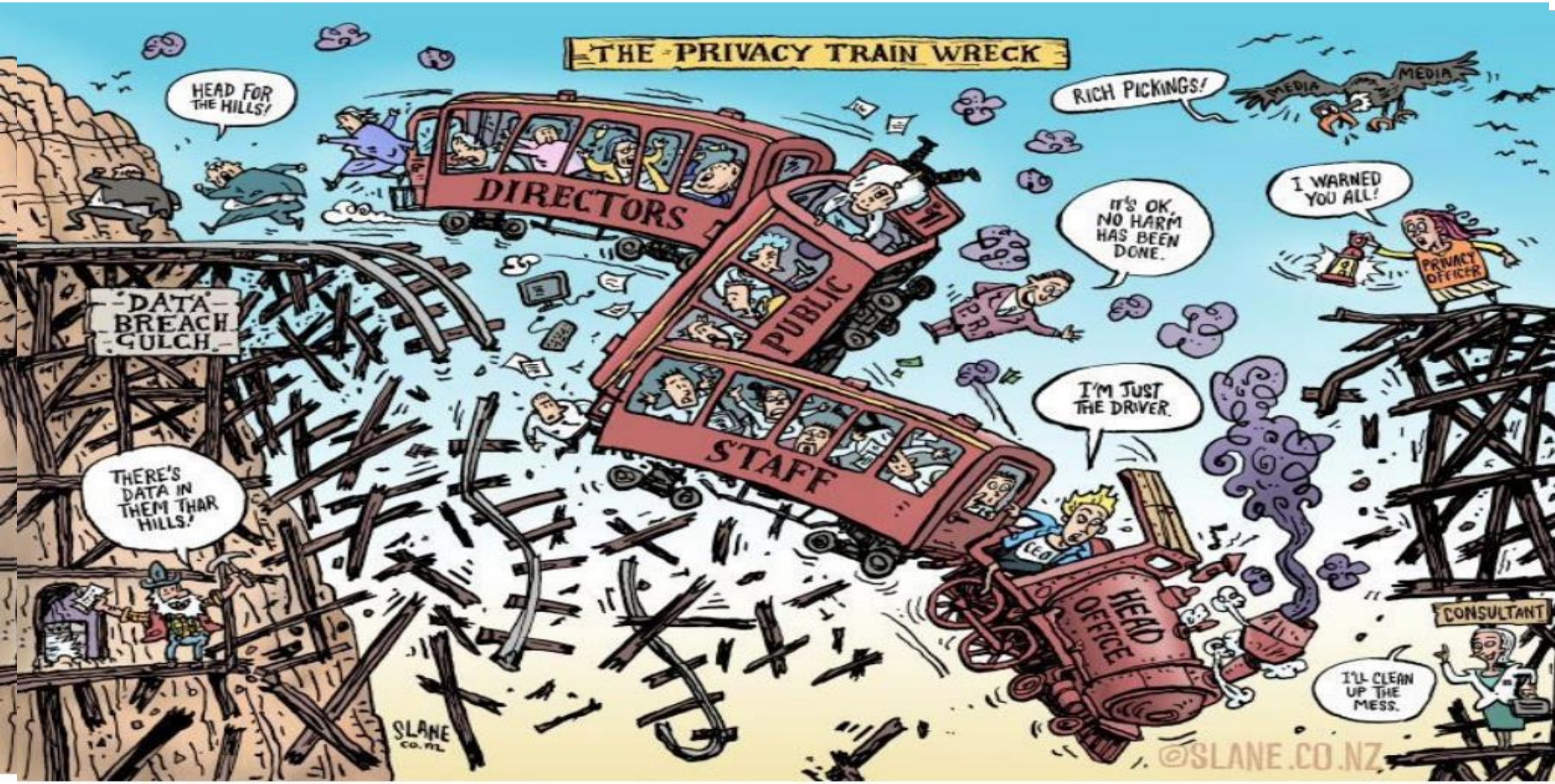
BERMÚDEZ • DURANA
ASOCIADOS

# *Rol de los profesionales de PD y efectividad del Programa de Protección de Datos*

**José Alejandro Bermúdez**
***Socio y ex-Superintendente Delegado de Protección de Datos (SIC)***

**RIPD – Montevideo, 14 de noviembre de 2019**


THE PRIVACY TRAIN WRECK
HEAD FOR THE HILLS!
DIRECTORS
PUBLIC
STAFF
RICH PICKINGS!
MEDIA
MEDIA
I WARNED YOU ALL!
PRIVACY OFFICER
IT'S OK, NO HARM HAS BEEN DONE.
I'M JUST THE DRIVER.
DATA BREACH GULCH
THERE'S DATA IN THEM THAR HILLS!
HEAD OFFICE
CEO
CONSULTANT
I'LL CLEAN UP THE MESS.
SLANE CO.NZ
©SLANE.CO.NZ

Entienda el

***¿Quién? ¿Qué? ¿Cuándo? ¿Dónde? ¿Por qué? ¿Cómo?***

**de sus prácticas de uso de datos**

BERMÚDEZ • DURANA
ASOCIADOS

# Área de Protección de Datos/Oficial de Protección de Datos

El oficial de protección de datos entiende:

- Las **normas** aplicables
- **Contexto** del tratamiento
- **Riesgos** para los titulares, la organización y terceros
- Control y documentos que se usarán como **evidencia** a lo largo de toda la organización, y
- **Historia**: cómo han sido implementadas y mantenidas las medidas a lo largo del tiempo

## ¿Qué debe incluir mi programa?

Cuatro componentes esenciales:

- **Compromiso** de la Gerencia
- **Controles** internos
- **Evaluación y monitoreo**
- **Documentación** para demostrar que el programa se ha implementado

# # 1 Compromiso

**Un programa exitoso requiere un compromiso desde la Gerencia. Si los directivos se la juegan por las Buenas Prácticas, el programa será exitoso**

Este compromiso implica designar a alguien como líder interno de protección de datos, destinar recursos para apoyarlo y mantener permanentemente informado a la Gerencia

# # 2 Controles

**¿Qué son los controles?**

Todas aquellas prácticas que vuelven operativo mi programa: *Procedimientos, Políticas, Inventarios de Datos, Sistema de Gestión de Riesgos, Educación y capacitación para el personal, protocolos de incidentes, contratos con terceros (proveedores por ejemplo), Mecanismos de comunicación*

# # 3 Evaluación y revisión continua

**De nada me servirá haber implementado buenas prácticas, si estas están desactualizadas.**

Una organización responsable está pendiente de todas aquellas novedades (legislativas por ejemplo) que puedan impactar su negocio para asegurarse que su programa no pierda vigencia

# # 4 Demostración y documentación

El principio de responsabilidad demostrada (*accountability*) se basa en la **implementación de buenas prácticas que se ajusten a las necesidades de mi organización** y mi **capacidad para demostrar** (con documentos) **que las he implementado**

