PROYECTO DE REAL DECRETO SOBRE SEGURIDAD Y RESILIENCIA DE LAS REDES Y SERVICIOS DE COMUNICACIONES ELECTRÓNICAS Y DETERMINADAS INFRAESTRUCTURAS DIGITALES

I

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. 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, ciertas 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.

II

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, los 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 los artículos 27 y 28 de este Real Decreto.

III

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.

En particular, respecto al principio de necesidad, esta norma aborda la necesidad de adoptar determinadas medidas que dotan de mayor seguridad e integridad de las redes de telecomunicaciones, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales de conformidad con el artículo 63 de la Ley General de Telecomunicaciones de manera coherente y coordinada con la normativa nacional y europea sobre ciberseguridad. En este sentido, se considera necesario establecer un marco jurídico actualizado que incluya las obligaciones de los sujetos obligados de disponer de un plan de seguridad por operador y por servicios y por tipología de incidentes, que identifique las medidas adoptadas de prevención, detección y respuesta ante incidentes y riesgos de seguridad en caso de que se produzca un acontecimiento como los acaecidos estos últimos años, sean naturales o no, con el fin de lograr el restablecimiento de los servicios lo antes posible. Para ello, se considera también necesario regular de forma detallada el procedimiento de información claro y ordenado sobre las notificaciones que los sujetos obligados deben realizar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales cuando se produce un incidente significativo que afecta a la integridad de las redes, determinadas infraestructuras digitales y a la continuidad de los servicios de telecomunicaciones, en especial el servicio de llamadas al número de emergencias y alertas públicas, 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. También es necesario establecer un procedimiento de ejecución y coordinación, así como el establecimiento de régimen de inspección y sanción en caso de incumplimiento de las obligaciones establecidas en el presente Real Decreto.

En referencia al principio de proporcionalidad, las condiciones establecidas en esta norma son proporcionales para el fin que se pretende alcanzar consistente en garantizar la seguridad e integridad de las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales. Obtener información sobre los incidentes significativos que afecten a la prestación de los servicios de comunicaciones electrónicas es necesario para que tanto los servicios de emergencia como los responsables políticos puedan adoptar, de la mejor manera posible, las decisiones necesarias para, entre otras cuestiones, salvar vidas y priorizar la gestión de los recursos y los servicios públicos en situaciones de especial criticidad.

Las medidas adoptadas en este Real Decreto cumplen con el principio de seguridad jurídica al estar alineadas y mantener coherencia con la Directiva (UE) 2022/2555, del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2) y con la Directiva (UE) 2022/2557, de 14 de diciembre, relativa a la resiliencia de las entidades críticas (Directiva CER), y en consonancia con el artículo 63 de la Ley General de Telecomunicaciones relativo a la seguridad e integridad de las redes y servicios de comunicaciones electrónicas.

Respecto al principio de transparencia, se han explicitado los motivos que justifican la presente norma habiéndose efectuado el trámite de audiencia e información pública previstas en el artículo 133 de la Ley 39/2015, de 1 de octubre.

Por último, se da cumplimiento al principio de eficiencia, ya que esta norma viene a establecer de manera actualizada y ordenada las notificaciones, en cuanto al contenido y plazo, que los operadores de telecomunicaciones ya 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.

IV

El proyecto ha sido informado por 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.

Este 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.

En su virtud, a propuesta del Ministro para la Transformación Digital y de la Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de ministros en su reunión del día xxxxx,

DISPONGO:

CAPÍTULO I

Disposiciones Generales

Artículo 1. Objeto.

1. Constituye el objeto de este Real Decreto regular las condiciones y actuaciones dirigidas a garantizar la seguridad y resiliencia de las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales en desarrollo de lo establecido en el artículo 63 de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, especialmente ante situaciones y acontecimientos que afecten a la seguridad de las redes, la interrupción del servicio o una importante degradación en las condiciones de prestación.

2. Asimismo, constituye el objeto de este Real Decreto la regulación de los supuestos y requisitos en que los operadores que suministren redes públicas o presten servicios de comunicaciones electrónicas disponibles al público, así como los titulares o gestores de determinadas infraestructuras digitales notifiquen al 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.

