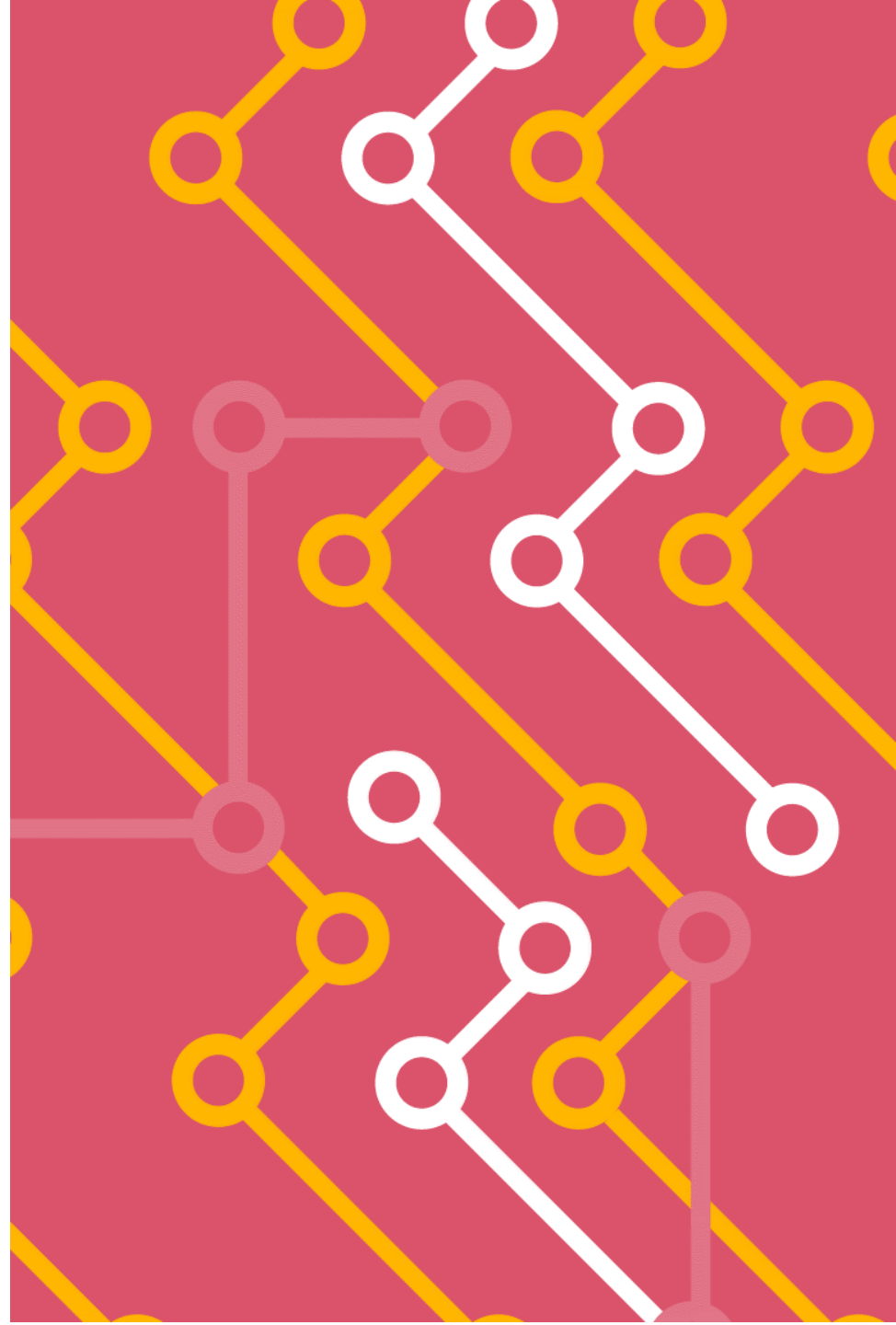


El valor de los datos personales en las empresas



Webinar

Marzo 2020



Agenda

1. Datos personales como activos sensibles
2. Nuevas obligaciones para las empresas
3. Medidas de protección
4. Reflexiones finales

