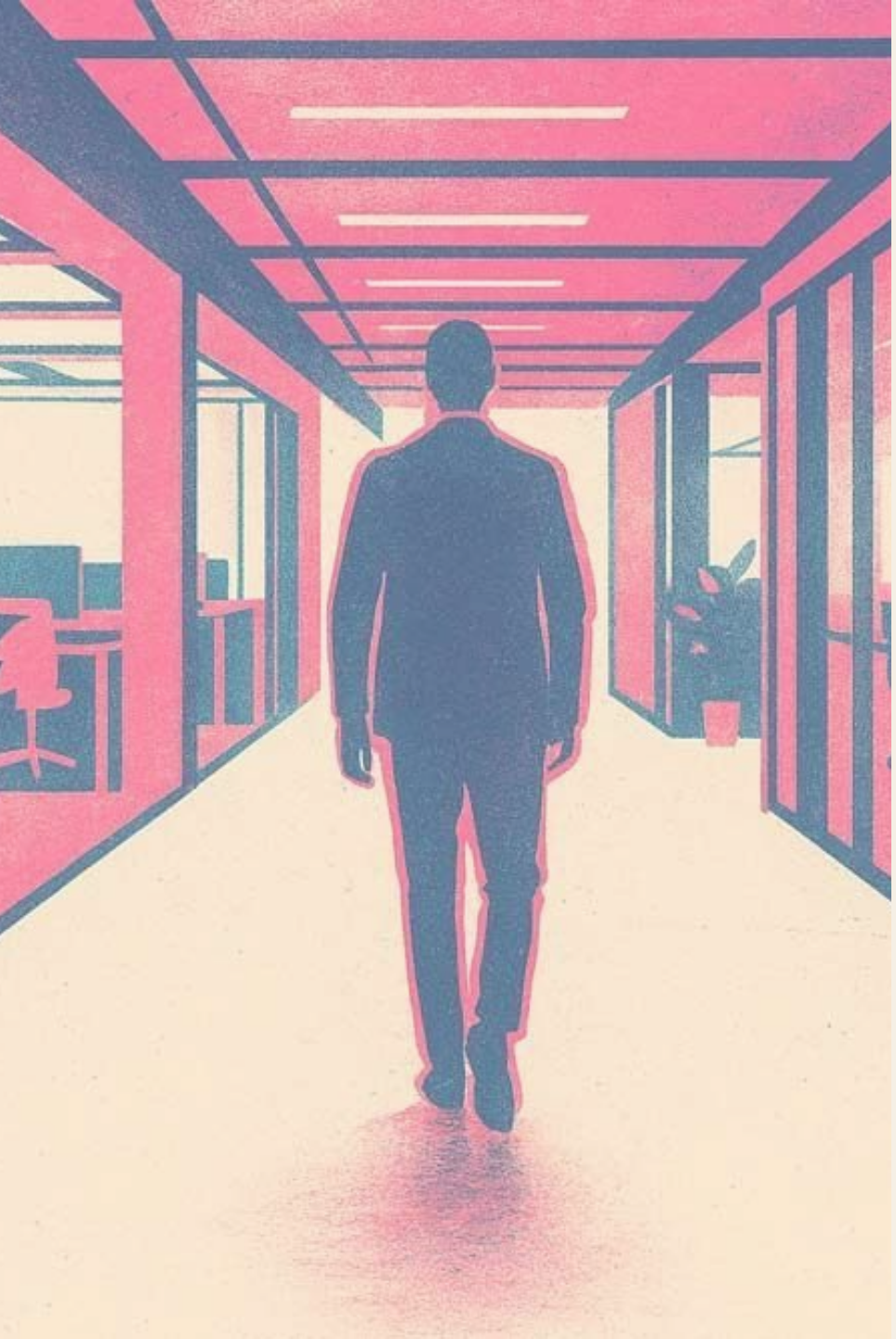
# PROTECCIÒN DE DATOS
# SECTOR DE LA SALUD

**Ley 19.628 y reformas 21.719/20.584**

**Lorena Donoso Abarca**
**Profesora Asociada**
**Facultad de derecho**
**Universidad de Chile**



# LA LEY 21.719 QUE MODIFICA LA LEY 19.628

1. Nombre actual: protección de la vida privada
2. Nuevo nombre: Protección de datos Personales

# DISPOSICIONES CLAVE

**Base legal (Ley 19.628)**

Define reglas de protección de datos en Chile: conceptos, derechos de titulares y deberes del responsable del tratamiento.

