Publicado en Madrid el 15/07/2021

S2 Grupo explica cómo afectarán a las empresas las novedades en el Esquema Nacional de Seguridad

Expertos de S2 Grupo aseguran que el "Plan de choque de ciberseguridad" puesto en marcha por el Gobierno es esencial para responder con mayor efectividad a la situación actual de ciberdelincuencia. En un comunicado, la comprase afirma que se han introducido medidas orientadas a facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua en las organizaciones

Los socios-directores de la empresa de ciberseguridad S2 Grupo, Miguel A. Juan y José Rosell, han analizado, por medio de un comunicado de prensa, qué repercusión tendrán los cambios en las empresas españolas el Gobierno español un “Plan de Choque de Ciberseguridad” aprobado por parte del Gobierno.

Esta iniciativa se aprobó el día 25 de mayo en el Consejo de Ministros y consiste principalmente en la puesta en marcha de un paquete de actuaciones urgentes en materia de ciberseguridad. Entre éstas se incluye la tramitación y aprobación de manera urgente de un Real Decreto que sustituya al Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica.

Los expertos de S2 Grupo han destacado que la necesidad de actualizar el ENS atiende a tres grandes cuestiones. En primer lugar, alinearlo con el marco legislativo actual y la Estrategia Nacional de Ciberseguridad 2019, para facilitar la seguridad en la Administración Digital. En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS para adaptarse a la realidad de ciertos colectivos o tipos de sistemas. Y, por último, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua.

Los principales cambios

Estas tres líneas maestras introducen cambios y novedades importantes, siendo especialmente significativos los siguientes:

Se define con mayor claridad qué organizaciones se encuentran bajo el ámbito de aplicación del ENS, incluyendo en esta actualización los sistemas que manejan o tratan información clasificada, y reforzando la necesidad de cumplimiento del ENS por parte de las entidades del sector privado, y su cadena de suministro, cuando éstas presten servicios o provean soluciones a las entidades del sector público.

Actualización de los principios básicos, donde cabe destacar la inclusión del principio "vigilancia continua", para permitir la detección de actividades anómalas y proporcionar la oportuna respuesta, e impulsar la revisión permanente del estado de la seguridad de los sistemas para detectar vulnerabilidades e identificar defectos de configuración.

Permitir alcanzar la adecuación al ENS de un modo más eficaz y eficiente, especialmente para

aquellas organizaciones más pequeñas y/o que cuentan con menos recursos. Con este objetivo, se introduce el concepto de "perfil de cumplimiento específico", que serán conjuntos de requisitos mínimos publicados por el Centro Criptológico Nacional a los que las organizaciones de un determinado colectivo se podrán acoger para cumplir con el ENS. Estos perfiles se definirán atendiendo a la semejanza que presentan una multiplicidad de entidades en cuanto a los riesgos a los que están expuestos sus sistemas de información (por ejemplo, el caso de las entidades locales).

Actualización de las medidas de seguridad del Anexo II, sobre la base de la existencia de un requisito general y unos posibles refuerzos. A este respecto, se introducen cambios destinados a aumentar la exigencia de medidas de seguridad ya existentes, otros enfocados a simplificar la implantación de requisitos que eran demasiado exigentes y, además, se han incorporado nuevas medidas que permiten proteger a las organizaciones frente a nuevas amenazas.

“La aparición de este Real Decreto, aunque haya venido motivada por la aprobación del Plan de Choque de Ciberseguridad, era muy necesaria. Su última actualización feu en 2015 y desde entonces el grado de evolución en la transformación digital de las organizaciones tanto del sector público como del sector privado y el incremento de los ciberataques, sumado a la situación provocada por la pandemia y los nuevos riesgos introducidos por el aumento del teletrabajo, ha supuesto que muchas de sus directrices no sean suficientes para garantizar un adecuado nivel de protección”, ha comentado José Rosell, socio-director de S2 Grupo.

“Esta actualización del ENS pretende ser más flexible, adaptándose de una manera más razonable al contexto de todas las organizaciones, pero sin menoscabo de la protección perseguida y exigible. En nuestra opinión estos cambios pueden ser muy beneficiosos para el ecosistema nacional, ya que pueden incentivar un mayor grado de adopción al ENS, lo que supondrá una mejora general del nivel de ciberseguridad de la Administración Pública española y, por supuesto, de un gran número de empresas del sector privado, bien por prestar servicios directamente a organismos públicos o bien por pertenecer a su cadena de suministro”, ha declarado Miguel A. Juan, socio-director de S2 Grupo.

Cómo afectará a las empresas las novedades introducidas en el Real Decreto de junio

José Rosell ha asegurado que la publicación de este nuevo Real Decreto de actualización del ENS tendrá impacto tanto en los organismos públicos, por ser legislación de obligado cumplimiento para ellos, como también en las organizaciones del sector privado que presten servicios a entidades del sector público, ya que éstas deben garantizar el mismo nivel de seguridad.

“Esta actualización propiciará una mejora en el nivel de ciberseguridad de las organizaciones, ya que introduce medidas orientadas a facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua”, ha continuado Rosell. También ha añadido que aquellas organizaciones dentro del ámbito de aplicación que ya estuvieran adecuadas al RD 3/2010 dispondrán de un plazo de dos años para adecuarse al nuevo Real Decreto desde la fecha de su publicación, mientras que el resto tendrán que cumplirlo desde su entrada en vigor.

Qué recomendaciones necesitan tener en cuenta las empresas u organizaciones

Miguel A. Juan ha explicado que se prevé un plazo de transición de dos años para la adaptación a los requisitos del nuevo ENS. Sin embargo, se recomienda a las organizaciones que trabajen en el análisis de implicaciones y cambios que este Real Decreto supone desde el momento de su entrada en vigor.

“La mejor forma es llevar a cabo Planes de Adecuación que tengan como principales objetivos evaluar el grado de cumplimiento actual teniendo en cuenta la actualización de las medidas de seguridad y la definición de iniciativas y proyectos encaminados a salvar aquellos incumplimientos detectados y, a la vez, mejorar el nivel de madurez en la gestión de la seguridad de la organización”, ha enfatizado el socio-director de S2 Grupo.

Qué queda todavía por abordar en esta materia
Desde S2 Grupo se ha destacado que tras la publicación definitiva del nuevo Real Decreto, que va a ser tramitado de urgencia, comenzarán los trabajos de adecuación por parte de las organizaciones que deben cumplirlo. Los cambios que se introducen están fundamentados en criterios sólidos y teniendo en cuenta la opinión de las organizaciones bajo el paraguas de aplicación y otras partes interesadas (consultoras, auditoras, organismos reguladores, etc.) desde la aparición del RD 3/2010 hace ya algo más de diez años. Sin embargo, será necesario esperar un tiempo para evaluar si los objetivos que se persiguen con esta actualización del ENS verdaderamente se cumplen, y se incrementa de manera notable el nivel de ciberseguridad a nivel nacional y el número de organizaciones que certifican su cumplimiento con el ENS.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Derecho E-Commerce Ciberseguridad