MEMORIA DEL ANÁLISIS DE IMPACTO NORMATIVO DEL PROYECTO DE REAL DECRETO SOBRE SEGURIDAD Y RESILIENCIA DE LAS REDES Y SERVICIOS DE COMUNICACIONES ELECTRÓNICAS Y DETERMINADAS INFRAESTRUCTURAS DIGITALES

RESUMEN EJECUTIVO

Ministerio	Ministerio para la Transformación Digital y de la Función Pública	**Fecha**	01/12/2025
Órgano proponente	Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales		
Título de la norma	**PROYECTO DE REAL DECRETO SOBRE SEGURIDAD Y RESILIENCIA DE LAS REDES Y, SERVICIOS DE COMUNICACIONES ELECTRÓNICAS Y DETERMINADAS INFRAESTRUCTURAS DIGITALES**		
Tipo de Memoria	Normal ■ Abreviada ☐		
OPORTUNIDAD DE LA PROPUESTA			
Situación que se regula	El presente Real Decreto tiene por objeto establecer un marco jurídico nacional que garantice la seguridad y resiliencia de las redes, los servicios de comunicaciones electrónicas y determinadas infraestructuras digitales frente a incidentes de seguridad que puedan provocar la interrupción del servicio o una degradación significativa en sus condiciones de prestación. A tal efecto, la norma determina los sujetos obligados y las obligaciones que les son exigibles en materia de gestión de riesgos y notificación de incidentes, tanto significativos como no significativos. Asimismo, impone a dichos sujetos y a los centros de recepción de llamadas del número de emergencias 112 y de alertas públicas la obligación de asegurar la continuidad del servicio y el encaminamiento de las llamadas en caso de interrupción o degradación. Finalmente, se establece el régimen de supervisión, inspección y sanción, en coherencia con la normativa europea aplicable en materia de ciberseguridad y resiliencia de entidades críticas.		
Objetivos que se persiguen	El objetivo de esta norma es fortalecer la capacidad de respuesta, recuperación y continuidad operativa de las infraestructuras digitales críticas, particularmente frente a incidentes que puedan poner en riesgo la seguridad nacional, afectar la prestación de servicios esenciales o comprometer la integridad de las redes de comunicaciones electrónicas.		

Principales alternativas consideradas	En el proceso de elaboración del presente Real Decreto se han analizado distintas alternativas regulatorias, conforme a los principios de necesidad, proporcionalidad, eficiencia y seguridad jurídica. Como resultado de dicha evaluación, se ha concluido que la aprobación de un Real Decreto constituye el instrumento jurídico más adecuado para desarrollar el artículo 63 de la Ley General de Telecomunicaciones. Esta opción permite establecer obligaciones claras, proporcionadas y equilibradas, alineadas con la experiencia práctica de los operadores, al tiempo que garantiza la coordinación institucional y habilita mecanismos eficaces de supervisión y sanción. Todo ello se articula de manera coherente con lo dispuesto en la Directiva NIS2 y la Directiva CER, evitando solapamientos normativos y reforzando la seguridad jurídica.
CONTENIDO Y ANÁLISIS JURÍDICO	
Tipo de norma	Real Decreto.
Estructura de la Norma	El proyecto está conformado por una parte expositiva y una parte dispositiva dividida en siete capítulos, con 37 artículos, dos disposiciones adicionales, una disposición derogatoria única y tres disposiciones finales.

Informes a recabar	• Informe de la Comisión Nacional de los Mercados y la Competencia, de conformidad con lo establecido en el artículo 5.2.a) de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia. • Informe de la Secretaría General Técnica del Ministerio para la Transformación Digital y de la Función Pública, conforme a lo dispuesto en el artículo 26.5, párrafo cuarto, de la Ley 50/1997, de 27 de noviembre, del Gobierno. • Informes del Ministerio de Interior, Ministerio de Defensa, Ministerio de Hacienda, Ministerio de Política Territorial y Memoria Democrática y Departamento de Seguridad Nacional de la Presidencia del Gobierno conforme a lo dispuesto en el artículo 26.5, párrafo primero, de la Ley 50/1997, de 27 de noviembre, del Gobierno. • Informe competencial del Ministerio de Política Territorial y Memoria Democrática conforme a lo dispuesto en el artículo 26.5, párrafo sexto, de la Ley 50/1997, de 27 de noviembre, del Gobierno. • Informe de la Oficina de Coordinación y Calidad Normativa del Ministerio de Presidencia, Justicia y Relaciones con las Cortes, en virtud de lo establecido en el artículo 26.9 de la Ley 50/1997, de 27 de noviembre, del Gobierno. • Dictamen del Consejo de Estado conforme a lo previsto en los artículos 19.1 y 22.3 de la Ley Orgánica 3/1980, de 22 de abril, del Consejo de Estado.
Consulta pública previa	Entre el 9 y el 26 de septiembre se ha realizado la consulta pública prevista en el artículo 133.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
Audiencia e información públicas	De conformidad con el artículo 26.6 de la Ley 50/1997, de 27 de noviembre del Gobierno, deberá llevarse a cabo el trámite de audiencia e información pública.
ANALISIS DE IMPACTOS	

<table>
<tr><td>Adecuación al orden de competencias</td><td colspan="2">El presente Real Decreto se dicta al amparo de la competencia exclusiva del Estado en materia de telecomunicaciones, reconocida en el artículo 149.1.21.ª de la Constitución Española, que atribuye al Estado la regulación de las bases y coordinación general de la actividad económica, así como la competencia exclusiva sobre las telecomunicaciones.</td></tr>
<tr><td rowspan="3">Impacto Económico y Presupuestario</td><td>Impacto económico para los sujetos obligados</td><td>☐ Supone una reducción de costes económicos para los sujetos obligados

■ Supone un coste económico para los sujetos obligados. Cuantificación estimada: entre 51 M€ y 73 M€

☐ No afecta a las cargas administrativas</td></tr>
<tr><td>Desde el punto de vista de las cargas administrativas</td><td>☐ Supone una reducción de cargas administrativas. Cuantificación estimada_____€

■ Incorpora nuevas cargas administrativas. Cuantificación estimada_____0__€

☐ No afecta a las cargas administrativas</td></tr>
<tr><td>Desde el punto de vista de los presupuestos, la norma</td><td>☐ Afecta a los presupuestos de la Administración General del Estado.

Afecta a los presupuestos de otras Administraciones Territoriales.

■ No implica un gasto.

☐ Implica un ingreso.</td></tr>
</table>

Impacto de Género	La norma tiene un impacto de género	Negativo ☐ Nulo ■ Positivo ☐
Impacto en materia de Competencia		■ La norma no tiene efectos significativos sobre la competencia. ☐ La norma tiene efectos positivos sobre la competencia. ☐ La norma tiene efectos negativos sobre la competencia.
Impacto en materia de protección de datos	Los efectos vienen especificados en la memoria	No tiene impacto en materia de protección de datos
Otros impactos considerados	▪ Impacto en la infancia y en la adolescencia: negativo ▪ Impacto en la familia: negativo ▪ Impacto por razón de materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad: negativo ▪ Impacto por razón de medio ambiente y cambio climático: negativo. ▪ Impacto en salud: negativo.	
Otras consideraciones	Análisis del impacto en protección de datos	

ÍNDICE DE LA MEMORIA

I.- OPORTUNIDAD DE LA PROPUESTA

1. Motivación
2. Objetivos.
3. Adecuación a los principios de buena regulación.
4. Alternativas.
5. Inclusión en el Plan Anual Normativo y Evaluación Ex Post.

II.- CONTENIDO Y ANÁLISIS JURÍDICO

1. Contenido.
2. Análisis jurídico.

III.- DESCRIPCIÓN DE LA TRAMITACIÓN

1. Descripción de los trámites realizados.
2. Trámites pendientes.

IV.- ADECUACIÓN DE LA NORMA AL ORDEN DE DISTRIBUCIÓN DE COMPETENCIAS

V.- ANÁLISIS DE IMPACTOS

1. Impacto económico
2. Impacto presupuestario.
3. Impacto en la unidad de mercado.
4. Análisis de las cargas administrativas.
5. Impacto por razón de género.
6. Impacto en la infancia y en la adolescencia.
7. Impacto en la familia.
8. Impacto en materia de medioambiente y por razón de cambio climático.
9. Impacto por razón de materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.
10. Impacto en salud.
11. Impacto en materia de protección de datos.

I.- OPORTUNIDAD DE LA PROPUESTA

I.1.- MOTIVACIÓN.

La pandemia de COVID-19 evidenció, de manera contundente, el papel esencial de las redes y servicios de comunicaciones electrónicas. Millones de personas dependieron de ellas para continuar con sus actividades laborales, acceder a servicios de salud y mantener sus relaciones sociales, entre otras muchas actividades, en un contexto de confinamiento y restricciones.

En unas sociedades y economías cada vez más tecnológicas y dependientes de un uso creciente e intensivo de las redes y servicios de comunicaciones electrónicas, esta dependencia también está poniendo de manifiesto una serie de vulnerabilidades críticas relacionadas con la seguridad y la integridad de las redes y servicios de comunicaciones electrónicas e infraestructuras digitales, lo que ha generado una urgente necesidad de fortalecer y dotar de mayor seguridad y resiliencia las redes y servicios de comunicaciones electrónicos y determinadas infraestructuras digitales ante posibles futuros incidentes, no sólo en materia de ciberseguridad sino también en el entorno físico. Así, en los últimos años se han producido una serie de incidentes que han puesto a prueba la seguridad y resiliencia de las redes y servicios de comunicaciones electrónicas, unos de forma natural, como la erupción volcánica en la isla de La Palma el 9 de septiembre de 2021, o la Depresión Aislada en Niveles Altos (DANA), que azotó la Península y Baleares, con mayor intensidad en la vertiente mediterránea el pasado mes de octubre de 2024, y otros no naturales como ha sido el apagón eléctrico que ha sufrido España de manera reciente.

La transformación digital impulsada por la evolución tecnológica alcanzada por la digitalización y virtualización de los servicios a través del Internet de las cosas (IoT), Inteligencia Artificial (IA), Big Data, y Computación en la Nube (Cloud), ha transformado radicalmente las tradicionales redes de telecomunicaciones y los servicios de comunicaciones electrónicas que, si bien ofrece grandes oportunidades en términos de eficiencia, conectividad, y desarrollo económico y social, también introduce importantes riesgos y vulnerabilidades en infraestructuras digitales para los que la regulación debe anticiparse y estar preparada.

La integridad y seguridad de las redes y servicios de comunicaciones electrónicas viene recogida en el artículo 63 de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones (en adelante, Ley General de Telecomunicaciones). Este artículo se ve complementado con la normativa sobre la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, plasmada en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación y el Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G.

A nivel europeo también se ha regulado la integridad y seguridad de las infraestructuras digitales, entre las que se encuentran las redes y servicios de comunicaciones electrónicas, en la Directiva (UE) 2022/2555, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea (en adelante, la Directiva NIS2), así como en la Directiva (UE) 2022/2557 de 14 de diciembre, relativa a la resiliencia de las entidades críticas (en adelante, la Directiva CER), que refuerzan las obligaciones de los operadores y empresas para prevenir, detectar, responder y recuperar, ante determinados incidentes de seguridad que puedan comprometer la disponibilidad y fiabilidad de las infraestructuras digitales y redes y servicios de comunicaciones electrónicas.

La Directiva NIS2 consagra una nueva regulación para garantizar un elevado nivel común de ciberseguridad en el ámbito de la Unión Europea En coherencia y coordinación con la futura normativa sobre ciberseguridad e infraestructuras críticas que transponga la Directiva NIS2 y CER, se considera necesario, aprobar un Real Decreto que establezca, para el sector de las redes y servicios de comunicaciones electrónicas y determinadas infraestructuras digitales, determinadas obligaciones específicas de seguridad y resiliencia en coordinación y coherencia con la normativa de ciberseguridad e infraestructuras críticas de conformidad con el artículo 63 de la Ley General de Telecomunicaciones.