**Refuerzo en datos sensibles (Ley 21.719)**

Eleva exigencias para consentimiento y confidencialidad, especialmente en datos sensibles como los de salud.

**Alineación con estándares**

Busca aproximar la regulación chilena a marcos internacionales de protección de datos, como el GDPR.

# NUEVO ESCENARIO

| | |
|---|---|
| **Modernización normativa** | Adecuar la normativa nacional a los estándares de referencia |
| **Protección de derechos** | Derechos de Acceso, Rectificación, Supresión, Oposición, Portabilidad |
| **Eficacia normativa** | Autoridad de control acorde a estándares internacionales |
| | Régimen infraccional |
| | Coordinación Nacional e Internacional |

# ÁMBITO DE APLICACIÓN Y SUJETOS

**Aplicación de la ley**

La ley se aplica a instituciones públicas y privadas dentro de sectores regulados, asegurando cumplimiento normativo.

**Beneficiarios principales**

Titulares de datos personales

**Sujetos obligados**

Responsable del tratamiento

# LOS PRINCIPALES CAMBIOS LEGALES

**Modificaciones Institucionales**

Crea la Agencia de Protección de Datos como Corporación autónoma de derecho público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio, que se relacionará con el Presidente de la República a través del Ministerio de Economía, Fomento y Turismo.

**Estándar**

Autonomía

Carácter técnico

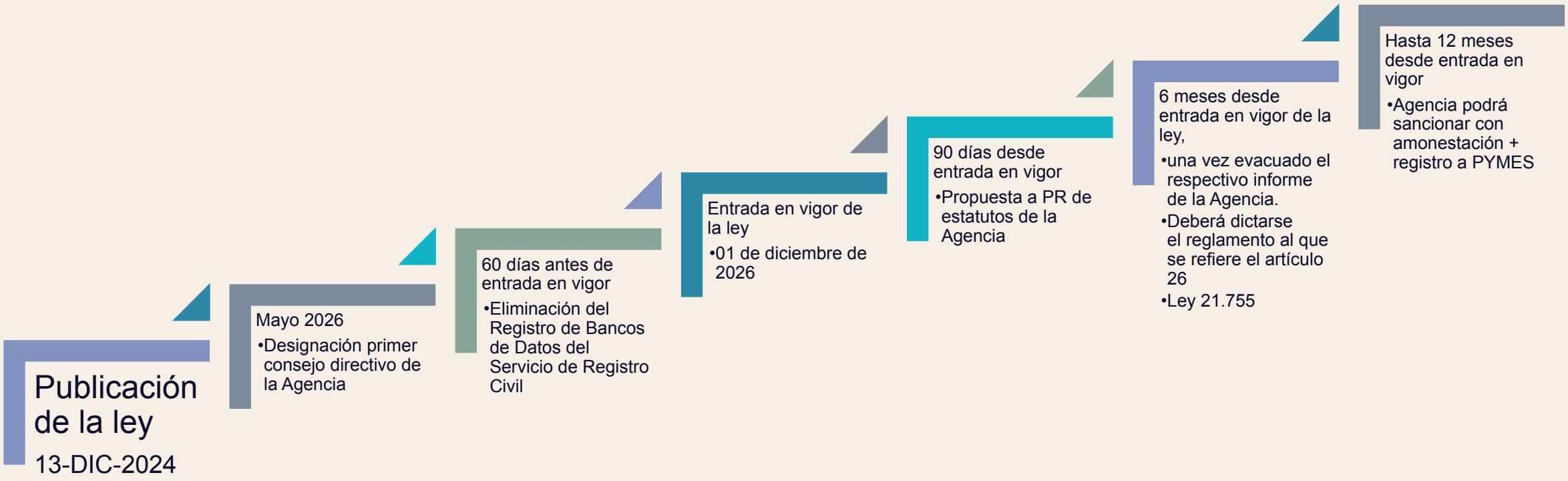
Atribuciones fiscalizadoras, educación, regulatorias, interpretativas, sancionatoria, asesora, coordinación nacional e internacional, certificadora de los modelos de cumplimiento

