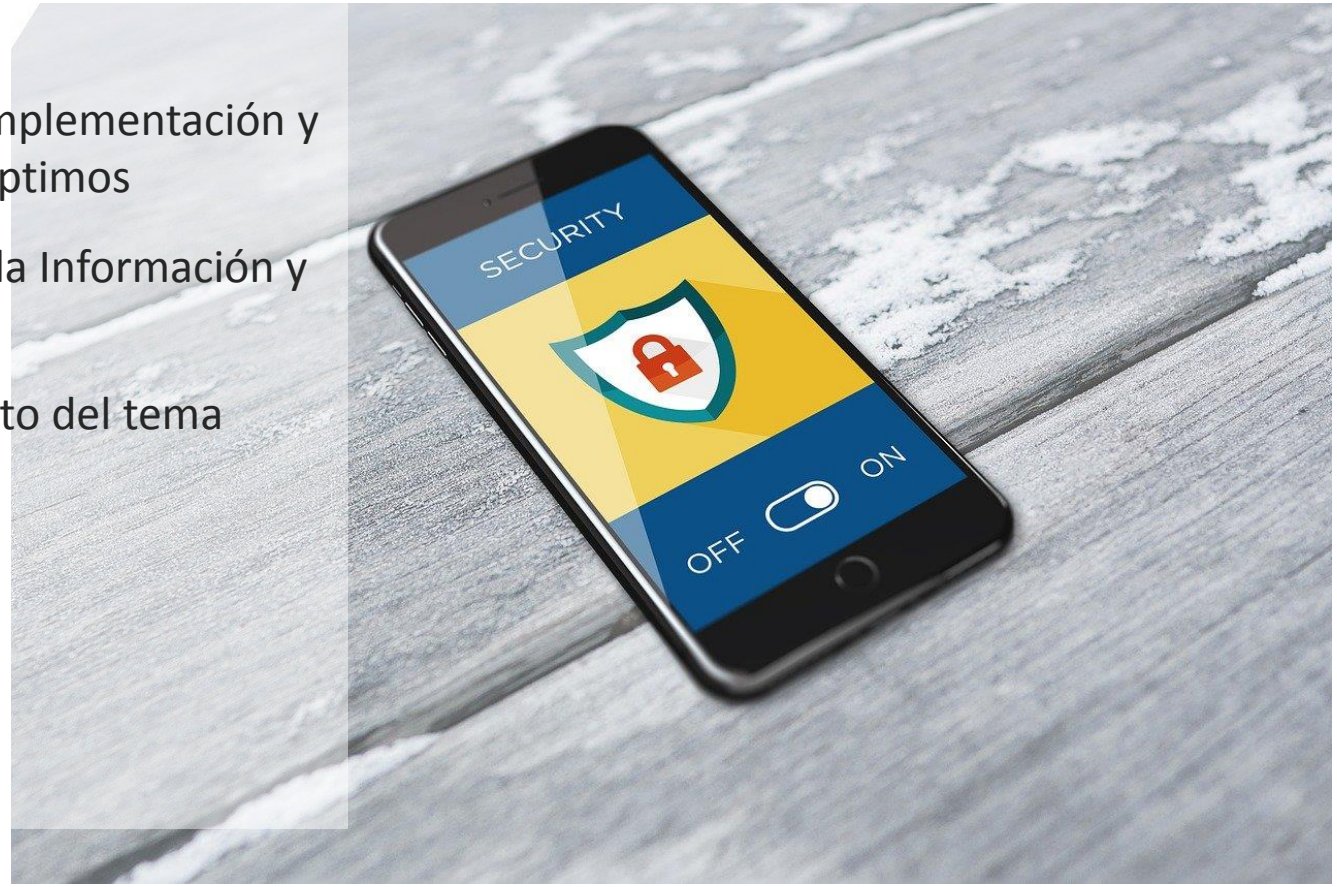
Protección de Datos Personales: un desafío para las organizaciones

Junio 2020

Objetivos

1. Lograr un mejor entendimiento respecto a la naturaleza e impacto de este tipo de normativa
2. Analizar los pasos a seguir para lograr una implementación y aseguramiento de cumplimiento continuo óptimos
3. Analizar el impacto mutuo en Seguridad de la Información y CyberSecurity
4. Aumentar el nivel de concientización respecto del tema



Temas

Track 1 Aspectos operativos y de gestión que hacen a la implementación de una Ley de Protección de Datos

Track 2 Antecedentes en la región: Ley de Protección de Datos Personales en Argentina

Track 3 Principales consideraciones desde el punto de vista de Seguridad y CyberSecurity a tener en cuenta

Track 1

Aspectos operativos y de gestión que hacen a la implementación de una Ley de Protección de Datos