3. Se entiende por seguridad de red o servicios, de conformidad con la definición 67 del Anexo II de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, la capacidad de las redes y servicios de comunicaciones electrónicas de resistir, con un determinado nivel de confianza, cualquier acción que comprometa la disponibilidad, autenticidad, integridad y confidencialidad de dichas redes y servicios, de los datos almacenados, procesados o transmitidos y la seguridad de los servicios conexos que dichas redes y servicios de comunicaciones electrónicas ofrecen o hacen accesibles.

Artículo 2. Ámbito de aplicación.

1. Este Real Decreto será de aplicación a los titulares y gestores de redes públicas de comunicaciones electrónicas ubicadas en España, a los prestadores de servicios de

comunicaciones electrónicas disponibles al público que se presten en España, así como al titular o gestor de cualquier recurso asociado que sirva de soporte para el funcionamiento de redes públicas o la prestación de cualquier servicio de comunicaciones electrónicas disponible al público que se ubique o se preste en España.

2. Este Real Decreto también es de aplicación a los titulares o gestores de las infraestructuras digitales que se ubiquen en España, como son, entre otros, las infraestructuras de cable submarino, sistemas de satélites, redes de distribución de contenidos (CDN), centros de procesamientos de datos (CPD) o puntos de intercambio de internet (IXP) y cualquier recurso asociado de estas infraestructuras, cuando contribuyan al funcionamiento de redes públicas de comunicaciones electrónicos o la prestación de servicios de comunicaciones electrónicas disponibles 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.

3. Se consideran sujetos obligados a efectos de este Real Decreto, los titulares y gestores de las redes, servicios de comunicaciones electrónicas e infraestructuras digitales mencionadas en los apartados anteriores que se encuentren incluidos en alguno de los siguientes supuestos:

a) Operadores de comunicaciones electrónicas con un número de usuarios en términos globales dentro de un mismo grupo empresarial en España, de conformidad con el artículo 42 del Código de Comercio, igual o superior a 500.000 usuarios,
b) Operadores de comunicaciones electrónicas con ingresos brutos de explotación anuales superiores a 50 millones de euros dentro de un mismo grupo empresarial, de conformidad con el artículo 42 del Código de Comercio, por el suministro de redes públicas o la prestación de servicios de comunicaciones electrónicas disponibles al público en España. Esta cifra podrá ser actualizada o modificada mediante orden aprobada por la persona titular del Ministerio para la Transformación Digital y de la Función Pública en función de la evolución técnica, económica y competitiva del mercado,
c) Operadores de comunicaciones electrónicas a los que se le hayan impuesto obligaciones específicas como operadores con peso significativo en algún mercado de referencia en virtud de lo establecido en el artículo 18 de la Ley General de Telecomunicaciones,
d) Operadores de comunicaciones electrónicas que sean designados para la prestación del servicio universal de telecomunicaciones o para la prestación

de obligaciones de servicio público en virtud de lo establecido en los artículos 40 y 43 de la Ley General de Telecomunicaciones, respectivamente,

e) Operadores de comunicaciones electrónicas que hayan sido calificados como operadores críticos o sean titulares o gestores de alguna infraestructura crítica declarada en virtud de lo establecido normativa relativa a la protección y resiliencia de entidades críticas,
f) Operadores de comunicaciones electrónicas que provean el servicio de conectividad a los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas,
g) Titulares y gestores de las infraestructuras digitales que contribuyen al funcionamiento de las redes o prestación de servicios de comunicaciones electrónicas de cualesquiera de los sujetos obligados mencionados en los supuestos anteriores.

Habida cuenta del carácter dinámico propio 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, criterios y requisitos podrán ser objeto de modificación mediante Orden aprobada por la persona titular del Ministerio para la Transformación Digital y de la Función Pública.

4. Este Real Decreto no es de aplicación a los titulares y gestores de redes de comunicaciones electrónicas, prestadores de servicios de comunicaciones electrónicas y de infraestructuras digitales vinculados a la Seguridad Nacional y a la Defensa.

5. Lo dispuesto en este Real Decreto se aplicará en coherencia y coordinación con el Sistema de Seguridad Nacional, conforme a la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

En particular, en el caso de producirse un incidente de seguridad en las redes, servicios de comunicaciones electrónicas e infraestructuras digitales que pueda derivar en una situación de interés para la Seguridad Nacional, podrán activarse los instrumentos previstos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

6. Lo dispuesto en este Real Decreto será sin perjuicio de la aplicación de 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.

