Comunidad de Madrid

Medios de Comunicación

Para cumplir con las medidas de la Unión Europea destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información

La Comunidad de Madrid actualiza la política de ciberseguridad de Metro

- Destinará 4,6 millones de euros e incluirá un plan de acción que se aplicará en próximos años
- La primera versión en materia de ciberseguridad fue aprobada en octubre de 2019 y precisa ahora ser revisada

1 de agosto de 2021.- La Comunidad de Madrid actualiza la política de ciberseguridad de la compañía de Metro para cumplir con las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea.

Para el suburbano madrileño es importante mantener la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y datos que se manejan en la compañía. Por ello, Metro de Madrid considera su política de ciberseguridad como una prioridad dentro de su estrategia empresarial.

Esta revisión incluye un plan de acción que se aplicará durante los próximos años y cuenta con un presupuesto estimado de 4,6 millones de euros, para cumplir con el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, relativo a seguridad de las redes y sistemas de información (Directiva NIS).

Este desarrollo reglamentario recoge las obligaciones que se deben de cumplir en materia de ciberseguridad por parte de los operadores de servicios esenciales, así como de los proveedores de servicios digitales y la gestión de incidentes de seguridad en el entorno de redes y sistemas de información.

La política de ciberseguridad de Metro de Madrid es el marco global de referencia que establece las directrices generales, objetivos, responsabilidades y pautas de actuación de la compañía en lo referente a dicha materia, de acuerdo a sus necesidades y la legislación vigente.

La primera versión de dicha normativa fue aprobada en octubre de 2019, pero requiere de una actualización ya que esta debe de adaptarse a la realidad del entorno, a los procesos de negocio de las empresas y a las obligaciones legales.