Gestión de datos personales en la empresa

Jessica Matus Arenas
Of Counsel de FerradaNehme y
Directora del Área de Tecnologías.
Directora de Fundación Datos Protegidos y socia en Marco Legal

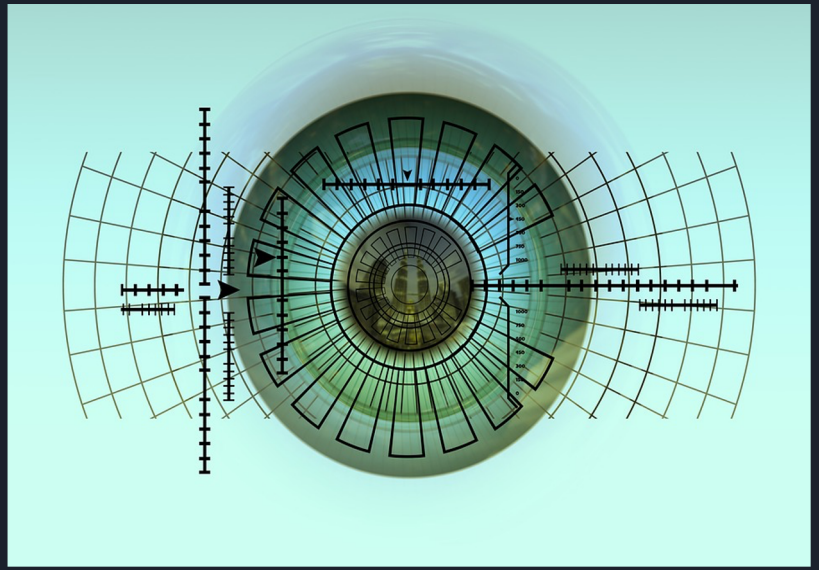
Objetivos

- Detección de riesgos de privacidad o datos personales en el tratamiento

- Principales obligaciones y deberes de los controladores de datos personales:
  - Mínimos de cumplimiento.
  - Herramientas.
  - Datos personales y COVID

¿Qué es la protección de datos?

- La facultad de control de la propia información frente a su tratamiento automatizado o no, en cualquier soporte que permita su utilización: almacenamiento, organización y acceso.
- Es una garantía individual.
- Inherente a todo ser humano.
- No es absoluto, reconoce limitaciones proporcionales:
    - Libertad de Expresión
    - Seguridad
    - Legítimo derecho a “saber”
    - Voluntad de la persona
- Consagrada a nivel supraconstitucional en Tratados Internacionales de Derechos Humanos. En Chile, reforma a la Constitución 2018.



1. Identificar los datos. Clasificar.

Datos de identificación	Nombre
Datos Identificabilidad	RUT. IP. IMEI. Número celular. Biometría. Patentes.
Características personales	Género. Edad. Domicilio.
Académicos y profesionales	Profesión. Grados académicos. Lugar de trabajo. Lugar de estudios.
Información financiera /comercial/patrimonial /tributaria.	Rango de gastos. Remuneración. Información de propiedades y bienes.
Datos transaccionales	Conexiones. Datos de navegación. Metadata Datos de trafica y localización.
Datos sensibles	Datos de salud. Datos referidos a política, religión, etnia. Datos de menores de edad

2. Identificación de procedencia de los datos

- Directo del titular
- De encuestas, entrevistas, formularios, de procesos automatizados
- De un tercero.
- De una cesión.
- De una fuente pública

3. Identificar habilitantes del tratamiento

- Interés legítimo. Ej. contrato bancario o telefónico y envío de publicidad.
- Cumplimiento de un contrato o precontrato de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.
- Autorización legal expresa.
- Interés vital.
- Fuente de acceso público.
- Consentimiento.

4. Obligaciones asociadas a la procedencia

- Consentimiento.
- Información a los titulares. Transparencia
- Política de privacidad.
- Términos y condiciones. Mecanismos para derechos ARCO

Transparencia de la información:

- Se toman medidas para facilitar al interesado toda la información relativa al tratamiento
- La información se facilita de forma concisa, transparente e inteligible
- La información se facilita en lenguaje claro y sencillo
- Se facilita por escrito o por otros medios, incluidos los electrónicos
- Se facilita verbalmente, previa acreditación de su identidad
- Se facilita al interesado el ejercicio de sus derechos.

