"LA GESTIÓN DEL RIESGO, COMO EL LEGISLADOR UNIFICA SEGURIDAD Y PRIVACIDAD EN UN ÚNICO MÉTODO DE ANALISIS PARA LAS ADMINISTRACIONES PÚBLICAS"

ARÁN FEIJOO COVELO

DELEGADO DE PROTECCIÓN DE DATOS (AYUNTAMIENTO DE SALVATERRA DE MIÑO)

SUMARIO:

Resumen: Gestión de riesgos, seguridad y privacidad

Palabras Clave (*Keywords*): Esquema nacional de seguridad , Reglamento UE 2016/679, Ley 3/2018, Disposición adicional Primera.

I. INTRODUCIÓN

Con la entrada en Vigor de la Ley orgánica 3/2018 de cinco de Diciembre que ha entrado en vigor el siete de Diciembre de 2018 se cierra el círculo normativo para el análisis de la gestión del riesgo en las administraciones públicas.

En su disposición adicional primera, “Medidas de seguridad en el ámbito del sector público” especifica que el esquema nacional e seguridad deberá adaptar las medidas a implementarse en función de los criterios de gestión del riesgo según lo establecido en el artículo 32 del reglamento UE 2016/679.

El artículo 32 del Reglamento UE 2016/679 nos habla de la seguridad en el tratamiento y especifica algunas de las medidas que se ha de tomar para garantizar la seguridad del tratamiento de los datos.

Por tanto en este artículo sobre la gestión del riesgo desarrollare cada uno de los tres apartados anteriores, Esquena Nacional de seguridad, Disposición adicional primera ley 3/2018 y artículo 32 del Reglamento UE 2016/679

II. ANALISIS DE LA GESTIÓN DEL RIESGO

La primera vez que aparece el concepto de análisis de la gestión del riesgo en nuestro ordenamiento jurídico es de la mano del esquema nacional de seguridad. el art. 6 del ENS señala como obligatorio, para todos los sistemas afectados por el ENS, el desarrollo de un Análisis de Riesgos, al que deberá seguir el correspondiente proceso de Gestión de Riesgos (art. 13).

El esquema Nacional de seguridad hace referencia expresa en su guía de interpretación a la definición de la gestión del riesgo que da la “Agencia de la unión europea para la seguridad de las redes y la información “

“La gestión de riesgos es el proceso de identificar, cuantificar y gestionar los riesgos que enfrenta una organización; es un proceso dirigido a obtener un equilibrio eficiente entre la obtención de oportunidades de ganancias y la minimización de vulnerabilidades y perdidas como parte integral de las practicas de gestión y un elemento esencial de la buena gobernanza, la gestión de riesgos debe ser recurrente para apoyar la mejora organizativa, el rendimiento y la toma de decisiones”

Este concepto de análisis de la gestión del riesgo , es una metodología que viene de la normativa internacional y europea por tanto podríamos decir que ajena a nuestra propia normativa , la encontramos ya en normas como la ISO 27001 y también en otras como la ley 31/95 de prevención de riesgos laborales y reglamento de desarrollo . Pues no olvidemos que la ley de prevención española viene de una transposición directa de una directiva europea, la 89/391/CEE. El análisis del riesgos es el pilar sobre el que tras una análisis de la probabilidad de que ocurra un riesgo y la consecuencia de que esto suceda , se categoriza el riesgo se asignan medidas preventivas para evitar que esto suceda y mecanismos de control para verificar que esas medidas preventivas se cumplen.

Fíjense en la importancia del concepto de medida preventiva, frente a la tradicional medida correctiva. Es decir cuando un riesgo se materializa existen medidas para paliar los daños producidos o minorarlos. Sin embargo el establecimiento de una medida preventiva requiere de un análisis previo de datos sobre la probabilidad de que el riesgo suceda (frecuencia del hecho,

antecedentes previos) y un estudio de la consecuencia para establecer medidas de seguridad que mantenga controlado la probabilidad de que el riesgo suceda.

Según el Esquema nacional de seguridad en su art. 6 es obligatorio que todos los sistemas afectados por el ENS realicen un análisis de la gestión del riesgo. Es por tanto que todas las administraciones locales debería tener en este momento una evaluación de riesgos, análisis de riesgos. Ya que el ENS según lo que fija el artículo 2 de la ley 11/2007 es de aplicación a

- Administración general del estado, administraciones de las comunidades autónomas y las entidades que integran las administraciones locales asi vinculadas o dependientes de las mismas.
- A los ciudadanos en sus relaciones con las administraciones públicas.
- A las relaciones entre las distintas administraciones públicas.