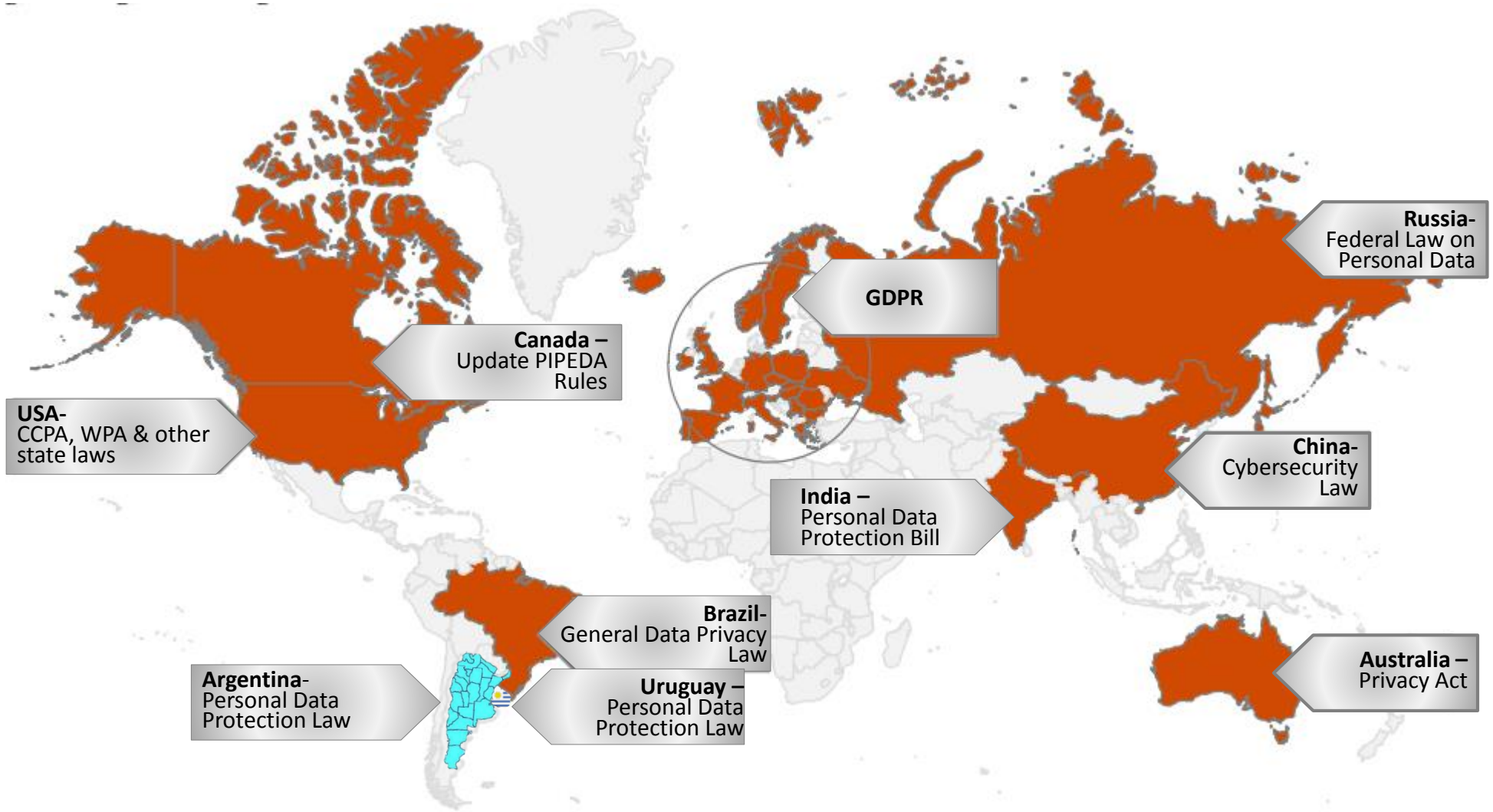
Contexto

- La digitalización ha impactado en el comportamiento de las organizaciones y la sociedad
- Línea difusa entre lo privado y lo público en las redes
- Cada vez se recolecta y procesan más datos personales
- El aumentado el valor de los datos y los riesgos asociados a su uso y gestión, requiere de un enfoque para garantizar la privacidad más estratégico y menos de Cumplimiento
- La sociedad y los gobiernos son cada vez más sensibles y críticos frente a esto
- Las organizaciones no están preparadas para tomar decisiones ágiles en torno a la privacidad: “Riesgo de Reticencia”

La protección de datos personales juega un papel cada vez más relevante en las organizaciones, bajo la presión de la sociedad y los gobiernos

Más allá de los aspectos de cumplimiento, garantizar la privacidad es un instrumento para que las organizaciones fortalezcan su reputación y satisfagan a clientes e inversionistas

Tendencias…

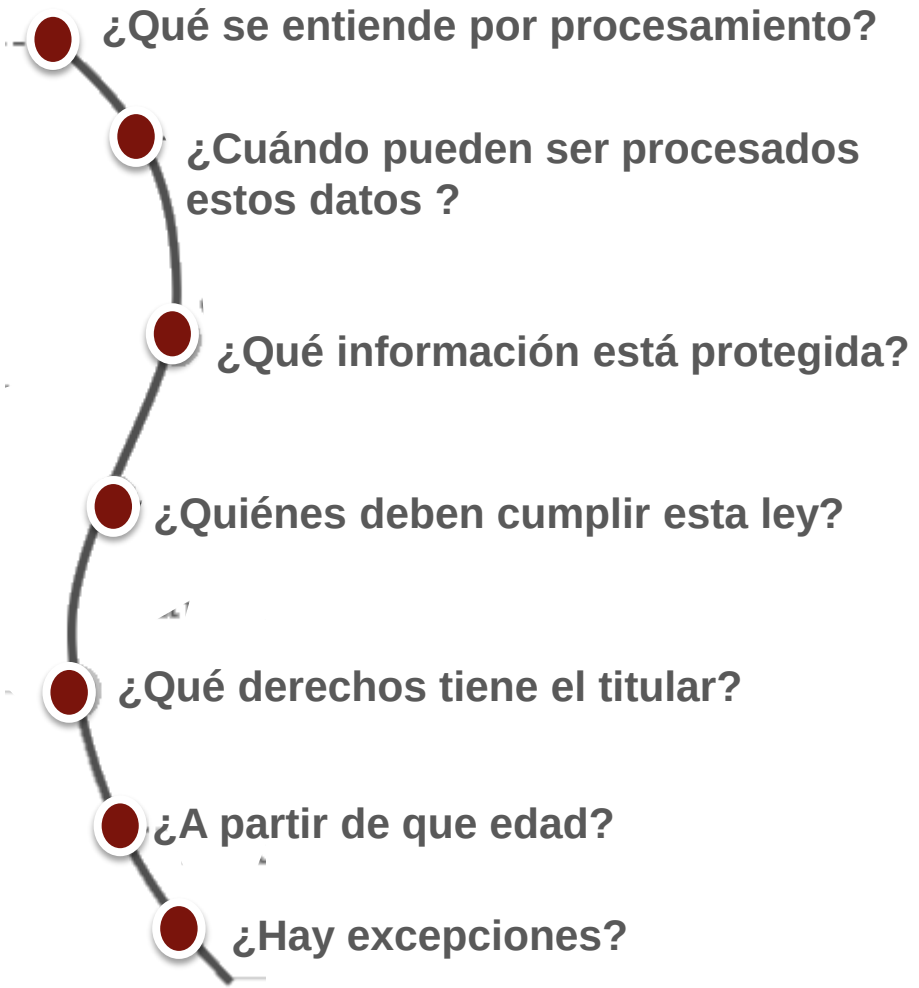

Russia- Federal Law on Personal Data
GDPR
Canada – Update PIPEDA Rules
USA- CCPA, WPA & other state laws
China- Cybersecurity Law
India – Personal Data Protection Bill
Brazil- General Data Privacy Law
Argentina- Personal Data Protection Law
Uruguay – Personal Data Protection Law
Australia – Privacy Act

GDPR

- Proteger los derechos de las personas naturales respecto del procesamiento e intercambio de sus datos personales
- Aplica a organizaciones europeas y no europeas que procesan datos de ciudadanos de CE
- Armonizar todas las leyes de la CE respecto de la protección de datos personales

¿Qué implica?