- Se facilita la identidad y los datos de contacto del responsable y, en su caso, del representante cuando se solicitan datos
- Se facilitan los datos de contacto del delegado de protección de datos
- Se facilitan los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento
- Se facilita información sobre el interés legitimo
- Se informa sobre los destinatarios o las categorías de destinatarios
- Se informa del plazo de conservación de los datos personales o los criterios utilizados para determinarlo
- Se informa sobre la existencia del derecho a solicitar el acceso, rectificación o supresión, la limitación del tratamiento, a oponerse y el derecho a la portabilidad
- Si el tratamiento se basa en el consentimiento se informa de la existencia del derecho a retirarlo en cualquier momento
- Se informa del derecho a presentar una reclamación ante una autoridad de control
- Se informa de las cesiones basadas en requisitos legales o contractuales
- Se informa de las cesiones basadas en un requisito necesario para suscribir un contrato
- Se informa de la existencia de decisiones automatizas, elaboración de perfiles, sobre la lógica aplicada, la importancia y consecuencias previstas del tratamiento
- Antes de realizar tratamientos de datos personales para una finalidad distinta de la que fueron recogidos, se informa al interesado y la información abarca esa otra finalidad y cualquier otra información pertinente

5. Identificación de roles internos

Titulares de datos

Responsables

Responsable de Seguridad CISO

Responsable de Datos DPO

Encargados y sub-encargados

Intermediarios

Trabajadores

Roles y perfiles

6. Aplicación de reglas: ¿Cómo se debe hacer? Principios de la protección de datos

Identificación del tipo de dato

Licitud
Finalidad
Minimización de datos
Calidad
Temporalidad
Mecanismos de control e información
Transparencia
Confidencialidad
Seguridad
Proporcionalidad (necesidad y pertinencia)
Responsabilidad

Equifax: 143 millones de registros.
- Bajó la acción de 141 a 89 USD.
- 5,8 billones de USD en pérdidas
- Impacto del 30 o 35% menos

7. Evaluar los riesgos y las medidas de seguridad a invertir

La seguridad son las **medidas técnicas y de organización** adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, cualquiera sea el método de tratamiento, particularmente a través de las redes de comunicación.

Sujetos obligados:

- Responsable
- Encargado del tratamiento
- Intermediarios
- Quiénes trabajan con los datos

Medidas laborales de resguardo interno:

Cláusulas contractuales y sanciones asociadas.

Acuerdos de confidencialidad

Perfiles y permisos de acceso documentados.

Políticas de seguridad conocidas

Obligaciones al término del contrato

Planes de formación y capacitación.

Otras herramientas imprescindibles:

Evaluación de impacto en protección de datos (PIAs)

ejercicio de análisis PREVIO de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos

Privacy by Design

Implica utilizar un **enfoque** orientado a la **gestión del riesgo** y de **responsabilidad proactiva** para establecer **estrategias** que incorporen la **protección de la privacidad** a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso).

Debate datos personales y privacidad COVID19

Tratamiento de la información **personal** y **sanitaria**

BD solicitantes de IMG

Filtración mapas

georeferenciación de contagiados

CoronApp

Comisaría Virtual

Detención vecino haitiano

Biometría

En la vía pública

En lugares de trabajo

En servicios de atención de salud

Rastreo de contacto/**movilidad** de personas

Relación privacidad - nuevas tecnologías

Privacy by Design o Privacidad desde el diseño.

Apps monitoreo - Notificación de exposición. Apple Google.

Centralización y descentralización.

Problemáticas.

Debate datos personales y privacidad COVID19

- La información sobre la **movilidad de personas**, sus antecedentes sanitarios o la obtención de la temperatura corporal.
- **Medidas laborales**: la realización de test, controles de temperatura, recabar datos de trabajadores sobre pertenencia a grupos de riesgo o el teletrabajo plantean una serie de cuestiones técnicas, jurídicas, organizativas e incluso sociales que requieren de un continuo análisis y nos sitúan ante una nueva etapa en la que los datos personales han de ser especialmente protegidos
- La incorporación de sedes electrónicas y la telematización de procedimientos administrativos o las nuevas formas de prestación de servicios como la teleasistencia van incrementando los datos personales que se manejan y por medios cada vez más sofisticados.

Muchas gracias.

jmatus@fn.cl
@srtamatus