**Mecanismos de fiscalización**

Implementación de sistemas para asegurar el cumplimiento y

# FASES DE IMPLEMENTACIÓN

# IMPLEMENTACIÓN



# PERIODO DE ADAPTACIÓN


24 meses previos,

salvo modelo de prevención de infracciones pospuesto para su dictación por la Agencia.

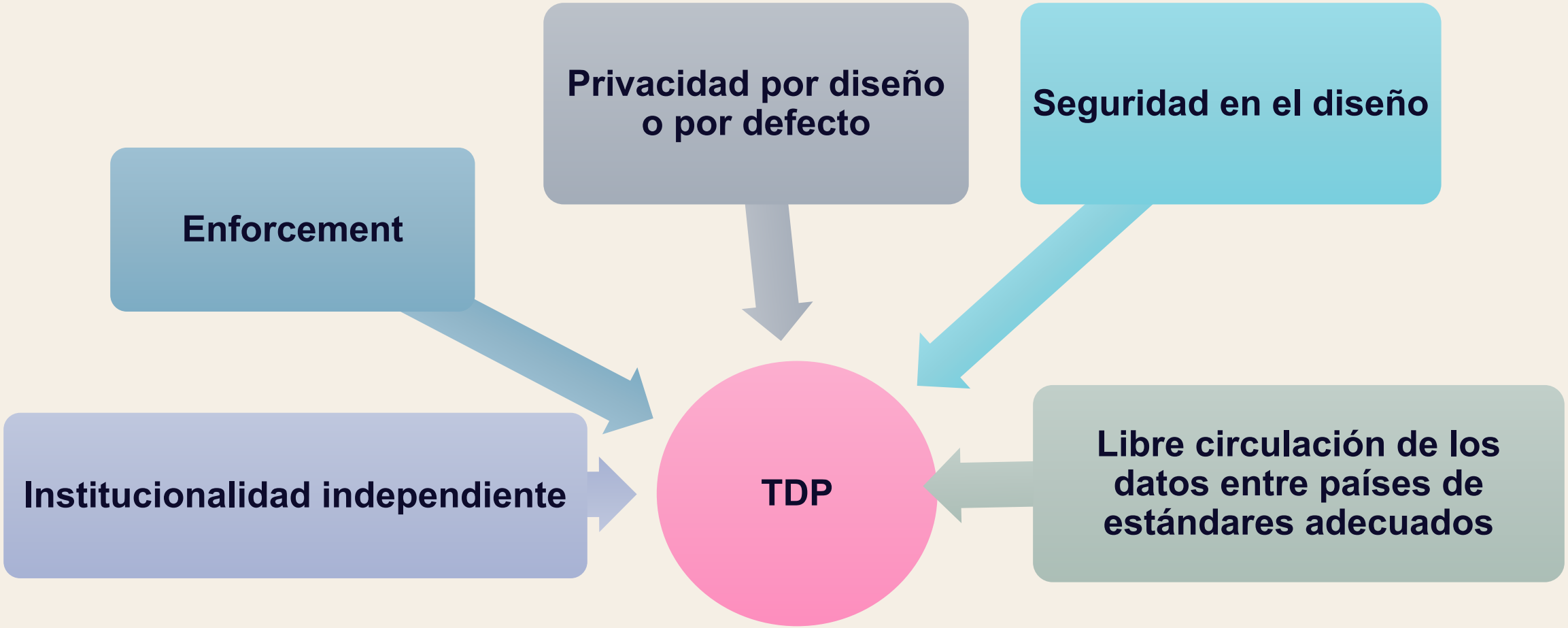
12 meses de amonestación para PYMES

A ESTA FECHA QUEDAN 8 MESES

PARA LA ADECUACIÒN

# DESAFÍOS Y CONSIDERACIONES EN LA IMPLEMENTACIÓN

# Estándares normativos



# RESPONSABILIDAD DEMOSTRABLE

**Protección de datos**

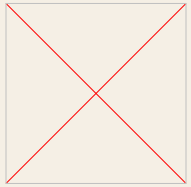
Implementar medidas técnicas y administrativas para asegurar la confidencialidad y seguridad de la información de salud.

