agencia española protección datos

INTEGRACIÓN DEL DPD EN LAS CORPORACIONES LOCALES. PRINCIPALES PROBLEMAS Y CUESTIONES QUE SUSCITA

Julián Prieto Hergueta

Agencia Española de Protección de Datos

Valencia, 25 de septiembre de 2019

RESPONSABILIDAD PROACTIVA

El RGPD incorpora dos enfoques fundamentales que inspiran la regulación del derecho fundamental a la protección de datos y que suponen un cambio en el modelo de cumplimiento por parte de los sujetos obligados:

- **EL ENFOQUE DE PROACTIVIDAD O "ACCOUNTABILITY"**
- **EL ENFOQUE DE LA EVALUACIÓN DEL RIESGO**

La responsabilidad proactiva surge del concepto de origen anglosajón, ACCOUNTABILITY, complejo y de difícil traslación al derecho continental, pues engloba aspectos como la asunción y determinación de responsabilidades, la transparencia, la rendición de cuentas, pero que sustancialmente refiere a la aplicación de la normativa de protección de datos y poder demostrarla

RESPONSABILIDAD PROACTIVA

agencia española protección datos

El concepto de responsabilidad proactiva exige que las organizaciones:

- **Apliquen y cumplan los requisitos que establece la regulación de protección de datos**
- **Sean capaces de demostrar ese cumplimiento**

El RGPD lo recoge en las siguientes previsiones:

- **Como principio de actuación en el art. 5.2 RGPD: el responsable del tratamiento será responsable del cumplimiento de los principios y capaz de demostrarlo (responsabilidad proactiva o accountability)**

- **Art. 24.1 RGPD: los responsables aplicarán las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el presente Reglamento. Tales medidas se revisarán y actualizarán cuando sea necesario**