Tan solo está excluido del ámbito de aplicación del ENS, los sistemas que tratan información clasificada que tratan por la ley 9/1968 de cinco de Abril.

La Administración de Justicia no está obligada por la Ley 11/2007, ni por lo tanto por el ENS. Sin embargo cuentan con un programa de actuación, denominado Esquema Judicial de Interoperabilidad y Seguridad (EJIS), suscrito por las Instituciones con responsabilidades en la Administración de Justicia (Ministerio de Justicia, el Consejo General del Poder Judicial, la Fiscalía General del Estado y las Comunidades Autónomas con competencias transferidas). El EJIS es un marco de colaboración para colegiar esfuerzos y cuyos objetivos fundamentales son la prestación de los servicios de Administración de Justicia bajo el paradigma de la interoperabilidad, accesibilidad, reusabilidad y seguridad

Es por tanto que en la teoría todas las administraciones locales parten del hecho de estar en posesión de un análisis para la gestión del riesgo, ya que el ENS es obligatorio para todas las administraciones locales sin excepción desde el 2007. El plazo que se daba a las administraciones para la implementación del Esquema nacional de seguridad era de 12 meses .En el caso de no ser posible se debería establecer un plan de adecuación para su implementación.

Una de las preguntas que pueden surgir a la hora de realizar un estudio de la gestión del riesgo, es el método a utilizar.

En el Reglamento europeo de protección de datos UE 2016/679 no especifica el cómo evaluar el riesgo , habla eso si del análisis de impacto que dará lugar a la gestión del riesgo pero no concreta como realizar dicho análisis, Esto es una constante en la normativa europea que podríamos denominar como finalista , es decir, no tipifica el cómo realizar las acciones tan solo indica el objetivo a garantizar y unas pautas generales dejando que el administrado atraves de entidades privadas o público privadas pueda desarrollar métodos de gestión o control del cumplimiento normativo.

Un ejemplo claro de esto son las entidades de clasificación o organizaciones como el grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales. Este grupo de trabajo creado de conformidad al artículo 29 de la directiva 95/46/CE, es un órgano consultivo e independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de la directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE

- Dar consejos de expertos a los Estados en relación con la protección de datos.
- Promover la misma aplicación de la Directiva de protección de datos en todos los estados miembros de la UE, así como de Noruega, Liechtenstein e Islandia.
- Facilitar a la Comisión un dictamen sobre las leyes comunitarias (primer pilar) que afectan al derecho a la protección de datos personales.

Como órgano consultivo, emitió Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679

