Spread the love

Entrada que debe actualizarse conforme al: Nuevo Esquema Nacional de Seguridad

Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS) está regulado en el Real Decreto 3/2010 de 8 de enero

Hamburgo. Ayuntamiento. Epc

El objeto del ENS es "*el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información*" y persigue "*fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas*". En principio se aplica sólo a las administraciones públicas para "*asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias*". Pero, como veremos, afecta también a algunas empresas del sector privado.

Es recomendable que las **entidades privadas** que manejen datos sensibles, de alto riesgo,

implanten este ENS ya que el RGPD, exige aplicar medidas que resultan adecuadas a la tecnología, tipología y volumen de datos tratados, tratamientos realizados, etc. de cada organización mediante análisis de riesgos previo, evaluaciones de impacto, etc. Pero además resulta obligatorio en los casos establecidos en la D.A. 1 de la Ley Orgánica 3/2018 de Protección de datos personales y garantía de derechos digitales, que se reproduce: *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.***

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos fue la primera en establecer el Esquema Nacional de Seguridad. En 2010 se aprobó el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos. En 2015 se publicó la modificación del Esquema Nacional de Seguridad a través del Real Decreto 951/2015, de 23 de octubre, en respuesta a la evolución del entorno regulatorio, en especial de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del Esquema.

Entre las obligaciones más destacables que derivan del ENS está la de clasificar los niveles de riesgo de ciberseguridad en tres grandes categorías (bajo, medio, alto) , así como las correspondientes medidas aplicables a cada uno de esos niveles.

Otra obligación afecta a la gobernanza empresarial, pues conforme al ENS, las entidades afectadas deben nombrar a responsables específicos**. Concretamente, conforme al art 10 del RD 3/2010 (ENS), en los sistemas de información de las entidades sometidas a ese RD, se deben establecer tres figuras de responsabilidad distintas: el *responsable de la información*, el *responsable del servicio* y el *responsable de la***

***seguridad*: El responsable de la información** será competente para determinar los *requisitos de la información tratada*; el r**esponsable del servicio** determinará los requisitos de los servicios prestados; y el **responsable de seguridad** determinará las decisiones que deban adoptarse para satisfacer los requisitos de seguridad de la información y de los servicios.

Pero, adicionalmente, conforme al ENS la ***responsabilidad de la seguridad de los sistemas de información* estará diferenciada de la responsabilidad sobre la prestación de los servicios**. A todo esto se une que la **política de seguridad de la organización, documento estratégico con el que deben contar las entidades sometidas al ENS, detallará las atribuciones de cada responsable, los mecanismos de coordinación** y lo de resolución de conflictos.

Como adelantábamos, el ENS también resulta aplicable a la empresa privada en algunos casos.

Para entender mejor el contexto, recordemos que **la Ley Orgánica, 3/2018** de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (en adelante, **LOPD-GDD)** adapta nuestro ordenamiento al *Reglamento (UE) 2016/679*", **RGPD**. Y, es aplicable tanto a la administración como a la empresa privada

- El RGPD dispone en su art. 5.2 el "***principio de la responsabilidad proactiva***", que, el responsable del tratamiento debe cumplir y ser capaz de demostrar que los datos personales son tratados de acuerdo con los principios de "**licitud, lealtad y transparencia"; "limitación de la finalidad"; "minimización de datos"; "exactitud"; "limitación del plazo de conservación" y de "integridad y confidencialidad".** Precisamente el principio de "**integridad y confidencialidad**" establece que se ha de garantizar una seguridad adecuada de los datos personales, para protegerlos "*contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental*
- El artículo 32 del RGPD, establece que **"***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***. Por tanto, las medidas de seguridad para proteger los datos personales no se recogen en una lista taxativa. Con este artículo 32, se introduce una suerte de **autoevaluación por el responsable de las medidas de seguridad que son necesarias para proteger los datos personales, ya sean estos**

objeto de tratamiento directamente por él o, en su caso, por encargados de tratamiento que tratan datos por cuenta suya

Vista de San Sebastian

La LOPD GDD, art 77, estableció, además, unos sistemas y medidas de protección de datos especiales ara la Administración Pública española. Ello se completa con la DA 1ª LOPD-GDD que establece un marco específico de seguridad en el sector público, a través del ENS, sustituyendo la autoevaluación del art 5.2 por un régimen específico para el sector público: ***"Medidas de seguridad en el ámbito del sector público:***

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*
3. ***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***

Por lo tanto, en la distintas entidades de la DA 1 , apartado 3 LOPD-GDD, ya sea en calidad de responsable o encargado del tratamiento, han de **categorizar** de acuerdo con el **Anexo I del ENS** (en categoría básica, media o alta) los sistemas de información utilizados para el

tratamiento y **de acuerdo con el Anexo II,** implementar aquellas medidas de seguridad (organizativas, operacionales y de protección) que sean acordes a la categoría otorgada al sistema. Ello para proteger la **integridad, confidencialidad y disponibilidad** de los datos personales que traten,

Casamento no Pazo

Cualquier entidad privada que preste o quiera prestar servicios a una Administración Pública ha de cumplir también con las medidas de seguridad que, en virtud del ENS, sean de aplicación a dicha administración de referencia. Y, en efecto, es habitual que las empresas privadas que se presentan a licitaciones del sector público encuentren reflejados en los pliegos la **exigencia inexcusable de que cumplan con el Esquema Nacional de Seguridad y que hayan superado un proceso de certificación** por una entidad debidamente acreditada.

¿El papel de responsable de seguridad en estas empresas podrá corresponder, es decir, coincidir con el RSI o Chief Information Security Officer (CISO) que deriva del RD 43/2021 -dentro del desarrollo del paquete NIS (Network Information and Security) ; al que aludíamos en entradas anteriores? Conforme al art 7 apartado 5 del Real Decreto 43/2021, así sería, al menos en el caso de las empresas privadas sometidas tanto a NIS como al ENS.