Delete Technology

Powered by blancco

Las implicaciones en la seguridad informática de las administraciones locales del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad.

Delete Technology Group S.A de C.V

Real Decreto 311/2022

Con fecha 4 de mayo se ha publicado en el Boletín Oficial del Estado el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), y que se enmarca en el paquete de actuaciones urgentes para reforzar las capacidades de defensa frente a las ciberamenazas sobre el sector público y las entidades colaboradoras que suministran tecnologías y servicios al mismo.Si bien este Real decreto es de rabiosa actualidad ya encontramos antecedentes de regulación en la Real decreto 3/2010 de 8 de enero advirtiendo que el ENS para el desarrollo e implantación de al administración electrónica aprobada por la ley 11/2007 de la administración electrónica, debería de estar constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información, mediante el establecimiento de políticas de seguridad en la utilización de los medios electrónicos, para ello se recomendaba que los productos y los sistemas de las TIC´s cuenten con una características apropiadas y estén correctamente implementadas

La presente actualización del ENS se incluye en la ejecución del Plan de Digitalización de las Administraciones Públicas 2021-2025, entronando con la política del gobierno de modernización de la economía, siendo uno de los principales instrumentos para el cumplimiento del Plan de Recuperación, Transformación y Resiliencia, aprobada por ley Real Decreto-ley 36/2020, de 30 de diciembre, y para la ejecución del Plan de Recuperación, Transformación y Resiliencia. y su Componente 11 denominado «Modernización de las Administraciones Públicas», así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025.

En este sentido conviene recordar que El Reglamento Europeo 2016/679, de 27 de abril, de Protección de Datos (RGPD), exige a las Administraciones locales, en los términos de su art. 32, la adopción de medidas de seguridad en orden a la protección de los datos de carácter personal, con el objetivo de tratar adecuadamente los riesgos de que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Por ello Las medidas de seguridad, en el caso de todas las Administraciones Públicas (incluidas las Entidades Locales), deben ser adoptadas en el marco del Esquema Nacional de seguridad, que ofrece diversos controles de seguridad cuya aplicación, en función del nivel de riesgo de los datos, permite evitar o, al menos, limitar sustancialmente, la generación de daños a terceros y reduce la exposición a la posible responsabilidad patrimonial de la Administración.

El acceso electrónico de los ciudadanos a los Servicios Públicos, obligó a las entidades públicas a hacer uso de los medios electrónicos; tanto mecanizando internamente los procesos administrativos, como ofreciendo al ciudadano estos servicios por los medios digitales legalmente establecidos. El nivel de exigencia de esta obligatoriedad ha aumentado exponencialmente en los últimos tiempos. Hoy en día está perfectamente asumido que la administración electrónica ha de apoyarse en herramientas que demuestran una mayor seguridad jurídica que la inherente a los procedimientos utilizados hasta la fecha.

Dicha seguridad comienza por el propio amparo otorgado por la normativa al Esquema Nacional de Seguridad. El cual de be aplicarse también, como hemos visto a los ayuntamientos. Pues si este tiene como como finalidad asegurar, precisamente, la seguridad, integridad, disponibilidad, autenticidad, y confidencialidad de los documentos electrónicos. Así pues, si existiere algún tipo de problema, este no ha de derivar, en ningún, caso de la falta de adaptación a la legalidad de la tecnología y aquí radica la importancia de la aprobación del nuevo Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

El Real Decreto impulsa la digitalización de las admiraciones en el periodo 2021-2025 para ello la actualización del ENS persigue y ampara la evolución de la política de seguridad de todas las entidades del sector público español, tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información y además contempla la constitución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos, referente para las administraciones públicas, y contribuyendo a mejorar el cumplimiento del ENS entre otras, de las entidades locales. Para ello se ampara en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público cuando establece que : El ENS tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada

Metas que se persiguen con las actualizaciones del Real Decreto 311/2022 de 3 de mayo:

Alinearse con el marco normativo existente hasta la fecha para garantizar, de modo, que la administración digital refleje con claridad su ámbito concreto de aplicación en beneficio de la ciberseguridad y de los derechos de los ciudadanos.Ajustar los requisitos establecidos en el ENS, garantizando su adaptación a las necesidades, colectivos de entidades y ámbitos tecnológicos existentes para una aplicación más eficaz y eficiente.Actualizar y revisar los principios básicos y las medidas de seguridad existentes para dar una mejor respuesta a las tendencias y necesidades que existan en la actualidad como las que puedan surgir en un futuro en temas de ciberseguridad. En conclusión, se dan mayores garantías para la protección de los sistemas de información en las entidades de su ámbito de aplicación, entre las que se encuentran los ayuntamientos, reducir vulnerabilidades y establecer mecanismos de respuesta y medidas de seguridad óptimas, dentro del marco jurídico, tecnológico, estratégico y de ciberamenazas actuales.Corresponde a los ayuntamientos a través del órgano competente para ello además de aprobar el documento de política de seguridad y privacidad, el incorporar las actualizaciones que se vayan aprobando, a través de la legislación que se vaya dictando en cada momento.

El Real Decreto entra en vigor el 04 de mayo de 2022 (Disposición Final Segunda). A partir de esta fecha, se dispone de un plazo de 24 meses para adecuar los sistemas de información preexistentes dentro del su ámbito de aplicación (artículo 2 de la norma), para alcanzar su plena adecuación al “ENS”.

A tal efecto los sistemas de categoría MEDIA o ALTA precisaran de una auditoria para la calificación de su conformidad, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS (artículo 38).

Con carácter extraordinario se realizara una auditoria de seguridad, cuando se produzcan modificaciones sustanciales en los sistemas de información, que repercutan en las medidas de seguridad requeridas.

La realización de la auditoria extraordinaria determinara la fecha de cómputo para el cálculo de los dos años establecidos para realizar la siguiente auditoria ordinaria. Todo ello a tenor de lo establecido en el artículo 31 y ANEXO III del Real Decreto 311/2022, así como en los términos que determine la correspondiente instrucción técnica de seguridad.

Andrés Lluch Figueres,
Técnico de Administración Especial, Jefe de área de RR.HH, y Calidad.
Diploma en Dirección Publica INAP VII edición

.

Delete Technology Group S.A de C.V
Av. Ejército Nacional 826A Oficina 104 Col. Polanco CDXM 11540 México

Delete Technology
Powered by blancco