



**REGLAMENTO GENERAL
DE PROTECCIÓN DE
DATOS (GDPR)**
*¿Qué hacer para estar
preparado?*

Consejos del
Área de Ciberseguridad
de ABAST



1. ¿Qué es el GDPR?
2. GDPR. Algunas cifras clave.
3. Enfoque por fases recomendado
4. Statement of Applicability (SoA)
5. Assessment
6. Servicios de consultoría de seguridad de ABAST

1. ¿Qué es el GDPR?

El Reglamento General de Protección de Datos (GDPR) ha sido diseñado para armonizar las leyes de privacidad de datos de todos los países europeos y defender la privacidad de los datos de los ciudadanos de la Unión Europea.

Su aplicación afecta a todas las empresas, independientemente de su tamaño y sector de actividad.

El GDPR tendrá un gran impacto en su organización, y concretamente en su departamento TIC.

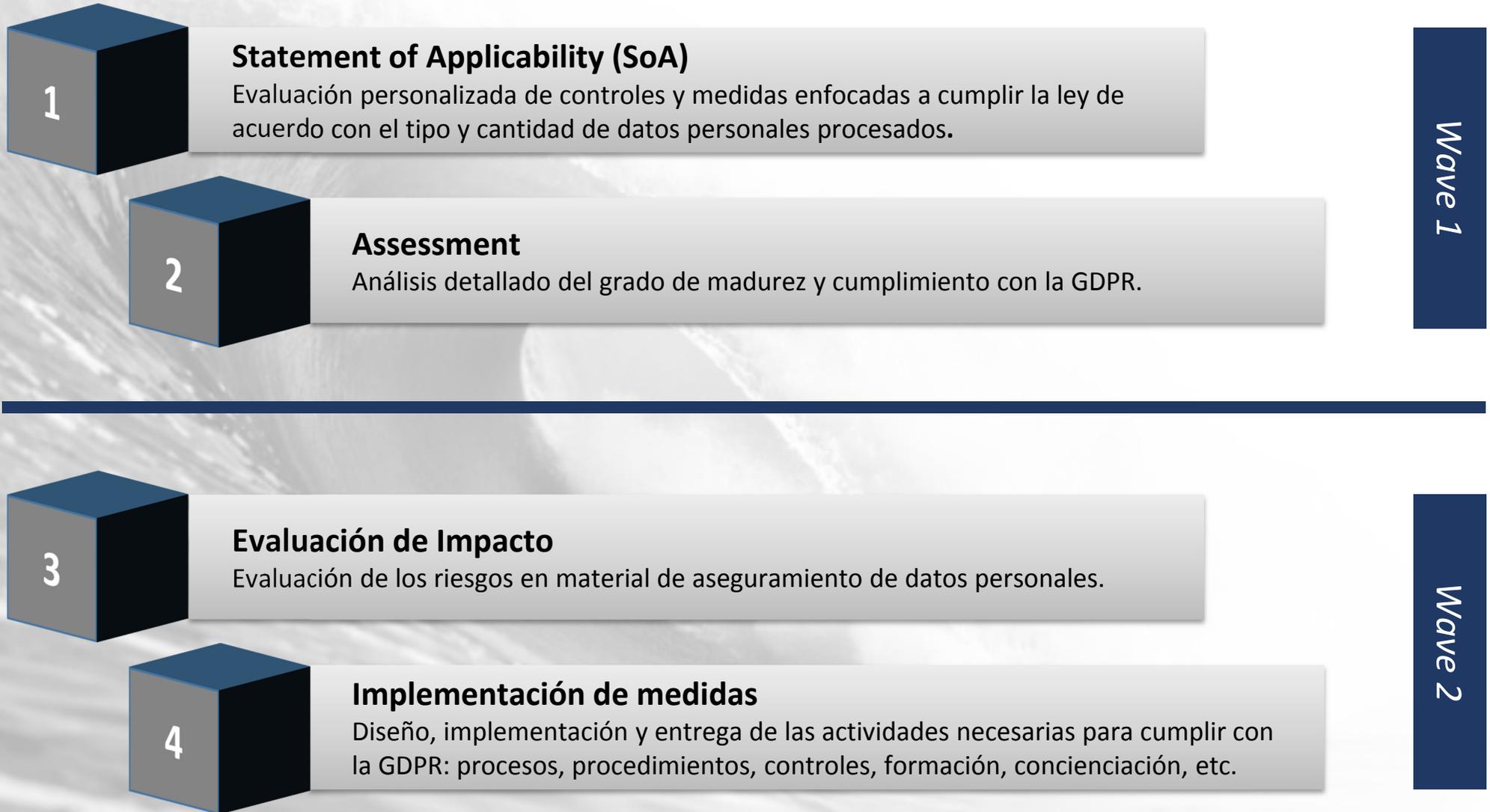
El reglamento entrará en vigor el 25 de mayo de 2018.

2. GDPR. Algunas cifras clave.



¹International Association of Privacy Professionals Study

3. Enfoque por fases recomendado



4. Statement of Applicability (SoA)

STATEMENT OF APPLICABILITY (SoA)

Descripción

Evaluación personalizada de controles y medidas enfocadas a cumplir la ley de acuerdo con el tipo y cantidad de datos personales procesados

Actividades

1. **Kick-off:** Sesión introductoria.
2. **Contexto:** Contexto organizativo.
3. **Aplicabilidad:** Identificación de las medidas de obligado cumplimiento.
4. **Definición del plan de proyecto:** Definición de pasos para realizar la auditoría, incluyendo el calendario de entrevistas.