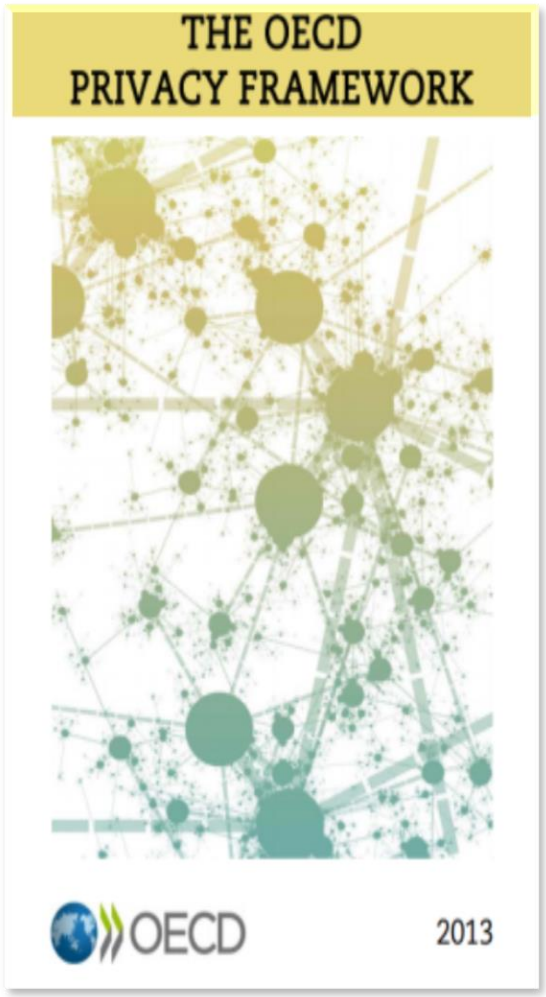
# Estructura de un Programa

**Parte A – Elementos fundamentales de un programa**

1. **Gobernanza y compromiso**
   a. Compromiso y respaldo de la alta dirección
   b. Área de protección de datos y/o Oficial de Protección de Datos
   c. Reportes
2. **Controles del programa**
   a. Inventario de datos personales
   b. Políticas
   c. Herramientas de evaluación y gestión de riesgos
   d. Entrenamiento y educación
   e. Manejo de incidentes
   f. Gestión de encargados
   g. Comunicación

**Parte B – Revisión y seguimiento continuo**

a. Desarrolle un plan de seguimiento y revisión
b. Monitoree y revise los controles del programa




BERMÚDEZ • DURANA
ASOCIADOS

# Guía para la implementación del principio de responsabilidad demostrada (2015)

**“El Oficial de privacidad tendrá la labor de estructurar, diseñar y administrar el programa que permita a organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente”**

Actividades concretas

- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales
- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales
- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales
- Impulsar una cultura de protección de datos dentro de la organización

# Guía para la implementación del principio de responsabilidad demostrada (2015) (II)

Actividades concretas (*continuación*)

- Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo
- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC
- Obtener las declaraciones de conformidad de la SIC cuando sea requerido
- Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia
- Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales

# Guía para la implementación del principio de responsabilidad demostrada (2015) (III)

Actividades concretas (*continuación*)

- Realizar un entrenamiento general en protección de datos para todos los empleados de la compañía
- Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización
- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers y gestión de proveedores, etc.)
- Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos
- Requerir que dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales

# Guía para la implementación del principio de responsabilidad demostrada (2015) (IV)

Actividades concretas (*continuación*)

- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal
- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio
- Realizar seguimiento al Programa Integral de Gestión de Datos Personales

# Sanciones recientes

**“Las herramientas o procesos inútiles no son consistentes con las exigencias de la regulación colombiana” (SIC- Dirección de Investigaciones de Protección de Datos)**

- (i) Evitar que se repitan hechos como los sucedidos
- (ii) Respetar y garantizar los derechos de los titulares
- (iii) Dar cumplimiento estricto a la ley
- (iv) Aplicar el principio de responsabilidad demostrada con especial énfasis en los mecanismos de monitoreo y control
- (v) Hacer efectivo el pleno respeto de los derechos de los titulares

# Sanciones recientes (2)

## Hitos de las resoluciones recientes:

- **Responsabilidad de los administradores**: no se han presentado sanciones a administradores dentro de las investigaciones pero la Delegatura ya ha reseñado el artículo 24 de la Ley 222 de 1995 sobre presunción de culpa de los administradores "*en los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos*". Adicionalmente, trae a colación que los administradores jurídicamente responden "*solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros*".

# Sanciones recientes (3)

**Hitos de la resolución**

- **Implementación del principio de responsabilidad demostrada**: En línea con las Guías de 2015 se debe (i) Diseñar y poner en marcha un PIGDP, (ii) desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP y (iii) Demostrar el debido cumplimiento.
- **Menos retórica y más acción**: acciones concretas de la administración. Compromiso real y sobre todo proveniente de la alta dirección.
- **Implementación de un sistema de control de riesgos:** que les permita a los responsables identificar, medir controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos.
- **"No es buena práctica ni puede tolerarse que el titular del datos deba rogar e insistir varias veces (…) para que se respeten sus derechos**".

# GRACIAS

BERMÚDEZ • DURANA
ASOCIADOS