- Mantener control continuo sobre dónde, cómo y quién procesa datos personales
- Guardar evidencia al respecto (procesamiento, estructura de gobierno y responsabilidades)
- Nombrar un Oficial de Protección de Datos (DPO)
- Realizar un Data Protection Impact Assesment (DPIA) e instrumentar las medidas de respuesta que corresponda
- Procesar los datos personales en línea con todo lo anterior
- Reportar brechas de cumplimiento (72 hrs)
- Poder ampliar la información respecto del incidente



Aspectos en que varían estos enfoque …

Recolección y acceso de Datos

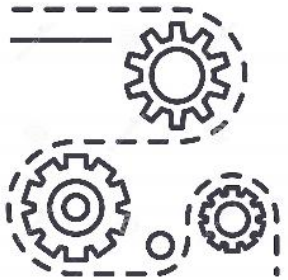
- Recopilación de información personal
- Actividades / responsabilidades del Data Controller
- Transferencias internacionales de datos
- Tratamiento de datos personales sensitivos, clientes, empleados, pacientes, etc.
- Localización de Servidores y datos

Terceras Partes

- Acuerdos con proveedores y procesadores de datos; y garantías obligatorias
- Requisitos de Seguridad

Derechos Individuales

- Gestión del consentimiento del sujeto
- Requisitos de notificación y divulgación
- Programas de privacidad