1

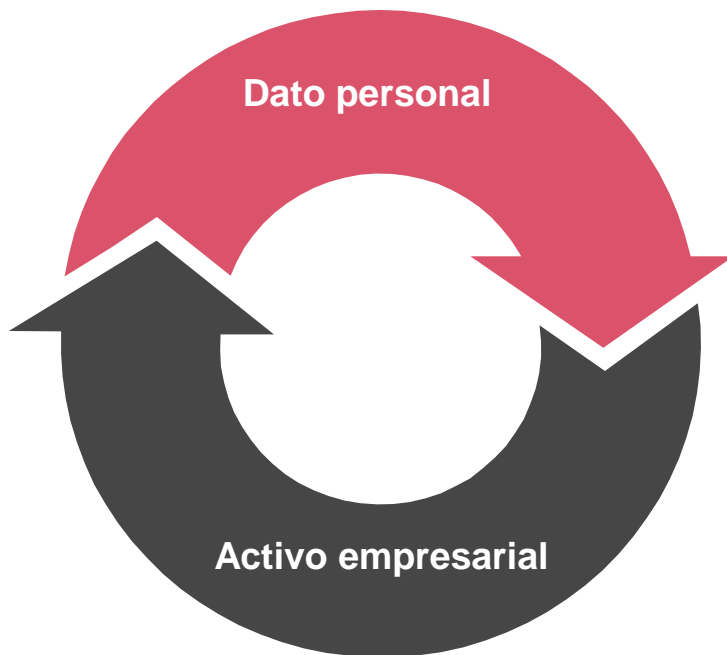
Los Datos

Personales

como activo

sensible

Los Datos Personales como activo sensible



No → Problema de cumplimiento normativo, que representa un costo adicional.

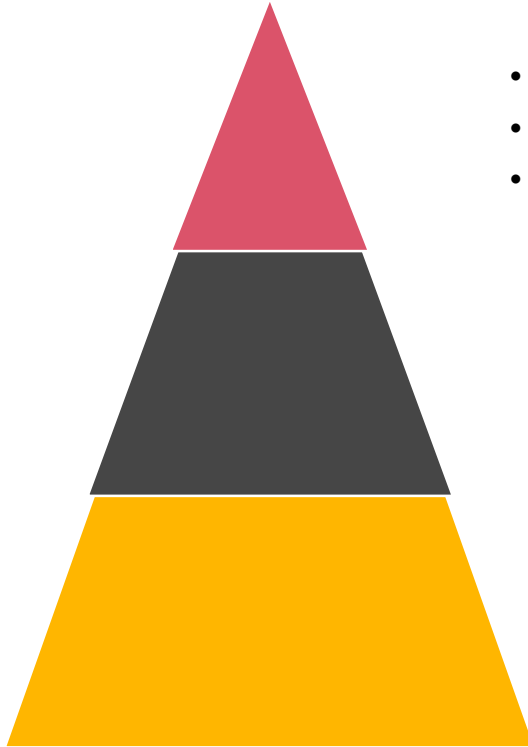
Si → Oportunidad para establecer estándares de cuidado que potencien status de la empresa y confianza de los clientes/usuarios.

Necesidad por nueva realidad y tratamiento de datos relativos a la salud

- Prestadores
- Médicos
- Empresas por datos de colaboradores

Los Datos Personales como activo sensible

Normativa



- Constitución de la República – Art.72
- Declaración Universal de Derechos Humanos
- Pacto de San José de Costa Rica

- Ley N° 18.331 – Protección de Datos Personales y Acción de Habeas Data
- Ley N° 19.670 – RC 2017 – Arts. 37 a 40
- Otras modificativas y complementarias

- Decreto N° 414/009
- Decreto N° 64/020
- Otros decretos
- RGPD UE

Datos personales registrados en cualquier soporte.
Tratados de diversos modos.
Ámbito privado y público.

Los Datos Personales como activo sensible

Concepto

¿Qué son datos personales?

Cualquier tipo de información que nos pueda identificar directamente o nos haga identificables.

Ej.: nombre, dirección, teléfono, CI, RUT, huella digital, número de socio, fotografía, ADN, etc.

¿Qué es la protección de datos personales?

Amparo de las personas contra toda posible utilización de sus datos por terceros no autorizados



Los Datos Personales como activo sensible

Impacto en la reputación de las empresas



Los Datos Personales como activo sensible

Datos relativos a la salud

- Especialmente protegidos (Art. 19 Ley 18.331)
- Relativos a la salud física o mental que tratan los establecimientos sanitarios públicos o privados y los profesionales de la salud.
- Previo consentimiento informado
- Respetar en la recolección y tratamiento de estos datos el secreto profesional y la normativa aplicable



2

Nuevas

obligaciones

para las

organizaciones

Nuevas obligaciones

Responsabilidad demostrada



“Las medidas adoptadas deberán ser documentadas, revisadas periódicamente y evaluadas en su efectividad”

- Políticas
- Protocolos
- Procesos

Nuevas obligaciones

Evaluación de Impacto en la Protección

¿Cuándo?

