La nueva norma ISO 31700 de Privacidad desde Diseño y por Defecto (PdD)

¿Por dónde empezar con la PdD para tu organización y cómo adoptar ISO 31700?

SARA ETULAIN

Abogada de protección de datos y privacidad

LinkedIn

JAVIER CASTELLANO

Consultor en protección de datos

LinkedIn

¡Envíanos tus preguntas!

✉️ sara.etulain@pridatect.com
✉️javier.castellano@pridatect.com

Contenido

- ¿Qué es la Privacidad desde el Diseño y por Defecto (PdD)?
- Los 7 principios fundamentales de PdD
- La nueva norma ISO 31700
- Sus requisitos de alto nivel y cómo ponerlos en práctica
- Ejemplos de buenas prácticas de otras empresas

¿Qué es la Privacidad desde el Diseño y por Defecto (PdD)?

La PdD significa la construcción de l**a privacidad como el modo de operación predeterminado** dentro del modelo de negocio de las organizaciones.

La privacidad desde el diseño → **adopción de medidas técnicas y organizativas** cuya finalidad es **aplicar de forma efectiva los principios de protección de datos**

La privacidad por defecto → **adopción de medidas técnicas y organizativas** cuya finalidad es **garantizar que por defecto solo se traten aquellos datos que sean necesarios para los fines del tratamiento**

Fue desarrollado por la ex Comisionada de Protección de Datos de Ontario, Ann Cavoukian

Existe desde hace más de 25 años

7 principios fundamentales

¿Dónde está regulado?

La PdD es un principio de la protección de datos recogido en el RGPD, pero no está recogido en un artículo concreto del RGPD, sino que se menciona en diferentes apartados:

1. **Considerando 78 del RGPD**
2. **Artículo 25.1 del RGPD**

Por tanto, se impone al responsable del tratamiento que:

- Establezca **medidas técnicas**
- Diseñe medidas organizativas

que sean **adecuadas para que se aplique la protección de datos de forma eficaz.**

Los 7 principios fundamentales de PdD

¿Qué significa en la práctica?

1. **PROACTIVO, NO REACTIVO; PREVENTIVO, NO CORRECTIVO**

anticiparse a los eventos que afecten a la privacidad antes de que sucedan

2. **LA PRIVACIDAD COMO CONFIGURACIÓN PREDETERMINADA**

que los datos personales estén automáticamente protegidos en cualquier sistema, aplicación, producto o servicio

3. **LA PRIVACIDAD INCORPORADA EN LA FASE DE DISEÑO**

la privacidad nace en el diseño, antes de que el sistema esté en funcionamiento

4. **FUNCIONALIDAD TOTAL**

“todos ganan” → sistemas plenamente funcionales, eficaces y eficientes, también con respecto a privacidad

Los 7 principios fundamentales de PdD

¿Qué significa en la práctica?

5	ASEGURAMIENTO DE LA PRIVACIDAD EN TODO EL CICLO DE VIDA	la privacidad nace en el diseño, antes de que el sistema esté en funcionamiento
6	VISIBILIDAD Y TRANSPARENCIA	poder demostrar la privacidad, verificando que el tratamiento es acorde a la información dada
7	ENFOQUE CENTRADO EN EL SUJETO DE LOS DATOS	el fin último debe ser garantizar los derechos y libertades de los usuarios

La nueva norma ISO 31700

La finalidad de la nueva norma es **establecer requisitos de alto nivel para que PdD se extienda a lo largo del ciclo de vida de un producto** de consumo, incluidos los datos generados por el uso del producto por el consumidor.

Los **beneficios de PdD pueden verse a través de tres principios** rectores:

- **Capacitación y transparencia**
- **Institucionalización y responsabilidad**
- **Ecosistema y ciclo de vida**

Requisitos de alto nivel y cómo ponerlos en práctica

REQUISITOS:

1. Diseñar funcionalidades que **permitan a los consumidores hacer valer sus derechos de privacidad**
2. **Asignación de funciones** y autoridades pertinentes
3. Llevar a cabo un **análisis de riesgos**
4. Diseñar **controles de privacidad**
5. Diseño de controles de privacidad para la **destrucción y el fin de uso de los datos personales**

EN PRÁCTICA:

- **Evite marcar casillas de verificación previamente.**
- **Ofrezca control a los usuarios (consentimiento granular).**
- **Incorpore avisos “justo a tiempo”.**
- **Demuestre respeto por la privacidad con personas a cargo de su cumplimiento.**
- **Minimice los datos tratados (podar, excluir, eliminar).**
- **Defina en una política qué cláusulas se comunicarán a los interesados.**
- **Documente las decisiones tomadas (quién, cuándo y justificación).**

Ejemplos prácticos de buenas prácticas

La empresa Juguetes S.A., una tienda en línea al por menor de juguetes, quiere vender sus productos por Internet y tiene un programa de fidelización.