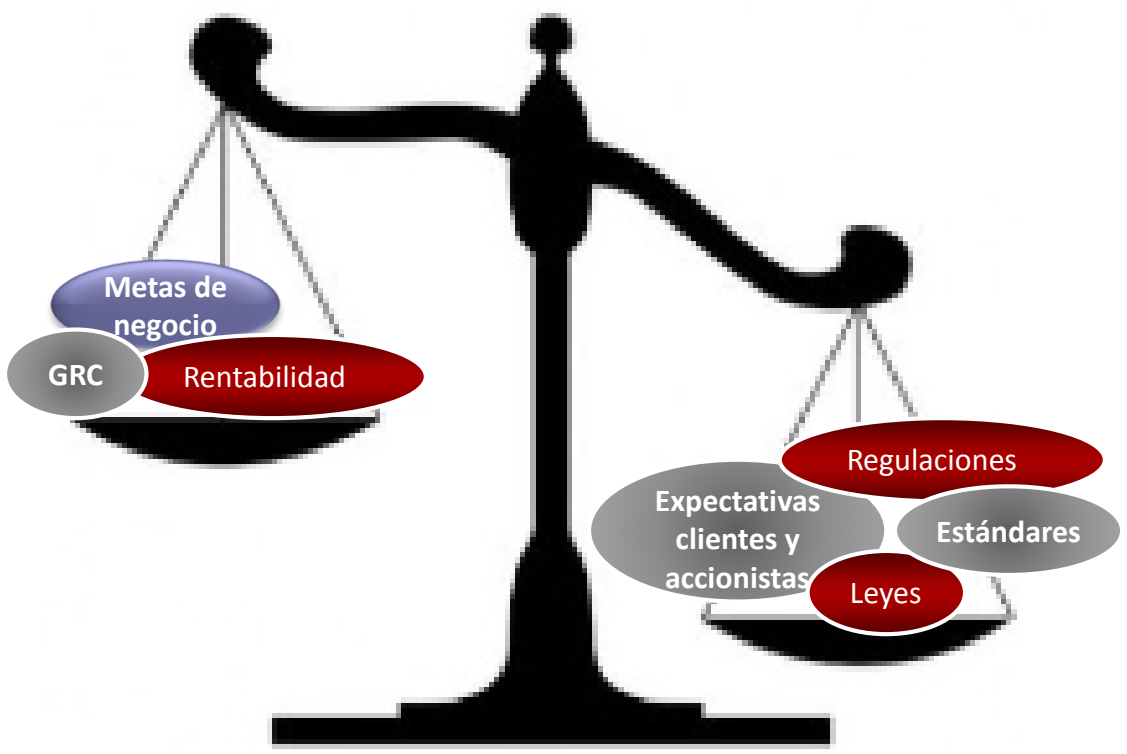


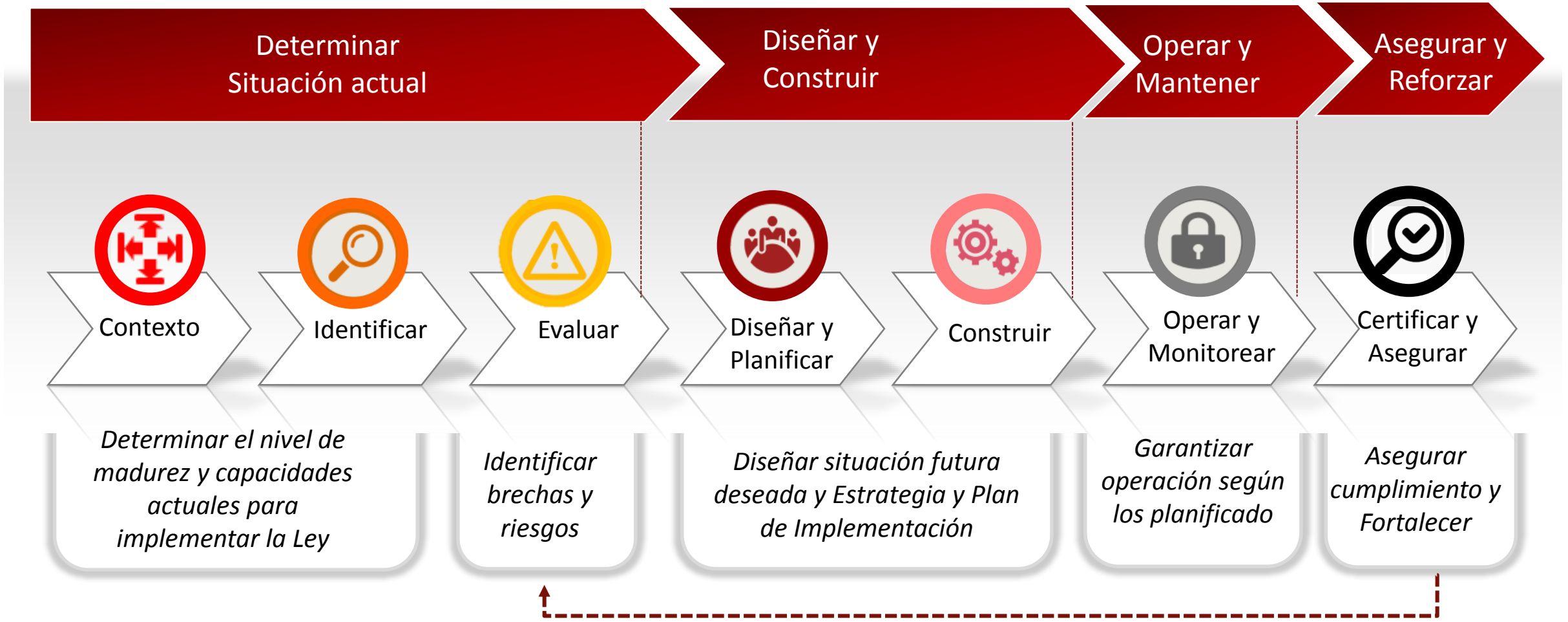
Procesamiento de Datos

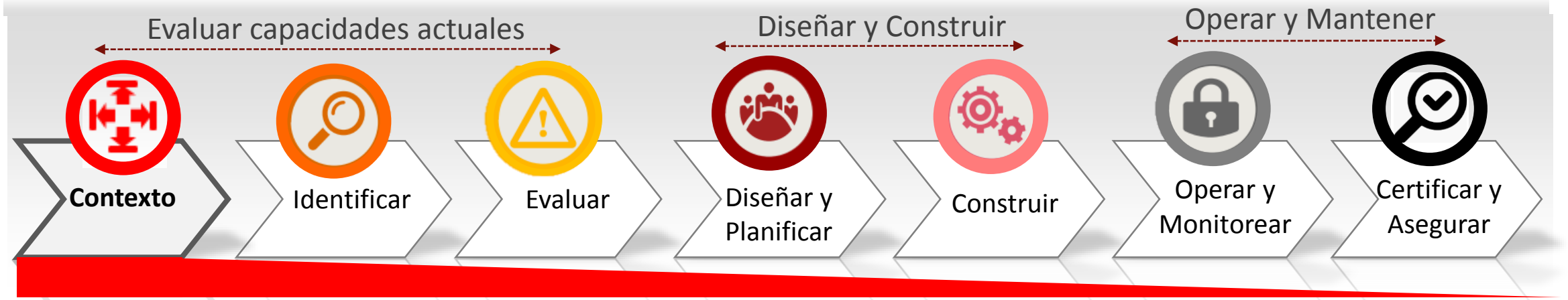
- Enfoque “Sectorial” Vs. “Omnibus”
- Jurisdicción y Territorialidad
- Necesidad de notificar las brechas de seguridad
- Obligaciones asociadas a la retención de datos
- Seguimiento en línea y actividad del DPO

Estrategias de implementación

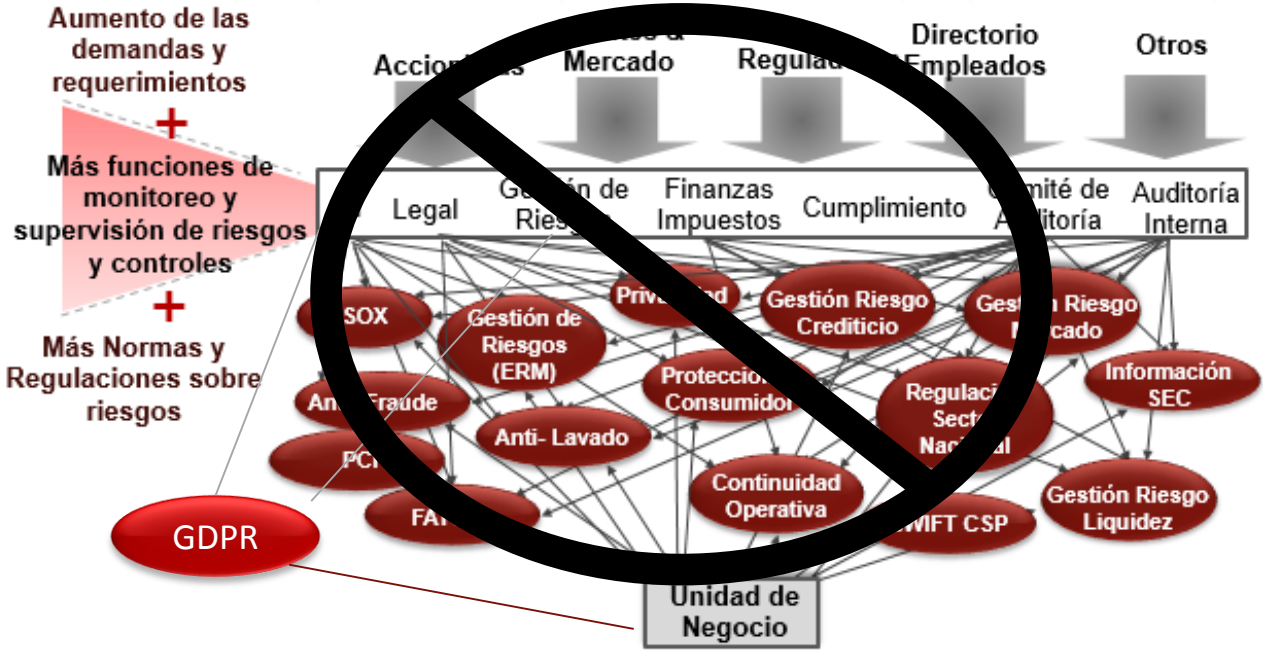
- Depende de los objetivos del negocio y las características /definiciones de Riesgo y Cumplimiento de la organización (Ej.: Apetito y Tolerancia al riesgo)
- Se podría considerar como un requisito de cumplimiento legislativo más, y sentirnos tentados de seguir los pasos habituales en forma lineal; pero dado que no hay mucha guía respecto de cómo priorizar asuntos a tratar, se podría ser ineficientes
- Las estrategias y plan de implementación son elementos a tener en cuenta como evidencia de cumplimiento, por lo que deben ser de calidad.

