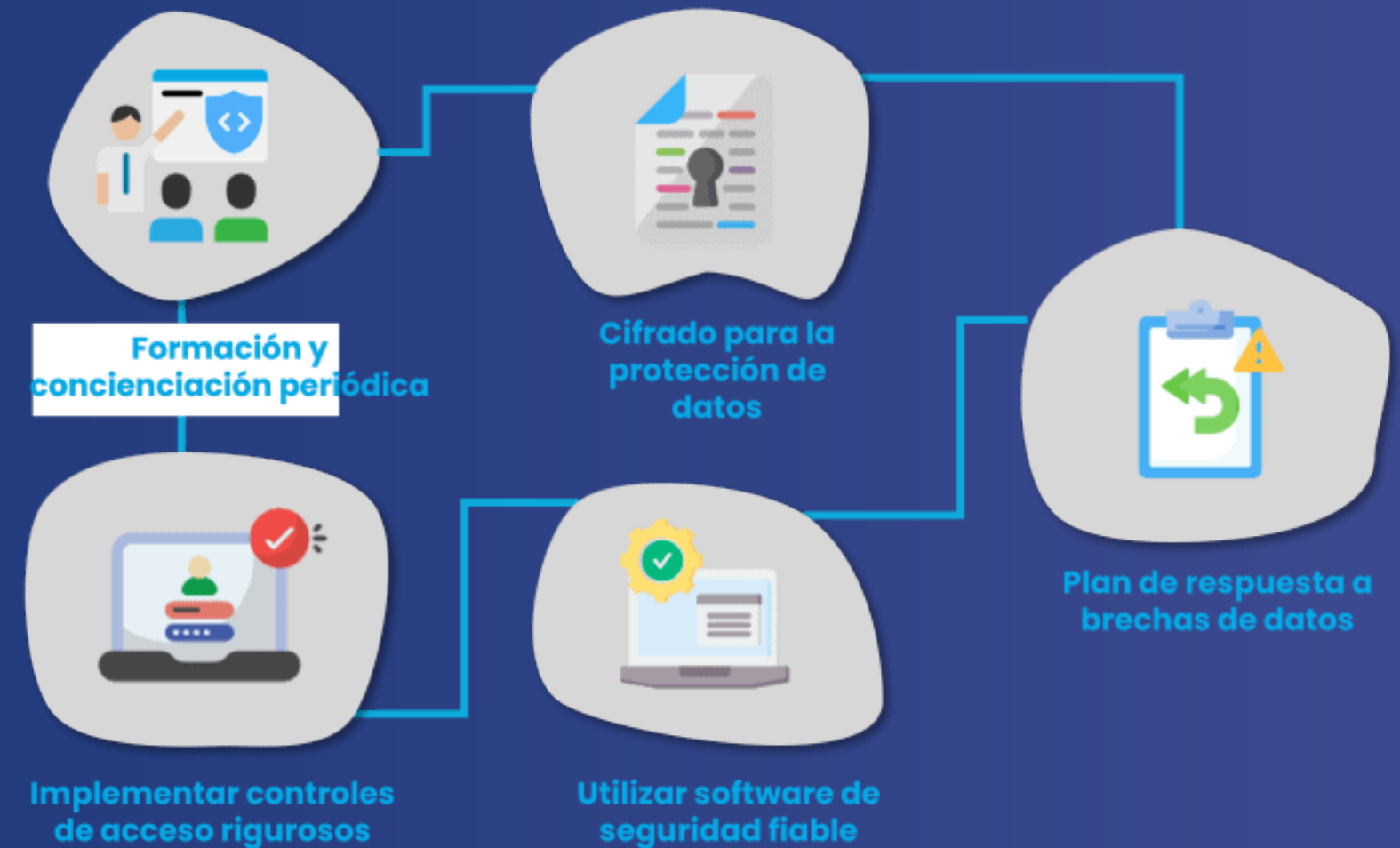


¿Por qué es importante?



# Protección de información sensible.

La información sensible es aquella que, si se revela o se usa mal, puede afectar gravemente la intimidad de una persona o exponerla a discriminación. Incluye datos de salud, origen étnico, orientación sexual, creencias religiosas, opiniones políticas, datos biométricos (como la huella dactilar o el reconocimiento facial) y datos financieros, como números de tarjetas o cuentas bancarias.