PROCESO DE VENTA

Peticiones de datos personales adicionales de manera granular:

- ¿Desea crear una cuenta?
- ¿Desea conservar la información de contacto después de la entrega para futuras:
  - Compras
  - Devoluciones
- ¿Cuál es el tamaño de su familia, su edad y los ingresos?

RESPUESTA BRECHA SEGURIDAD

La organización activa su programa de apoyo al consumidor:

- Hace un anuncio de privacidad en la web que confirma que no ha habido ninguna violación de la privacidad.
- Crear respuestas predeterminadas para confirmar al cliente que ni su pedido ni su pago se vieron afectados por la brecha.

Ejemplos prácticos de buenas prácticas

La empresa GYM, S.L., un club deportivo urbano, quiere ofrecer a sus socios una app de registro de actividad deportiva.

APP DEPORTIVA

El gimnasio encarga el desarrollo de una aplicación que recopila información sobre el acondicionamiento físico y datos de salud a un proveedor.

- Evaluar las capacidades de privacidad del proveedor.
- Evaluar periódicamente el impacto a la privacidad (ej. mediante EIPD).
- Documentar los riesgos que puede suponer un acceso ilegítimo a los datos (ej. análisis de riesgos).

COMUNICACIONES A CLIENTES

La empresa nombra a un encargado de las comunicaciones sobre privacidad.

- Nombrar persona a cargo de las comunicaciones relativas a la privacidad.
- Redacción de información relativa a la app.
- Redacción de campañas de información sobre situación de privacidad de la empresa.
- Respuestas predeterminadas para hacer frente a peticiones de clientes.

Identificación de riesgos y protección de datos simplificada

Detecta e identifica riesgos

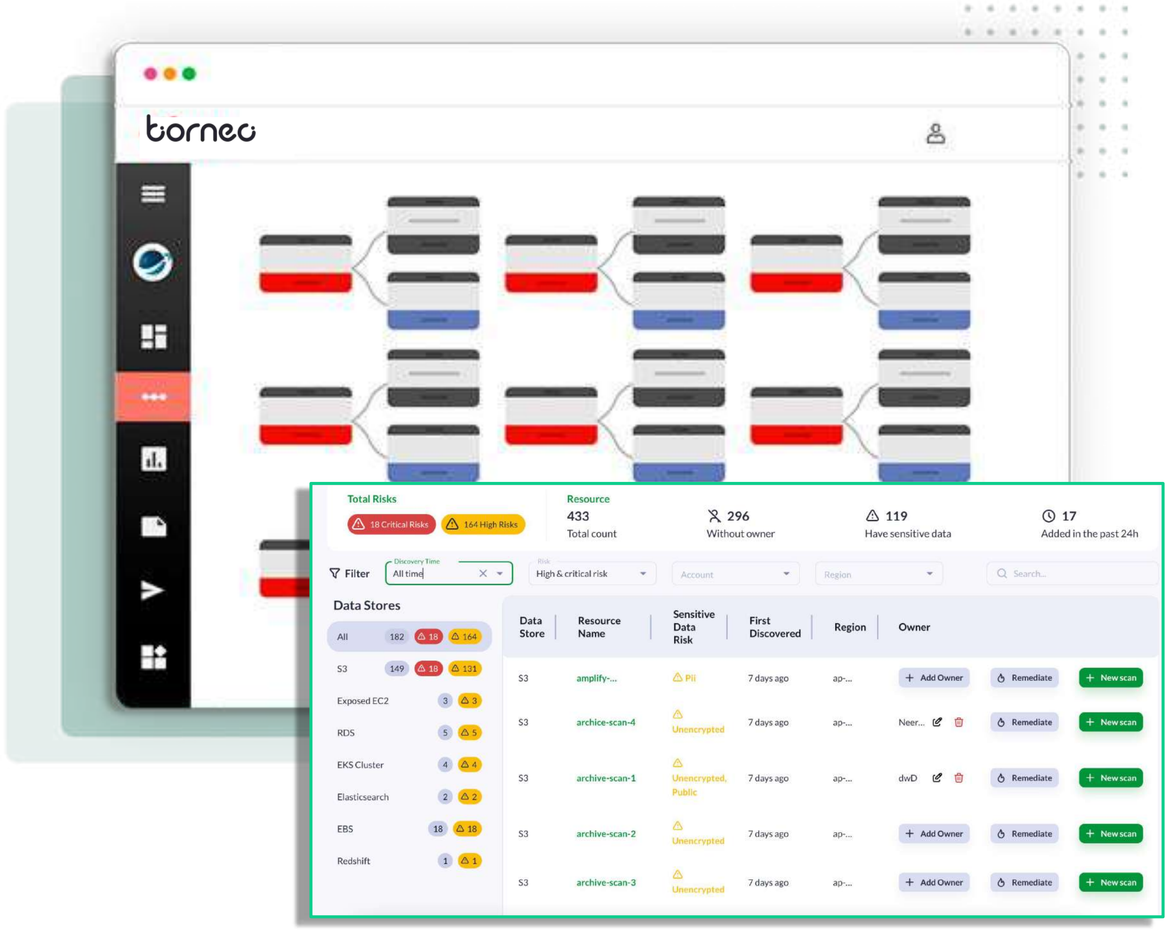
Detecta todos los tratamiento de datos personales (**clientes, empleados, proveedores…**) e identifica los riesgos . Podemos identificar y analizar, las amenazas y vulnerabilidades en tus procesos.