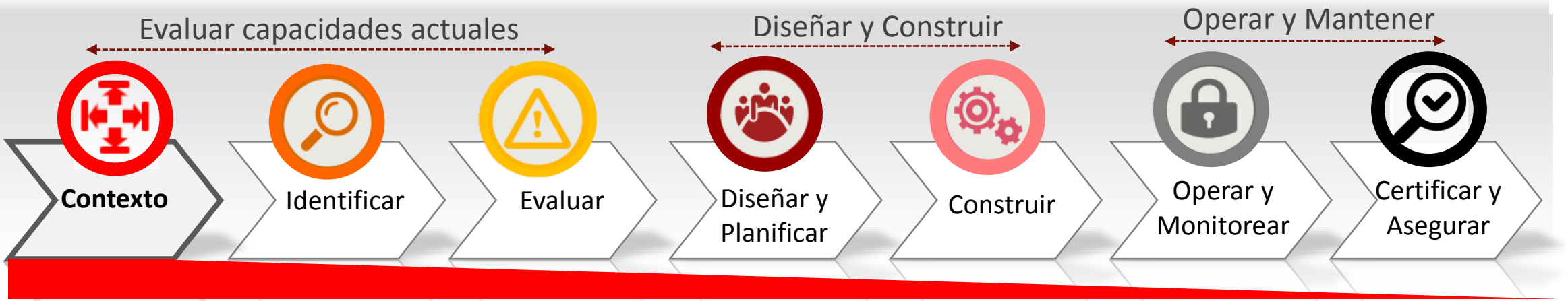



Determinar Situación actual
Diseñar y Construir
Operar y Mantener
Asegurar y Reforzar
Contexto
Identificar
Evaluar
Diseñar y Planificar
Construir
Operar y Monitorear
Certificar y Asegurar
Determinar el nivel de madurez y capacidades actuales para implementar la Ley
Identificar brechas y riesgos
Diseñar situación futura deseada y Estrategia y Plan de Implementación
Garantizar operación según los planificado
Asegurar cumplimiento y Fortalecer

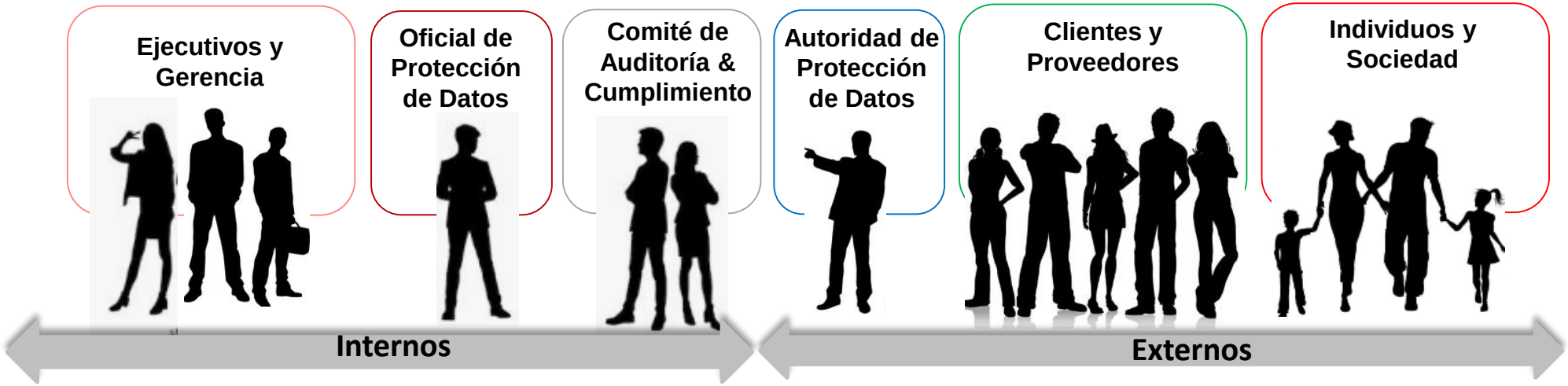


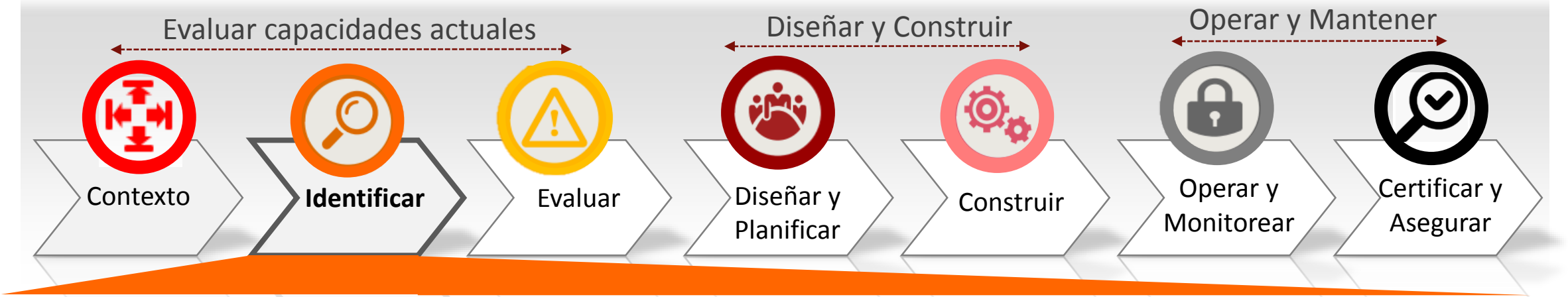
- Integrar requisitos de cumplimiento
- Revisar Tolerancia y Apetito al Riesgo, fórmula de cálculo de Exposición y metodología de análisis de riesgos
- Definir visión compartida