7. Igualmente, lo dispuesto en este Real Decreto será sin perjuicio de la aplicación de la normativa nacional o europea relativa a la coordinación y gobernanza de la ciberseguridad en lo que respecta a los incidentes específicos de ciberseguridad.

8. Asimismo, lo dispuesto en este Real Decreto será sin perjuicio de la aplicación de la normativa nacional o europea relativa a la protección y resiliencia de entidades críticas.

Artículo 3. Las redes y servicios de comunicaciones electrónicas y determinadas infraestructuras digitales como instalaciones y servicios de carácter esencial en situaciones de emergencia.

1. Las redes públicas de comunicaciones electrónicas, los servicios de comunicaciones electrónicas disponibles al público, así como las infraestructuras digitales que contribuyen al funcionamiento de dichas redes o a la prestación de los mencionados servicios son calificados como instalaciones y servicios de carácter esencial en situaciones de emergencia derivadas de incidentes de seguridad que afecten a la seguridad de las redes, la interrupción del servicio o una importante degradación en las condiciones de prestación.

2. En estas situaciones de emergencia, todas las autoridades públicas, 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.

3. A tal efecto, dichas autoridades y órganos adoptarán las medidas administrativas, técnicas y operativas que resulten necesarias para lograr dicha recuperación y restablecimiento lo antes posible o su necesario mantenimiento.

Entre otras medidas, 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.

Igualmente, dichas autoridades y órganos 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. Entre otras medidas, se podrá 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.

4. Las Fuerzas y Cuerpos de Seguridad del Estado prestarán el auxilio y apoyo que resulte necesario para que el personal y representantes de los operadores y titulares o gestores de infraestructuras digitales y de las empresas contratadas por ellos

puedan desplegar sus actividades y operaciones dirigidas recuperar la seguridad y operatividad de las instalaciones e infraestructuras o facilitar su mantenimiento.

5. 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 conforme a lo indicado en el artículo 7.4, gozarán de prioridad en las actuaciones de restablecimiento del suministro eléctrico.

6. Asimismo, 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

Planificación para garantizar la seguridad y resiliencia de las redes y servicios de comunicaciones electrónicas y de determinadas infraestructuras digitales

Artículo 4. Plan Nacional de seguridad y resiliencia de redes y servicios de comunicaciones electrónicas.

1. Con el objeto de garantizar la seguridad y resiliencia de las redes y servicios de comunicaciones electrónicas y determinadas infraestructuras digitales en España, el Ministerio para la Transformación Digital y de la Función Pública, aprobará, por medio de Orden Ministerial, un Plan Nacional de Seguridad y Resiliencia de Redes y Servicios de Comunicaciones Electrónicas.

2. Este Plan Nacional de Seguridad y Resiliencia, desarrollará y coordinará un plan de respuesta y restablecimiento a incidentes de seguridad en el que se fijarán los objetivos y las medidas de la gestión de cada tipología de incidentes.

Dicho Plan incluirá en todo caso:

a) Los objetivos de las medidas y obligaciones recogidas en el Plan Nacional de Seguridad y Resiliencia de Redes y Servicios de Comunicaciones Electrónicas.
b) Las funciones y responsabilidades asignadas a las diferentes autoridades con competencia en materia de incidentes de seguridad en las redes y servicios de comunicaciones electrónicas y determinadas infraestructuras digitales, teniendo en cuenta, entre otros factores, en función de que sean infraestructuras críticas o incidentes de ciberseguridad.
c) Los procedimientos de gestión de la crisis provocada por un incidente de seguridad de las redes o servicios de comunicaciones electrónicas y canales

para el intercambio de información tanto entre los sujetos obligados con la Administración o entre Administraciones.

d) Medidas de anticipación y preparación que deben incluir, entre las que se incluyen, actividades de formación.
e) Los sujetos obligados, así como las infraestructuras implicadas.
f) Los procedimientos y mecanismos para garantizar la participación y apoyo de España en la gestión coordinada de incidentes de seguridad de redes y servicios de comunicaciones electrónicas a gran escala a nivel de la Unión Europea.

3. El Plan Nacional de Seguridad y Resiliencia de Redes y Servicios de Comunicaciones Electrónicas, deberá contemplar procedimientos y mecanismos para la gestión de crisis que incluyan las fases de prevención, detección, respuesta, retorno a la normalidad y evaluación, asegurando su integración y coherencia con los planes y estrategias del Sistema de Seguridad Nacional.