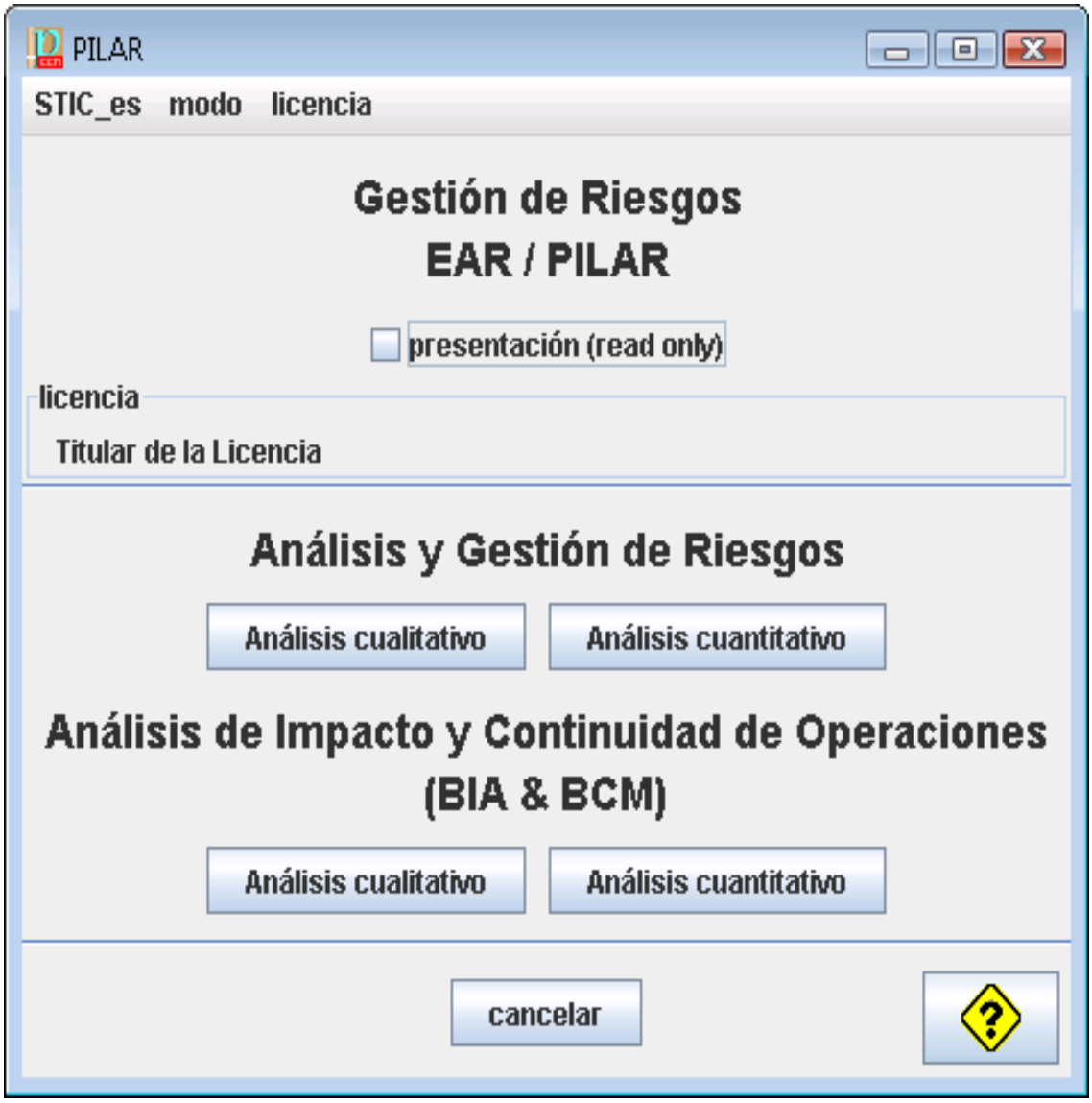
Es decir las pautas y criterios recomendables para la elaboración de una evaluación de impacto, léase riesgos, de cara a realizar una adecuada gestión de los mismos.

Pese a que sus directrices no son de obligado cumplimiento, el hecho de que el grupo este constituido por un representante de cada una de las agencias de protección de datos nacionales y de su reconocido prestigio hacen que sean las pautas más adecuadas para rellenar el hueco dejado por el RGPD a la hora de fijar los riesgos.

En todo caso las administraciones locales españolas. El análisis de la gestión del riesgo está basado en la metodología basadas MAGERIT, en su calidad de método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas

apropiadas que deberían adoptarse para controlar estos riesgos, de aplicación en la Administración General del Estado, Autonómica y Local.

Para ello, la Centro criptologico nacional pone a disposición de las administraciones locales la herramienta PILAR.



III LOPD Y ENS

La Disposición Adicional Única del Real Decreto 1720/2007, señala: La normativa anterior a la entrada en vigor del Reglamento europeo de Protección de datos y su ley desarrollo, es decir la ley 15/99 y el Reglamento 1720/2007 no relacionaba expresamente la normativa de protección de datos y el ENS.

Podríamos decir que las administraciones públicas se apoyaban en la seguridad de los datos en transacciones electrónicas en base a artículos como la disposición adicional única del Real decreto 172072007 que decía “Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido”.
Sin embargo con el RGPD aún no en vigor, la agencia española de protección de datos y el CCN-CERT establecieron mecanismos de colaboración en 2017 (12/21017) indicando que

El **Esquema Nacional de Seguridad** y el RGPD establecen la obligación de que la Administraciones Públicas realicen análisis de riesgos para determinar el posible impacto de los tratamientos de datos sobre los derechos y libertades de las personas y las medidas de seguridad aplicables.