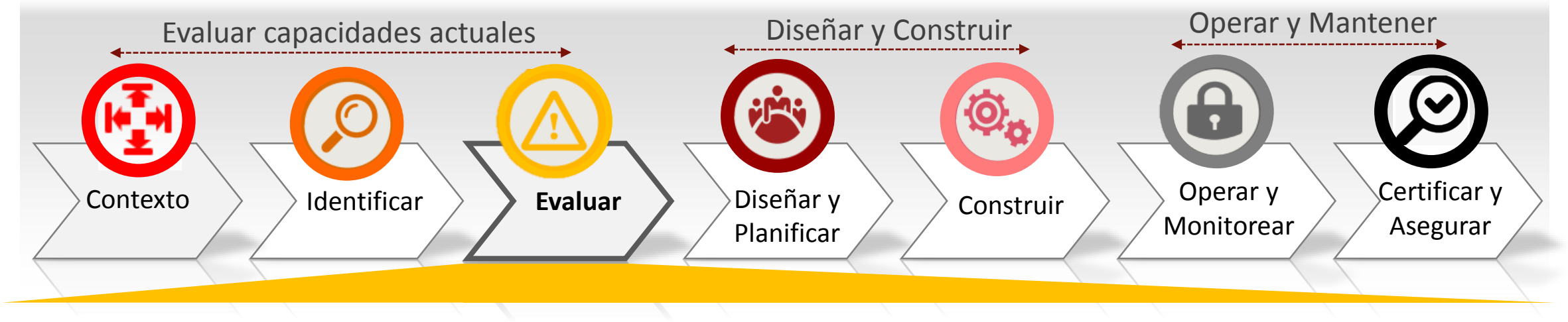


- Establecer prioridades para todas las partes
- Definir bases para un piloto





- Identificar y clasificar procesos relevantes:
  - *Recopilación de información personal*
  - *Procesamiento y gestión de datos en general y personales en particular (clientes, proveedores, personal, etc.)*
  - *Eliminación de datos*
  - *Transferencias internacionales de datos*
- Mapeo de datos
- Identificar áreas
- Identificar aplicaciones relevantes
- Identificar Infraestructura y localización de Servidores y Storages



- Realizar el DPIA **(Data Protection Impact Assessment)** dentro de los límites establecidos (eventual piloto)
- Apunta a identifica problemas en una etapa temprana para que puedan resolverse de manera costo-beneficio razonable.

- Identifica y evalúa **brechas existentes** (Prioriza)
- Brinda una buena visión de los **riesgos** relacionados
- Brinda información para priorizar y mitigar los riesgos identificados.
- Debes ser actualizado cada vez que se inicia un nuevo proyecto que implica procesamiento de datos personales

- Realizar el DPIA **(Dat**
  Protection Im
  Assessmen
  límites esta
  piloto)
- Apunta a i
  en una eta
  que pueda
  manera co
  razonable.

Tipos de impactos

Cumplimiento

- Auditorías
- Exclusión de tratados y alianzas comerciales
- Multas y sanciones

Financiero

- Pérdida de ingresos
- Costos de litigios
- Sanciones civil y / o criminal por infracciones de datos
- Costos de remediación

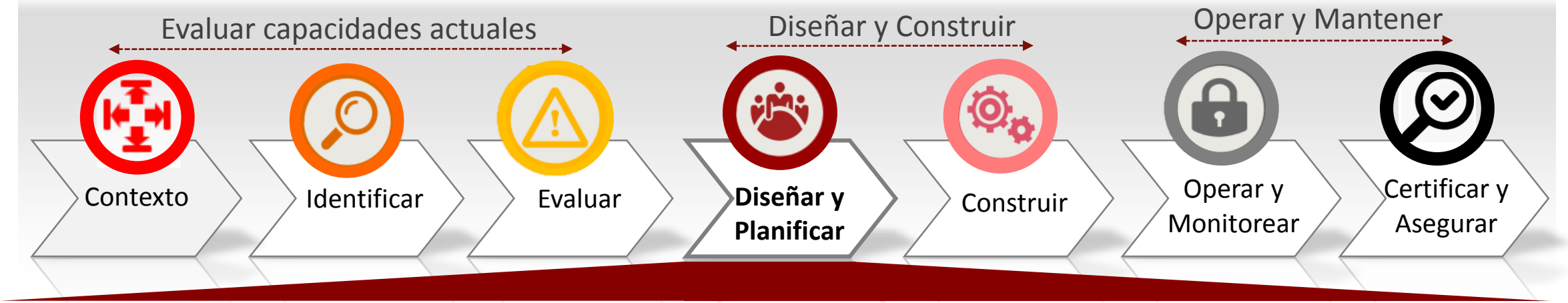
Reputacional

- Daño de la marca
- Pérdida de confianza de clientes, empleados, pacientes
- Desgaste del consumidor

Operacional

- Restricción en operaciones
- Invalidación función de compartir y datos compartidos; y compra/venta de datos
- Respuestas ante incidentes

- Analizar y priorizar las recomendaciones (respuestas) definidas en la etapa anterior
- Diseñar controles
- Definir Programa de Privacidad
- Definir la Estrategia de Implementación (parcial/ incremental o no)
- Definir la Estrategia de Supervisión y Monitoreo
- Definir los Programas de Assurance y Mejora Continua
- Definir el Plan de implementación



1. Estrategia y Gobierno

- Definir alcance, estructura de gobierno, roles y responsabilidades. Tener en cuenta emprendimientos de Transformación Digital
- Asegura y respalda el Programa de Privacidad