- Previo al inicio del tratamiento
- En el plazo de un año desde el 21.2.2020

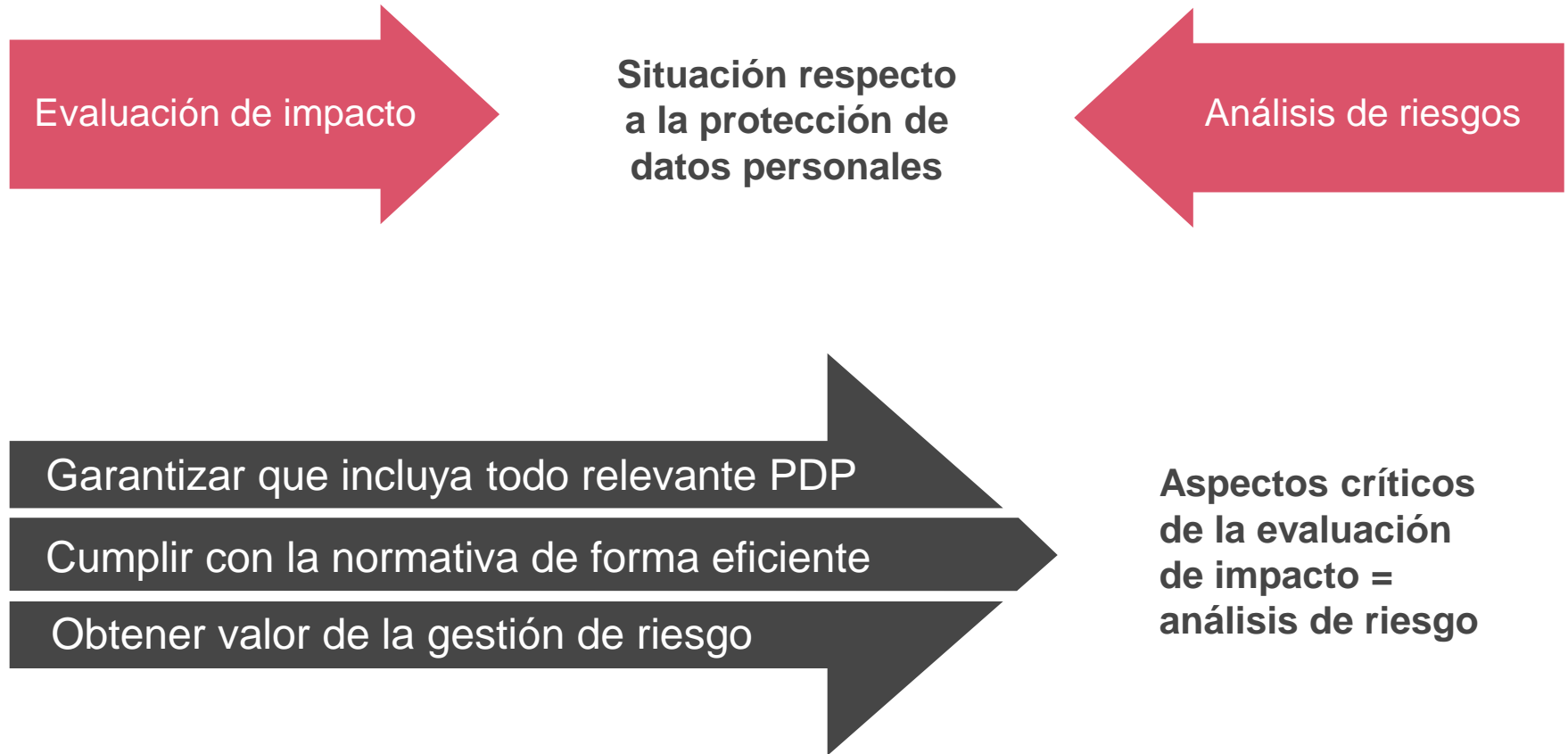
¿Quién?