4. El Plan Nacional de Seguridad y Resiliencia deberá ser elaborado en el plazo de un año a contar desde la entrada en vigor de este Real Decreto, y deberá ser actualizado cada 3 años, con el objetivo de adaptarse a las nuevas necesidades en función de la evolución tecnológica.

Artículo 5. Obligación de gestión adecuada de los riesgos de seguridad.

1. Con objeto de garantizar la seguridad y resiliencia de las redes, servicios de comunicaciones electrónicas y determinadas infraestructuras digitales, los sujetos obligados gestionarán adecuadamente los riesgos de seguridad que puedan afectar a sus redes o servicios de comunicaciones electrónicas que prestan y determinadas infraestructuras digitales, tratando de evitar o reducir al mínimo el impacto de los incidentes de seguridad, tanto en los usuarios como en otras redes, servicios e infraestructuras digitales, para lo cual adoptarán las medidas técnicas y organizativas adecuadas.

2. Asimismo, los operadores garantizarán la mayor disponibilidad posible de los servicios de comunicaciones vocales y de acceso a internet a través de las redes públicas de comunicaciones electrónicas en caso de fallo catastrófico de la red o en casos de fuerza mayor y adoptarán todas las medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencia y la transmisión ininterrumpida de las alertas públicas.

Artículo 6. Plan de acción general de cada sujeto obligado para garantizar la seguridad y resiliencia de redes y servicios de comunicaciones electrónicas.

1. En aras de cumplir con la obligación de prevención, detección y gestión adecuada de los riesgos de seguridad, cada uno de los sujetos obligados deberá elaborar un Plan de acción general.

2. Este Plan de acción general debe incluir un análisis de riesgos sobre la seguridad de su red o de la prestación de servicios de comunicaciones electrónicas o infraestructura digital, identificando si se trata de redes o infraestructuras esenciales, e identificando, además de las medidas de prevención y detección, los mecanismos y priorizaciones en las medidas a adoptar para la gestión y recuperación de los servicios ante una interrupción del servicio o una importante degradación en las condiciones de prestación.

3. En este Plan se identificarán además los edificios e instalaciones que se consideren esenciales y sobre los que adoptarán medidas específicas y prioritarias para garantizar la seguridad de las redes y la continuidad de los servicios.

De igual forma, se detallarán los criterios que se han tenido en cuanta para identificar los edificios e instalaciones como esenciales, así como las medidas específicas y prioritarias que se han adoptada en cada edificio o instalación para garantizar la seguridad de las redes y la continuidad de los servicios.

4. Cada sujeto obligado deberá presentar el Plan de acción general 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.

Artículo 7. Plan específico de cada sujeto obligado para cada red, servicio o infraestructuras digitales que se utilice para garantizar su seguridad.

1. Además de la elaboración de un Plan de acción general, los sujetos obligados tienen obligación de presentar un Plan específico para cada una de las redes, servicios e infraestructuras digitales de las que sean titulares o gestores.

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).

Habida cuenta del carácter dinámico propio 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.

2. Asimismo, los sujetos obligados tienen obligación de presentar un Plan específico para cada tipología de incidencia que se determine mediante Orden aprobada por la persona titular del Ministerio para la Transformación Digital y de la Función Pública. 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.

3. 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.

4. 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 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.

5. 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.

6. 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.

Artículo 8. Análisis e instrucciones de los planes de los sujetos obligados.

1. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales analizará el Plan de acción general y los Planes específicos que presente cada sujeto obligado.

2. A la vista de dicho análisis, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá dictar instrucciones y directrices para que se proceda

a la modificación tanto del Plan de acción general como de cualesquiera de los Planes específicos presentados por cada sujeto obligado en aras de garantizar la seguridad de las redes y servicios de comunicaciones electrónicas y las infraestructuras digitales.

Artículo 9. Plan Nacional Civil de Emergencia en materia de redes y servicios de comunicaciones electrónicas.

1. El Consejo de Ministros, a propuesta del Ministerio del Interior y previo informe del Ministerio para la Transformación Digital y de la Función Pública, aprobará el Plan Nacional Civil de Emergencia en materia de redes y servicios de comunicaciones electrónicas.

