Nota de prensa

Seguridad y resiliencia de las redes

El Gobierno somete a audiencia pública el real decreto sobre seguridad y resiliencia de las redes de telecomunicaciones

- **Este proyecto normativo tiene como objetivo último reforzar las medidas de seguridad en el sector de las telecomunicaciones, evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y recuperar las comunicaciones lo antes posible**

- **Las redes, servicios e infraestructuras digitales son calificados como instalaciones y servicios de carácter esencial en situaciones de emergencia. Por tanto, en una emergencia, todas las autoridades, órganos administrativos y las Fuerzas y Cuerpos de Seguridad del Estado colaborarán para facilitar su recuperación o su mantenimiento**

- **Los operadores de telecomunicaciones y demás sujetos a los que afectará este desarrollo normativo estarán obligados a presentar un Plan General de Seguridad y planes específicos por tipo de red, servicio, y por tipo de incidente. Esos planes detallarán, entre otras, las condiciones de autonomía eléctrica que tienen sus infraestructuras de telecomunicaciones**

- **También se refuerzan las obligaciones de notificación de incidentes y se pone un foco especial en la operatividad y continuidad de los centros de emergencia (número 112) y alertas públicas**

Madrid, 02 de diciembre de 2025.- El Ministerio para la Transformación Digital y de la Función Pública ha publicado hoy el texto del borrador del Real Decreto de Seguridad y Resiliencia de las Redes y Servicios de Comunicaciones Electrónicas e Infraestructuras Digitales, con el fin de someterlo a audiencia pública.

Diversos incidentes como la pandemia del COVID-19, la erupción volcánica de La Palma, la DANA que asoló la Comunidad Valenciana en 2024 y el reciente

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

C/ Mármol, 2 – 28005 Madrid

Nota de prensa

apagón eléctrico de abril pasado han puesto de manifiesto la trascendencia de las redes y servicios de telecomunicaciones y la necesidad de establecer un marco jurídico completo, detallado y actualizado de seguridad y resiliencia de las redes y servicios de telecomunicaciones.

Este proyecto normativo tiene como objetivo último reforzar las medidas de seguridad en el sector de las telecomunicaciones, evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y recuperar las comunicaciones lo antes posible.

En el texto que se somete desde hoy a audiencia pública las redes y servicios de telecomunicaciones y determinadas infraestructuras digitales son calificados como instalaciones y servicios de carácter esencial en situaciones de emergencia. Por tanto, en una emergencia, todas las autoridades, órganos administrativos y las Fuerzas y Cuerpos de Seguridad del Estado colaborarán y contribuirán para facilitar su recuperación o mantenimiento.

Nuevas obligaciones: planes de seguridad

Las obligaciones de este real decreto afectarán, entre otros, a los operadores de telecomunicaciones en España y aquellos que operan infraestructuras digitales como cables submarinos, sistemas satelitales, centros de datos y puntos de intercambio de internet que cumplan ciertos criterios: más de medio millón de usuarios o más de 50 millones de ingresos. También aquellos que estén designados como operadores críticos, o presten servicios de emergencia, entre otros. No se aplica a redes vinculadas a Seguridad Nacional y Defensa.

Todos los sujetos mencionados deberán presentar un Plan General de Seguridad con análisis de riesgos y medidas prioritarias, así como planes específicos por tipo de red y servicio, y por tipo de incidente.

En estos planes, cada operador de telecomunicaciones clasificará todas sus instalaciones en distintas categorías. En el caso de que haya una interrupción de suministro eléctrico, las infraestructuras de primer nivel deberán tener garantizada la operatividad durante al menos 24 horas. Las instalaciones clasificadas de nivel intermedio deberán ser operativas durante al menos 12 horas. El resto deberá tener garantizada la operatividad durante cuatro horas.

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

C/ Mármol, 2 – 28005 Madrid

Nota de prensa

En el caso de una red móvil, estas cuatro horas deben mantener la cobertura al 85% de la población. Cada operador establecerá una estrategia en la que podrá priorizar unas tecnologías sobre otras (voz sobre datos, por ejemplo) o instalaciones que considere conveniente en función a su vinculación a la prestación de servicios públicos y servicios de relevancia económica y social.

El proyecto normativo pone también un foco especial en reforzar la operatividad y continuidad de las comunicaciones de emergencia dirigidas a los centros del 112 y alertas públicas. Estos centros, así como los operadores que les dan conectividad, deben confeccionar y presentar Planes de Seguridad.

Procedimiento de notificaciones y supervisión

Con el fin de disponer de información fidedigna en el menor tiempo posible, se refuerzan las obligaciones de notificación de incidentes. Así, se prevé que haya una notificación inicial como máximo una hora después de comenzar el suceso, notificaciones intermedias periódicas, una notificación final y un informe detallado posterior que analice las causas, el impacto, las medidas adoptadas y lecciones aprendidas.

Además, se definen criterios para clasificar incidentes como significativos o menores en función del número de usuarios afectados, la duración, el área geográfica afectada y el tipo de servicio.

La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales será la autoridad competente para supervisar el cumplimiento de las obligaciones y la coordinación con organismos nacionales, CCAA y con entidades europeas e internacionales.

El texto prevé la creación de la Mesa de coordinación de seguridad y resiliencia de redes y servicios de comunicaciones electrónicas, que será un foro de debate e interlocución y permitirá el contacto entre todos los implicados y la realización de simulacros.

La audiencia estará abierta hasta el 8 de enero de 2026.

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

C/ Mármol, 2 – 28005 Madrid