TEMA 82. ADAPTACIÓN DE APLICACIONES Y ENTORNOS A LOS REQUISITOS DE LA NORMATIVA DE PROTECCIÓN DE DATOS SEGÚN LOS NIVELES DE SEGURIDAD. HERRAMIENTAS DE CIFRADO Y AUDITORÍA

Actualizado a 24/09/2020

1. CONTEXTO NORMATIVO

Norma	Observaciones
Histórico	
REGLAMENTO (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)	De aplicación desde el 25 de mayo de 2018. Deroga la Directiva 95/46/CE. Desarrolla el derecho a la protección de los datos de carácter personal establecido en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE).
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (**LOPDGDD**).	Deroga la Ley Orgánica 15/99 de Protección de Datos y el Real Decreto 1720/2007, si "*contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la LOPDGDD.*" Respeta en todo momento el Reglamento General de Protección de Datos y clarifica su contenido.

Guías de la AEPD	Observaciones
Novedades para los ciudadanos para el Sector Privado Obligaciones para el Sector Público, y	En la carpeta de Doc. Adicional
Evaluación de impacto y Análisis de Riesgos	En la carpeta de Doc. Adicional
Listas de tipos tratamientos exentas y obligadas a una evaluación de impacto	En la carpeta de Doc. Adicional. *Son documentos pequeños que merece mucho la pena repasarlos*.

2. TEMAS RELACIONADOS

TEMA 27. La política de protección de datos de carácter personal.
TEMA 38. Auditoría informática
TEMA 79. El cifrado

3. MEDIDAS DE ADAPTACIÓN

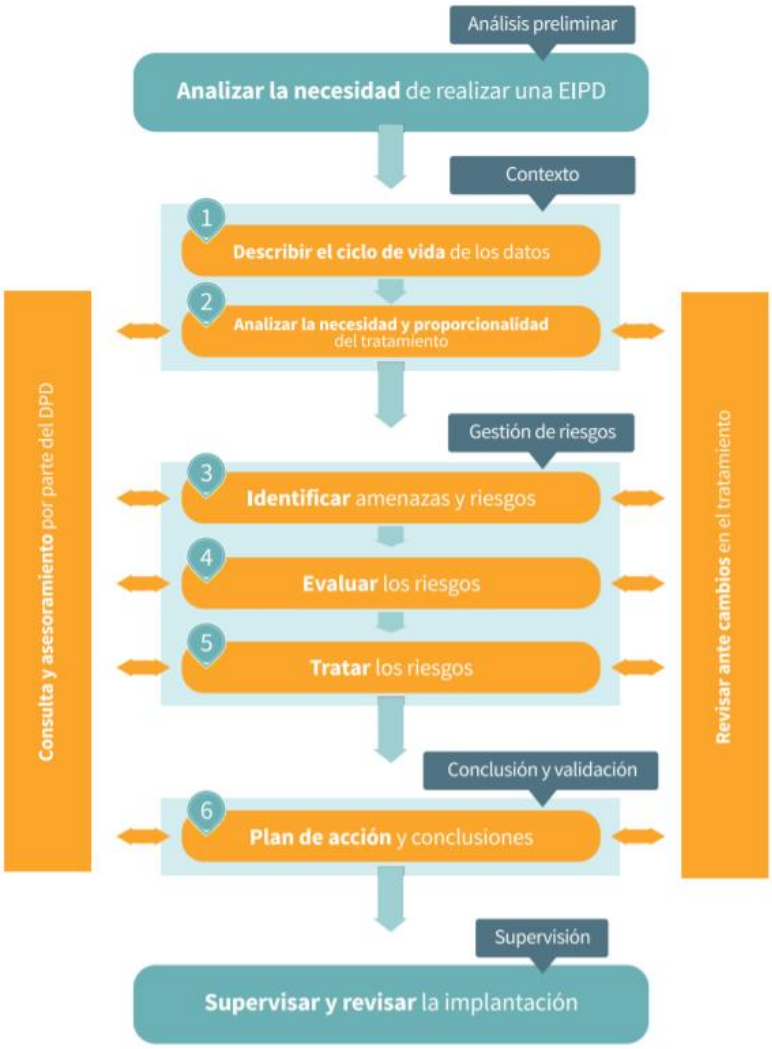
3.1. REGLAMENTO 679/2016

Con la entrada en vigor del nuevo reglamento Europeo de Protección de Datos en mayo de 2018, se cambia el paradigma de aplicación de la normativa de protección de datos. El Reglamento 679/2016 no propone medidas concretas para aplicar sobre los sistemas de información. En todo caso, el reglamento habla del **principio de responsabilidad proactiva**, que se materializa en:

- Registro de actividades de tratamiento, indicando las actividades de tratamiento de datos personales, la finalidad y la base jurídica.