En este sentido, la AEPD público un documento en el que pone de manifiesto que esas medidas de seguridad −en el caso de las Administraciones públicas− estarán marcadas por los criterios establecidos en el Esquema Nacional de Seguridad. El Proyecto de Ley Orgánica de Protección de Datos, en ese momento en fase de tramitación, lo recogía de la misma forma en su disposición adicional primera.

De esta manera desde Diciembre de 2018, la herramienta PILAR añadió un modulo de cumplimiento que permitía a las administraciones locales verificar los requisitos establecidos en el RGPD, facilitando la gestión normativa tanto del Reglamento como del Esquema Nacional de Seguridad.

Finalmente el cinco de Diciembre de 2018 se publico la ley de protección de datos 3/2018 que en su disposición adicional primera recoge de forma explícita que:

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado,

adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Es por tanto que de esta forma el ENS y la LOP quedan entrelazados siendo el ENS de forma oficial el sistema para la Gestión del Riesgo a emplear para el cumplimiento de los requisitos tanto de seguridad de la información como para la protección de datos de carácter personal.

Por último no puedo dejar de realizar un análisis del artículo que genera la obligación de realizar un análisis de riesgos antes de establecer las medidas de prevención, en base a la categoría de los riesgos evaluados previamente.

El artículo 32 del Reglamento, denominado “Seguridad del tratamiento” dice

“Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros”

Este párrafo es el que determina la obligación de realizar un análisis de riesgos como paso previo a establecer una adecuada gestión de los mismos.

Es por ello que el artículo 32 enlaza con el artículo 24 del mismo RGPD donde hace referencia a las responsabilidades del responsable del tratamiento y cita

“Teniendo en cuenta la naturaleza ,el ámbito, el contexto y los fines del tratamiento asi como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas ,el responsable del tratamiento aplicara medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente reglamento. Dichas medidas se revisaran y actualizaran cuando sea necesario”

Es por tanto que el propio RGPD establece quien es el obligado a realizar este análisis de riesgos, estableciendo las medidas técnicas y organizativas necesarias y siendo necesario revisar el estudio cuando sea necesario.

Al respecto de la metodología, volvemos a la cuestión ya tratada de cómo realizarlo, la Guía sectorial de Protección de datos en la administración local publicada en Abril de 2018 por la Agencia Española de Protección de datos en colaboración con la Federación española de Municipios y Provincias nos habla de “métodos de reconocido prestigio” en su pag 19.

Parece evidente que con la entrada en vigor de la ley 3/2018, el método fijado en su disposición adicional primera que el “Método de reconocido prestigio” es el que se desprende del ENS