Para darle consistencia y coherencia al presente Real Decreto con la normativa europea vigente y con los textos normativos que se deriven de la transposición de los anteproyectos normativos existentes en relación con las Directivas NIS2 y Directiva CER, las obligaciones recogidas en las Directivas mencionadas resultarán de aplicación, en todo caso, a los incidentes de ciberseguridad y a aquellos incidentes que se ocasionen en el sector de las redes, servicios de comunicaciones electrónicas e infraestructuras digitales que no estén previstos en el presente Real Decreto.

I.2. OBJETIVOS

El presente Real Decreto tiene por objeto establecer un marco normativo nacional que garantice la seguridad y resiliencia de las redes, los servicios de comunicaciones electrónicas y determinadas infraestructuras digitales frente a incidentes significativos de seguridad que puedan afectar a dichas redes o infraestructuras, o provocar una degradación sustancial en la calidad de los servicios prestados. Para ello, la norma incorpora obligaciones específicas en materia de seguridad y resiliencia aplicables al sector de las redes y servicios de comunicaciones electrónicas y determinadas infraestructuras digitales, desarrollando lo previsto en el artículo 63 de la Ley General de Telecomunicaciones y articulándose de manera coherente y coordinada con las disposiciones de las Directivas NIS2 y Directiva CER.

El artículo 63 de la Ley General de Telecomunicaciones, establece la necesidad de garantizar la integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas. En su apartado 1, se establece que los operadores de redes públicas de comunicaciones electrónicas y de servicios de comunicaciones electrónicas disponibles al público, gestionarán adecuadamente

los riesgos de seguridad que puedan afectar a sus redes y servicios, a fin de garantizar un adecuado nivel de seguridad, y de evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios para lo que deberán adoptar las medidas técnicas y organizativas adecuadas que consideren. Por su parte, el apartado 2, incluye también la obligación de los operadores, de garantizar la integridad de las redes de telecomunicaciones con el fin de asegurar la continuidad de los servicios de comunicaciones electrónicas.

En consonancia con lo anterior, el Capítulo I de este Real Decreto define su objeto y quiénes son los sujetos obligados al cumplimiento de las obligaciones en él contenidas. Por su parte, el Capítulo II establece los distintos planes que deben tener elaborados los sujetos obligados, general por operador y específico por servicios y tipología de incidentes, con el fin de garantizar la seguridad y resiliencia de las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales.

El artículo 63.3 de la Ley General de Telecomunicaciones incluye la obligación de los operadores que suministren redes públicas o presten servicios de comunicaciones electrónicas disponibles al público de notificar al actual Ministerio para la Transformación Digital y de la Función Pública los incidentes de seguridad que hayan tenido un impacto significativo en el suministro de las redes o los servicios. En este sentido, los artículos 20 a 23 de la Orden IET/1090/2014, de 16 de junio, por la que se regulan las condiciones relativas a la calidad de servicio en la prestación de los servicios de comunicaciones electrónicas (Orden de calidad, en adelante), ya se establecían los criterios para determinar qué se debe catalogar como suceso significativo, al tiempo que se establecen unas obligaciones de notificación, y sus plazos, en relación con este tipo de sucesos. No obstante, la evolución tecnológica, el cambio climático y determinadas circunstancias que se han venido sucediendo en los últimos años, nos muestran que esta Orden de Calidad, en este ámbito, ha quedado obsoleta y resulta oportuno actualizar la tipología de incidentes que deben tenerse en cuenta para garantizar una detección de riesgos y planificar las oportunas actuaciones de respuesta ante estos eventos que ponen a prueba la integridad y seguridad de redes y servicios de comunicaciones electrónicas.

La Orden de Calidad también establece los plazos y procedimientos de notificación para cada tipo de incidentes. Por el mismo motivo mencionado anteriormente, se considera que estos plazos y procedimientos deben ser actualizados y adaptados a la nueva realidad. De esta manera, la disponibilidad y manejo, tanto por los operadores como por las instituciones públicas competentes, de información fiable y lo más actualizada posible, por un lado, y una adecuada respuesta en la gestión de las consecuencias derivadas de cada incidente que posibilite una rápida recuperación de la funcionalidad de las redes de comunicaciones electrónicas, la continuidad en la prestación de los servicios y la operatividad de las infraestructuras digitales, por otro lado, no son cuestiones ortogonales, sino que están claramente imbricadas, de forma que deben ser ahormadas mediante un claro reforzamiento de los plazos y manejo de información estructurada y más detallada cuando acaece algún incidente que afecte a la seguridad de las redes o al normal desenvolvimiento de los servicios de comunicaciones electrónicas para facilitar la rápida recuperación de las redes y servicios. Así, este Real Decreto desarrolla, en su Capítulo III, los

nuevos plazos y los procedimientos de notificación para cada uno de los tipos de incidentes de seguridad que sufran las redes y servicios de comunicaciones electrónicas, así como determinadas infraestructuras digitales.

De igual forma, el apartado 3 del mencionado artículo 63, prevé la necesidad de establecer un mecanismo de colaboración e información entre el Ministerio para la Transformación Digital y de la Función Pública y otras autoridades nacionales competentes de otros Estados miembros y con la Agencia Europea de Seguridad en las Redes y la Información (ENISA). También prevé que el Ministerio podrá informar al público o exigir a los operadores que lo hagan, en caso de estimar que la divulgación del incidente de seguridad reviste interés público. En desarrollo de esta previsión legal, el Capítulo VI en sus artículos 24, 25 y 26 de este Real Decreto regulan los mecanismos de cooperación del Ministerio para la Transformación Digital y de la Función Pública con las autoridades, nacionales y a nivel europeo en materia de seguridad.

En aras de reforzar la cooperación y coordinación entre todos los agentes involucrados y favorecer la imprescindible colaboración pública-privada en la planificación, detección de riesgos y gestión común de unos incidentes que afectan a una materia de interés común como es la seguridad y resiliencia de las redes y servicios de comunicaciones electrónicas, la disposición adicional segunda constituye una mesa de coordinación en la que intervienen una pluralidad de agentes para configurarse como foro de diálogo, de compartir experiencias y necesidades y de establecimiento de protocolos y mejores prácticas ante el suceso de futuros incidentes como los que han venido ocurriendo en los últimos años que afecten a la seguridad de redes y servicios de comunicaciones electrónicas y de determinadas infraestructuras digitales.

El apartado 4 del artículo 63 prevé un mecanismo de comunicación a los usuarios en el supuesto de que se produzca un incidente de seguridad que afecte a los servicios de comunicaciones electrónicas prestados. Este apartado ha sido desarrollado e concretado en el artículo 15 de este Real Decreto, incluyendo, además de la obligación de notificación, la comunicación sobre el tiempo previsto de reparación y medidas adoptadas para mitigar esta incidencia.

El apartado 5 del artículo 63 establece el procedimiento de inspección y régimen sancionador, así como la posibilidad de adoptar medidas adicionales a las identificadas en materia de integridad y seguridad de redes y servicios de comunicaciones electrónicas. Este apartado ha sido desarrollado en este Real Decreto en el Capítulo VII así como en el artículo 13, donde se habilita a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales para imponer nuevas obligaciones, formular recomendaciones, orientaciones o asesoramiento operativo a los sujetos obligados sobre la aplicación de posibles medidas paliativas en relación con las medidas de contingencia adoptadas durante las incidencias notificadas o para disminuir el riesgo de que se repitan.

Por su parte, la obligación recogida en la Ley General de Telecomunicaciones de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad y la obligación de someterse a una auditoría de seguridad realizada por un organismo

independiente, a costa del propio sujeto obligado, y poner el resultado a disposición del Ministerio para la Transformación Digital y de la Función pública se encuentran previstos en el artículo 23 del presente Real Decreto.

El Capítulo IV recoge las obligaciones de los centros de recepción de llamadas de emergencias y alertas públicas, y de los sujetos obligados por este Real Decreto, de garantizar la mayor disponibilidad de los servicios de emergencias en caso de fallo catastrófico de la red o en casos de fuerza mayor, y la obligación de adoptar las medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencia y la transmisión ininterrumpida de las alertas públicas, en línea con el apartado 6 del artículo 63.

El Capítulo V de este Real Decreto regula y desarrolla las medidas adoptadas en el artículo 4.6 la Ley General de Telecomunicaciones en relación con la asunción por la Administración General del Estado de la gestión directa de determinados servicios de comunicaciones electrónicas disponibles al público, para garantizar la seguridad pública y la seguridad nacional o el cumplimiento de obligaciones de servicio público de conformidad con el apartado 7 de del artículo 63.

El apartado 8 del artículo 63, relativo a la a la protección de datos personales y garantía de los derechos digitales y su normativa de desarrollo, se han previsto y desarrollado en el Capítulo VI en sus artículos 27 y 28 de este Real Decreto.

I.3. ADECUACIÓN A LOS PRINCIPIOS DE BUENA REGULACIÓN.

En la elaboración y tramitación de este Real Decreto se han observado los principios de buena regulación previstos en el artículo 129 de Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas:

a) **Principio de necesidad**.

Se considera necesario adoptar una serie de medidas que refuercen la seguridad y resiliencia de las redes de telecomunicaciones, los servicios de comunicaciones electrónicas y determinadas infraestructuras digitales, desarrollando así lo previsto en el artículo 63 de la Ley General de Telecomunicaciones. Es necesario que estas medidas se articulen de forma coherente y coordinada con el contenido de la Directiva NIS2 y la Directiva CER, garantizando una integración normativa eficaz y alineada con los objetivos europeos en materia de ciberseguridad y protección de infraestructuras críticas.

Las Directivas mencionadas establecen obligaciones en materia de ciberseguridad y resiliencia desde un enfoque transversal y multisectorial, lo que dificulta abordar con suficiente profundidad las especificidades técnicas, operativas y estratégicas propias del sector de las redes, los servicios de comunicaciones electrónicas y determinadas infraestructuras digitales. En consecuencia, se considera necesario establecer una regulación nacional que, en plena consonancia con ambas Directivas, permita abordar de forma integral la seguridad y resiliencia de estos

sectores estratégicos, atendiendo a sus particularidades y reforzando la capacidad de respuesta ante incidentes de seguridad.

En este sentido el Real Decreto incorpora la consideración de servicios e instalaciones con "carácter esencial" las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales en situaciones de emergencias. Asimismo, prevé la elaboración de un "Plan Nacional de Seguridad y Resiliencia" para este tipo de redes y servicios que desarrollará y coordinará un plan de respuesta y restablecimiento a incidentes de seguridad en el que se fijarán los objetivos y medidas para la gestión de cada tipología de incidentes. Además, incluye la obligación de los sujetos obligados de disponer de un "Plan de acción general por operador" y "Plan específico para cada red, servicio o infraestructura" que recoja las medidas adoptadas de prevención, detección y respuesta ante incidentes y riesgos de seguridad elaboradas por cada operador en caso de que se produzca un incidente significativo con el objetivo de lograr el restablecimiento de los servicios lo antes posible. Finalmente, se incluye la elaboración de un "Plan Nacional Civil de Emergencias" con el objetivo de diseñar una estrategia para movilizar recursos y bienes relativos a redes, servicios de comunicaciones electrónicas e infraestructuras digitales que coadyuve a recupera cuanto ante las condiciones de normalidad.

Por otro lado, se considera necesario actualizar y regular de forma detallada el "contenido y plazos de las notificaciones" que los sujetos obligados deben realizar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales cuando se produce un incidente que afecta a la integridad de las redes, determinadas infraestructuras digitales y/o a la continuidad de los servicios de telecomunicaciones.

De igual forma, se considera necesario recoger la "obligación de los centros de recepción de llamadas de emergencias y alertas públicas" de adoptar las medidas técnicas que consideren necesarias para el correcto encaminamiento de las llamadas de emergencias, así como regular la obligación de los sujetos obligados de adoptar un plan específico para el encaminamiento de las llamadas al centro de recepción de llamadas de emergencias y alertas públicas. De igual forma, se considera necesario recoger un mecanismo de notificaciones a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales ante la interrupción del servicio de llamadas de emergencias con el objetivo de que tanto los equipos de emergencias como los responsables políticos dispongan, desde el primer momento, información clara, fiable y lo más exacta posible sobre la evolución de la integridad de las redes de telecomunicaciones, prestación de los servicios de comunicaciones electrónicas y determinadas infraestructuras digitales para adoptar, en el menor tiempo posible, las decisiones que sean necesarias en cada momento.

