ECIJA
Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa: Actualización en el Esquema Nacional de Seguridad

Madrid, 9 de mayo 2022

El pasado 4 de mayo de 2022 se publicó el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, "**ENS**"). El mismo pretende actualizar el vigente RD 3/2010, de 8 de enero, para adaptarlo a la nueva realidad y al incremento de las ciberamenzas tanto cuantitativa como cualitativamente. El objetivo de esta reforma es garantizar una mejor respuesta ante los ciberataques, así como mejorar la protección en el tratamiento de datos por el Sector Público y aquellas entidades del Sector Privado que colaboren con aquél, estableciendo unos principios básicos y unos requisitos mínimos de seguridad y medidas de protección que deberán llevarse a cabo.

El esfuerzo realizado para la actualización del ENS responde al objetivo de "Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia", así como a los principios generales previstos en la Ley de Régimen Jurídico del Sector Público, que se refieren a la seguridad como un elemento clave para la interacción de las Administraciones Públicas por el medio electrónico.

(I) Modificaciones

Entre los cambios que introduce el nuevo ENS se encuentran varias novedades:

- **Ámbito de aplicación de ENS**. Una de las más relevantes tiene que ver con su ámbito de aplicación. Se define con mayor claridad qué organizaciones se encuentran bajo el ámbito de aplicación del ENS. En este sentido, señala de manera mucho más clara la necesidad de cumplimiento del ENS por parte de las **entidades del sector privado, y su cadena de suministro, cuando éstas presten servicios al Sector Público**.

- **Cumplimiento de datos protección de datos**. La nueva reforma otorga un mayor protagonismo a medidas enfocadas a **cumplir con la normativa de protección de datos** (RGPD/LOPDGDD), lo que obligará a que se realice un análisis de riesgos de conformidad con la normativa de protección de datos.

- **Diferenciación de responsabilidades.** Además del responsable de la información, del responsable de servicio y del responsable de la seguridad, también habrá que designar un **responsable del sistema**. Así, el responsable de seguridad será distinto del responsable del sistema (salvo en excepciones justificadas).

- **Nuevos principios básicos**. Se introduce el principio de **vigilancia continua**. De esta forma, el sistema debe permitir la detección de actividades o comportamientos anómalos, y su oportuna respuesta, impulsando la evaluación permanente del estado de la seguridad de los activos para detectar vulnerabilidades e identificar posibles deficiencias de configuración.

- **Nueva figura para proveedores**. Aparece una nueva figura para servicios externalizados: El **POC** (Persona de Contacto) de Seguridad de la Información. Dicho POC será el responsable de seguridad de la organización contratada, quien formará parte del área o tendrá contacto directo con la misma, pero quien ostentará la responsabilidad final será la entidad del sector público destinataria de los servicios.

- **Respuesta ante incidentes de seguridad**. Con la nueva reforma, el **CCN-CERT** coordinará la respuesta a incidentes de seguridad. Las AAPP notificarán al CCN-CERT los incidentes que tengan un impacto significativo, siendo el CCN el coordinador nacional que dará respuesta técnica a los equipos CSIRT.

- **Cumplimiento de personal y cualificación**. Se exige una **mayor cualificación** para el personal que participe en materia de seguridad, debiendo estar dedicado e instruido en todas las fases del ciclo del proceso. Asimismo, se supervisará al personal para verificar que cumplen con las normas y procedimientos, así como con sus deberes y obligaciones.

- **Medidas de seguridad**. La mejora de diversas medidas de seguridad para mejorar su eficacia y para adecuarse a lo previsto en el Reglamento Nº. 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. De manera general, las **medidas de seguridad aplicables son sustancialmente más estrictas** para los sistemas de todas las categorías.

(II) Objetivos de la modificación

Todas estas novedades del ENS persiguen tres principales objetivos:

- En primer lugar, se pretende garantizar una claridad de aplicación del ENS en el ámbito de la ciberseguridad y de los derechos de los ciudadanos, y para ello se intentará **simplificar, precisar y armonizar los diferentes mandatos del ENS**, además de eliminar aquellos aspectos que puedan considerarse excesivos, añadiendo los que se realmente se identifican como necesarios.

- En segundo lugar, dada la similitud de riesgos a los que están expuestos los sistemas de información y servicios de multitud de entidades, y con el propósito de adaptarse a la realidad que sufren estos colectivos, se ha considerado necesario la elaboración de un "**perfil de cumplimiento específico**". Dicho perfil permitirá a las entidades no solo la racionalización de sus recursos de la manera más segura posible, sino también el cumplimiento eficaz y eficiente del ENS.

- En tercer lugar, la **revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad** es claramente un objetivo perseguido para conseguir respuestas más adecuadas a las tendencias en el ámbito de la ciberseguridad, asi como reducir las vulnerabilidades y promover una vigilancia continua.

Por último, es menester señalar que **los sistemas de información afectados por el ENS deberán ser adaptados al mismo en un período de 2 años desde su entrada en vigor, incluidos los del**

Sector Privado. En este mismo sentido cabe señalar que las **entidades certificadoras cuentan con un periodo de adecuación de sus esquemas de certificación de 6 meses para llevar a cabo las auditorias de aquellas entidades que quieran recertificarse este año o las que se certifican por primera vez.**

Área de TMT de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60