**Políticas internas**

Desarrollar y actualizar protocolos internos para el manejo de datos, alineados con la normativa vigente.

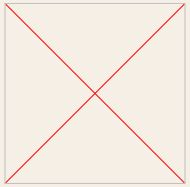
**Capacitación del personal**

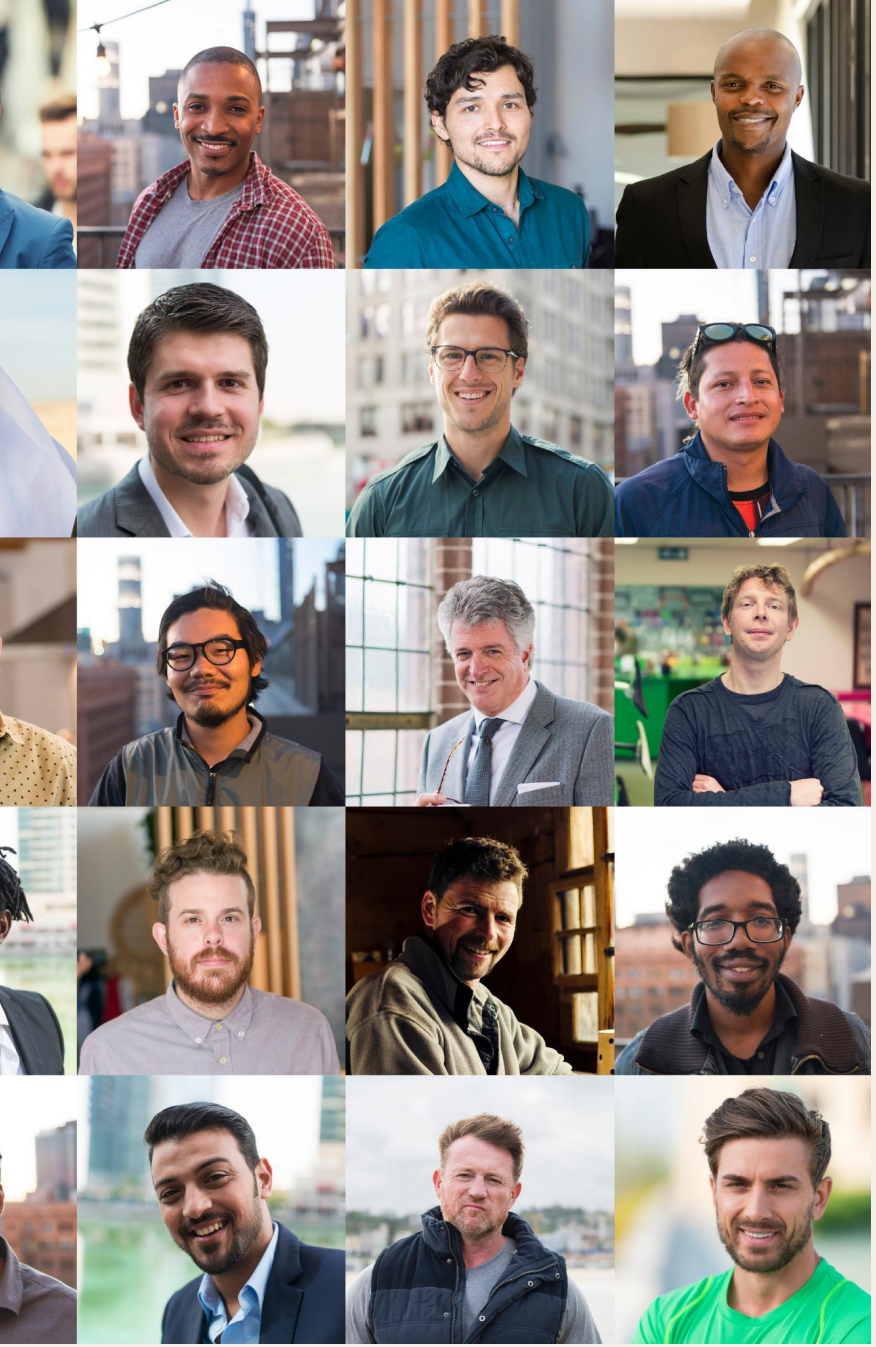
Formar a los empleados en buenas prácticas de privacidad y respuesta ante incidentes de seguridad.