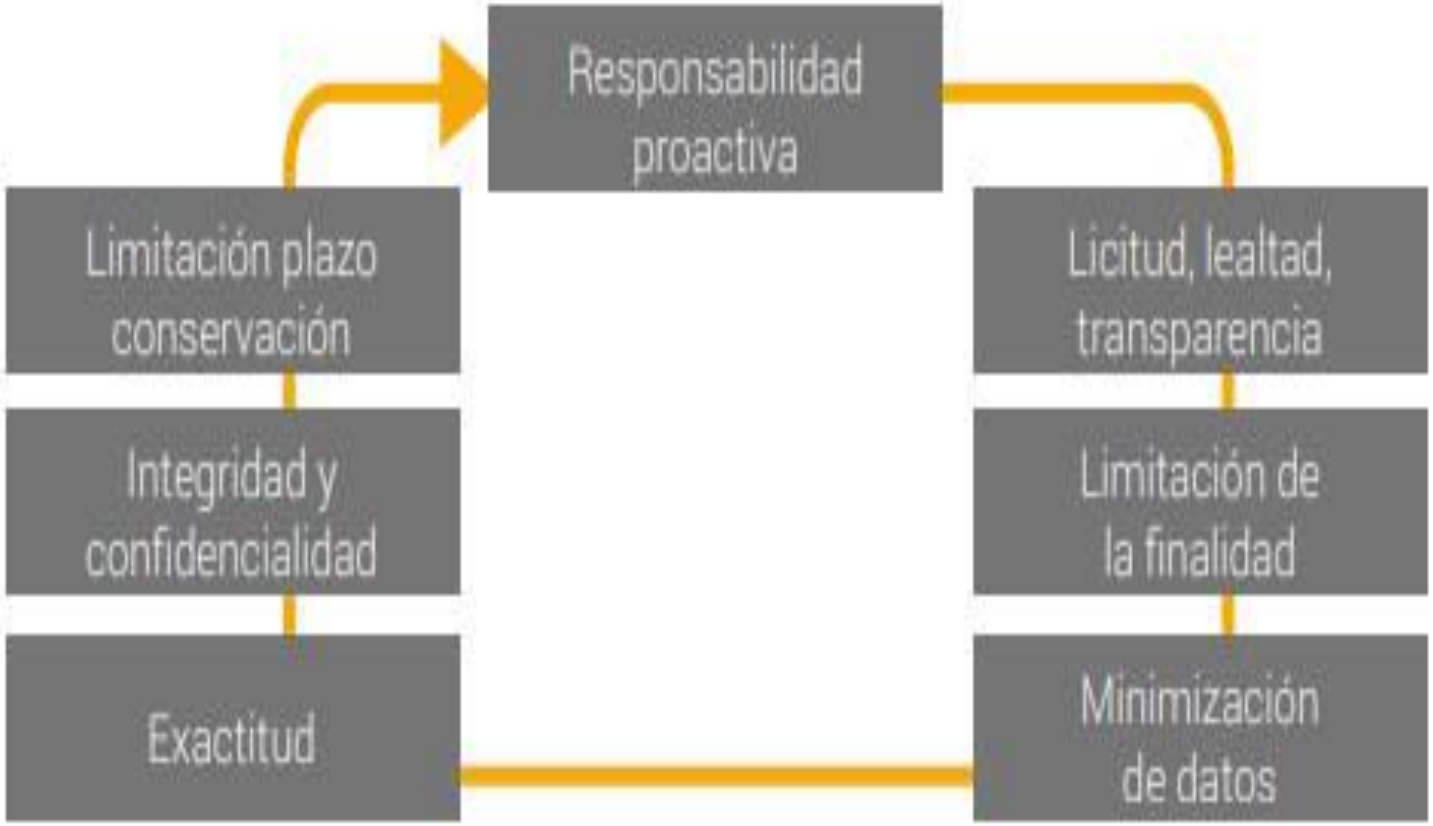
PRINCIPIOS

agencia española protección datos

Principios

- Licitud, lealtad, transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud
- Integridad y confidencialidad
- Limitación del plazo de conservación
- Responsabilidad proactiva

PRINCIPIOS


Responsabilidad proactiva
Licitud, lealtad, transparencia
Limitación de la finalidad
Minimización de datos
Exactitud
Integridad y confidencialidad
Limitación plazo conservación

MEDIDAS DE RESPONSABILIDAD PROACTIVA

MEDIDAS DE RESPONSABILIDAD PROACTIVA

Varían en función de la naturaleza de los datos tratado, los tratamientos y los riesgos que puedan suponer

Obligatorias

- **Registro de actividades de tratamiento**
- **Protección de Datos desde el Diseño**
- **Protección de Datos por Defecto**
- **Acuerdo de corresponsabilidad transparente**
- **Cooperación con la autoridad de control**
- **Análisis de riesgos y adopción de medidas de seguridad adecuadas**
- **Evaluaciones de Impacto**
- **Autorización previa o consultas previas con APD**
- **Brechas de seguridad**
- **Delegado Protección de Datos (DPD)**
- **Transferencias internacionales de datos**

MEDIDAS DE RESPONSABILIDAD PROACTIVA

agencia española protección datos

Voluntarias

- Evaluaciones de Impacto
- Delegado Protección de Datos
- Códigos de conducta
- Certificaciones

Otras medidas

- Establecimiento derotocolos para la atención de derechos
- Establecimiento de protocolos para la prevención, detección, gestión y notificación de brechas de seguridad
- Selección encargados del tratamiento
- Formación staff y usuarios

Políticas de protección de datos

Seguimiento y control de su cumplimiento (tales medidas se revisarán y actualizarán cuando sea necesario. Art. 24.1 RGPD)

- Auditorias periódicas

DELEGADO DE PROTECCIÓN DE DATOS

El **DELEGADO DE PROTECCIÓN DE DATOS (DPD)** como medida de responsabilidad proactiva. El RGPD requiere su **designación obligatoria** para los siguientes tratamientos:

- Cuando el tratamiento se realice por una autoridad u organismo público (independientemente de los datos que se estén procesando y se deja al ámbito interno la fijación del sector público)
- Cuando las actividades principales del responsable del tratamiento o del encargado consisten en operaciones de tratamiento que exigen un control periódico y sistemático de los datos a gran escala
- Cuando las actividades principales del responsable del tratamiento o del encargado consisten en tratar a gran escala categorías especiales de datos o datos personales relativos a condenas y delitos penales

DELEGADO DE PROTECCIÓN DE DATOS

A su vez, la **LOPDPGDD** incluye como supuestos obligatorios (art. 34), entre otros:

- Colegios profesionales y sus consejos generales
- Centros educativos y universidades públicas y privadas
- Centros sanitarios
- Prestadores de servicios de información que elaboren perfiles de usuarios a gran escala
- Entidades de ordenación, supervisión y solvencia de entidades de crédito
- Aseguradoras y reaseguradoras
- Responsables de ficheros comunes de solvencia patrimonial
- Operadores del juego
- …

TAMBIÉN DPD DE DESIGNACIÓN VOLUNTARIA

DELEGADO DE PROTECCIÓN DE DATOS

- **Autoridad organismo público incluyen las autoridades nacionales, regionales y locales.**
- **Demás, una labor pública puede llevarse a cabo, y la autoridad pública puede ejercerse, no solo por las autoridades y organismos públicos sino también por otras personas físicas o jurídicas regidas por el derecho público o privado, en sectores como, según la legislación nacional de cada Estado miembro, los servicios de transporte público, el suministro de agua y energía, las infraestructuras viarias, la radiodifusión pública, la vivienda pública o los órganos disciplinarios de las profesiones reguladas.**
- **En estos casos, los interesados pueden estar en una situación muy similar a la que se produce cuando una autoridad u organismo público trata sus datos. En particular, los datos pueden tratarse para fines similares y las personas suelen tener un poder de decisión igualmente escaso o nulo sobre si sus datos se tratan y de qué manera, y pueden, por tanto, requerir la protección adicional que pueda aportar la designación de un DPD.**
- **Aunque no existe obligación en tales casos, el Grupo de Trabajo del artículo 29 recomienda como buena práctica que las organizaciones privadas que llevan a cabo una función pública o ejercen autoridad pública designen un DPD. La actividad de dicho DPD abarca todas las operaciones de tratamiento realizadas, también las que no están relacionadas con el desempeño de una función pública o el ejercicio de una autoridad pública**

DELEGADO DE PROTECCIÓN DE DATOS

Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial (RGPD considerando 97)

Designar un Delegado de Protección de Datos

- **Podrá designarse un único DPD para varias autoridades u organismos dependiendo de tamaño y características, pero accesible para usuarios y afectados de cada responsable**
- **El DPD puede ser un miembro del personal del responsable del tratamiento o del encargado del tratamiento (DPD interno) o «cumplir las tareas sobre la base de un contrato de servicios», que se puede celebrar con un individuo u organización**
  - **Equipo de personas bajo la responsabilidad del contrato designado**
  - **Cada miembro del equipo debe cumplir los requisitos del RGPD**

DELEGADO DE PROTECCIÓN DE DATOS

agencia española protección datos

Funciones

- Informar y asesorar a responsable y encargado, documentando esa actividad
- Supervisar la puesta en práctica de las políticas de protección de datos, incluidas la formación y la auditoría
- Supervisar la aplicación del Reglamento en lo relativo a privacidad desde el diseño y por defecto, y derechos de los interesados
- Asegurar la existencia y mantenimiento de documentación obligatoria
- Supervisar gestión de quiebras de seguridad

DELEGADO DE PROTECCIÓN DE DATOS

agencia española protección datos

Tareas del DPD

- Preliminares
- Organizativas
- Control de cumplimiento
- Asesoramiento
- Cooperación y consulta a la autoridad de control
- Gestión de las reclamaciones de los interesados
- Concienciación y formación

Tareas ligadas al principio de responsabilidad proactiva y capacidad de demostrar cumplimiento

DELEGADO DE PROTECCIÓN DE DATOS

agencia española protección datos

Tareas del DPD

Tareas preliminares

- Analizar el contexto de la organización, aproximación a los tratamientos, organigrama, funciones, competencias, relaciones externas, relaciones informales, prestadores, servicios en la nube, …
- Mapa de los procesos y actividades de tratamiento de la organización
- Identificar requisitos legales
- Responsables del servicio Estructura ICT, seguridad de la información, políticas, tratamientos manuales,
- Estructura, recursos, para la gestión de la protección de datos, red de DPD
- Metodología: Sistema de gestión integral de la protección de datos
- Apoyo de la dirección

DELEGADO DE PROTECCIÓN DE DATOS

Tareas del DPD

- **Tareas organizativas**
  - **Análisis de riesgos (seguridad):**
    - Niveles de impacto
    - Áreas de análisis clásicas
      - Red y recursos técnicos: Acceso a través de Internet, conexión externa, usuarios no autorizados, metodologías para el diseño y la implantación de aplicaciones
      - Procesos y procedimientos: Definición de roles y responsabilidades, uso de los recursos, conexión con medios propios, envío de soportes, activación de registros de acceso.
      - Terceras partes y personas: acceso por un número no definido de empleados, acceso por terceras partes, obligaciones ambiguas, formación en protección de datos y seguridad, políticas para la destrucción segura.
      - Tipo de sector para ver exposición: sector expuesto a los ataques, ataques anteriores, brechas, tratamiento de gran escala de datos y/o personas.