2. Gestión de Políticas

- Políticas, procedimientos, lineamientos y sus respectivos cambios deben estar documentados

3. Transferencia de Datos fuera de fronteras

- Definir estrategia teniendo en cuenta que datos, son enviados a dónde para qué y ajustar mecanismos de evaluación

4. Gestión del Ciclo de Vida de los Datos

- Mapeo y clasificación de datos
- Mecanismos para identificar nuevos procesamientos y usos de datos personales y eliminación segura
- Gobierno de datos
- Prevención Perdida de Datos
- Diseño controles correspondientes

5. Procesamiento de derechos de los individuos

- Garantizar correcto procesamiento de derechos (consentimientos) y solicitudes de los individuos

6. "Privacy by Design " (PbD)

- Tomar resultados del DPIA
- Incorporar controles de privacidad y evaluación del impacto a través del ciclo de vida de los datos para nuevas iniciativas

7. Seguridad de la Información

Diseñar / revisar controles alineados a los existentes:

- Estrategia de Seguridad
- Análisis de Riesgos de IT /Gestión de Riesgos de IT
- Gestión de Identidades y Control de Acceso
- Seguridad de Bases de Datos
- Seguridad Cloud
- CyberRisk & Governance
- Procesos de respaldo
- Network Security
- Gestión de Vulnerabilidades
- Recuperación de Desastres/Continuidad del Negocio
- Estrategias de Encripción, etc.

8. Gestión de Incidentes

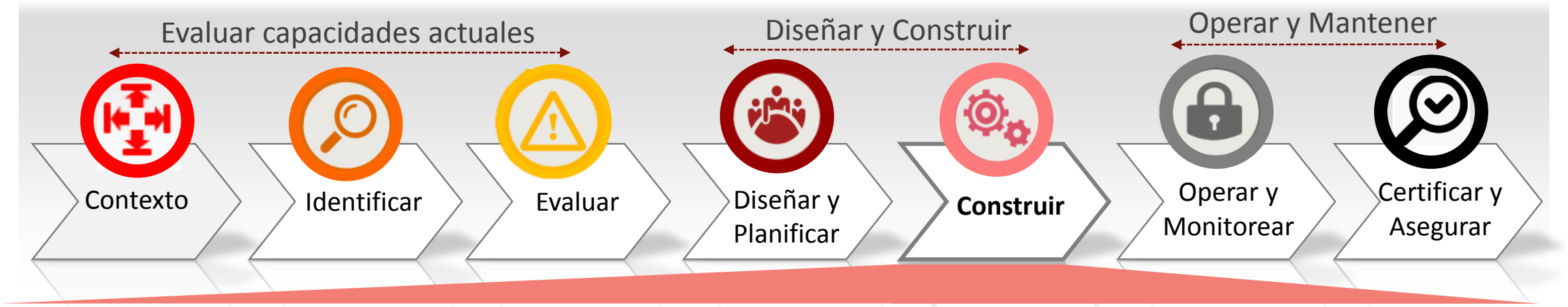
- Gestión de incidentes (preparación y respuesta)
- Mecanismos para identificar nuevos procesamientos y usos de datos personales y eventuales brechas
- Diseñar controles correspondientes

9. Responsabilidad de Procesadores de datos

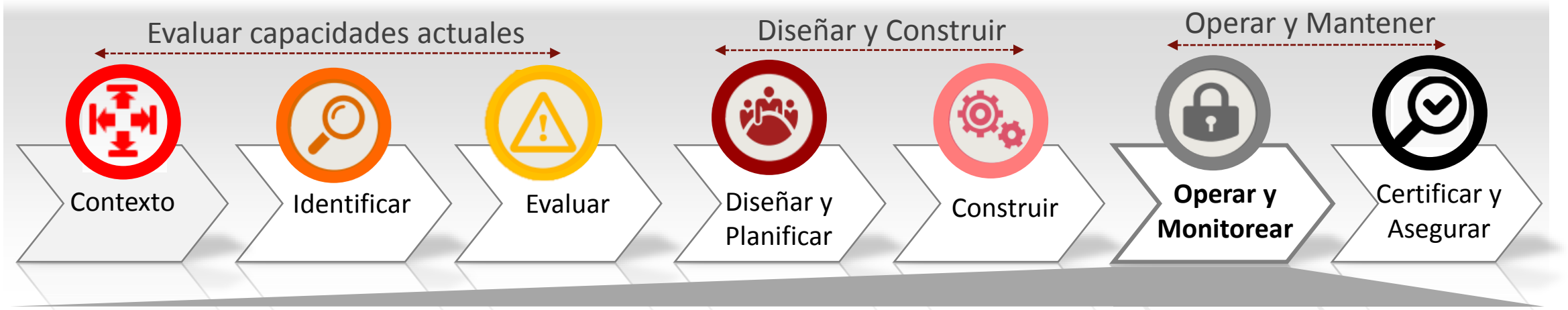
- Definir requerimientos de privacidad p/ 3eros; identificar y mitigar eventuales riesgos
- Inventariar 3eros
- Validar mecanismos de acceso/transferencia de datos y ver cómo se refleja en los contratos

10. Capacitación y Concientización

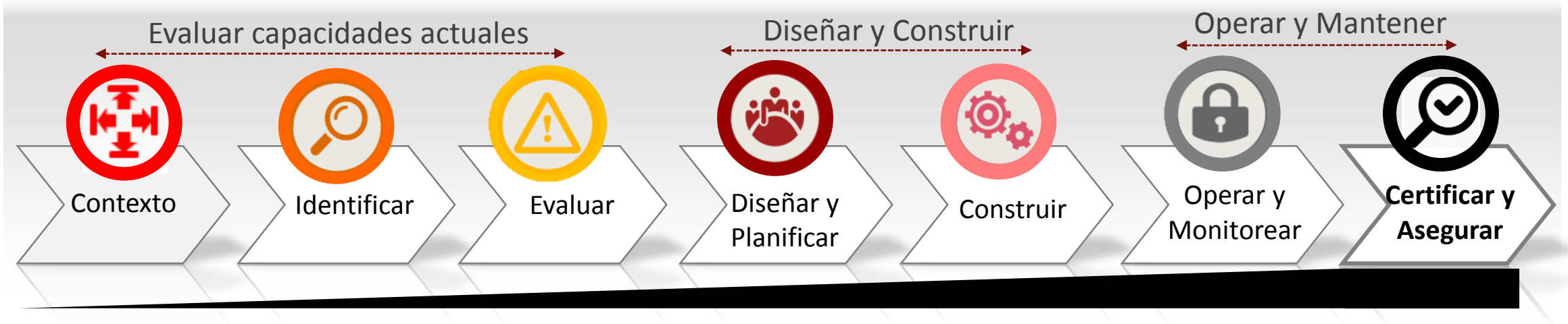
- Inventariar quienes requieren este entrenamiento y definir los Planes