**Respuesta ante incidentes**

Actuar rápidamente ante vulneraciones, notificando a las autoridades y a los pacientes afectados.





# FACTORES CRÍTICOS DE ÉXITO DEL PROCESO DE ADAPTACIÓN

**Conocer las actividades de tratamiento de datos**

**Implementar los Principios del tratamiento de Datos**

**Implementar mecanismos de supervisión y control**

**Capacitación Continua multicapa**

# DOCUMENTACIÓN Y RECURSOS REQUERIDOS

| | |
|---|---|
| **Documentación precisa** | Inventario de datos personales |
| **Recursos humanos** | Roles y funciones claves internos |
| | Normalización de relación con proveedores |
| **Recursos tecnológicos** | Contar con herramientas que permitan implementar la ley |

# IMPACTO ESPERADO Y PRÓXIMOS PASOS

# MECANISMOS DE SEGUIMIENTO Y EVALUACIÓN

## Registro de actividades de tratamiento

- Análisis detallado y documentado de los tratamientos de datos que realiza la organización

## Comités de supervisión

- Equipo de trabajo destinado a impulsar y supervisar la implementación y cumplimiento de la ley.

## Auditorías periódicas

- Trabajo con expertos para asegurar la transparencia y correcto desarrollo de las actividades.

## Reportes de avance

- Se elaboran reportes de progreso para evaluar resultados y hacer ajustes necesarios a tiempo.

# DATOS PERSONALES

Los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

- Sensibles
- Datos Económicos (especialmente protegidos)
- Datos personales a secas

**Datos provenientes del cuerpo humano**

- Muestras biológicas
- Datos biométricos
- Lectura de sensores quirúrgicos invasivo

**Datos económicos**

- Datos Bancarios
- Integración de sociedades
- Comportamientos de pago y morosidades
- Riesgo Comercial
- Facturación
- Giro comerrial

**Datos laborales**

- Profesión u oficio
- Fuente laboral
- Empleador
- Remuneración

**Hábitos**

- Trayectos
- Rutinas, Hobbies, hábitos alimentarios

**Datos de identidad**

- Nombre
- Dirección
- Datos de contacto: teléfono, correo electrónico

**Datos de salud**

- Historia clínica
- Documentos sanitarios:
  - Recetas, resultados de exámenes, licencias médicas

# DATOS PERSONALES ESPECIALMENTE PROTEGIDOS

**Datos personales sensibles.**

- Aquellos datos personales cuyo tratamiento podría dar lugar a discriminaciones arbitrarias en contra de la persona del titular.
  - Pretende ser una enumeración cerrada, pero no lo lograron totalmente
  - Recoge la protección de la persona contra los sesgos y prejuicios generalmente presentes en las sociedades.
  - Datos sobre ideologías, creencias, afiliaciones sindicales
  - Datos de salud, perfil biológico, perfil genómico

**Datos personales sujetos a regímenes especiales de tratamiento**

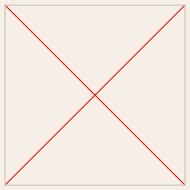
- Datos personales que no son sensibles, pero tienen un régimen especial de tratamiento.
  - Datos económicos, bancarios, financieros y comerciales
    - Su tratamiento queda a los principios de tratamiento de datos personales.
    - Obligación de utilizar información objetiva en la evaluación de riesgos comerciales.
    - Prohibición de comunicar deudas en determinadas circunstancias
  - Datos relativos a sanciones penales y administrativas
    - Tratamiento de datos por organismos públicos
    - Prohibición de comunicar nominativamente sanciones extinguidas por cualquier causa
  - Datos personales de Niños, Niñas y Adolescentes