DELEGADO DE PROTECCIÓN DE DATOS

agencia española protección datos

Tareas del DPD

- **Tareas organizativas**
  - **Análisis de riesgos (derechos de las personas):**
    - **Utilizar datos para una finalidad no compatible.**
    - **Riesgo de reidentificación**
    - **Tratamiento de datos por más tiempo del necesario.**
    - **Tratamiento de datos no actualizados**
    - **Tratamiento de datos de menores**
    - **Tratamiento de datos de colectivos vulnerables**
    - **No informar a los interesados**
    - **Transferencia de datos sin las garantías adecuadas**

DELEGADO DE PROTECCIÓN DE DATOS

agencia española protección datos

Tareas del DPD

- **Tareas organizativas**
  - **Análisis de posibles riesgos elevados - EIPD**
    - Evaluación sistemática y exhaustiva de aspectos personales de personas físicas, elaboración de perfiles -> decisiones injustas.
    - Tratamiento a gran escala de categorías especiales de datos - discriminación
    - Observación sistemática a gran escala de una zona de acceso público -> efectos en los derechos fundamentales
  - Listas aprobadas por las autoridades de control
  - Diferencias en los roles del responsable y del DPD en relación con las EIPD:
    - El responsable pedirá el asesoramiento del DPD, entre otros casos:
      - Si debe realizarse una EIPD
      - Metodología a utilizar
      - Si realizar la EIPD internamente o subcontratarla.
      - Controles a aplicar
      - Si la EIPD ha sido realizada correctamente
      - Documentar los desacuerdos

DELEGADO DE PROTECCIÓN DE DATOS

Tareas del DPD

- **Tareas de revisión del cumplimiento**
  - **Supervisar internamente el cumplimiento del RGPD:**
    - **Recopilar información para identificar actividades de tratamiento**
    - **Analizar y revisar el cumplimiento de las actividades de cumplimiento**
    - **Informar, asesorar y emitir recomendaciones al responsable y encargado.**
    - **Revisión continúa.**
    - **Documentación actualizada**
    - **Revisión del marco regulatorio y contractual dentro de la organización con el fin de identificar el impacto y poder emitir recomendaciones a las personas y a la dirección.**

DELEGADO DE PROTECCIÓN DE DATOS

Tareas del DPD

- **Tareas de gestión de las reclamaciones de los interesados (internas y externas)**
  - **Investigación:**
    - **Derivada de la tarea de supervisar el cumplimiento (art. 39 (1) b).**
    - **Recursos y acceso a los datos e instalaciones, encargados**
    - **Necesidad de que los responsables hagan explícito en sus guías internas.**
  - **Limitaciones en enforcement (hacer cumplir).**
  - **Consulta a la autoridad de control.**

DELEGADO DE PROTECCIÓN DE DATOS

Tareas del DPD

- **Tareas de asesoramiento general**
  - **Informar, ofrecer asesoramiento y hacer recomendaciones para la mejora práctica de la protección de datos en la organización y la aplicación de la normativa de protección de datos.**
  - **Adopción o adaptación de las políticas de protección de datos, seguridad de la información, procedimientos, etc.**
  - **Seguimiento de la legislación, jurisprudencia, documentos EDPB**
  - **Participación en las reuniones del Comité de Dirección cuando se tomen decisiones en materia de protección de datos.**
  - **Ser informado y seguimiento en el caso de brechas.**

DELEGADO DE PROTECCIÓN DE DATOS

Tareas del DPD

- **Tareas de asesoramiento: Políticas, contratos, transferencias internacionales. Códigos de conducta y certificaciones**

  - **Elaboración y actualización de políticas de protección de datos, formularios, declaraciones, política de cookies**
  - **Registros de acceso**
  - **Seguimiento de las actualizaciones de seguridad**
  - **Adopción de acuerdos administrativos**
  - **Contratos**
  - **Transferencias internacionales**
  - **Asesorar en la adhesión a códigos de conducta como forma de demostrar cumplimiento.**
  - **Asesoramiento para obtener certificaciones**