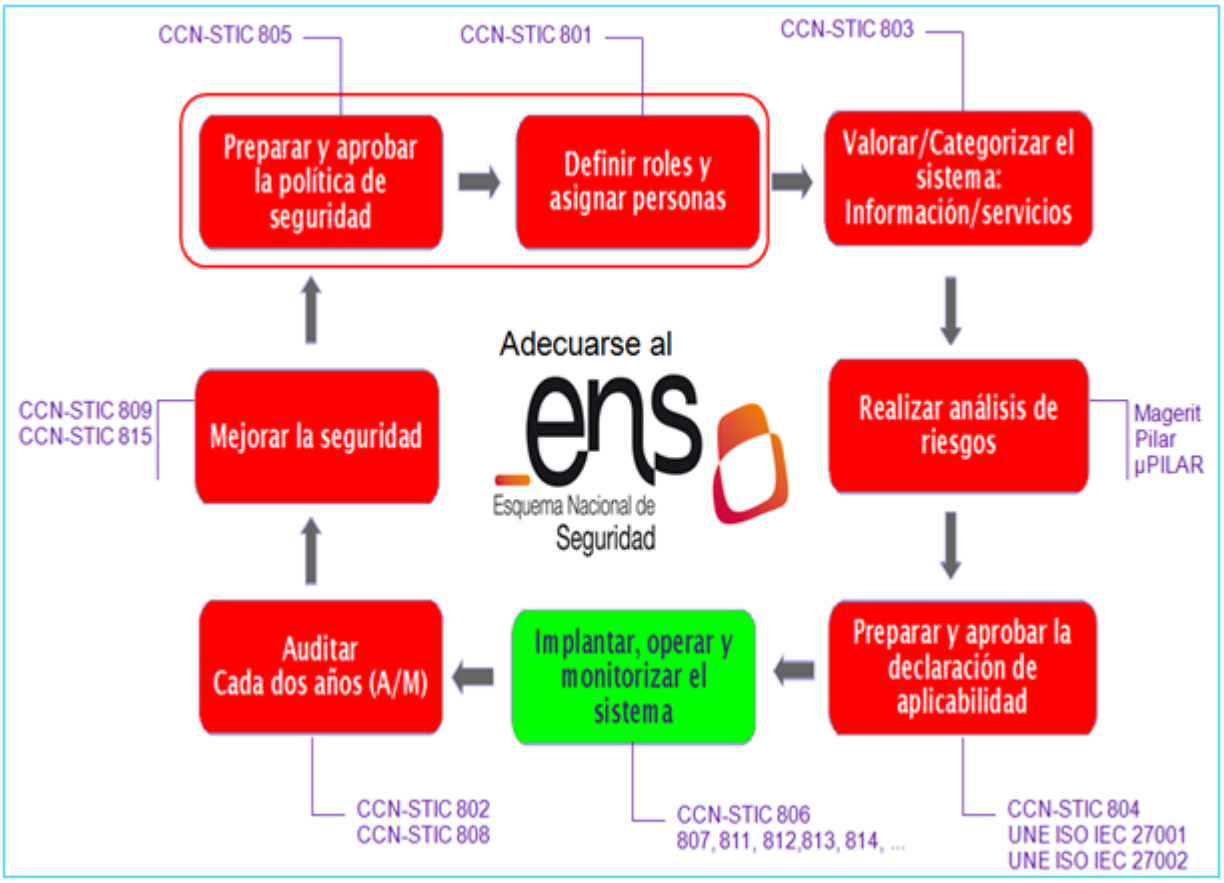


Figura: Adecuación al Esquema Nacional de Seguridad.

IV CONCLUSIONES

Para el cierre de este artículo, me gustaría dejar de forma clara y concisa algunas conclusiones al respecto de la Gestión del riesgo en nuestra normativa actual y su relación con las administraciones públicas.

La introducción del concepto de la Gestión del riesgo, no es nuevo en nuestro ordenamiento jurídico por el Real decreto 67/2010 de prevención de riesgos para la administración del estado que resume y actualiza la normativa en prevención de riesgos para administraciones públicas y que establece la evaluación de riesgos como herramienta fundamental de análisis de las probabilidades y las consecuencias para establecer el nivel de riesgo y en función de ese nivel se establecen las medidas preventivas de carácter técnico y organizativo necesarias que se revisaran en función de las circunstancias.

Que la normativa de PRL al igual que la ley de Protección de datos de carácter personal 3/2018 vienen de normativa europea , en un caso de la directiva 83/391CEE y en el otro del reglamento 2016/679 UE.

Que la normativa europea a diferencia de la tradicional normativa nacional, es fundamentalmente finalista no dando de forma taxativa las pautas de cómo cumplir tan solo indicando lo que hay que cumplir , dejando la forma de evidenciar su cumplimiento a criterios establecidos por organismos consultivos.

Que el Reglamento no especifica en su artículo 32 como realizar los análisis para la gestión del riesgo y que mediante la ley 3/2018 el legislador ha fijado que el método será el establecido por el esquema nacional de seguridad creado por el RD 3/2010.

Es por tanto que con la publicación de la ley 3/2018 el cinco de Diciembre y su entrada en vigor el siete de Diciembre se cierra el círculo para la unión del ENS y LOPD en lo que concierne a protección de datos y seguridad de la información, empleando una misma herramienta PILAR para ambos supuestos.

BIBLIOGRAFÍA

Guia para la Protección de datos y administración Local.: Agencia española de protección de datos, FEM , COSITAL .Abril 2018
https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del reglamento UE 2016/679. Grupo protección de datos art 29. Octubre 2017.
https://www.aepd.es/media/criterios/wp248rev01-es.pdf

Guía de Implantación esquema nacional de seguridad. AMETIC. Enero 2011 , publicado por el Ministerio de Política territorial y administración pública.
http://www.esquemanacionaldeseguridad.es

WEB, S CONSULTADAS

http://www.privacy-regulation.eu

https://administracionelectronica.gob.es

https://www.aepd.es

https://edps.europa.eu

https://www.ccn.cni.es

https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.8/Pilar_5.4.8/bcm_es/index.html