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.
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (**LOPDGDD**).	Respeta en todo momento el Reglamento General de Protección de Datos y clarifica su contenido.
AEPD	
Novedades para los ciudadanos, para el Sector Privado y obligaciones para el Sector Público Evaluación de impacto y Análisis de Riesgos Listas de tipos tratamientos exentas y obligadas a una evaluación de impacto (Importante)	

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

Supone un cambio de paradigma, sin medidas concretas. Está centrado en el **principio de responsabilidad proactiva**, materializado en:

- Registro de actividades de tratamiento (RAT)
- Análisis de riesgos y adopción de medidas de seguridad (Artículo 25)
    - Evaluar los riesgos y aplicar medidas para mitigarlos (como el cifrado): identificación, evaluación y tratamiento de riesgos, con una monitorización continua.
- 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).
- Medidas de protección de datos desde el diseño y por defecto
- Seguridad del tratamiento (Artículo 32), incluyendo las medidas de seguridad:
    - Técnicas y organizativas para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.
        - Pseudonimización y el cifrado de datos personales
        - Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento
        - Capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico

        - 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, 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), incluye:
    - Análisis de necesidad de EIPD
    - Definición del contexto: ciclo de vida de los datos, análisis de necesidad y proporcionalidad
    - Gestión de riesgos: identificación de amenazas y riesgos, evaluación de riesgos y tratamiento riesgos.
    - Conclusión y validación: plan de acción y conclusiones
    - Supervisión y revisión de la implantación
- Designación de un Delegado de protección de datos (Artículo 37)
- Definición de Códigos de conducta
- Transferencias internacionales

Según el RGPD, 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.

4. HERRAMIENTAS

4.1. CIFRADO

- 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 (almacenamiento y transmisión). 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. https://pilar.ccn-cert.cni.es/index.php
- **Guía de Seguridad CCN-STIC 802 (CCN)**, establece la guía de Auditoría a realizar cada 2 años o tras cambios sustanciales:
    - Categoría Básica: autoevaluación.
    - Categoría Media o Alta: auditoria formal. 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 Registro de Actividades de Tratamientos de Datos Personales
- 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
- 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 RGPD. 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 IT. 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.

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. 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. Descubre todo el activo conectado 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