# DATOS SENSIBLES Y ALCANCE

## Categorías de Datos Sensibles

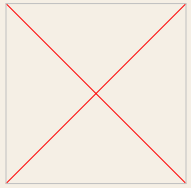
Salud física y mental, creencias u otros datos que afectan la intimidad.

## Alcance Jurídico



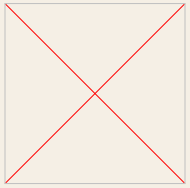
Define protocolos de almacenamiento, acceso y uso bajo exigencias legales.

## Medidas de Protección



Consentimiento explícito y resguardos reforzados para su tratamiento.

## Acceso por Terceros



Solo terceros autorizados, bajo condiciones estrictas y trazabilidad.

# MEDIDAS PARA ASEGURAR EL CUMPLIMIENTO

**Protocolos de seguimiento**

Protocolos para monitorear el cumplimiento y detectar riesgos oportunamente.

**Capacitaciones continuas**

Capacitaciones constantes para asegurar el conocimiento y aplicación correcta de la ley.

**Comunicación efectiva**

Mecanismos claros para una comunicación fluida y efectiva entre los equipos.

# IMPLEMENTAR PROTECCIÓN DESDE EL DISEÑO Y POR DEFECTO

Deber de aplicar medidas técnicas y organizativas adecuadas desde el diseño con anterioridad y durante el tratamiento de los datos personales, teniendo en consideración:

- El estado de la técnica;
- los costos de implementación;
- la naturaleza, ámbito, contexto y fines del tratamiento de datos; y
- los riesgos asociados a dicha actividad.
- Probabilidad y gravedad variables para los derechos de los titulares

Las medidas aplicar deben garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales específicos y estrictamente necesarios para dicha actividad, considerando

- el número de datos recogidos
- la extensión del tratamiento
- el plazo de conservación y
- su accesibilidad

# CONSENTIMIENTO INFORMADO

**01**

**Información al Titular**

Explicar finalidad y alcance del uso de datos.

**02**

**Obtención del Consentimiento**

Entregar el formato claro y completo.

**03**

**Resolución de Dudas**

Aclarar preguntas antes de decidir.

**04**

**Decisión Libre**

Aceptar o rechazar sin presión.

**05**

**Registro del Consentimiento**

Documentar fecha, alcance y evidencia.

**06**

**Revisión Periódica**

Confirmar vigencia y actualizar cambios.

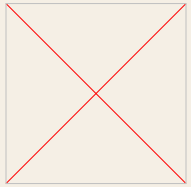
# SEGURIDAD DE REGISTROS

## Encriptación

Convierte los datos en información ilegible para terceros, asegurando la confidencialidad.

## Control de Accesos

Define autenticación y permisos por rol, limitando quién ve o modifica registros.



## Monitoreo en Tiempo Real

Detecta y alerta ante actividades sospechosas, reduciendo fugas y accesos no autorizados.

## Normas Internacionales

Alineación con estándares como ISO 27001 y HL7 fortalece la seguridad y la interoperabilidad.

# GARANTIZAR UN NIVEL DE SEGURIDAD ADECUADO AL RIESGO

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.”.

## PROCEDIMIENTO DE INCIDENTES

**01**

**Detección**

Identificar rápidamente incidentes mediante monitoreo constante y alertas automáticas.

**02**

**Reporte**

Documentar y comunicar el incidente a responsables internos y externos según protocolo.

**03**

**Mitigación**

Aplicar medidas inmediatas para contener el incidente y limitar daños potenciales.

**04**

**Notificación**

Informar a autoridades y titulares afectados de forma transparente y oportuna.

**05**

**Restablecimiento**

Restaurar sistemas y servicios, asegurando integridad y disponibilidad de los datos.