- Datos sensibles como negocio principal
- Datos especialmente protegidos por la ley permanente o establemente.
- Datos para crear o utilizar perfiles personales
- Datos de grupos de personas en situación de vulnerabilidad
- Grandes volúmenes de datos personales (> 35.000 titulares)
- Se transfieran datos internacionalmente
- Otros que considere la URCDP



Nuevas obligaciones

Evaluación de Impacto en la Protección



Nuevas obligaciones

Evaluación de Impacto en la Protección



Análisis de riesgos completo

- Participación de todos los involucrados
- Entendimiento de los procesos de negocio involucrados en el ciclo de vida de los datos para aplicar a los componentes más relevantes (aspectos legales, tecnológicos y capacitación/concientización).
- Revisión de grado de mitigación de los riesgos identificados



Eficiencia en el análisis

- Integración del análisis con las prácticas de gestión de riesgos ya existentes
 - Definición clara y adecuada a la organización de los criterios de análisis (tablas de probabilidad e impacto, exposición y nivel de tolerancia, etc.)
 - Mecanismo de documentación simple y contenga toda la información relevante



Maximización de valor de gestión de riesgos

- Logro de objetivos y beneficios.
- Metodología adaptada a la organización para aprovechar a todo nivel (objetivos estratégicos y operacionales).
- Matrices focalizadas en aspectos con impacto más allá de la gestión de DP (seguridad de la información, gestión de proveedores, gestión de clientes, capacitación).
- Capacitación en gestión de riesgos general.

Nuevas obligaciones

Delegado de Protección de Datos Personales

PLAZO

90 días desde el 21.2.2020 o desde el inicio del tratamiento de DP.

OBLIGADOS

- Entidades públicas, estatales o no estatales y las privadas de propiedad estatal.
- Entidades privadas que traten datos sensibles como negocio principal.
- Entidades privadas que realicen tratamiento de grandes volúmenes de datos (>35.000 titulares).
- La Unidad podrá expedirse sobre otros casos.



Nuevas obligaciones

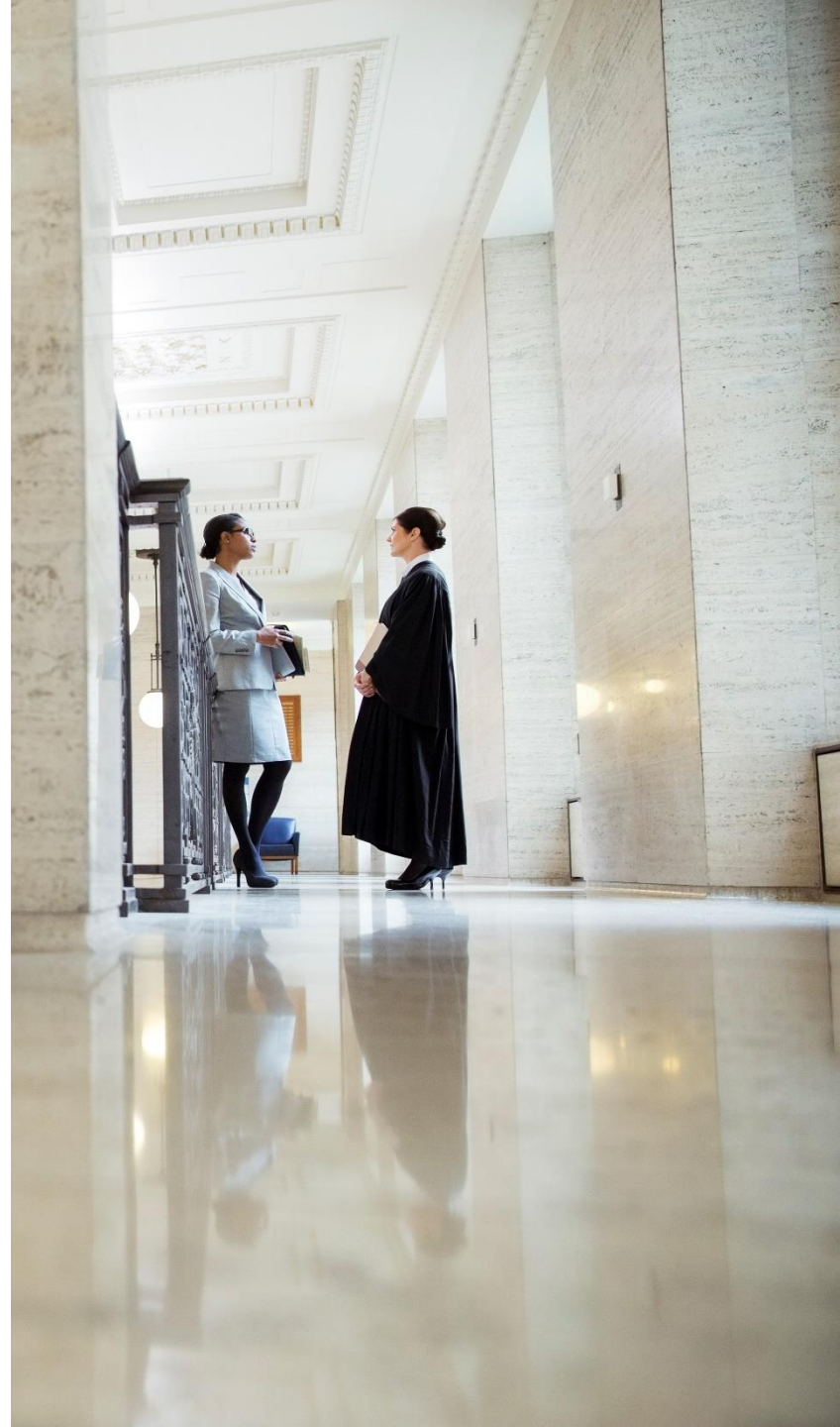
Delegado de Protección de Datos Personales