Actúa cuando sea necesario

El conocimiento de los riesgos en tu empresa nos permite definir las medidas necesarias para reducirlos y mitigarlos. Nuestra plataforma te ayuda con la definición y sugerencias de medidas para tu empresa.

Supervisión contínua y alertas

La protección de datos es una tarea constante dentro de una empresa. Nuestra plataforma no solo ayuda con la implementación inicial, también con la supervisión continua de riesgos, medidas y administración de tareas entre empleados de tu empresa.



¿Quieres saber más sobre cómo podemos ayudarte con tus esfuerzos de privacidad y prevención de brechas de datos?

¡Solicita tu demo!

Contacta con nosotros y toma el control de la **gestión de la protección de datos** de empresa y garantiza el cumplimiento del RGPD, ofreciendo la mayor seguridad a tus clientes.

SARA ETULAIN

Abogada de protección de datos y privacidad

LinkedIn

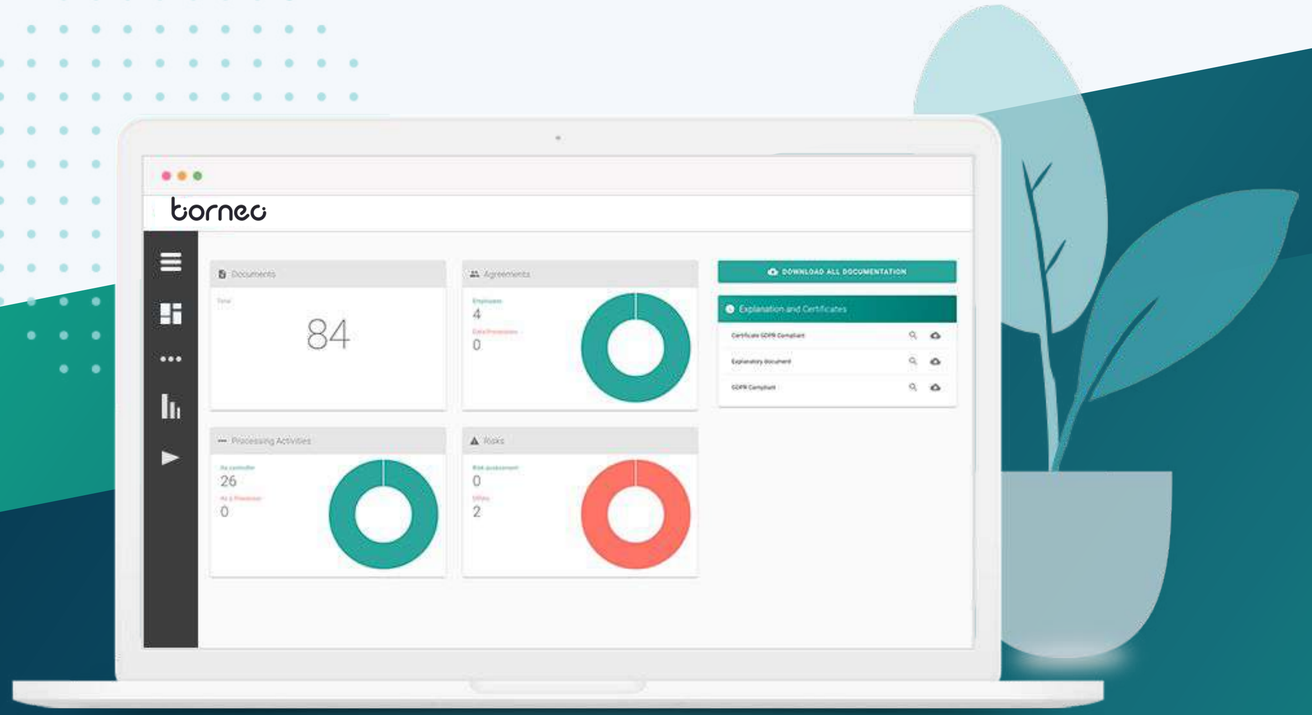
JAVIER CASTELLANO

Consultor en protección de datos

LinkedIn

¡Envíanos tus preguntas!

✉️ sara.etulain@pridatect.com
✉️javier.castellano@pridatect.com



¡**Gracias** por ver nuestro **webinar!**