De igual forma se considera necesario establecer un "procedimiento de ejecución y coordinación" con otras autoridades nacionales, con las Comunidades Autónomas y europeas afectadas, así como un "régimen de inspección y sanción" en caso de incumplimiento de las obligaciones previstas en el presente Real Decreto de forma coordinada y coherente con el contenido de la Directiva NIS2 y Directiva CER que establecen un enfoque transversal y multisectorial las obligaciones en materia de ciberseguridad y resiliencia.

Por último, en materia de coordinación y cooperación, se considera necesario constituir una “mesa de coordinación” en la que intervienen una pluralidad de agentes para configurarse como foro de diálogo, de compartir experiencias y necesidades y de establecimiento de protocolos y mejores prácticas ante el suceso de futuros incidentes como los que han venido ocurriendo en los últimos años que afecten a la seguridad de redes y servicios de comunicaciones electrónicas y de determinadas infraestructuras digitales.

B) Principio de proporcionalidad.

Las obligaciones que se incluyen en este Real Decreto se consideran proporcionadas y equilibrada al no representar una carga excesiva para los sujetos obligados ni desde el punto de vista económico ni desde el punto de vista administrativo.

La obligación de elaborar un “Plan general por operador” y de los “Planes específicos” no es una novedad para los sujetos obligados. La exigencia de estos planes se ajusta a la experiencia previa de los operadores que ya vienen elaborando planes similares en el ejercicio ordinario de sus funciones, lo que demuestra que cuentan con los trabajos ya realizados y con la capacidad técnica y organizativa para cumplir con esta obligación.

Dentro de los “Planes específicos” se prevé que, en situaciones de interrupción del suministro eléctrico, los sujetos obligados deben garantizar su operatividad ante la situación de interrupción del suministro eléctrico al menos durante 24 horas, las instalaciones o infraestructuras esenciales de nivel intermedio al menos durante 12 horas mientras que el resto de las instalaciones e infraestructuras deberán garantizar su operatividad durante al menos 4 horas. Además, para el caso de concreto de la red de acceso dentro de una red de comunicaciones móviles a través de la cual se proveen servicios de comunicaciones electrónicas disponibles al público en bandas armonizadas europeas, dicha red de acceso debe estar diseñada y dotada de los equipos electrógenos y elementos de suministro eléctrico propios que permite garantizar su operatividad y continuidad de servicio durante al menos 4 horas para el 85% de la población en España. En el diseño, planificación y ejecución de esta estrategia de mantenimiento de operatividad de las infraestructuras e instalaciones y de continuidad en la prestación de servicios, el operador podrá utilizar todas las estaciones base, ya sean fijas o portátiles, bandas de frecuencias y tecnologías que estime oportuno, así como podrá priorizar todas aquellas ubicaciones, centros e instalaciones que considere conveniente en función a su vinculación a la prestación de servicios públicos y servicios de relevancia económica y social.

En este sentido, se considera que la obligación de elaborar estos planes es proporcional y equilibrada y no supone una carga excesiva, ni económica ni administrativa para los sujetos obligados.

En cuanto a la obligación de “notificación de incidentes de seguridad” por parte de los sujetos obligados, también se considera proporcionada y equilibrada ya que, en

la actualidad, los operadores de telecomunicaciones también vienen realizando notificaciones similares a las identificadas en este Real Decreto. Si bien la obligación de notificación puede suponer alguna carga administrativa adicional a las que incurren en la actualidad, estas cargas son proporcionales, equilibradas, y se encuentran justificadas al fin que se pretende obtener, puesto que obtener información en tiempo y de forma ordenada sobre los incidentes de seguridad permite adoptar, de la mejor manera posible, las decisiones necesarias para priorizar la gestión de los recursos y los servicios públicos en situaciones de especial criticidad.

La creciente heterogeneidad de las redes y servicios de comunicaciones electrónicas —incluyendo redes y servicios fijos, móviles y audiovisuales— junto con la multiplicidad de incidentes de naturaleza multifactorial que se han venido concatenando en los últimos años, hacen que la medida incluida de habilitar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales para que, mediante orden ministerial, pueda dar instrucciones o modificar los planes presentados por los operadores y del contenido de las notificaciones sea proporcional y equilibrada. Esta habilitación se justifica en virtud del principio de flexibilidad regulatoria, al ser indispensable para adaptar los planes a la evolución tecnológica y a los riesgos emergentes que afectan la continuidad y calidad de los servicios ofrecidos. Asimismo, dicho mecanismo garantiza una respuesta proporcional y adecuada ante situaciones imprevistas, reforzando la capacidad de actuación de la Administración en un entorno dinámico y complejo como en es el de los servicios e infraestructuras digitales.

C) **Principio de seguridad jurídica**.

Las medidas adoptadas en este Real Decreto cumplen con el principio de seguridad jurídica al desarrollar el contenido del artículo 63 de la Ley General de Telecomunicaciones de forma coherente y coordinada con la Directiva NIS2 y con la Directiva CER.

Como se ha comentado con anterioridad, estas Directivas establecen obligaciones en materia de ciberseguridad y resiliencia con un enfoque transversal y multisectorial que no permite abordar con suficiente profundidad las particularidades técnicas, operativas y estratégicas del sector de las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales.

Por ello, resulta necesario establecer una normativa nacional que, de forma coherente y coordinada con las Directivas anteriormente mencionadas, regule de forma holística la seguridad y resiliencia para las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales ante un incidente de seguridad que suponga la interrupción del servicio o una fuerte degradación de su calidad.

D) **Principio de transparencia.**

Se cumple el principio de transparencia al haberse efectuado el trámite de audiencia e información pública previstas en el artículo 133 de la Ley 39/2015, de 1 de octubre.

E) **Principio de eficiencia.**

Se considera eficiente la aprobación de este Real Decreto al integrar en un único texto normativo, de manera desarrollada y ordenada, tanto el contenido del artículo 63 de la Ley General de Telecomunicaciones como de la Orden de Calidad que regula actualmente el contenido y plazo de las notificaciones que los operadores de telecomunicaciones vienen reportando a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales cuando se producen incidentes significativos que afectan gravemente a la integridad de las redes y a la continuidad de los servicios que se prestan a través de infraestructuras digitales.

I.4.- ALTERNATIVAS.

En el proceso de elaboración del Real Decreto se han valorado diversas alternativas regulatorias, atendiendo a los principios de necesidad, proporcionalidad, eficiencia y seguridad jurídica llegando a la conclusión de que la elaboración de un Real Decreto es el instrumento jurídico idóneo para regular los objetivos descritos en el I.2.

Se han analizado las siguientes alternativas:

A) Mantener el marco normativo vigente sin desarrollo reglamentario adicional.

Una primera alternativa consistía en no desarrollar reglamentariamente el contenido recogido en el artículo 63 de la Ley General de Telecomunicaciones.

A nivel europeo también se ha regulado la integridad y seguridad de las infraestructuras digitales, entre las que se encuentran las redes y servicios de comunicaciones electrónicas, en la Directiva (UE) 2022/2555, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea (en adelante, la Directiva NIS2), así como en la Directiva (UE) 2022/2557 de 14 de diciembre, relativa a la resiliencia de las entidades críticas (en adelante, la Directiva CER), que refuerzan las obligaciones de los operadores y empresas para prevenir, detectar, responder y recuperar, ante determinados incidentes de seguridad que puedan comprometer la disponibilidad y fiabilidad de las infraestructuras digitales y redes y servicios de comunicaciones electrónicas.

La Directiva NIS2 consagra una nueva regulación para garantizar un elevado nivel común de ciberseguridad en el ámbito de la Unión Europea. Por tanto, en coherencia y coordinación con la futura normativa sobre ciberseguridad e infraestructuras críticas que transponga la Directiva NIS2 y CER, se considera necesario, aprobar un Real Decreto que establezca, para el sector de las redes y servicios de comunicaciones electrónicas y determinadas infraestructuras digitales, determinadas obligaciones específicas de seguridad y resiliencia en coordinación y

coherencia con la normativa de ciberseguridad e infraestructuras críticas de conformidad con el artículo 63 de la Ley General de Telecomunicaciones.

B) Establecer recomendaciones técnicas no vinculantes *"guidelines"*.

Se ha valorado la posibilidad de emitir recomendaciones técnicas con el contenido necesario sin establecer obligaciones jurídicas vinculantes. Esta opción ha sido rechazada por su limitada capacidad de exigibilidad y supervisión, especialmente en situaciones de emergencia o crisis, donde se requiere una respuesta coordinada, rápida y jurídicamente respaldada.

C) Desarrollar un marco reglamentario específico mediante Real Decreto.

Tras los inconvenientes descritos con anterioridad, se ha optado por la elaboración de un Real Decreto que regule de forma proporcionada y equilibrada la seguridad de las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales, y de forma también coherente y coordinada con la normativa nacional y europea sobre ciberseguridad.

I.5.- INCLUSIÓN EN EL PLAN ANUAL NORMATIVO Y EVALUACIÓN EX POST.

El presente Real Decreto no se ha incluido en el Plan Anual Normativo 2025 puesto que la elaboración de este texto normativo se fundamenta en las consecuencias de los incidentes sobrevenidos que han evidenciado la necesidad urgente de reforzar la regulación en materia de seguridad de redes e infraestructuras digitales. En particular, los efectos de la DANA (Depresión Aislada en Niveles Altos) en septiembre de 2025, que provocó graves interrupciones en los servicios de telecomunicaciones en diversas zonas del territorio nacional, así como el apagón masivo ocurrido en octubre del mismo año, que afectó a infraestructuras críticas y puso de manifiesto vulnerabilidades sistémicas, han generado un nuevo escenario de riesgo que no había sido contemplado en el momento en que se elaboró el Plan normativo. Las consecuencias de estos incidentes justifican la adopción de medidas normativas específicas, mediante Real Decreto, que permitan fortalecer la resiliencia y capacidad de respuesta del sector frente a amenazas complejas y multifactoriales.

No corresponderá su evaluación *ex post*.

II.- CONTENIDO Y ANÁLISIS JURÍDICO

II.1.- CONTENIDO

El proyecto de Real Decreto está conformado por una parte expositiva y una parte dispositiva dividida en siete capítulos, con 37 artículos, dos disposiciones adicionales, una disposición derogatoria única y tres disposiciones finales.

Capítulo I con el epígrafe "Disposiciones Generales"

Recoge los dos primeros artículos:

El artículo 1 contiene el objeto del Real Decreto consistente en establecer las condiciones y actuaciones dirigidas a garantizar la seguridad, y resiliencia de las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales, especialmente ante situaciones y acontecimientos que afecten a la seguridad de las redes, la interrupción del servicio o una importante degradación de las condiciones de prestación. De igual forma, constituye el objeto de este Real Decreto regular los supuestos y requisitos en que los sujetos obligados tienen obligación de notificar al Ministerio para la Transformación Digital y de la Función Pública cuando surja un incidente de seguridad que tenga un impacto significativo en el suministro de las redes o de los servicios.

El artículo 2 determina cuál es el ámbito de aplicación de este Real Decreto. En este sentido, se establece que será de aplicación:

- A los titulares y gestores de redes públicas de comunicaciones electrónicas ubicados en España.
- A los prestadores de servicios de comunicaciones electrónicas disponibles al público que se presten en España.
- A los titulares o gestores de cualquier recurso asociado que sirva de soporte para el funcionamiento de redes públicas o la prestación de cualquier servicio de comunicaciones electrónicas ubicados en España como son, entre otros, cables submarinos, sistemas satelitales, redes de distribución de contenidos (CDN), centros de procesamiento de datos (CPD) o puntos de intercambio de internet (IXP) y cualquier recurso asociado de estas infraestructuras cuando contribuyan al funcionamiento de redes de comunicaciones electrónicas disponible al público.
  A estos efectos, los titulares y gestores de redes públicas de comunicaciones electrónicas y prestadores de servicios de comunicaciones electrónicas disponibles al público deberán identificar las infraestructuras digitales que contribuyen al funcionamiento de sus propias redes o prestación de sus servicios de comunicaciones electrónicas y deberán comunicarlas a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales antes del 31 de enero de cada año natural.

Todos los sujetos obligados identificados en el punto anterior deben cumplir una serie de parámetros recogidos en el apartado 3 del artículo 2. El Real Decreto prevé que estos parámetros puedan ser modificados a través de Orden ministerial.