DELEGADO DE PROTECCIÓN DE DATOS

Tareas del DPD

- **Tareas de asesoramiento: Privacidad por diseño y por defecto**
  - **Deber de incorporar la protección de datos por diseño y por defecto. « Principio de responsabilidad activa».**
  - **Resultado de un proyecto desde el inicio del mismo que cubra todo el ciclo de vida en los que se identifiquen los riesgos y los requerimientos.**
  - **Basado en un enfoque basado en el riesgo en los que los activos a ser protegidos son los individuos, en particular, sus derechos y libertades fundamentales.**
  - **Medidas apropiadas y efectivas en relación con esos riesgos.**
  - **Necesidad de integrar las salvaguardas y controles en el proceso.**
  - **Responsables, encargados, desarrolladores de productos y tecnología.**
  - **Diligencia a la hora de seleccionar a los proveedores en los concursos debiendo poder demostrar cumplimiento.**
  - **Participación en el diseño, desarrollo, pruebas de los productos, servicios que traten datos personales.**

DELEGADO DE PROTECCIÓN DE DATOS

Tareas del DPD

- **Cooperación y consulta a la autoridad de control: Punto de contacto**
  - **Colaboración para la concienciación**
  - **Enfoque preventivo**
  - **Consulta**
  - **Evaluación del progreso en la implantación de medidas**
  - **Contestación a las reclamaciones (art. 37 LOPDPGDD)**

Dos de cada tres reclamaciones que se envían al responsable o al DPD se resuelvan de forma satisfactoria para el particular. Además, la mitad de las reclamaciones admitidas en la Agencia se resuelven **en una media de 100 días, sin tener que esperar los más de 200 días de media del modelo anterior**.

DELEGADO DE PROTECCIÓN DE DATOS

agencia española protección datos

Tareas del DPD

- **Concienciación y formación**

  - La concienciación estimula el enfoque preventivo
  - Plan de formación
  - Herramientas para la información interna y externa
  - Publicación del registro de actividades
  - Formularios para el ejercicio de derechos
  - Contacto del DPD

FUNCIONES GENERALES DEL DPD

aepd agencia española protección datos

Tareas preliminares

- Analizar el contexto de la organización, aproximación a los tratamientos, organigrama, funciones, competencias, relaciones externas, relaciones informales, prestadores, servicios en la nube, …

- Identificar requisitos legales

- Responsables del servicio Estructura ICT, seguridad de la información, políticas, tratamientos manuales,

- Estructura, recursos, para la gestión de la protección de datos, red de DPDs.

- Metodología: Sistema de gestión integral de la protección de datos

- Apoyo de la dirección

Tareas organizativas

- Registro de actividades de tratamiento
- Revisar las actividades de tratamiento
- Análisis de riesgos
- Análisis de posibles riesgos elevados- EIPD

Tareas de asesoramiento

- Asesoramiento general
- Privacidad por diseño y por defecto
- Revisión del cumplimiento de las políticas

Tarea de monitorización, revisión y seguimiento

Cooperación con la AEPD

Gestión de las reclamaciones de los interesados

Información y concienciación

DELEGADO DE PROTECCIÓN DE DATOS

POSICIÓN DEL DPD

- Apoyo activo por parte de la alta dirección. Rinde cuentas al más alto nivel de la organización
- Disponibilidad de tiempo para cumplir sus obligaciones
- Apoyo adecuado en términos de recursos humanos y materiales
- Comunicación oficial de su designación a la Autoridad de Control y a todo el personal
- Acceso a otros servicios dentro de la organización para que puedan recibir apoyo esencial, aportaciones o información de esos otros servicios
- Acceso a los tratamientos de datos
- Formación continua
- Es el interlocutor con la AEPD
- Documentará y comunicará las vulneraciones relevantes a los órganos de administración y dirección