- Implementar las medidas de respuesta diseñadas de acuerdo a lo planificado, en particular: todas las políticas y procedimientos



- Poner en marcha los mecanismos implementados para garantizar, en el día a día, el cumplimiento y mantener las responsabilidades asignadas



- Obtener certificación y aseguramiento independiente

- Definir alcance y áreas foco de la auditoría
- Elaborar programas de trabajo y definir la evidencia a reunir

- Testear el diseño y efectividad de controles de privacidad en los 10 dominios del programa

- Identificar gaps en diseño y efectividad de controles a partir del análisis de la evidencia reunida

Sugerir las medidas de respuesta

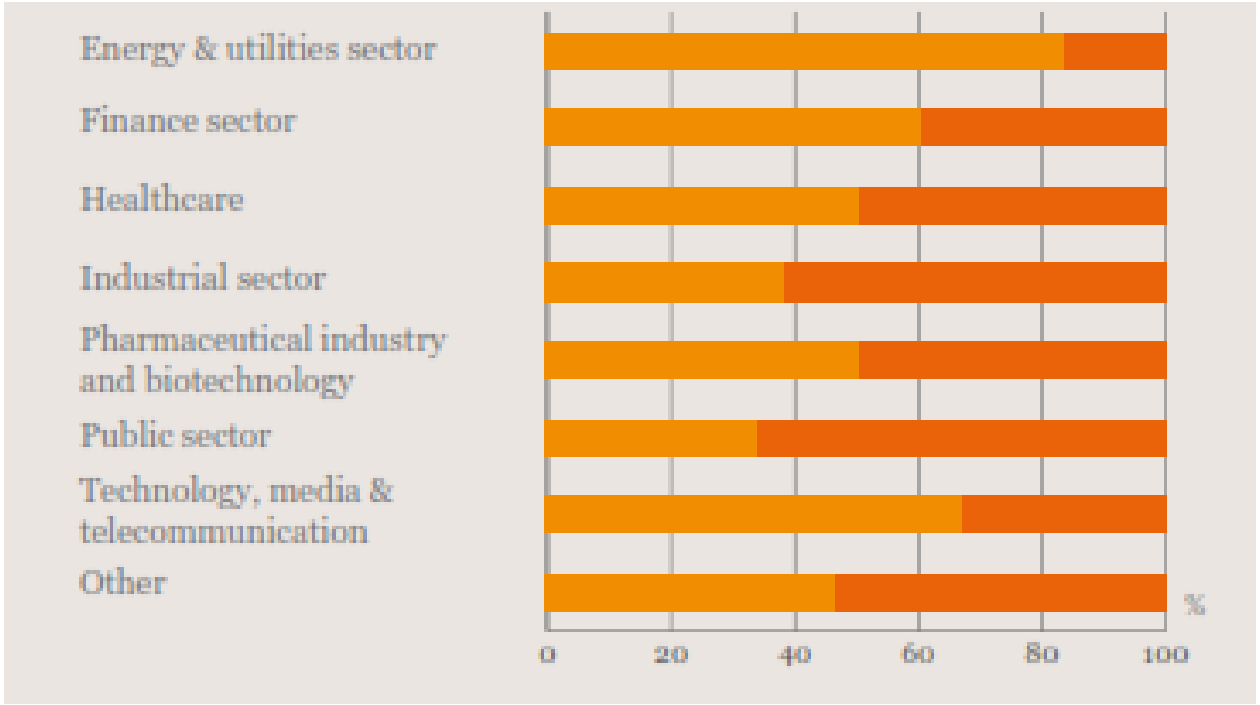
- Validar las respuestas implementadas re testeando los controles con problemas

Desafíos

- **Identificación de todo el personal involucrado en el procesamiento de datos personales**: *suelen ser el eslabón más débil en la cadena de "seguridad", requieren capacitación*
- **Claro entendimiento del flujo de los datos personales en sus procesos**
- **Sellos y Certificaciones**. *No suelen ser de gran ayuda*
- **Nivel de preparación**. *Hace a la diferencia. Las organizaciones de sectores regulados suelen estar en mejor condición*
- **Transparencia.** *La comunicación e información relacionada a políticas y procedimientos vinculados al procesamiento de datos personales debe ser claro, sencillo, comprensible y accesible*
- **Data Controller**. *Tiene que tener la capacidad de integrar las medidas definidas a las ya existentes (Seguridad Informática y Cybersecurity). No necesita ser un especialista pero si capaz de realizar un diseño integrado*
- **ERM robusto**. *Se debe revisar el Apetito y Tolerancia al Riesgo de la organización*
- **El tamaño de la organización aumenta en forma exponencial las dificultades de implementación y cumplimiento**
- **Incapacidad de reportar las brechas de cumplimiento a tiempo**: *Dificultades en la detección oportuna, Falta de un protocolo de comunicación claro (Directiva), Actuación en "silos", etc.*
- **Evidencia (Registros)** *Hay que generar/almacenar pistas de auditoría de las actividades del DPO) y del resto del personal involucrado (según la Ley)*

- **Presupuestos.** *No todos los sectores tienen la misma predisposición/capacidad de inversión*

Law Square Survey, 2016 – Preparación para la implementación de GDPR



Track 2

Antecedentes en la región: Ley de Protección de Datos Personales en Argentina

Track 3

Principales consideraciones desde el punto de vista de Seguridad y CyberSecurity a tener en cuenta