# Proteger esta información en las bases de datos requiere combinar varias medidas:

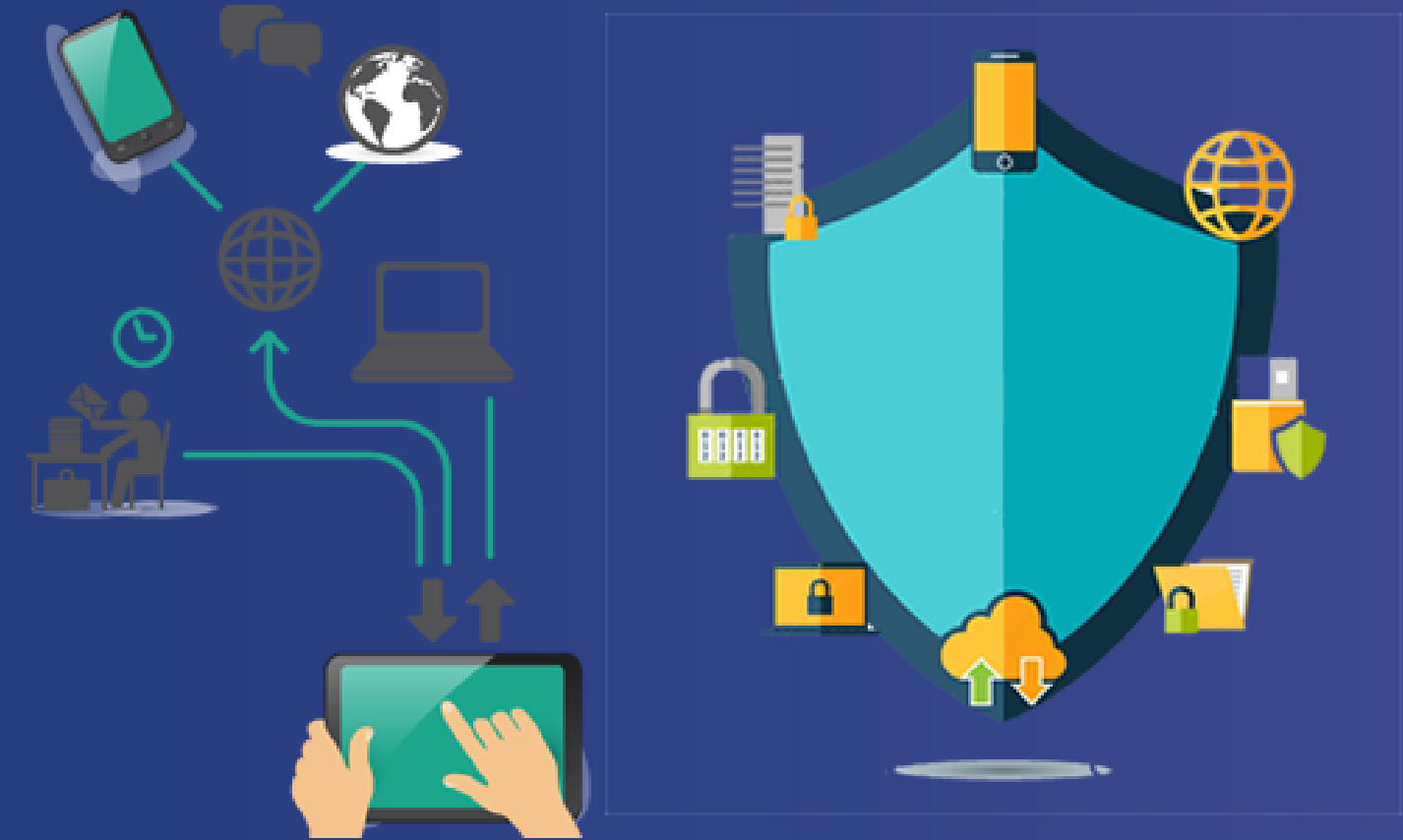
- **Cifrado:** convierte los datos en un código ilegible para quien no tenga la clave, tanto cuando están almacenados como cuando viajan por la red.
- **Control de acceso:** solo pueden ver la información las personas autorizadas, y únicamente la que necesitan para su trabajo. Se aplica con usuarios, contraseñas seguras y autenticación de dos pasos.



- **Anonimización y seudonimización:** consisten en quitar o reemplazar los datos que identifican a la persona, de modo que la información pueda analizarse sin exponer quién es su titular.
- **Copias de respaldo y auditorías:** permiten recuperar la información ante una falla y registrar quién accedió a qué datos y cuándo, para detectar usos indebidos.
- **Capacitación del personal:** muchas filtraciones no ocurren por fallas técnicas, sino por errores humanos, como abrir un correo fraudulento o compartir una contraseña.