FORMACIÓN

Formación acreditada en Derecho y especialización en protección de DP.

FUNCIONES

- Asesorar en diseño, formulación y aplicación de políticas de protección de datos;
- Supervisar el cumplimiento de la normativa;
- Proponer medidas para estar conforme a la normativa y estándares internacionales, verificando su efectiva realización;
- Ser el nexo entre la entidad y la URCDP.



Nuevas obligaciones

Delegado de Protección de Datos Personales

- **Persona física**, que realice su labor de manera independiente o como empleado de la entidad.
- **Persona jurídica**, comunicando a la URCDP la nómina del órgano de administración, y las personas físicas que se designen para llevar a cabo la función.



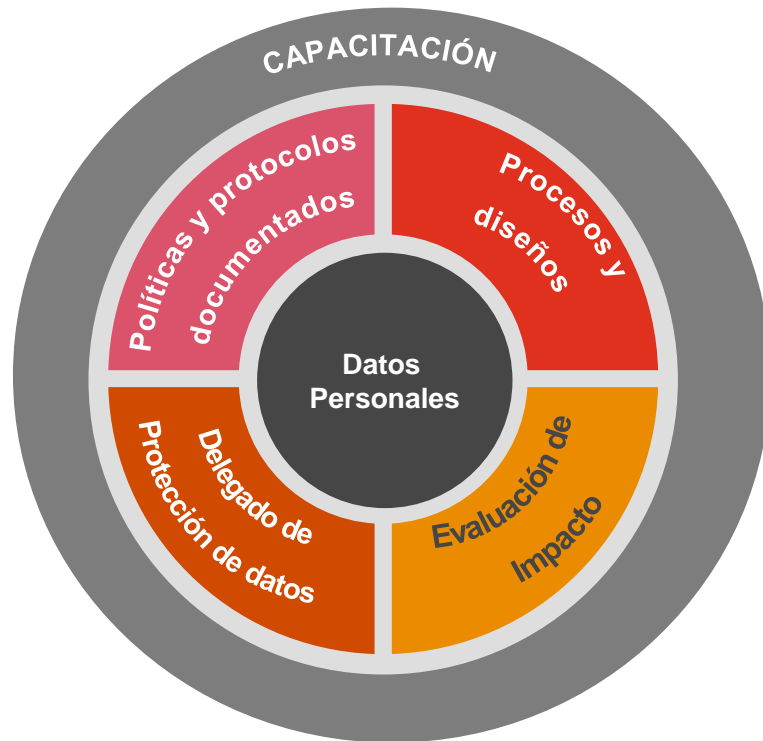
3

Medidas

de

protección

Medidas de Protección



- **Políticas y protocolos documentados**
Medidas de prevención y acción documentadas con procedimientos aplicables y aplicados.
- **Procesos y diseños adecuados**
Privacidad por diseño y por defecto.
- **Evaluación de Impacto**
Gestión de los riesgos asociados y acciones de mitigación.
- **Delegado de protección de DP**
Delegado instruido, tercerizado o con asesoramiento especializado externo.
- **Capacitación**
De todos los individuos que traten datos personales.