Quedan excluidos de este Real Decreto los titulares y gestores de redes de comunicaciones electrónicas, servicios de comunicaciones electrónicas e infraestructuras digitales que estén vinculadas a la Seguridad Nacional y Defensa.

En todos lo no regulado en el presente Real Decreto, así como a los incidentes de ciberseguridad, será de aplicación la normativa nacional y europea relativa a la

coordinación y gobernanza de la ciberseguridad y a la protección y resiliencia de entidades críticas.

El artículo 3 determina el carácter de instalación o servicio esencial de las redes y servicios de comunicaciones electrónicas y determinadas infraestructuras digitales en situaciones de emergencia cuando surjan incidentes de seguridad que afecten a la seguridad de las redes, la interrupción del servicio o una importante degradación en las condiciones de prestación.

En estas situaciones de emergencia, todas las autoridades, órganos administrativos y las Fuerzas y Cuerpos de Seguridad del Estado colaborarán y contribuirán para facilitar la más pronta y extensa posible recuperación de la integridad y seguridad de la red, restablecimiento del servicio u operatividad de la infraestructura o facilitar su mantenimiento, adoptando las medidas administrativas, técnicas y operativas que resulten necesarias. Entre otras, se otorgarán los salvoconductos y permisos de acceso que permitan al personal de los operadores y titulares o gestores de infraestructuras digitales y de las empresas contratadas por ellos el acceso a las instalaciones e infraestructuras para su reparación, reconstrucción o mantenimiento; se darán prioridad y declararán la urgencia en la tramitación de cualquier procedimiento que tenga como objetivo último la recuperación de la integridad y seguridad de la red, restablecimiento del servicio u operatividad de la infraestructura o facilitar su mantenimiento, como por ejemplo, otorgar licencias y permisos de carácter provisional y transitorio, ya sea de carácter urbanístico, ordenación del territorio, medioambiental o de cualquier otro tipo, que posibiliten que los operadores y titulares o gestores de infraestructuras digitales puedan recuperar la seguridad y operatividad de las instalaciones e infraestructuras.

También se prevé que las Fuerzas y Cuerpos de Seguridad del Estado presten el auxilio y apoyo necesario para que el personal pueda desplegar sus actividades y operaciones dirigidas recuperar la seguridad y operatividad de las instalaciones e infraestructuras o facilitar su mantenimiento.

En el caso concreto de la interrupción del suministro eléctrico, las instalaciones o infraestructuras que se consideren por el operador esenciales de primer nivel y de nivel intermedio en los planes presentados gozarán de prioridad en las actuaciones de restablecimiento del suministro eléctrico. De igual forma, en los supuestos en que para la reparación, reconstrucción o mantenimiento de las instalaciones e infraestructuras de las redes y servicios de comunicaciones electrónicas e infraestructuras digitales resulte necesario el suministro de combustible, será prioritario dicho suministro para las citadas instalaciones e infraestructuras.

Capítulo II con el epígrafe "Planificación para garantizar la seguridad, y resiliencia de las redes y servicios de comunicaciones electrónicas y determinadas infraestructuras digitales".

Contiene los artículos del 4 a 8:

El artículo 4 define el "Plan Nacional de Seguridad y Resiliencia de redes, determinadas infraestructuras digitales y servicios de comunicaciones electrónicas".

Este Plan será aprobado, por medio de Orden Ministerial, por el Ministerio para la Transformación Digital y de la Función Pública. Tiene como objetivo desarrollar y coordinar un plan de respuesta y restablecimiento de incidentes de seguridad en el que se establezcan los objetivos, funciones y responsabilidades asignadas a las diferentes autoridades, procedimientos de gestión de crisis y posibles medidas de anticipación como podría ser actividades de formación.

Se prevé que este Plan Nacional debe elaborarse en el plazo de un año a contar desde la entrada en vigor del presente Real Decreto y actualizado cada 3 años.

El artículo 5 establece la obligación de gestión adecuada de los riesgos de seguridad. Para ello se establece la obligación de los sujetos obligados de gestionar adecuadamente los riesgos de seguridad tratando de evitar o reducir al mínimo el impacto de los incidentes de seguridad tanto en los usuarios como en las redes. En este sentido se incluye también la obligación de los operadores de garantizar la mayor disponibilidad posible de los servicios de comunicaciones vocales, de acceso a internet a través de las redes de telecomunicaciones en caso de fallo catastrófico de la red o casos de fuerza mayor y adoptarán todas las medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencias y a transmisión ininterrumpida de las alertas públicas.

El artículo 6 establece la obligación de disponer de un “Plan de acción general de cada sujeto obligado para garantizar la seguridad y resiliencia de las redes y servicios de comunicaciones electrónicas”. Este Plan debe incluir además de un análisis de riesgos sobre la seguridad de su red, la identificación de si se trata de una red o infraestructura esencial e identificando también las medidas de prevención y detección, los mecanismos y priorizaciones en las medidas a adoptar para la gestión y recuperación de los servicios ante la interrupción o importante degradación en la prestación de los servicios.

En este Plan general los operadores identificarán los edificios e instalaciones que se consideren esenciales y sobre los que adoptara medidas específicas y prioritarias para garantizar la seguridad de las redes y la continuidad del servicio. También detallará los criterios que se han tenido en cuenta para considerar los edificios como esenciales, así como las medidas específicas y prioritarias que se han adoptado en cada edificio o instalación para garantizar la seguridad de las redes y la continuidad de los servicios.

El Plan general debe ser entregado a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales en el plazo de 6 meses desde la entrada en vigor del Real Decreto y será actualizado cada 2 años.

El artículo 7 establece la obligación de disponer cada sujeto obligado de un “Plan específico para cada red, servicio o infraestructuras digitales que se utilice para garantizar su seguridad.

Este plan específico deberá presentarse globalmente para cada una de las siguientes tipologías de redes, servicios e infraestructuras digitales:

a) Redes y servicios de comunicaciones fijas.

b) Redes y servicios de comunicaciones móviles.
c) Servicios de mensajería instantánea.
d) Redes soporte de servicios de comunicación audiovisual.
e) Cables submarinos.
f) Sistemas de satélites.
g) Determinadas infraestructuras digitales que contribuyen al funcionamiento de redes públicas de comunicaciones electrónicas y prestación del servicio de comunicaciones electrónicas, previamente identificados por los operadores de comunicaciones electrónicas, de conformidad con el artículo 2.2 de este Real Decreto, como pueden ser las Redes de distribución de contenidos (CDN), los Centros de procesamientos de datos (CPD) y Puntos de intercambio de internet (IXP).

Se prevé que como consecuencia del carácter dinámico del sector de las comunicaciones electrónicas y de las infraestructuras digitales, del incesante proceso de innovación tecnológica característico de estos ámbitos y las continuas y sucesivas transformaciones regulatorias, económicas, comerciales y competitivas en que se devuelven los agentes en estos mercados, los anteriores supuestos y tipologías podrán ser objeto de modificación mediante Orden aprobada por la persona titular del Ministerio para la Transformación Digital y de la Función Pública.

Adicionalmente, los sujetos obligados tienen obligación de presentar un Plan específico para cada tipología de incidencia que se determine mediante Orden. Inicialmente se identifican las siguientes tipologías de incidencias: una afectación grave a la planta de red externa, una interrupción del suministro eléctrico, evento meteorológico con afectación grave a la red, servicio o infraestructura, erupción volcánica, seísmo, inundación, incendio, fallo informático grave y ataque cibernético grave.

En ambos planes específicos, los sujetos obligados describirán las prioridades y medidas de prevención, detección, así como las medidas que se adoptarán para la recuperación de los servicios en caso de interrupción o importante degradación de las condiciones en la prestación de éstos.

En los planes específicos se podrá contemplar que, como medidas dirigidas a gestionar adecuadamente el incidente ocurrido, el sujeto obligado podrá adoptar decisiones con el objetivo de garantizar el mantenimiento de los servicios más básicos y esenciales de comunicaciones electrónicas, posibilitar el mantenimiento de la comunicación en la mayor extensión posible a los distintos ciudadanos y territorios y evitar incurrir en situaciones de congestión de tráfico y a tal efecto el plan podrá prever y el sujeto obligado, llegado el caso, podrá ejecutar medidas como priorizar determinado tipo de tráfico, como aquel vinculado a los servicios de emergencia, la realización de comunicados oficiales o el dirigido a cuentas oficiales, priorizar el tráfico consistente en comunicaciones vocales y mensajes SMS frente al tráfico de transmisión de datos, o suspender provisionalmente la aplicación o funcionamiento de determinadas tecnologías o servicios que demanden un mayor consumo energético o una mayor capacidad de transmisión de datos.

Además, estos planes específicos incluirán información estimada sobre el porcentaje de tráfico y tiempo de servicio que, en caso de catástrofes naturales o

posibles situaciones de emergencia energética, la infraestructura de red es capaz de garantizar la continuidad, operatividad y funcionamiento del servicio. En particular, en situaciones de interrupción del suministro eléctrico, el sujeto obligado deberá determinar dentro de la red, servicio o infraestructura digital aquellas instalaciones o infraestructuras que se consideren esenciales por su importancia e incidencia en el mantenimiento de la operatividad y funcionamiento del servicio. Estas instalaciones o infraestructuras esenciales de primer nivel deberán garantizar su operatividad ante la situación de interrupción del suministro eléctrico al menos durante 24 horas, las instalaciones o infraestructuras esenciales de nivel intermedio al menos durante 12 horas mientras que el resto de las instalaciones e infraestructuras deberán garantizar su operatividad durante al menos 4 horas.

En el caso concreto de la red de acceso dentro de una red de comunicaciones móviles a través de la cual se proveen servicios de comunicaciones electrónicas disponibles al público en bandas armonizadas europeas, dicha red de acceso debe estar diseñada y dotada de los equipos electrógenos y elementos de suministro eléctrico propios que permite garantizar su operatividad y continuidad de servicio durante al menos 4 horas para el 85% de la población en España. En el diseño, planificación y ejecución de esta estrategia de mantenimiento de operatividad de las infraestructuras e instalaciones y de continuidad en la prestación de servicios, el operador podrá utilizar todas las estaciones base, ya sean fijas o portátiles, bandas de frecuencias y tecnologías que estime oportuno, así como podrá priorizar todas aquellas ubicaciones, centros e instalaciones que considere conveniente en función a su vinculación a la prestación de servicios públicos y servicios de relevancia económica y social.

Las instalaciones o infraestructuras que se consideren por el operador esenciales de primer nivel y de nivel intermedio en situaciones de interrupción del suministro eléctrico deben ser comunicadas a la empresa encargada del transporte y las empresas distribuidoras de electricidad para que puedan ser incluidas en sus planes de contingencia eléctrica.

En los planes específicos y en el diseño de medidas de gestión de incidentes y mitigación de las posibles consecuencias y perjuicios que se puedan ocasionar, el sujeto obligado deberá incorporar los mecanismos y técnicas más avanzadas e innovadoras en la detección y prevención de riesgos y en la gestión de los incidentes acaecidos, en particular, aquellas técnicas vinculadas al uso de servicios de inteligencia artificial que coadyuven a la planificación, diseño y gestión de riesgos que posibiliten disponen y suministrar redes y servicios de comunicaciones electrónicas e infraestructuras digitales más seguros y resilientes.

Al igual que ocurre con los planes generales, cada sujeto obligado deberá presentar estos planes específicos a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales en el plazo máximo de 6 meses a contar desde la entrada en vigor de este Real Decreto y deberá ser actualizado cada dos años.

El artículo 8 establece que la Secretaría de Estado de Telecomunicaciones e infraestructuras Digitales analizará los distintos planes presentados por los sujetos obligados y, a la vista del análisis, podrá dictar instrucciones y directrices para

modificarlos con el objetivo de garantizar la seguridad de las redes y servicios de comunicaciones electrónicas y las infraestructuras digitales.

El artículo 9 establece el "Plan Nacional Civil de Emergencias en materia de redes y servicios de comunicaciones electrónicas" en el que se diseñará una estrategia para movilizar recursos y bienes relativos a redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales para recuperar lo antes posible las condiciones de normalidad.