**06**

**Revisión**

Analizar el incidente para mejorar procedimientos y prevenir futuras vulneraciones.

# 72HRS

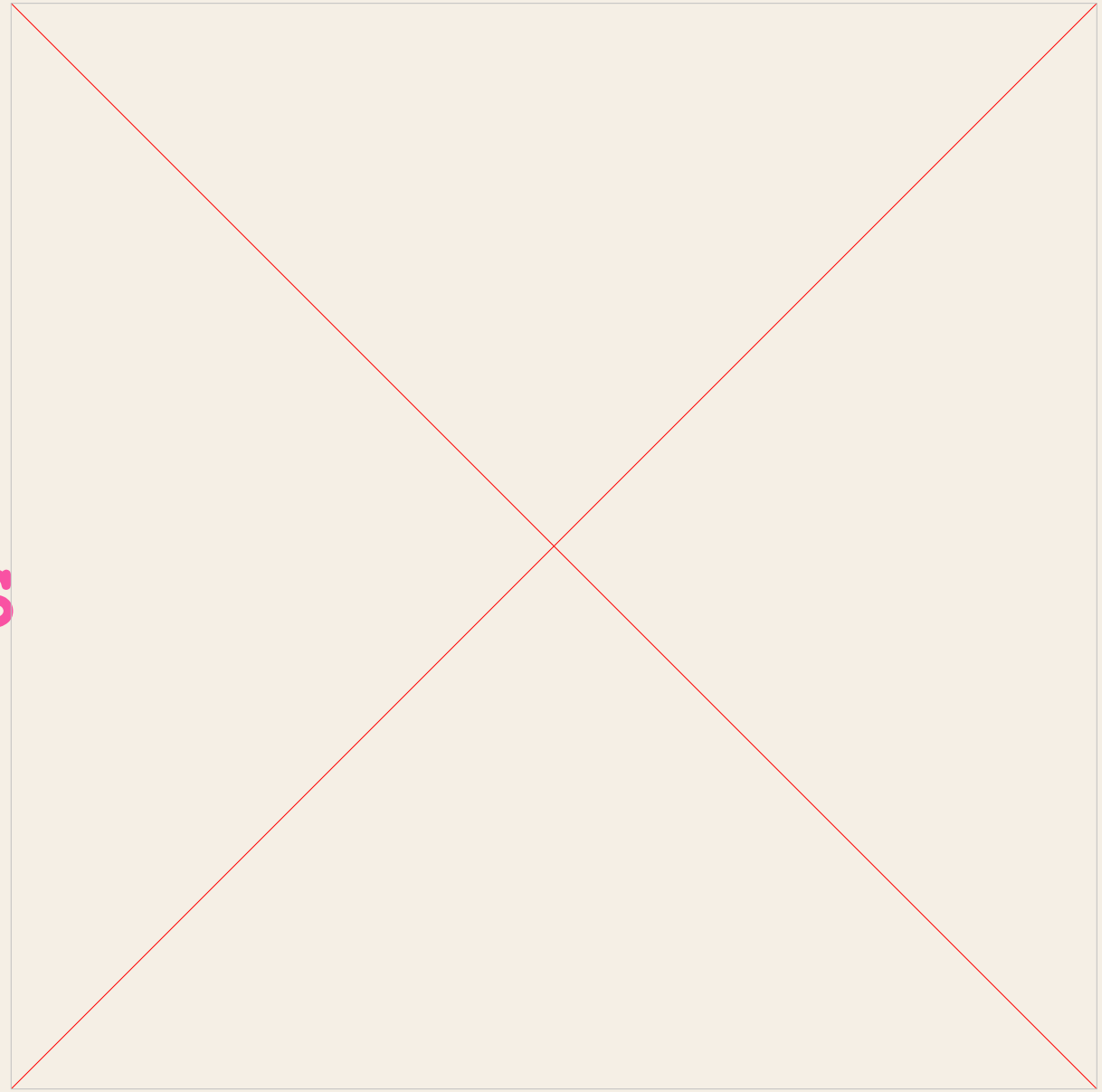
# REALIZAR EVALUACIONES DE IMPACTO EN PROTECCIÓN DE DATOS PERSONALES

Cuando sea probable que un tipo de tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, se pueda producir un alto riesgo para los derechos de las personas titulares de los datos personales, el responsable del tratamiento deberá realizar, previo al inicio de las operaciones del tratamiento, una evaluación del impacto en protección de datos personales.