4

Reflexiones

finales

Reflexiones finales



La realidad cambió y obligó a revisar el tratamiento, procesamiento, recolección y transferencia de los datos personales.



La nueva regulación nacional acompaña la tendencia internacional con impacto directo en la reputación corporativa.



Las políticas y procesos deben ser aplicables, aplicados y documentados.

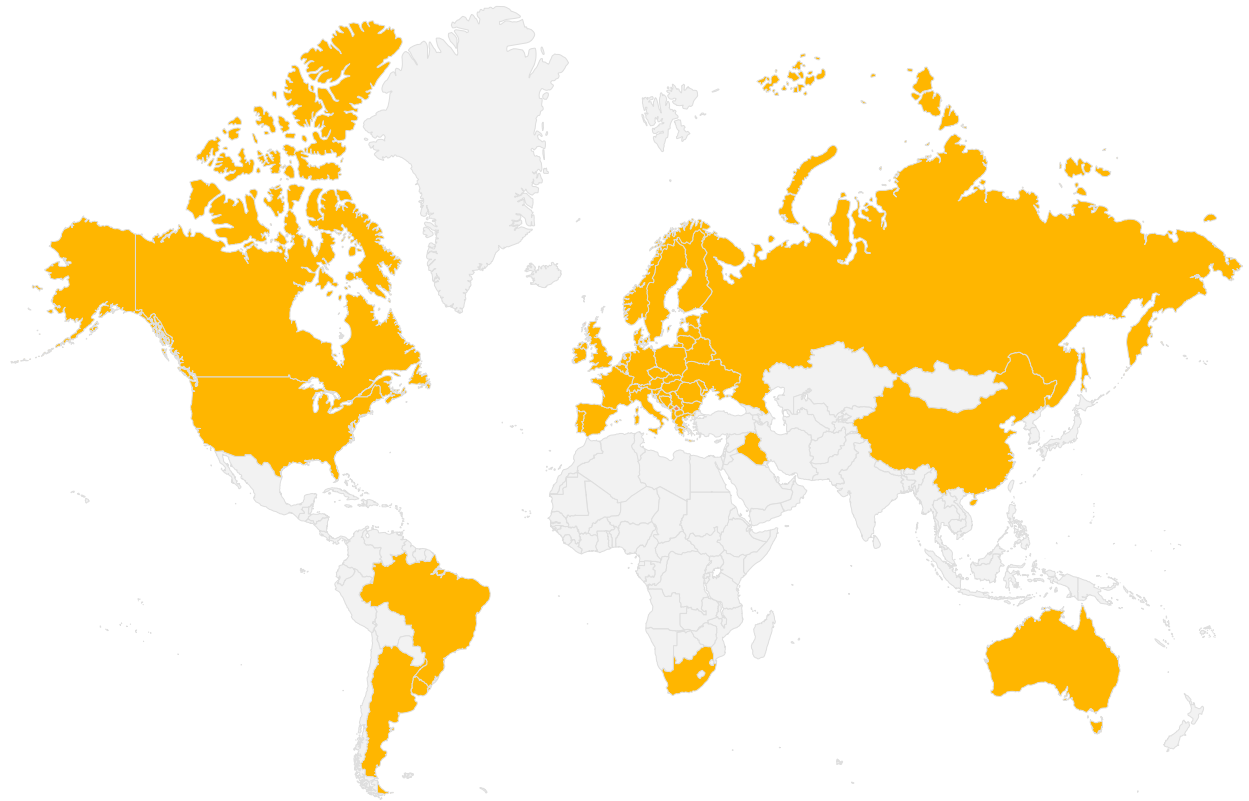


Es fundamental contar con apoyo de expertos y capacitación en la materia, ya que está en constante movimiento.