DELEGADO DE PROTECCIÓN DE DATOS

EJERCICIO INDEPENDIENTE DE SUS FUNCIONES

- **Ninguna instrucción de los responsables o encargados sobre el ejercicio de las tareas del DPD**
- **Ningún despido o sanción al delegado por el desempeño de sus tareas, salvo dolo o negligencia grave**
- **No son personalmente responsables por el incumplimiento del RGPD, es responsabilidad del responsable o del encargado. No es aplicable el régimen sancionador de la LOPDPGDD a los DPD (art. 70.2)**
- **Ausencia de conflicto de intereses con otras posibles tareas y deberes**
  - **El DPD no puede ocupar un puesto dentro de la organización que lo conduzca a determinar los propósitos y los medios del tratamiento de los datos personales. Debido a la estructura organizativa específica en cada organización, esto debe ser considerado caso por caso.**
  - **Como regla general, las posiciones conflictivas pueden incluir posiciones de alta dirección, jefe de Recursos Humanos o jefe de departamentos de TI, pero también otros roles más bajos en la estructura organizativa si tales posiciones o roles conducen a la determinación de propósitos y medios de tratamiento**

DELEGADO DE PROTECCIÓN DE DATOS

REQUISITOS DEL DPD: El RGPD exige que «se designe sobre las base de cualidades profesionales y, en particular, conocimientos especializados sobre la legislación y las prácticas en materia de protección de datos y sobre la capacidad para cumplir las tareas a que se refiere el artículo 39»:

- **Experiencia en las leyes y prácticas nacionales y europeas en materia de protección de datos, incluida una comprensión en profundidad del RGPD**
- **Comprensión de las operaciones de tratamiento realizadas**
- **Comprensión de las tecnologías de la información y la seguridad de los datos**
- **Conocimiento del sector empresarial y de la organización**
- **Capacidad para promover una cultura de protección de datos**
- **No se prevé cómo acreditar cualidades profesionales**
  - **Podrá demostrarse por mecanismos voluntarios de certificación (LOPDPGDD)**

DELEGADO DE PROTECCIÓN DE DATOS

agencia española protección datos

NIVEL DE CONOCIMIENTOS:

- **Acorde a la sensibilidad, complejidad y cantidad de los datos que trate la organización**
- **En el caso de una autoridad u organismo público u sólido conocimiento de las normas y procedimientos administrativos**

CAPACITACIÓN SECTOR PÚBLICO

- **Cursos INAP**
- **MOOC de formación para Delegados de Protección de Datos de Administraciones Públicas:**

DELEGADO DE PROTECCIÓN DE DATOS

MOOC de Formación para DPD de Administraciones Públicas

- **MÁS INFORMACIÓN EN: www.aepd.es**
- **PARA REGISTRARSE**
- **https://forma2.inap.es/courses/AEPD/AEPD19-01/2019_T2/about**

DELEGADO DE PROTECCIÓN DE DATOS

agencia española protección datos

IMPORTANTE

DESIGNAR DPD

- **Sólo se han comunicado 2.230 DPD de Administraciones Locales de 8.124.**
- **La AEPD tendría competencias sobre 6.926 Ayuntamientos, 947 serían de competencia de la APDCAT y 251 de la AVPD. Desde el 1 de octubre el Consejo de Transparencia y Protección de Datos de Andalucía será el competente sobre los municipios de la Comunidad Autónoma de Andalucía**
- **De las 43 ciudades de más de 150.000, 13 no han designado DPD (otras 2 más en el ámbito de la AVPD)**

MATERIALES Y RECURSOS AEPD

- GUÍA PROTECCIÓN DE DATOS Y ADMINISTRACIÓN LOCAL
- GUÍA PARA EL RESPONSABLE DEL TRATAMIENTO DE DATOS
- GUÍA PARA EL CUMPLIMIENTO DEL DEBER DE INFORMAR
- DIRECTRICES PARA LA ELABORACIÓN DE CONTRATOS DE ENCARGO DE TRATAMIENTO
- GUÍA DE ANÁLISIS DE RIESGOS
- LISTADO DE CUMPLIMIENTO NORMATIVO
- GUÍA DE EVALUACIONES DE IMPACTO
- MODELO DE INFORME DE EIPD PARA LAS APP
- GUÍA DE BRECHAS DE SEGURIDAD
- HERRAMIENTA FACILITA_RGPD (versión 2.0)
- HERRAMIENTA GESTIONA_EIPD
- Todo esto y mucho más en…

aepd agencia española protección datos

VISITEN NUESTRA WEB

MUCHAS GRACIAS

www.aepd.es

@AEPD_es