# Principios éticos en el manejo de datos

La ética va más allá de lo que la ley exige. Se trata de actuar correctamente incluso cuando nadie está vigilando. Quienes administran bases de datos, ya sean programadores, administradores o analistas, deben guiarse por principios como estos:



- **Consentimiento:** los datos solo se recogen si la persona sabe qué se recopila y acepta que se use.
- **Finalidad:** la información se usa únicamente para el propósito que se informó al titular, no para otros fines distintos.
- **Minimización:** se recoge solo lo estrictamente necesario, porque mientras menos datos se guardan, menor es el riesgo.
- **Transparencia:** la organización explica de forma clara cómo trata los datos y a quién se los comparte.
- **Confidencialidad:** los datos no se revelan a personas o entidades no autorizadas.
- **Exactitud y calidad:** la información debe ser correcta y estar actualizada, porque un dato erróneo puede perjudicar a una persona.
- **Responsabilidad:** quien maneja los datos responde por su uso y debe asumir las consecuencias si ocurre un mal manejo.

# Legislaciones y normativas de protección de datos

En Panamá



## Marco Legal Principal

Ley 81 (26 de marzo de 2019): Establece las reglas generales para que las empresas cuiden los datos personales.

Decreto Ejecutivo 285 (2021): Reglamenta la ley, explica su aplicación e introduce la figura del Oficial de Protección de Datos (OPD).

## Derechos ARCO y Portabilidad

Derechos ARCO: Acceder, Rectificar, Cancelar y Oponerse (portabilidad) a nuestros datos personales.

## Incumplimiento y Sanciones

Sanciones: Multas e incluso la suspensión/cierre de la base de datos por incumplimiento.



# Legislaciones y normativas de protección de datos

## En el mundo



### 🌐 Convenio 108 (1981)

Primer acuerdo internacional con fuerza legal obligatoria para la protección de personas frente al tratamiento automatizado de datos.

### 🛡️ RGPD de la Unión Europea (2018)

El referente mundial en protección de datos; contempla multas de hasta 20 millones de euros o el 4% de la facturación anual global.

### 🌍 Expansión Global (CCPA y LGPD)

Inspirados en Europa, en 2018 surgieron la **CCPA en California** y la **LGPD en Brasil**, consolidando la tendencia normativa mundial.

# Riesgos asociados a las filtraciones de información

Impacto económico, tiempos de respuesta y amenazas

**\$4.44M**

Costo promedio global por filtración de datos  
(según informe de IBM) en 2025.

**\$7.42M**

Costo promedio en el sector salud (máximo  
afectado)

## Tiempo de Detección en Latinoamérica

Toma un promedio de **316 días (más de 10 meses)** detectar y contener una brecha de seguridad. A mayor tiempo de respuesta, mayor es el perjuicio financiero.

## Principal Vector de Ataque: Phishing

Los correos fraudulentos y el engaño de ingeniería social siguen siendo la causa primaria de robo de credenciales e ingresos no autorizados.



# Uso responsable de los datos en las organizaciones.

**¿Cómo deben manejarse los datos personales?**

Las organizaciones que almacenan información personal tienen la responsabilidad de utilizarla de manera legal, transparente y segura.

## Principios fundamentales:

**Seguridad:** proteger las bases de datos contra accesos no autorizados, pérdidas o filtraciones.

**Finalidad:** utilizar los datos únicamente para el propósito informado al usuario.

**Minimización:** recopilar solamente los datos que realmente sean necesarios.

**Exactitud:** mantener la información correcta y actualizada.

**Conservación limitada:** no almacenar los datos durante más tiempo del necesario.

**Transparencia y consentimiento:** informar a las personas qué datos se recopilan, para qué se utilizan y, cuando corresponda, obtener su consentimiento.



# Caso Real de Violación de Privacidad



**Equifax: una filtración que expuso datos de millones de personas**

**Año: 2017**

**Organización: Equifax, empresa de información crediticia de Estados Unidos**

**Afectados: aproximadamente 147 millones de personas**

**Un grupo de atacantes aprovechó una vulnerabilidad de seguridad en los sistemas de Equifax.  
La investigación de la FTC señaló que la empresa no había aplicado oportunamente una actualización de seguridad crítica y que existían otras deficiencias, como credenciales almacenadas en texto plano y una segmentación insuficiente de los sistemas.**

**¿Qué información quedó expuesta?**

- Nombres y fechas de nacimiento**
- Números de Seguro Social**
- Direcciones**
- Información de tarjetas de pago**
- Otros datos personales**

**La FTC indicó que fueron expuestos al menos 145,5 millones de números de Seguro Social y 209.000 números de tarjetas de pago**

# El Impacto de la IA, el Big Data y la Inferencia de Datos

El Nuevo Paradigma de la Privacidad en la Era Algorítmica

— IMPACTO NORMATIVO Y ÉTICO

# ¿Qué es la Inferencia de Datos?

## Privacidad Tradicional

Protección de datos entregados de forma explícita (DNI, historial clínico, nombre).