Este Plan debe ser actualizado cada dos años.

Capítulo III con el epígrafe "Notificaciones ante incidentes de seguridad en las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales"

Contiene los artículos 10 al 18.

El artículo 10 recoge la obligación de los sujetos obligados de notificar los incidentes de seguridad que hayan tenido un impacto significativo en las redes, determinadas infraestructuras digitales o servicios de comunicaciones electrónica y los parámetros considerados para determinar la importancia del impacto de un incidente de seguridad. Además, recoge la obligación de que los sueltos obligados dispongan de los medios materiales y humanos necesarios para dar cumplimiento a la obligación de notificación con independencia de los medios disponibles para restablecer la situación a la normalidad.

El artículo 11, define el concepto de incidentes de seguridad en las redes, determinadas infraestructuras digitales y servicios de comunicaciones electrónicas y establece los parámetros para considerar si un incidente debe ser considerado de menor significación o significativo, así como el momento en que debe considerarse como inicio y fin de un incidente de seguridad.

El artículo 12 define los tipos, procedimientos y contenido de la notificación inicial, intermedia y final que debe realizarse por el sujeto obligado a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

En cuanto a las notificaciones iniciales, se prevé que estas se llevarán a cabo por correo electrónico en el plazo máximo de 1 horas desde que el sujeto obligado tuvo conocimiento del incidente. En el caso de que no sea posible la notificación mediante correo electrónico, el sujeto obligado deberá ponerse en contacto con la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales a través del medio que lo permita y se acordará la vía para transmitir la notificación y la información. En lo que respecta al contenido, incluirá al menos información sobre el momento exacto del inicio del incidente, una breve descripción de la causa que lo ha originado y, en particular, si en esos momentos se considera que es un incidente de ciberseguridad o de cualquier otro tipo o híbrido, los servicios afectados y, en particular si afecta al servicio de emergencias o al servicio de alertas públicas, persona de contacto y datos de comunicación y, cualquier otra información que el sujeto obligado considere relevante.

Para las notificaciones intermedias, si han transcurrido más de 2 horas desde la notificación inicial sin que se haya solventado en su totalidad el incidente, el sujeto obligado tenderá que remitir, por correo electrónico, durante las primeras 24 horas desde el inicio del suceso, cada 2 horas, a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales actualización de la información contenida y aportar información adicional que le solicite la Secretaría de Estado. En cuanto al contenido, deberá aportarse remitirá una descripción detallada sobre la incidencia y las infraestructuras digitales afectadas, impacto de la avería, si se ha reestablecido el servicio de emergencias y alertas públicas, si hay otros operadores afectados, actualización del número de líneas y/o usuarios afectados en función del servicio, un análisis preliminar de la causa de la avería, si la causa es interna o externa y detalle sobre la causa, si se debe a fallo en los sistemas, congestión de red, errores humanos, acciones maliciosas, fenómenos naturales, fallo de terceras partes como puede ser suministro eléctrico, robo de cable, terremotos o inundaciones, así como cualquier información adicional que pueda ir reportando el operador.

De igual forma, se establece que, si el incidente afectara a más de un sujeto obligado, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales indicará durante las primeras 24 horas, las horas exactas en que deberá remitirse las notificaciones intermedias. Transcurridas las primeras 24 horas desde el inicio del suceso, las notificaciones intermedias se remitirán a las 9: 00 horas, a las 16:00 horas y a las 21:00 horas, por medio de correo electrónico, hasta que se lleve a cabo la notificación final. No obstante, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá modificar los periodos de tiempo y horas identificadas anteriormente en función de la afectación y gravedad del incidente.

Por último, se prevé que una vez resulta la incidencia, el sujeto obligado remitirá por correo electrónico tan pronto como tenga conocimiento del restablecimiento del servicio afectado una notificación. No obstante, sin perjuicio de lo anterior, en el plazo máximo de 24 horas desde que el operador notifique la finalización del suceso, el sujeto obligado remitirá una notificación final en la que indique, además del momento exacto de finalización del incidente, una actualización lo más detallada posible de ultima información reportada.

Por último, transcurridos 10 días desde la notificación final, el sujeto obligado debe remitir, por correo electrónico, un informe detallado con el contenido detallado en el artículo 11.

De igual forma, se prevé que los sujetos obligados que sufran un incidente considerado de menor significación según lo estipulado en el artículo 11.2, deberán notificar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales por correo electrónico dicho incidente, así como su resolución tan pronto como sea posible.

Por último, se prevé que los sujetos obligados comunicarán a la Secretaría de Estado de Telecomunicaciones e infraestructuras Digitales, en el plazo de 3 meses desde la entrada en vigor, los datos de contacto de los responsables de estas notificaciones cuyos datos serán actualizados, al menos, una vez al año.

El artículo 13 establece las medidas paliativas que puede adoptar la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales en relación con las medidas de contingencia adoptadas por los sujetos obligados durante las incidencias notificadas o para disminuir el riesgo de que se repitan. Concretamente se establece que se podrán imponer nuevas obligaciones, formular recomendaciones, orientaciones o asesoramiento a los sujetos obligados sobre aplicación de posibles medidas correctivas.

El artículo 14 recoge el procedimiento de colaboración con otros Estados Miembros afectados. Para ello, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales será quien informe al otro Estado miembro.

El artículo 15 identifica las medidas de notificación a las personas físicas y jurídicas destinatarias de los servicios afectados por un incidente de seguridad significativo en la red o servicios de comunicaciones electrónicas. Para ello, los sujetos obligados lo comunicarán a la mayor brevedad, y en todo caso, antes del plazo de 72 horas desde que se detectó el incidente.

El artículo 16 establece las notificaciones a otras autoridades competentes en el supuesto de incidentes de seguridad significativos que afectan a infraestructuras críticas y en materia de ciberseguridad.

El artículo 17 recoge la posibilidad de notificar, de forma voluntaria, otro tipo de incidentes o información pertinente.

El artículo 18 contiene la información que la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá proveer a los sujetos obligados. Concretamente, se prevé que cuando así lo estime oportuno en función del número de sujetos obligados afectados, del tipo de incidente, sus repercusiones, etc, para facilitar el flujo de información a suministrar por los sujetos obligados y la información a la que es óptimo que accedan los sujetos obligados o para lograr una mejor coordinación en la resolución del incidente y una más pronta y mejor restablecimiento del servicio y operatividad de la infraestructura, suministrará información sobre el incidente, su grado de afectación y medidas paliativas y de resiliencia que se pueden adoptar o se están adoptando por otros agentes o sujetos, preservando la información confidencial y de secreto comercial que compete a cada sujeto obligado.

Capítulo IV recoge en el epígrafe "Comunicaciones de emergencia a través del número de emergencias 112 y alertas públicas"

Recoge los artículos del 19 al 21:

El artículo 19 establece la obligación de los centros de recepción de comunicaciones de emergencia a través del número de emergencias 112 y alertas públicas. Se establece que los centros de recepción de comunicaciones de emergencias tienen la obligación de garantizar la seguridad y el encaminamiento de las llamadas al número de emergencias y alertas públicas. Para ello, adoptarán las medidas técnicas que consideren adecuadas, planes específicos, estrategias, o

redundancia del servicio a través del propio operador que le ofrece el servicio de encaminamiento o a través de otro proveedor.

Estas medidas deben ser presentadas a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales en el plazo máximo de 6 meses desde la entrada en vigor de este Real Decreto y serán actualizados cada 2 años.

El artículo 20 describe la obligación de los sujetos obligados de garantizar el mantenimiento del servicio a los centros de recepción de comunicaciones de emergencias a través del número de emergencias 112 y alertas públicas. Se establece la obligación de los sujetos obligados de presentar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales en el plazo de 6 meses, y actualizado cada dos años, un plan específico que incluya las medidas para garantizar el mantenimiento del servicio y la transmisión de las comunicaciones de emergencia a los centros de recepción de comunicaciones de emergencia incluyendo mecanismos de redundancia u otras alternativas que garanticen la continuidad del servicio. A la vista de las alternativas, la Secretaría de Estado podrá modificar dicho Plan.

El artículo 21 establece la obligación, tanto de los centros de recepción de llamadas de emergencias como de los sujetos obligados, de notificación a la Secretaría de Estado, sin dilación alguna y en el plazo máximo de 1 hora desde que tuvo conocimiento en el supuesto de interrupción del servicio de llamadas de emergencias y sistema de alertas públicas.

La interrupción de este tipo de servicios es un incidente significativo y deben realizarse a la Secretaría de Estado las siguientes notificaciones:

Una notificación inicial, que será remitida por correo electrónico a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, tanto por los centros de recepción de llamadas de emergencias como por parte de los sujetos obligados, en el plazo máximo de 1 hora desde que se tuvo conocimiento del incidente. En cuanto al contenido, la notificación inicial incluirá, al menos, información sobre el momento exacto del inicio del incidente, una breve descripción de la causa que ha originado ese incidente, el área geográfica afectada, número de líneas estimadas afectadas, medidas de contingencia adoptadas durante la primera horas que el servicio de llamadas de emergencias y/o alertas públicas se ha visto interrumpido, planes previstos para la recuperación del servicio afectado, duración estimada de la incidencia y persona de contacto y canales de comunicaciones utilizados para informar tanto a los usuarios como a la administración y cualquier otra información de relevancia.

Si transcurrida 1 hora desde la notificación inicial no se hubiera reestablecido el servicio de llamadas de emergencias, tanto los centros de recepción de llamadas como los sujetos obligados remitirán cada hora, por medio de correo electrónico a la Secretaría de Estado de Telecomunicaciones, todas las notificaciones intermedias que fueran necesarias para actualizar la información hasta la notificación final. En cuanto al contenido, se proporcionará con más detalle la información reportada en la notificación inicial sobre la incidencia y las infraestructuras digitales afectadas, impacto de la avería, si hay otros operadores

afectados, actualización del número de líneas afectadas, un análisis preliminar de la causa de la avería, si la causa es interna o externa y detalle sobre la causa, si se debe a fallo en los sistemas, congestión de red, errores humanos, acciones maliciosas, fenómenos naturales, fallo de terceras partes como puede ser suministro eléctrico, robo de cable, terremotos o inundaciones, así como cualquier información adicional que pueda ir reportando el operador.

Por último, tan pronto como se tenga conocimiento del restablecimiento del servicio, los centros de recepción y los sujetos obligados lo notificarán a la Secretaría de Estado. Además, en el plazo máximo de 24 horas desde la notificación de la finalización del suceso, se remitirá una notificación final en la que se indicará, además del momento exacto de la restauración del servicio de llamadas al número de emergencias y/o alertas públicas, una actualización lo más detallada posible de la última información reportada en la notificación inicial o en la notificación intermedia si esta se ha llevado a cabo.

En el plazo máximo de 5 días hábiles desde la notificación de la restauración del servicio de llamadas al número de emergencias, se remitirá a la Secretaría de Estado un informe detallado sobre el incidente.

El apartado 5 contempla que la Secretaría de Estado podrá confeccionar y remitir un formulario específico de notificación durante las notificaciones iniciales, intermedias y finales. También se prevé, en el apartado 6, que tanto los centros de recepción como los sujetos obligados deberán comunicar a la Secretaría de Estado en el plazo de 3 meses desde la aprobación de este Real Decreto, los responsables de las notificaciones que deberá ser actualizado una vez al año.

Capítulo V en el epígrafe "Asunción por la Administración General del Estado de la gestión directa de determinados servicios de comunicaciones electrónicas disponibles al público para garantizar la seguridad pública y la seguridad nacional o el cumplimiento de las obligaciones de servicio público"

Recoge el artículo 22 la asunción por parte de la Administración General del Estado la gestión directa de determinados servicios de comunicaciones electrónicas para garantizar la seguridad pública y la seguridad nacional. Estos acuerdos se adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración Pública competente.

El apartado 6 prevé que los acuerdos de asunción de la gestión directa del servicio deberán ser comunicados por el Gobierno en el plazo de 24 horas al órgano jurisdiccional competente para que, en un plazo de 48 horas, establezca si los mismos son acordes a los derechos fundamentales y libertados públicas procediendo a su anulación en caso negativo.

Capítulo VI en el epígrafe "Supervisión y Cooperación"

Contiene los artículos del 23 al 28.