La evaluación de impacto se requerirá siempre en casos de:

| | | | |
|---|---|---|---|
| a) Evaluación sistemática y exhaustiva de aspectos personales de los titulares de datos, basadas en tratamiento o decisiones automatizadas, como la elaboración de perfiles, y que produzcan en ellos efectos jurídicos significativos. | b) Tratamiento masivo de datos o gran escala. | c) Tratamiento que implique observación o monitoreo sistemático de una zona de acceso público. | d) Tratamiento de datos sensibles y especialmente protegidos, en las hipótesis de excepción del consentimiento. |

# IMPLEMENTAR LOS DERECHOS DE LOS TITULARES DE DATOS PERSONALES



# BENEFICIOS PARA LOS TITULARES DE DATOS

## Facilidades en el ejercicio de derechos

- Los titulares de datos personales tendrán mayores posibilidades de ejercer sus derechos.
- Habeas Data administrativo ante la Agencia

## Mayor cumplimiento normativo

- El régimen infraccional desincentiva el incumplimiento
- Indemnización por daño al titular además de sanción administrativa

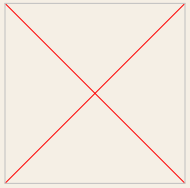
## Claridad en derechos y obligaciones

- Los beneficiarios tendrán información clara sobre sus derechos y responsabilidades bajo la nueva normativa.

# DERECHOS Y DEBERES

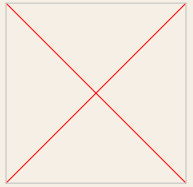
**Derecho de acceso**

¿qué datos de mi persona se tratan en su organización?



**Derecho de rectificación**

Corrección de datos que no respondan a la realidad



**Derecho de oposión**

No deseo que siga tratando los datos que aporté voluntariamente.

**Derecho de supresión**

Elimine los datos que tiene de mi respecto de los que carece de fundamento legal

# OTROS DERECHOS

**Derecho de portabilidad**

¿qué datos de mi persona se tratan en su organización?

**Derecho a la interoperabilidad de los datos de la ficha clínica**

¿qué datos de mi persona se tratan en su organización?

**Derecho de oposición a decisiones automatizadas**

¿qué datos de mi persona se tratan en su organización?

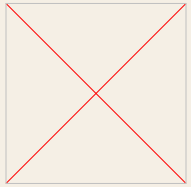
# SUPERVISIÓN Y FISCALIZACIÓN

**Supervisory Functions**

Inspections, sanctions, and institutional guidance.

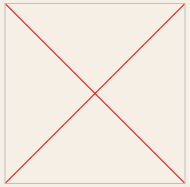
**Observed Compliance Levels**

Higher compliance driven by stricter oversight.



**Areas for Improvement**

Transparency, reporting, and staff training.



**Impact of Oversight**

Stronger protection of sensitive data.

## Revisiones periódicas

- Dado el avance tecnológico requiere evaluaciones constantes para garantizar que la ley se mantenga relevante y efectiva.

## Coordinación regulatoria

- Adecuación normativa en distintas materias es esencial

## Normativa complementaria

- La Agencia deberá dictar las instrucciones que permitan la implementación efectiva por los organismos públicos e instituciones privadas.

DESAFÍOS

# SÍNTESIS

**Avance Administrativo**
La Ley 21.719 representa un progreso fundamental en la modernización de la normative de protección de datos personales

**Implementación Correcta**
Una planificación detallada es esencial para la correcta aplicación de la ley.

**Superación de Desafíos**
Superar obstáculos es clave para lograr los beneficios esperados de la ley.

**Fortalecimiento Economía digital**
La ley fortalece a Chile y lo adecúa a los requerimientos de la Economía Digital