Objetivos

- Documentar qué requerimientos son de obligado cumplimiento –y el grado de cumplimiento- para cumplir con la ley.

Mecanismos de control

- Kick-off meeting
- Seguimiento de proyecto

Duración

1 día

Pre-requerimientos

- Aprobación formal de propuesta

Requerimientos para cerrar la fase

- Aceptación del plan de proyecto

Carga estimada para el cliente

4 h

Entregables

1. Plan de Proyecto
2. Calendario de entrevistas

Coste:

Tiempo: Bajo
Complejidad: Bajo
Recursos: Bajo

Beneficio operativo

Bajo

4. Statement of Applicability (SoA)

Ejemplo SoA

| APLICABILIDAD | PRIORIDAD | COMPLEJIDAD |
|---------------|-----------|-------------|
| APLICA | MEDIA | BAJA |

1. Documentar las actividades de tratamiento

Se debe crear un registro de las actividades de tratamiento que los responsables y los encargados de tratamiento llevan a cabo.

2. Evaluar y definir los mecanismos de recogida del consentimiento

- Nombre y datos de contacto del responsable y/o co-responsable, así como del delegado de protección de datos (si hubiera).
- Finalidad del tratamiento.
- Descripción de las categorías de interesados y categorías de datos personales tratados.
- Transferencias internacionales de datos
- Cuando sea posible, plazos previstos para la supresión de datos.
- Cuando sea posible, descripción general de las medidas técnicas y organizativas de seguridad.

3. Definición de las cláusulas informativas

4. Definición de los encargos del tratamiento

5. Evaluación de Impacto

6. Consulta previa a la autoridad de tratamiento de datos

7. Revisión de los mecanismos utilizados en las transferencias a terceros países

8. Análisis del riesgo e implementación de las medidas que deben ser implementadas antes del 25/05/2018

9. Establecer un protocolo de notificación de violaciones de seguridad

10. Definición del perfil DPO

11. Concienciación

5. Assessment

ASSESSMENT

Descripción

Evaluación detallada de requerimientos y medidas dirigidas a dar cumplimiento a el GDPR de acuerdo con el tipo y cantidad de datos personales procesados. Constituye el elemento inicial que deberá definir cómo implementar las iniciativas de privacidad de datos, haciendo una evaluación de las medidas que deben ser implementadas, porqué deben ser implementadas, cómo implementarlas y el grado necesario de implementación.

Actividades

1. **Identificación de medidas:** Identificación del grado de implementación de las medidas.
2. **Dependencias:** Definición de dependencias.
3. **Assessment:** Ejecución de la evaluación de acuerdo al plan definido.
4. **Reporte:** Definición y presentación del reporte, que incluye No-cumplimientos y Recomendaciones

| Objetivos | Mecanismos de control | Duración |
|---|---|--------------------------------|
| <ul style="list-style-type: none"> ▪ Auditar el nivel de cumplimiento con la GDPR. ▪ Documentar las medidas que deben llevarse a cabo y justificación de las excluidas. ▪ Recomendaciones. | <ul style="list-style-type: none"> ▪ Seguimiento de proyecto | 2 – 3 semanas |
| Pre-requerimientos | Requerimientos para cerrar la fase | Carga estimada para el cliente |
| <ul style="list-style-type: none"> ▪ Aceptación del plan de proyecto | <ul style="list-style-type: none"> ▪ Aprobación informe de auditoría ▪ Presentación ejecutiva | 30 h |
| Entregables | Coste: | Beneficio operativo |
| 1. Informe de auditoría | Tiempo: Medio Complejidad: Alto Recursos: Medio | Alto |

6. Servicios de consultoría de seguridad de ABAST

¿Quiere asegurarse de cumplir con el GDPR? En ABAST disponemos de un conjunto de auditores, consultores y técnicos capacitados para ofrecerle asesoramiento, realizar una evaluación de cumplimiento y facilitar una hoja de ruta cuantificada y realista, acorde con las necesidades de su organización.

Nuestro equipo

Con un plan de formación continua, el equipo del área de consultoría de ABAST tiene una larga experiencia en servicios de seguridad y está certificado por las organizaciones internacionales más prestigiosas.

Estas son algunas de las certificaciones con las que contamos:

- CISA, Certified Information System Auditor.
- CISM, Certified Information Security Manager.
- ISO/IEC 27001 Certified Lead Auditor.
- ISO/IEC 22301 Certified Lead Auditor.
- ISO 27001 Implementer.
- IT Service Manager (ITIL v2).
- ITIL Expert v3.
- Cobit-based IT Governance.
- ISO/IEC 20.000 Certified Auditor.
- PMI Project Management Professional Certification.



AENOR



6. Servicios de consultoría de seguridad de ABAST

ABAST en cifras

49,51%
Crecimiento
en facturación
en los últimos
2 años

+600
Certificaciones
en **+20**
diferentes
tecnologías

Alianzas
estratégicas con
los **principales**
fabricantes de
HW y SW

6
Unidades
especializadas
para la
integración de
soluciones

Estrategia de
Ciberseguridad
360º

Soluciones
avaladas por
más de **30**
años de
experiencia

Miembros
fundadores
del capítulo
español **ITSMf**

Éxito afianzado
en base a la
flexibilidad y
el talento



Más información:
seguridad@abast.es

Nelia Argaz
(+34 618 099 107)

Barcelona
Tel. 933 666 900
C/ Ecuador 39-45
08029 Barcelona

Madrid
Tel. 914 061 601
Calle de la Basílica 19, 9º B
28020 Madrid