## Inferencia por Inteligencia Artificial

Deducción algorítmica de atributos sensibles no revelados a partir de residuos digitales inofensivos.

## Atributos Deducidos sin Consentimiento

- **Estado de salud: Diagnósticos y riesgos futuros**
- **Ideología política: Inclinação de voto y opiniones**
- **Capacidad financiera: Riesgo de impago y solvencia**
- **Orientación personal: Hábitos y vida privada**

*"Ya no necesitamos que las personas revelen sus secretos; los algoritmos pueden deducirlos a partir de los residuos digitales que dejan atrás, creando 'gemelos digitales' para predecir y modificar su comportamiento."*

**Shoshana Zuboff**

La era del capitalismo de la vigilancia (2019)

# El Colapso de la Anonimización Tradicional

87%

**Re-identificable con solo 3 datos**

Código postal, fecha de nacimiento y género.

99.9%

**Precisión con datos de movilidad**

Ubicación continua de smartphone o tecleo.

## Falla Estructural de la Anonimización Clásica

**Cruce de Bases de Datos:** Mediante técnicas de re-identificación, la IA combina registros aparentemente desvinculados con fuentes públicas.

**Dato Personal en Potencia:** Todo registro anonimizado mantiene su condición identificable si se cuenta con la capacidad computacional para revertir el proceso.

# Riesgos Éticos: Sesgo y Opacidad

## Discriminación Algorítmica

Los modelos entrenados con datos históricos absorben y escalan prejuicios humanos.

**Ejemplo:** Detección de "riesgo de impago" basándose en el código postal o tipo de dispositivo móvil.

## El Problema de la "Caja Negra"

Los modelos de Deep Learning sufren de opacidad intrínseca e inexplicable.

**Impacto:** Imposibilidad de impugnar denegaciones automatizadas de crédito, empleo o seguros de salud.

*"Los modelos matemáticos no son objetivos. Son opiniones encapsuladas en matemáticas, y a menudo codifican los prejuicios de sus creadores."*

**Cathy O'Neil**

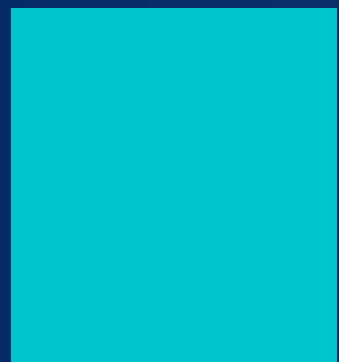
Armas de destrucción matemática (2016)

# Conclusión

Las bases de datos son fundamentales para las organizaciones modernas, pero el valor de la información también implica una gran responsabilidad. La privacidad, la ética y la seguridad deben formar parte del diseño y administración de las bases de datos.

Una gestión responsable requiere combinar tecnología, procedimientos, capacitación y cumplimiento de las normas. Proteger los datos no significa solamente evitar ataques informáticos, sino también garantizar que la información sea utilizada de manera legítima, responsable y transparente.

La protección efectiva de la privacidad exige trascender el control sobre los datos entregados y regular la capacidad predictiva de los algoritmos.



# BIBLIOGRAFÍA

- UNESCO. (2024). Módulo 8: Privacidad, protección de datos y usted. UNESCO.
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2013). Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.
- Asamblea Nacional de Panamá. (2019). Ley 81 de 26 de marzo de 2019, sobre protección de datos personales.
- Cooley LLP. (s. f.). Global privacy roundup: The world beyond Europe and California.
- Banco Interamericano de Desarrollo. (s. f.). Protección de datos y GDPR en América Latina.
- IBM. (2025). Cost of a Data Breach Report 2025.
- LexLatin. (2021). Publican reglamento para la ley de protección de datos en Panamá.
- Ministerio de la Presidencia de Panamá. (2021). Decreto Ejecutivo 285 de 28 de mayo de 2021.
- Órgano Judicial de Panamá. (2026). La protección de datos personales en la República de Panamá.
- Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 (RGPD).

**GRACIAS**