- Análisis de riesgos y adopción de medidas de seguridad (Artículo 25)
    - Evaluar los riesgos inherentes al tratamiento, y aplicar medidas para mitigarlos (como el cifrado).
    - Incluidos los derivados del tratamiento como la destrucción, pérdida o alteración.

- Notificación de brechas de seguridad (Artículo 33), el responsable del tratamiento estará obligado a notificar en menos de 72 horas a la autoridad de control (AEPD) brechas de seguridad que supongan un riesgo para los derechos y libertades de las personas físicas.
- Medidas de protección de datos desde el diseño y por defecto, es necesario identificar los datos, las fuentes de información y definir el ciclo de vida y flujo de los mismos, para su protección.
    - *Recogida de datos*: analizar los tipos de datos que se recaban con un criterio de minimización en función de los productos y servicios seleccionados por el usuario;
    - *Tratamiento de los datos*: analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos;
    - *Conservación*: implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios;
    - *Accesibilidad*: limitar el acceso por parte de terceros a dichos datos personales.
- Seguridad del tratamiento (Artículo 32), incluyendo las medidas de seguridad para su adecuación al nivel de seguridad
    - Técnicas y organizativas para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.
        - la pseudonimización y el cifrado de datos personales.
        - la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento
        - la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico
        - un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento
    - Adecuadas al riesgo de probabilidad y gravedad, se definen en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento.
- Evaluaciones de impacto sobre la protección de datos (**EIPD)** (artículo 35)



- Designación de un Delegado de protección de datos DPD (Artículo 37), de manera conjunta entre el responsable de los datos y el encargado del tratamiento. Se debe incluir en un registro público.
- Definición de Códigos de conducta
- Transferencias internacionales

Según el RGPD:

- El encargado del tratamiento permitirá y contribuirá a la realización de auditorías
- El delegado de protección de datos supervisará la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Para garantizar la verificación del cumplimiento de las normas corporativas vinculantes, se realizarán mecanismos como auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado.
- La autoridad de control, AEPD en el caso de España, llevará a cabo investigaciones en forma de auditorías de protección de datos

Sin embargo, no se establece un frecuencia ni obligación de realización de las auditorías expresamente.

3.2. LOPDGDD

Tampoco hace referencia frecuencia ni obligación de realización de las auditorías. Solo se indica:

- La AEPD desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas. (Artículo 51)
- La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva (Artículo 54), pudiendo dictar las directrices generales o específicas a resultas de los planes.

4. HERRAMIENTAS

4.1. CIFRADO

- El cifrado de la información es un proceso que consiste en volver ilegible la información que se considera relevante. Solamente será legible previa aplicación de una clave.
- Se recomienda la lectura del Tema 79
- Según el ENS (RD 3/2010), el cifrado de la información solo aplica para el nivel ALTO en la dimensión de confidencialidad, tanto en su almacenamiento como en su transmisión, solo estará en claro durante su uso. En la Guía de Seguridad de las TIC CCN-STIC 807, se establece la Criptología de empleo en el Esquema Nacional de Seguridad.

4.2. AUDITORIA

PARA SECTOR PÚBLICO:

- **PILAR (CCN):** Herramientas de análisis y gestión de riesgos de sistemas de información, según las amenazas determina los riesgos potenciales sobre los activos de la organización, estableciendo las salvaguardas recomendadas para reducir el riesgo a valores residuales. Incluye una verificación al RGPD. Se debe realizar de manera continua y recurrente. Utiliza la metodología Magerit. Salidas:
  - Impacto potencial y residual.
  - Riesgo potencial y residual.
  - Mapa de riesgos.
  - Plan de mejora de la seguridad
  - Continuidad de Operaciones
  - Análisis cuantitativos y cualitativos
  - Monitorización continúa del Estado de Riesgo
  - https://pilar.ccn-cert.cni.es/index.php
- **Guía de Seguridad CCN-STIC 802 (CCN)**, establece la guía de Auditoría:
  - Categoría Básica: autoevaluación cada 2 años o con cambios sustanciales.
  - Categoría Media o Alta: auditoria formal cada 2 años o con cambios sustanciales. Garantías metodológicas y de independencia, profesionalidad y adecuación requeridas.
- **ASSI-RGPD (Auditoría de Seguridad de los Sistemas de Información - Reglamento General de Protección de Datos):** Aplicación para cualquier AA. PP para:

- Mantener un Registro de Actividades de Tratamientos de Datos Personales (RAT)
- Facilitar el cumplimiento del resto de obligaciones del RGPD y la LOPD-GDDP:
  - Análisis de riesgos
  - Evaluación del impacto de las operaciones de tratamiento (si procede según la lista de Obligadas – ver carpeta Adicional>AEPD>Guías)
- Realizar el proceso de autoevaluación y/o auditoría que exige el ENS y la normativa de protección de datos (acceso el primer módulo)
- Proponer las medidas ENS aplicables según los riesgos y el impacto
- Desarrollado por el Ministerio de Trabajo, Migraciones y Seguridad Social
- https://administracionelectronica.gob.es/ctt/assirgpd

PARA SECTOR PRIVADO:

- **Facilita RGPD (AEPD)**: Herramienta gratuita de ayuda para empresas que realicen un tratamiento de datos personales de escaso riesgo para el cumplimiento del Reglamento General de Protección de Datos.
  - https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDI3NzMzOTgxNTk2NjIyOTUzNDE2?updated=true
- **Facilita EMPRENDE (AEPD)**: Herramienta gratuita de apoyo a emprendedores y startups cuyos tratamientos se caracterizan por un fuerte componente innovador que hace uso de nuevas tecnologías. Al finalizar su ejecución se generan un conjunto de documentos adaptados que sirven de guía y apoyo para cumplir con las obligaciones. Se obtiene:
  - una política de información en dos niveles compuesta por las cláusulas de informativas a proporcionar en el momento de la recogida de datos y una política de privacidad.
  - el Registro de Actividades de Tratamiento (RAT) precumplimentado.

- el modelo de hoja de registro de incidentes para cumplir con el artículo 33.5 relativo a la documentación de las brechas de seguridad.
- un conjunto de cláusulas contractuales a incluir en los contratos que suscriba con los encargados de tratamientos de datos y proveedores.
- si su empresa cuenta con una página web que utiliza cookies y tecnologías similares, una política de cookies
- un conjunto de directrices y recomendaciones, para ayudarle en el proceso de adecuación, en relación con la gestión de brechas de seguridad, la atención al ejercicio de los derechos, recomendaciones sobre videovigilancia, indicaciones específicas con relación a la gestión de los riesgos de sus tratamientos, así como a las estrategias de privacidad y medidas de seguridad que deberá implementar.
- Una relación de recomendaciones para prevenir el acoso digital.
- https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDI3NzM0MDMxNTk2NjIzMjY0OTQ0/?updated=true

- **BIA (Business Impact Analysis):** Herramienta de análisis que identifica los procesos críticos para la operación de una organización, y posteriormente los prioriza según su criticidad y el coste ocasionado por su interrupción. Se utiliza para la elaboración del Plan de Continuidad orientado a la recuperación y restauración de los procesos en caso de desastre o interrupción parcial o total no deseada.

PARA DELEGADOS DE PROTECCIÓN DE DATOS

- **Informa RGPD (AEPD):** prestar soporte en aquellas dudas y cuestiones que puedan derivarse de la aplicación del Reglamento General de Protección de Datos (RGPD). El DPD debe haberse comunicado dicho nombramiento a la AEPD previamente.

PARA RESPONSABLES DEL TRATAMIENTO

- **GESTIONA EIPD (AEPD)**: herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.
  - https://gestiona.aepd.es/

GENÉRICAS (NO SOLO PROTECCIÓN DE DATOS):

- Auditoría de análisis de red, generando informes con el estado de los componentes:
  - **Network Inventory Advisor** – Auditoría de todo el software y hardware que se encuentra en la red de manera sencilla. Descubre todos los activos que se encuentran en la red y realiza un análisis.
  - **MAPILabReports** – Reportes del estado de la infraestructura de la tecnología de la información, auditoría de seguridad, etc.
- Auditorías informáticas, herramientas de ayuda:
  - **ACL – Audit Command Language** – Herramienta para la programación de pruebas CAAT (análisis de pruebas asistidas por computador)
  - **IDEA** – Equivalente a la herramienta ACL Existen además numerosas herramientas tanto de software libre como de pago que permiten la auditoría de redes, aplicaciones, o asistir a los auditores en sus tareas.