El artículo 23 hace referencia a la supervisión y ejecución de las obligaciones de seguridad y resiliencia de la red, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales.

La autoridad competente en España para la recepción de las notificaciones a que se refiere el capítulo III de este Real Decreto, la supervisión de las obligaciones de seguridad y resiliencia reguladas y adopción de medidas para garantizar el cumplimiento de las obligaciones recogidas en este Real Decreto corresponde a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales. Se prevé que, en la adopción de estas medidas, la Secretaría de Estado pueda establecer metodologías de supervisión que permitan priorizar con un enfoque basado en el riesgo.

Además, se prevé que, para supervisar el cumplimiento, la Secretaría de Estado podrá requerir a los sujetos obligados que proporcionen toda la información pertinente. También, podrá requerir que realice, a su coste, una auditoría externa sobre el cumplimento de la información. En cualquier caso, las obligaciones serán efectivas, proporcionadas y disuasorias.

En el caso de que las medidas de ejecución adoptadas por la Secretaría de Estado resulten ineficaces, la Secretaría fijará un plazo para subsanar las deficiencias.

El apartado 10 de este artículo contempla que en lo no regulado expresamente en este artículo resultaran de aplicación las medidas de ejecución y supervisión recogidas en la normativa nacional y europea sobre ciberseguridad.

El artículo 24 recoge el procedimiento de cooperación nacional que incluye los organismos competentes en materia de ciberseguridad y la Comisión Nacional de los Mercados y de la Competencia.

El artículo 25 establece el mecanismo de cooperación con las Comunidades Autónomas. Concretamente se prevé que se desarrollarán los mecanismos de colaboración mutua para que, tanto la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales como las Comunidades Autónomas, puedan ejercer las funciones y competencias asignadas por el ordenamiento jurídico para coordinarse de la mejor manera posible en el desempeño de estas competencias que coadyuve a la consecución del objetivo común de la más pronta y eficaz resolución de los incidentes y el más rápido y pleno restablecimiento de la seguridad de las redes, la continuidad de los servicios y la operatividad de las infraestructuras a las que se refiere este real decreto.

En particular, se prevé que la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales desarrollará los cauces de transmisión de información oportunos para que las Comunidades Autónomas dispongan de información en el menor tiempo posible de los incidentes significativos que afecten a las redes y servicios de comunicaciones electrónicas y determinadas infraestructuras digitales, y en concreto, respecto de aquellas redes, servicios e infraestructuras con implantación en su territorio. También se prevé que desarrollará los mecanismos de colaboración oportunos para que las Comunidades Autónomas puedan contribuir en la fijación de los objetivos, prácticas e instrumentos que se diseñen para

conseguir el objetivo de reforzar la seguridad y resiliencia de las redes públicas y servicios de comunicaciones electrónicas disponibles al público y de las infraestructuras digitales que contribuyen a su funcionamiento y prestación.

El artículo 26 por su parte recoge el procedimiento de cooperación en el ámbito de la Unión Europea.

El artículo 27 recoge el procedimiento de cooperación en lo relativo a los incidentes que afecten a datos personales y, el artículo 28 establece el procedimiento de autorización para la cesión de datos personales.

Capítulo VII en el epígrafe "Inspección y régimen sancionador en materia de seguridad y continuidad de las redes y servicios de comunicaciones electrónicas e infraestructuras digitales"

Contiene los artículos del 29 al 37.

El artículo 29, con respecto a la función de inspección, establece que ésta corresponde a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Por su parte, el artículo 30 hace referencia a la facultad de inspección. Concretamente establece que los servicios de inspección de la Secretaría de Estado de Telecomunicaciones podrán realizar las inspecciones que consideren necesarias al objeto de verificar el cumplimiento de las obligaciones establecidas en este Real Decreto. Para ello, podrán recabar todos los datos adicionales que consideren necesarios, así como realizar sus propias medidas y comprobaciones en la red y en las aplicaciones informáticas de los operadores.

Se prevé que los sujetos obligados tendrán la obligación de someterse a las inspecciones que efectúe el personal de inspección y que la negativa u obstrucción para comparecer a los actos de inspección, la realización de las pruebas técnicas, o facilitar la información o documentación requerida será sancionada como obstrucción a la labor inspectora.

El artículo 31 hace referencia a la responsabilidad administrativa por las infracciones de los preceptos contenidos en este Real Decreto que será exigible a la persona física o jurídica que desarrolle la actividad.

El artículo 32 prevé que la infracción de cualquiera de las obligaciones recogidos en este Real Decreto será considerada como grave conforme al artículo 107.22 de la Ley General de Telecomunicaciones cuya sanción, conforme al artículo 33, será multa por importe de hasta dos millones de euros, de conformidad con el artículo 109 de la Ley General de Telecomunicaciones. Además de la sanción, cuando se trate de una persona jurídica, se podrá imponer una multa de hasta 30.000 euros a sus representantes legales o a las personas que integran los órganos directivos o los órganos colegiados de administración que hayan intervenido en el acuerdo o decisión. Quedarán excluidas de la sanción aquellas personas que, formando parte de órganos directivos o de los órganos colegiados de administración, no hubieran asistido a las reuniones o hubieran votado en contra o salvando su voto.

El artículo 33 también prevé que tendrá la consideración de incumplimiento reiterado la sanción firme en vía administrativa por la comisión de dos o más infracciones del mismo tipo infractor en un período de tres años.

El artículo 34 hace referencia a los criterios para la determinación de la cuantía de la sanción en el que, además de delimitar estos criterios, establece que en el caso de la infracción consistente en proporcionar información engañosa, errónea o incompleta a sabiendas o con negligencia grave para la elaboración de los informes previstos en el Real Decreto, en la fijación de la cuantía de la sanción se tendrá en cuenta además el perjuicio causado a la competencia, a los usuarios o a la Administración pública.

El artículo 35 incluye la posibilidad de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales de adoptar medidas cautelares si el incumplimiento de las obligaciones está perjudicando la integridad de la red o afectando a la continuidad de los servicios de comunicaciones electrónicas.

En cuanto a la prescripción, el artículo 36 recoge que las infracciones graves prescribirán a los dos años de conformidad con el artículo 113 de la Ley General de Telecomunicaciones. El plazo de prescripción comenzará a computarse desde el día en que se hubieran cometido y será interrumpida la prescripción con la iniciación, con conocimiento del interesado, del procedimiento sancionador. Se recoge también que el plazo de prescripción volverá a correr si el expediente sancionador estuviera paralizado durante más de un mes por causa no imputable al presunto responsable.

En el supuesto de infracción continuada, la fecha inicial del cómputo será aquella en que deje de realizarse la actividad infractora o la del último acto con que la infracción se consume. No obstante, se entenderá que persiste la infracción en tanto los equipos de telecomunicación o instalaciones objeto del expediente no se encuentren a disposición de la Administración o quede constancia fehaciente de su imposibilidad de uso.

De igual forma, se recoge que las sanciones impuestas por faltas graves prescribirán a los dos años. El plazo de prescripción de las sanciones comenzará a computarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a correr el plazo si aquél está paralizado durante más de un mes por causa no imputable al infractor.

La competencia sancionadora, de conformidad con el artículo 37, corresponde a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales de conformidad con el artículo 114 de la Ley General de Telecomunicaciones.

Disposiciones Adicionales

Contiene dos Disposiciones Adicionales:

Disposición Adicional Primera: Establece la coordinación de este Real Decreto con la normativa relativa a la coordinación y Gobernanza de ciberseguridad y sobre la resiliencia de las entidades críticas.

Concretamente se establece que este Real Decreto resultará de aplicación incidentes significativos descritos en el artículo 11 de este Real Decreto. Al resto de incidentes de seguridad les resultará de aplicación la normativa nacional o europea relativas a la coordinación y gobernanza de ciberseguridad y sobre la resiliencia de las entidades críticas.

Sin perjuicio de lo anterior, se prevé que a los sujetos obligados en este Real Decreto también le resultará de aplicación la normativa nacional o europea relativas a la coordinación y gobernanza de ciberseguridad y sobre la resiliencia de las entidades críticas en lo no previsto ni regulado en el presente Real Decreto.

Disposición adicional segunda. Mesa de coordinación de seguridad y resiliencia de redes y servicios de comunicaciones electrónicas.

Esta Disposición adicional segunda regula la mesa de coordinación de seguridad y resiliencia con el fin de facilitar la colaboración, coordinación, cooperación, el intercambio de información y la participación de todos los agentes involucrados en la seguridad y resiliencia de las redes y servicios de comunicaciones electrónicas, así como de contribuir a la mejora continua de la capacidad de respuesta ante incidentes significativos, se crea la Mesa de coordinación de seguridad y resiliencia de redes y servicios de comunicaciones electrónicas.

La Mesa actuará como órgano de cooperación estratégica y técnica, foro de diálogo y consulta, y espacio para la elaboración de propuestas, recomendaciones y buenas prácticas en materia de seguridad y resiliencia, sin asumir funciones de coordinación operativa directa en la gestión de incidentes.

Esta Mesa, está integrada por representantes del Ministerio para la Transformación Digital y de la Función Pública, del Ministerio del Interior, del Ministerio de Defensa, del Departamento de Seguridad Nacional, de las Comunidades Autónomas, de la Federación Española de Municipios y Provincias, de la Comisión Nacional de los Mercados y de la Competencia, de las asociaciones más representativas de operadores de comunicaciones electrónicas, de infraestructuras digitales, de fabricantes de equipos de telecomunicaciones y de consumidores y usuarios. La determinación concreta de su composición se efectuará mediante orden de la persona titular del Ministerio para la Transformación Digital y de la Función Pública.

Se prevé que la Mesa de coordinación de seguridad y resiliencia de redes y servicios de comunicaciones electrónicas aprobará su reglamento de organización y funcionamiento y podrá proponer la realización de pruebas, simulacros y ejercicios prácticos con la finalidad de verificar el funcionamiento de las medidas y obligaciones establecidas sobre la seguridad y resiliencia de redes y servicios de comunicaciones electrónicas, extraer conclusiones sobre la puesta en práctica de estas actuaciones y proponer fórmulas de mejora sobre la seguridad y resiliencia de estas redes y servicios.

Disposición derogatoria

Contiene una disposición derogatoria que suprime el capítulo IV de la Orden IET/1990/2014, de 16 de junio, por la que se regulan las condiciones relativas a la calidad del servicio en la prestación de los servicios de telecomunicaciones, relativo a los sucesos que lleven una degradación importante en la calidad de los servicios, así como las disposiciones de igual o inferior rango a este Real Decreto que se oponga a lo dispuesto en ella.

Disposiciones finales

Contiene tres disposiciones finales que recogen el título competencial, el desarrollo reglamentario y aplicación, así como la entrada en vigor que, según se establece en la Disposición final tercera, será al día siguiente al de su publicación en el "Boletín Oficial del Estado".

II.2.- ANÁLISIS JURÍDICO

Congruencia con el ordenamiento jurídico nacional

El presente Real Decreto se ajusta al ordenamiento jurídico nacional, al desarrollar el contenido del artículo 63 de la Ley General de Telecomunicaciones. Parte de dicho contenido, en particular el procedimiento de notificación de incidentes de seguridad ha sido regulado hasta ahora por la denominada Orden de Calidad, cuyo contenido se integra y actualiza en este Real Decreto, con el fin de dotarlo de mayor coherencia, sistematicidad y eficacia normativa.

Asimismo, el Real Decreto guarda plena congruencia con el Real Decreto-ley 7/2022, de 29 de marzo, por el que se establecen los requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, así como con el Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G.

En coherencia y coordinación con la Directiva NIS2 y CER, en la actualidad se considera congruente con la normativa nacional la aprobación de este Real Decreto que establezca, para un sector determinado como el que nos ocupa, determinadas obligaciones específicas, para garantizar la seguridad y resiliencia de las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales.

Congruencia con el derecho de la unión europea

Este Real Decreto es coherente con la Directiva NIS2 y la Directiva CER que establecen un marco regulatorio de carácter general y transversal, aplicable a todos los sectores, orientado a reforzar la resiliencia y la respuesta ante incidentes de seguridad. Estas Directivas regulan de forma complementaria la gestión de incidentes de seguridad que afectan a sectores esenciales y servicios críticos, estableciendo obligaciones específicas para reforzar la resiliencia operativa y la ciberseguridad en la Unión Europea.