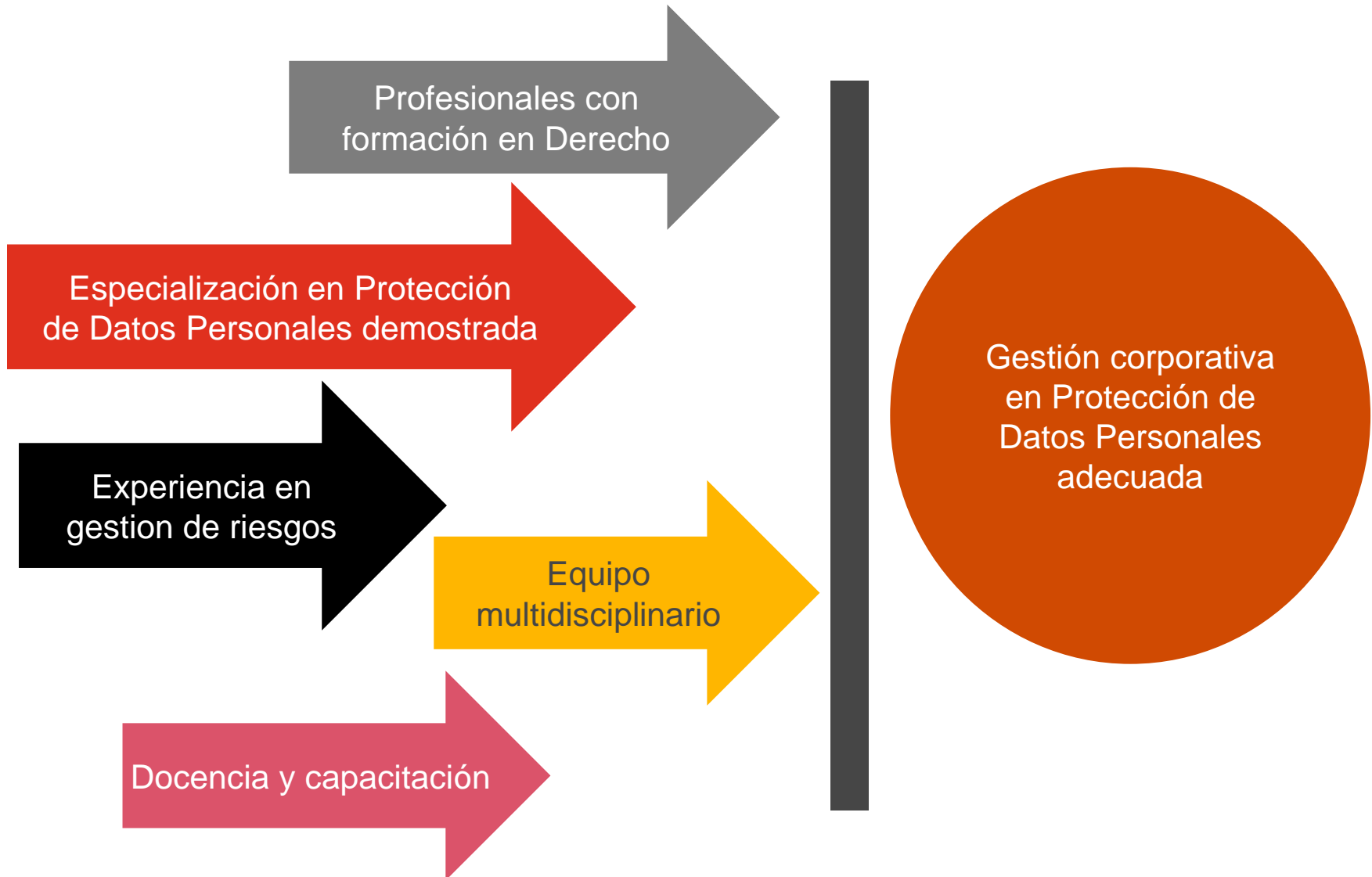
Experiencia PwC

La red PwC cuenta con más de 2.900 profesionales en ciberseguridad y privacidad, que incluye protección de datos personales.

Funciona como una Red de apoyo de consultores, abogados, auditores, tecnólogos y demás profesionales altamente capacitados y especializados con experiencia en ayudar a negocios globales en todas las industrias.



Experiencia PwC



Compliance Hub

Compliance Hub centraliza en un solo lugar las respuestas a los desafíos que tienen las organizaciones públicas y privadas en materia de integridad, ética, transparencia, cumplimiento de regulaciones (PDP) y cuestiones legales.



Gracias

pwc.com.uy



© 2020 PricewaterhouseCoopers Ltda., PricewaterhouseCoopers, PricewaterhouseCoopers Professional Services Ltda. y PricewaterhouseCoopers Software Ltda. Todos los derechos reservados. PwC refiere a la firma miembro de Uruguay y en algunas ocasiones a la red PwC. Cada firma miembro es una entidad legal separada. Por favor visite www.pwc.com/structure para más detalles.