Desde una perspectiva jurídica, la Directiva NIS2 establece un marco normativo común para lograr un elevado nivel de ciberseguridad en la Unión Europea, imponiendo a los Estados miembros y a las entidades públicas y privadas de sectores esenciales y críticos la obligación de adoptar medidas técnicas, operativas y organizativas para gestionar los riesgos de ciberseguridad. En particular, regula la notificación obligatoria de incidentes significativos, la gestión de riesgos, la supervisión por parte de autoridades competentes y el intercambio de información sobre amenazas.

Por su parte, la Directiva CER se centra en la resiliencia de las entidades críticas frente a una amplia gama de riesgos, incluidos los de origen natural, humano o tecnológico, y establece requisitos para la identificación de entidades críticas, la evaluación de riesgos, la planificación de la continuidad operativa y la notificación de incidentes que afecten gravemente a la prestación de servicios esenciales.

También guarda coherencia con los artículos 40 y 41 de la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se aprueba el Código Europeo de las Comunicaciones Electrónicas. Estos artículos regulan la seguridad de las redes y servicios, y la gestión de los riesgos relacionados con la ciberseguridad y la resiliencia operativa, si bien han sido modificados por la Directiva NIS2 que refuerza las obligaciones en materia de ciberseguridad y coordinación entre Estados miembros.

En cuanto a la seguridad de las redes y servicio, se establece que los Estados miembros deben garantizar que los proveedores de redes públicas y servicios de comunicaciones electrónicas adopten medidas técnicas y organizativas adecuadas para gestionar los riesgos que afecten a la seguridad de las redes y servicios. Estas medidas deben asegurar un nivel de seguridad adecuado al riesgo existente, especialmente en relación con:

- ✓ La prevención de accesos no autorizados.
- ✓ La protección de la integridad y disponibilidad de las redes.
- ✓ La notificación de incidentes de seguridad significativos a las autoridades nacionales competentes.

Además, se contempla la posibilidad de que las autoridades nacionales de reglamentación impongan requisitos adicionales en función de la evolución tecnológica y la naturaleza de los riesgos.

En cuanto a la gestión de riesgos y notificación de incidentes, el artículo 41 complementa al artículo 40 estableciendo que obligaciones específicas de notificación de incidentes de seguridad. En particular:

- ✓ Los proveedores deben informar sin demora indebida a la autoridad competente sobre cualquier incidente que tenga un impacto significativo en la prestación de servicios.
- ✓ Las autoridades pueden informar al público si lo consideran necesario para prevenir o mitigar los efectos del incidente.

- ✓ Se prevé la cooperación entre autoridades nacionales y europeas para compartir información sobre amenazas y vulnerabilidades.

Sin embargo, este Real Decreto viene más allá y se circunscribe al ámbito de las redes y servicios de comunicaciones electrónicas, así como a determinadas infraestructuras digitales, adoptando medidas concretas y operativas que permiten una aplicación directa y especializada de los principios generales establecidos por las mencionadas directivas europeas, atendiendo a las particularidades técnicas y funcionales del sector de las telecomunicaciones y servicios digitales.

Vigencia de la norma y entrada en vigor

El presente Real Decreto entrará en vigor el día siguiente a su publicación en el Boletín Oficial del Estado.

Conforme al artículo 2.1 del Código Civil, las normas entran en vigor a los veinte días de su completa publicación en el Boletín Oficial del Estado, salvo que en ellas se disponga otra cosa. En este sentido, el Real Decreto puede establecer válidamente en su disposición final que su entrada en vigor se produzca al día siguiente de su publicación, haciendo uso de la habilitación legal para fijar un plazo distinto.

En el caso que nos ocupa, esta anticipación en la vigencia responde a la necesidad de aplicar de forma inmediata medidas urgentes ante una inminente eventualidad que requiera una rápida implementación, especialmente cuando el contenido del Real Decreto desarrolla medidas de seguridad ante posibles incidentes significativos de seguridad que supongan la interrupción del servicio o una importante degradación en la calidad de estos como los que nos han sucedido en los últimos años. Por tanto, la entrada en vigor al día siguiente de su publicación se ajusta plenamente al ordenamiento jurídico español y garantiza la eficacia normativa en caso de producirse un incidente de seguridad de forma inmediata que requieren que las obligaciones se encuentren vigente lo antes posible.

III.- DESCRIPCIÓN DE LA TRAMITACIÓN REALIZADA

III.1.- CONSULTA PÚBLICA PREVIA A LOS INTERESADOS

Inicio de la tramitación

El pasado 11 de septiembre de 2025, la Secretaría de estado de Telecomunicaciones e Infraestructuras Digitales publicó la consulta pública previa relativa al futuro Real Decreto sobre seguridad y resiliencia de infraestructuras digitales, con el objetivo de recabar aportaciones de operadores, ciudadanos y demás partes interesadas. El plazo para la presentación de alegaciones finalizó el 26 de septiembre de 2025. Esta iniciativa se enmarca en lo previsto en el artículo

133.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Alegaciones realizadas por parte de los interesados.

- **Sobre la necesidad y oportunidad de la norma:**

Se han manifestado posiciones divergentes con respecto a la necesidad y oportunidad de la norma. Una posición considera que las redes han demostrado una elevada capacidad de respuesta ante crisis recientes, por lo que cualquier nueva obligación debe estar debidamente justificada, ser técnicamente viable y ajustarse al principio de proporcionalidad, mientras que otra posición valora positivamente la propuesta, destacando la necesidad de reforzar la resiliencia en contextos críticos y la complementariedad tecnológica.

- **Coordinación normativa y seguridad jurídica:**

Existe consenso generalizado sobre la necesidad de asegurar la coherencia normativa. Se solicita una alineación con las Directivas europeas NIS2 y CER, que evite duplicidades normativas, solapamientos y contradicciones con la normativa que se apruebe como desarrollo del artículo 63 de la Ley General de Telecomunicaciones. Alguna parte propone que cualquier desarrollo se articule como *"guidelines*" o recomendaciones y no como imposición normativa directa.

- **Autonomía energética y continuidad operativa**

La mayoría de los operadores coinciden en rechazar obligaciones generalizadas sobre autonomía eléctrica al señalar limitaciones técnicas, económicas y logísticas, especialmente en emplazamientos rurales o externos. Sin embargo, otra parte de los alegantes apoyan el refuerzo de la autonomía energética en centros críticos, siempre que se habiliten mecanismos de financiación pública y se garantice el acceso prioritario a suministros esenciales en emergencias.

- **Planes de resiliencia y sostenibilidad financiera**

Una parte de los operadores defienden los planes ya implantados como eficaces y sostenibles, solicitando que la norma los reconozca y evite duplicidades administrativas. Se reclama que cualquier evolución normativa se articule como recomendación técnica y que se habiliten ayudas públicas, especialmente en zonas de baja rentabilidad.

- **Notificación de incidentes:**

Existe una posición ampliamente compartida sobre la necesidad de mantener el marco actual conservando los plazos y umbrales establecidos en la Orden de Calidad. Se propone incorporar una nueva categoría de "otros sucesos de relevancia" y evolucionar hacia un entorno digital controlado (online) que permita el análisis automático por parte de la administración.

- **Inclusión y accesibilidad**

Un alegante solicita que la norma incorpore un enfoque inclusivo, reconociendo la criticidad diferencial de los servicios para personas con discapacidad. Se propone que la información durante crisis sea universalmente accesible y que se prioricen las conexiones vitales en los planes de restauración.

- **Colaboración institucional y gobernanza compartida:**

Una parte de los alegantes apoyan la creación de una" mesa de emergencias" coordinada por la administración, con participación de operadores, proveedores, cuerpos de seguridad y autoridades locales. Se reclama una coordinación multinivel (autonómica, nacional, europea) y la creación de un repositorio común de información.

- **Sujetos obligados y cadena de valor digital**

Se solicita ampliar el ámbito de aplicación de la norma a otros agentes relevantes del ecosistema digital, como proveedores OTT, redes sociales, plataformas de nube e inteligencia artificial. Se propone definir obligaciones específicas para estos agentes, como protocolos de recuperación y notificación de caídas de SLAs críticos.

- **Diversidad tecnológica y soluciones híbridas**

Algunas empresas defienden el papel estratégico del satélite y la radiodifusión como tecnologías complementarias, especialmente en situaciones de emergencia. Se reclama el reconocimiento normativo de soluciones híbridas (terrestre + satelital) y la creación de puntos de conectividad de emergencia en instituciones públicas.

- **Seguridad física y protección frente a vandalismo**

Se solicita también el endurecimiento de la legislación penal frente al robo de cobre y actos vandálicos que afecten a infraestructuras críticas. También se propone garantizar salvoconductos, acceso a combustible, apoyo policial y agilidad en licencias durante situaciones de emergencia.

III. 2. TRÁMITE DE AUDIENCIA E INFORMACIÓN PÚBLICA

De conformidad con el artículo 26.6 de la Ley 50/1997, de 27 de noviembre del Gobierno, deberá llevarse a cabo el trámite de audiencia e información pública.

III.3. INFORMES RECABADOS

Se han de recabar los siguientes informes en el procedimiento de tramitación:

- Informe de la Comisión Nacional de los Mercados y la Competencia, de conformidad con lo establecido en el artículo 5.2.a) de la Ley 3/2013, de 4

de junio, de creación de la Comisión Nacional de los Mercados y la Competencia.

- Informe de la Secretaría General Técnica del Ministerio para la Transformación Digital y de la Función Pública, conforme a lo dispuesto en el artículo 26.5, párrafo cuarto, de la Ley 50/1997, de 27 de noviembre, del Gobierno.

- Informes del Ministerio de Interior, Ministerio de Defensa, Ministerio de Hacienda, Ministerio de Política Territorial y Memoria Democrática y Departamento de Seguridad Nacional de la Presidencia del Gobierno conforme a lo dispuesto en el artículo 26.5, párrafo primero, de la Ley 50/1997, de 27 de noviembre, del Gobierno.

- Informe competencial del Ministerio de Política Territorial y Memoria Democrática conforme a lo dispuesto en el artículo 26.5, párrafo sexto, de la Ley 50/1997, de 27 de noviembre, del Gobierno.

- Informe de la Oficina de Coordinación y Calidad Normativa del Ministerio de Presidencia, Justicia y Relaciones con las Cortes, en virtud de lo establecido en el artículo 26.9 de la Ley 50/1997, de 27 de noviembre, del Gobierno,

- Dictamen del Consejo de Estado conforme a lo previsto en los artículos 19.1 y 22.3 de la Ley Orgánica 3/1980, de 22 de abril, del Consejo de Estado.

IV.- ADECUACIÓN DE LA NORMA AL ORDEN DE DISTRIBUCIÓN DE COMPETENCIAS

El presente Real Decreto se dicta al amparo de lo dispuesto en el artículo 149.1.21.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de telecomunicaciones.

Esta habilitación constitucional permite al Estado establecer la regulación básica y la coordinación general de la actividad económica en este ámbito, garantizando la unidad de mercado y la homogeneidad normativa en todo el territorio nacional.

En consecuencia, las disposiciones contenidas en esta norma se enmarcan en el ejercicio legítimo de dicha competencia exclusiva, resultando necesarias para asegurar el funcionamiento eficaz, seguro y armonizado de las redes y servicios de comunicaciones electrónicas, así como de las infraestructuras digitales estratégicas.

V.- ANÁLISIS DE IMPACTOS

1. Impacto económico y presupuestario.
2. Impacto en la unidad de mercado y competencia
3. Análisis de las cargas administrativas.
4. Impacto por razón de género.
5. Impacto en la infancia y en la adolescencia.
6. Impacto en la familia.
7. Impacto en materia de medioambiente y por razón de cambio climático.
8. Impacto por razón de materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.
9. Impacto en salud.
10. Impacto en materia de protección de datos.

V.1. Impacto económico y presupuestario

Este Real Decreto supone un impacto económico y presupuestario adicional al actual de los sujetos obligados puesto que los costes en los que podrían incurrir por la elaboración de planes – generales y específicos - y, en especial, por la obligación introducida en el artículo 7.4 de este Real Decreto, relativa a que en situaciones de interrupción del suministro eléctrico, el sujeto obligado deberá mantener el suministro eléctrico en las infraestructuras que haya declarado como de primer nivel al menos durante 24 horas, las de nivel intermedio al menos durante 12 horas mientras que el resto de instalaciones durante al menos 4 horas.

En el caso concreto de la red de acceso dentro de una red de comunicaciones móviles a través de la cual se proveen servicios de comunicaciones electrónicas disponibles al público en bandas armonizadas europeas, la red de acceso debe estar diseñada y dotada de los equipos electrógenos y elementos de suministro eléctrico propios que permite garantizar su operatividad y continuidad de servicio durante al menos 4 horas para el 85% de la población en España. Se prevé que para ello el operador podrá utilizar todas las estaciones base, ya sean fijas o portátiles, bandas de frecuencias y tecnologías que estime oportuno, así como podrá priorizar todas aquellas ubicaciones, centros e instalaciones que considere conveniente en función a su vinculación a la prestación de servicios públicos y servicios de relevancia económica y social.

Se ha llevado a cabo un análisis sobre el impacto económico que esta obligación podría suponer para los operadores de telecomunicaciones según la información y datos proporcionados por los operadores y analizando las referencias nacionales e internacionales (BEREC, GSMA, Ofcom, FCC).

Según el análisis realizado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, el coste vinculado al despliegue adicional de baterías o equipos electrógenos para el conjunto de las redes de comunicaciones móviles a través de las cuales se proveen servicios de comunicaciones electrónicas disponibles al público en bandas armonizadas europeas, en España es de una horquilla entre 50.960.000€ y 72.800.000€, teniendo en cuenta que:

- el total de los emplazamientos a cubrir (85% cobertura poblacional) es de 10.400,
- se puede estimar que en torno a un 30% de los emplazamientos ya disponen de baterías o equipos electrógenos con capacidad para garantizar el suministro eléctrico durante 4 horas, de manera que el número total de emplazamientos podría situarse en la cifra de 7.280.
- el coste unitario por emplazamiento o site, aplicando un 30% de descuento por volumen, el coste por site es de 7.000€.

Se procede a continuación a analizar el coste señalado:

Emplazamientos móviles y cobertura poblacional

En su "Informe Económico-Sectorial 2023", publicado el 2 de julio de 2024, la CNMC menciona que: "*Se han declarado un total de 41.892 emplazamientos en 2023 en los que los operadores de telecomunicaciones tenían instaladas 200.624 estaciones base, promediando entre 4 y 5 estaciones base por emplazamiento*."

Esto es, existen al menos 42.000 emplazamientos (con al menos una BTS móvil) potenciales candidatos a ser actualizados con baterías o equipos electrógenos que permitan la continuidad del suministro eléctrico durante al menos 4 horas.

Por otro lado, la población de España (oct-2025) era de 49 millones de habitantes (INE). El objetivo es dar cobertura a un mínimo del 85% de la población). Eso equivale a ≈ 41,6 millones de personas.

- El promedio país en población/sites es = 49 M / 42.000 ≈ 1.167 personas por site (incluye rural y small cells). Sin embargo, esta "densidad media" en el país es el resultado de zonas con densidades muy diferentes.

- En áreas densas un site de capa de cobertura (700/800 MHz) suele servir significativamente más población que la media (capas solapadas y mayor densidad de usuarios), de modo que para alcanzar 85 % de población con selección "óptima" de sites en zonas densas, el número de sites es muy inferior a 0,85×41.892.

  A este respecto:
  a. En España, ≈ 82 % de la población es urbana (2024) [1].
  b. Las grandes áreas urbanas (>50 k hab.) concentran ≈ 69 % de la población y >77 % del empleo; además, el 40,2 % vive en municipios >100 k. Esto permite "cubrir mucho" con relativamente pocos sites bien elegidos.

- Para dimensionar el mínimo de emplazamientos necesarios que aseguren cobertura al 85 % de la población, se adopta un parámetro de **4.000 personas por site**. Esta hipótesis se apoya en

[1] https://data.worldbank.org/indicator/SP.URB.TOTL.IN.ZS?end=2024&locations=ES&start=1960

(i) la fuerte **concentración urbana** de España (≈ 82 % urbana; 69 % en grandes áreas urbanas),
(ii) **densidades municipales** que superan con holgura 4–5 k hab/km² en núcleos y anillos periurbanos, y
(iii) **inter-site distances** (distancia media entre emplazamientos) de **0,6–1,0 km** en capas de **cobertura <1 GHz**, documentadas en referencias 3GPP/ETSI/Ofcom[2]. En tales condiciones, el área efectiva por *site* (≈ 0,866·ISD²) multiplicada por las densidades habituales arroja **PSS ≥ 4.000**, por lo que el valor resulta **prudente y proporcional** para un escenario de selección priorizada de *sites*

En definitiva, el número mínimo de emplazamientos para proporcionar cobertura durante al menos 4 horas a al menos el 85% de la población sería es de 41,6 M / 4.000 ≈ 10.400 emplazamientos.

Descuentos por volumen

Por otro lado, en la referencia de 10.000 €/site hay que considerar las economías de escala que se verían involucradas en un despliegue adicional: en operaciones nacionales con coberturas del 70–90 %, es estándar negociar contratos marco multianuales con "tier-pricing" por volumen (≥1.000/≥5.000/≥10.000 unidades), estandarizar ingeniería e instalación y optimizar logística y compras conjuntas (en este caso baterías + rectificadores), lo que reduce de forma estructural el coste unitario.

A efectos de estimación, se adopta una hipótesis de **descuento medio del 30 % sobre el coste unitario de referencia (10.000 €/site)** cuando la adquisición de soluciones de respaldo energético se articule como compra agregada mediante acuerdos marco y lotes escalonados entre operadores.

Este supuesto se apoya en:

- evidencia empírica de compras agregadas en el sector público europeo/UK con ahorros de hasta el 30 % y superiores en categorías estandarizadas, [3]
- un entorno de mercado de baterías con caídas de precio cercanas al 20 % interanual por economías de escala y competencia de proveedores, y
- la generalización de esquemas de precios escalonados (tiered/volume pricing) del 20-30 % en contratos B2B de gran volumen. Aun cuando las economías de escala "de ingeniería" puedan estar condicionadas por restricciones de ciertos emplazamientos, ello no impide capturar descuentos comerciales relevantes sobre el suministro bajo un acuerdo marco bien diseñado[4]

[2] https://www.etsi.org/deliver/etsi_tr/138900_138999/138901/18.00.00_60/tr_138901v180000p.pdf
[3] https://wires.onlinelibrary.wiley.com/doi/full/10.1002/wene.463
[4] https://hbr.org/2020/10/what-b2b-companies-get-wrong-about-volume-discounts

Infraestructuras existentes

Se puede estimar que en torno a un 30% de los emplazamientos ya disponen de baterías o equipos electrógenos con capacidad para garantizar el suministro eléctrico durante 4 horas, de manera que el número total de emplazamientos podría situarse en la cifra de 7.280.

Se considera que el coste aproximado de una horquilla entre 51 M€ y 73 M€ en el que incurrirían conjuntamente los operadores de comunicaciones móviles para que el 85% de la población disponga de la continuidad del servicio, entre ellos del servicio de llamadas al número de emergencias, durante al menos 4 horas es proporcional y equilibrado para el fin que se pretende conseguir de evitar la interrupción de los servicios de comunicaciones electrónicas en situaciones de emergencia.

Para la Administración, el impacto presupuestario directo es nulo: las funciones de supervisión, coordinación y respuesta pueden apoyarse en estructuras ya existentes, si bien conviene prever costes marginales en herramientas de gestión de incidentes, elaboración de guías técnicas y campañas de verificación/auditoría. No se prevén compromisos de gasto público salvo que se articule un programa de cofinanciación o ayudas; en ese caso, el impacto presupuestario sería el que se determine reglamentariamente en la correspondiente convocatoria.

V.2 Impacto en la Unidad de mercado y en la competencia.

Este Real Decreto es compatible con los principios de unidad de mercado. No introduce barreras injustificadas ni discriminatorias y también aplica criterios objetivos y proporcionales, sin distorsionar la competencia. En primer lugar, las obligaciones impuestas en este Real Decreto aplican a todos los sujetos obligados que vienen recogidos en el artículo 2. Sólo estarían excluidos los operadores de comunicaciones electrónicas cuyos ingresos brutos de explotación anual sea inferior a 50M€ dentro de un mismo grupo empresarial. Por tanto, la exclusión de estos operadores en ningún caso afecta a la competencia.

En cuanto a la obligación recogida en el artículo 7.4 del Real Decreto relativa a que, en situaciones de interrupción del suministro eléctrico, para el caso concreto de la red de acceso dentro de una red de comunicaciones móviles a través de la cual se proveen servicios de comunicaciones electrónicas disponibles al público en bandas armonizadas europeas, la red de acceso debe estar diseñada y dotada de los equipos electrógenos y elementos de suministro eléctrico propios que permite garantizar su operatividad y continuidad de servicio durante al menos 4 horas para el 85% de la población en España, si bien esta obligación afecta a los operadores principales de comunicaciones móviles, especialmente de aquellos que disponen de red propia al estar habilitados para el uso del espectro radioeléctrico, las obligaciones se imponen a dichos operadores por igual sin que en ningún caso afecte a la competencia, siendo además estos operadores los operadores más significativos en el sector de las telecomunicaciones no viéndose afectado por estas obligaciones los operadores más pequeños ni con ingresos más reducidos.

V.3. Análisis de las cargas administrativas.

En cuanto a las cargas administrativas, si bien este Real Decreto incluye modificaciones a las notificaciones de incidentes de seguridad que los sujetos obligaciones tienen que remitir a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, estas cargas administrativas son proporcionales y equilibradas para la necesidad de que tanto la Administración como los Cuerpos de Seguridad del Estado tengan la información completa y en tiempo para poder adoptar las decisiones correctas ante un incidente de seguridad que afecte, entre otras cosas, a la interrupción del servicio o una importante degradación en la calidad del mismo.

V.4 Impacto por razón de género

De conformidad con lo dispuesto en el artículo 26.3.f) de la Ley 50/1997, de 27 de noviembre, y el artículo 19 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, el presente Real Decreto no presenta impactos diferenciados por razón de género en la aplicación de esta norma.

V.5 Impacto en la infancia y en la adolescencia

De acuerdo con lo establecido en el artículo 22 quinquies de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil, se señala que se considera que un determinado texto normativo tenga un impacto positivo sobre la infancia y la adolescencia. Según la descripción anterior, este Real Decreto no tiene impacto en la infancia y en la adolescencia.

V.6 Impacto en la familia.

Este Real Decreto no presenta impacto en materia de familia.

V.7 Impacto en el medioambiente y por razón de cambio climático

El presente Real Decreto no tiene impacto ambiental directo, aunque la aplicación del mismo si puede venir causado por emergencias ambientales derivadas del cambio climático.

V.8 Impacto por razón de materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

El presente Real Decreto no tiene impacto directo por razón de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

No obstante, según lo manifestado en un escrito de alegaciones, este Real decreto puede presentar una brecha de resiliencia para colectivos vulnerables. En este sentido, se reclama que la evaluación del impacto de incidentes no se base solo en criterios cuantitativos (en función del número de usuarios afectados) sino también en la criticidad del servicio para personas con discapacidad (teleasistencia, geolocalización, alarmas).

También consideran que la información que se proporciona durante los incidentes significativos debería ser accesibles. En este sentido, la comunicación de los operadores y autoridades deben ser compatibles con lectores de pantalla, subtituladas, con interpretación en lengua de signos, y lenguaje claro.

V.9 Impacto en salud

Este Real Decreto no tiene impacto directo en materia de salud, aunque el incumplimiento de las obligaciones que se establecen en este Real Decreto para el encaminamiento y recepción de llamadas de emergencias y alertas públicas puede poner en riesgo la salud y la vida de las personas.

V.10 Impacto en materia de protección de datos.

El presente Real Decreto no tiene impacto directo en materia de protección de datos, aunque prevé en sus artículos 24 y 25 la cooperación en lo relativo a los incidentes que afecten a datos personales y la autorización para la cesión de datos personales en el caso de que se considere necesario.