2. En dicho Plan se llevará a cabo un análisis de la diferentes amenazas y situaciones excepcionales que pueden afectar a la convivencia ciudadana y diseñará una estrategia para movilizar recursos y bienes relativos a redes, servicios de comunicaciones electrónicas e infraestructuras digitales que coadyuve a superar dicha situación excepcional y recuperar cuanto antes las condiciones de normalidad.

3. Los sujetos obligados están obligados a poner a disposición de las autoridades competentes las infraestructuras, bienes y recursos que sean necesarios y sean requeridos para ello en cada situación en ejecución de este Plan.

4. Este Plan debe ser actualizado cada 2 años.

CAPÍTULO III

Notificaciones ante incidentes de seguridad en las redes y servicios de comunicaciones electrónicas y en determinadas infraestructuras digitales

Artículo 10. Obligación de notificación de los incidentes de seguridad que hayan tenido un impacto significativo en las redes, determinadas infraestructuras digitales o servicios de comunicaciones electrónicas o determinadas.

1. Los sujetos obligados tienen la obligación de notificar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales los incidentes de seguridad que hayan tenido un impacto significativo en el suministro de las redes o en la prestación de los servicios de comunicaciones electrónicas o en la operatividad y funcionamiento de las infraestructuras digitales.

2. Con el fin de determinar la importancia del impacto de un incidente de seguridad se tendrá en cuenta en particular los siguientes parámetros cuando se disponga de ellos:

a) El número de usuarios afectados por el incidente de seguridad,
b) La duración del incidente de seguridad,
c) El área geográfica afectada por el incidente de seguridad,
d) La medida en que se ha visto afectado el funcionamiento de la red o del servicio,
e) El alcance del impacto sobre las actividades económicas y sociales.

3. Para dar debido cumplimiento a esta obligación de notificación de los incidentes significativos de seguridad, los sujetos obligados deberán tener disponible de manera expresa y específica todos los medios materiales y humanos necesarios para cumplir dicha obligación sin demora indebida, con independencia de los medios y recursos que se destinen a superar el incidente de seguridad y restablecer la situación de normalidad.

Artículo 11. Definición de incidentes de seguridad en las redes o servicios de comunicaciones electrónicas y en determinadas infraestructuras digitales.

1. Son considerados incidentes de seguridad los incidentes sufridos por cualquier sujeto obligado, cuando afecten a las redes e infraestructuras digitales y servicios de comunicaciones electrónicas, que supongan una interrupción del servicio o una importante degradación en las condiciones de prestación en el sentido que se determina a continuación.

2. Incidentes considerados de menor significación.

Aquellos que conllevan una interrupción total o una degradación de los servicios de comunicaciones electrónicas, a través de cualquier infraestructura digital, a menos de 10.000 líneas durante al menos 1 hora en horario comprendido entre las 07:00 horas y las 24:00 horas o al servicio soporte del servicio de comunicación audiovisual a menos de 10.000 usuarios durante al menos 1 hora.

3. Incidentes considerados como significativos.

Son aquellos que conllevan una interrupción total o una degradación de los servicios de comunicaciones electrónicas, a través de cualquier infraestructura digital, que cumplan, al menos, una de las siguientes condiciones:

a) El incidente afecta a más de 10.000 líneas durante más de una hora en el horario comprendido entre las 07:00 horas y las 24:00 horas o al servicio soporte del servicio de comunicación audiovisual a más de 10.000 usuarios durante al menos 1 hora.
b) El incidente afecta al mismo tiempo a varios operadores como consecuencia de catástrofes naturales o posibles interrupciones de suministro eléctrico que afecten a los servicios de telecomunicaciones o servicios prestados a través de infraestructuras digitales.

c) El incidente afecta a la interrupción del servicio que prestan los centros que tramitan llamadas de emergencia independientemente del número de líneas afectadas.
d) El incidente afecta a más del 10 por ciento de las líneas existentes en el territorio de cualquier isla de las comunidades autónomas de Baleares y Canarias, o de cualquiera de las ciudades autónomas de Ceuta y Melilla, durante más de dos horas.
e) El incidente afecta a la interrupción o degradación significativa del servicio prestado a través de una infraestructura digital sin que exista impacto directo sobre líneas o usuarios de servicios de comunicaciones electrónicas, o no sea posible determinarlo.
f) Cualquier otro incidente que suponga la interrupción o degradación significativa del servicio prestado a través de una infraestructura digital y que por su afectación al normal desempeño de determinadas actuaciones económicas o sociales o la prestación de servicios públicos o tenga una repercusión social significativa, sea así considerado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

4. El incidente se inicia en el instante en que el servicio comienza a interrumpirse o degradarse. Finaliza en el instante en que todos los servicios se han reestablecido en condiciones de normal funcionamiento disponible para su uso.

5. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, podrá elaborar guías que desarrollen el presente Real Decreto y determine:

a) El procedimiento de cálculo del número de líneas o servicios afectados,
b) La delimitación del umbral de afectación de la calidad del servicio a partir del cual será necesario realizar las notificaciones correspondientes, cuando no se trate de una interrupción total del servicio,
c) La determinación de las condiciones en las que la interrupción o degradación significativa del servicio prestado a través de una infraestructura digital relevante deberá ser notificada, cuando no exista impacto directo sobre líneas o usuarios de servicios de comunicaciones electrónicas, o no sea posible determinarlo.

4. Los sujetos obligados tendrán la obligación de notificar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, conforme al procedimiento previsto en el artículo 12, los incidentes significativos de seguridad recogidos en el apartado 3.

Artículo 12. Notificación.

1. Los sujetos obligados que sufran un incidente significativo de seguridad, deberán notificar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, sin demora indebida, las siguientes notificaciones:

a) Notificación inicial.

La notificación inicial se remitirá en todo caso cuando el operador sufra un incidente de seguridad significativo de los previstos en el artículo 11.3.

Esta notificación se llevará a cabo por correo electrónico a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales en el plazo máximo de 1 hora 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.

La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales dispondrá de acceso, confidencial y completo, a la información integra sobre el incidente de seguridad, siempre que sea relativa a sus respectivas responsabilidades y competencias.

La notificación inicial incluirá al menos:

i) información sobre el momento exacto del inicio del incidente,
ii) una breve descripción de la causa que ha originado ese incidente y, en particular, si en esos momentos se considera que es un incidente de ciberseguridad o de cualquier otro tipo o híbrido,
iii) los servicios afectados y, en particular, si el incidente afecta al servicio de emergencias o al servicio de alertas públicas,
iv) persona de contacto y datos de comunicación,
v) cualquier otra información que el sujeto obligado considere relevante.

b) Notificaciones intermedias.

Si transcurrido el plazo de 2 horas desde la notificación inicial realizada por el sujeto obligado no se hubiera solventado en su totalidad el incidente notificado, el sujeto obligado tendrá 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 todas aquellas notificaciones intermedias necesarias para actualizar la información incorporada a la notificación inicial y aportar la información adicional que se le demande desde la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

En las notificaciones intermedias que se realicen a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales se proporcionará con más detalle la información reportada en la notificación inicial. Se 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.

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.

Trascurridas 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.

Sin perjuicio de lo anterior, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá modificar los periodos de tiempo y las horas identificadas en el apartado anterior en función de la afectación y gravedad del incidente de seguridad producido.

c) Notificación final.

El operador notificará a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales la finalización del suceso, por correo electrónico, tan pronto como tenga conocimiento del restablecimiento del servicio afectado.

Sin perjuicio de lo anterior, en el plazo máximo de 24 horas desde que el operador notifique la finalización del suceso, tendrá que remitir una notificación final en la que se indicará, además del momento exacto de finalización del incidente, 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.

d) Informe detallado.

El informe detallado se remitirá por correo electrónico a la Secretaría de Estado de Infraestructuras Digitales en el plazo máximo de 10 días desde la notificación del operador de la finalización de cualquiera de los incidentes significativos.

El informe detallado contendrá, como mínimo, la siguiente información:

a) Descripción detallada sobre la incidencia:

   i. Hora de inicio y fin del incidente. Duración total del incidente,
   ii. Tipo de incidente e infraestructuras digitales afectadas (ej. fallo de red, interrupción del servicio, caída del servidor, CPDs, etc.),
   iii. Área geográfica afectada,
   iv. Servicios afectados (servicio de voz, datos, fijo o móvil, servicios de difusión, servicios satelitales, etc.).

b) Impacto del incidente:

i. Afectación al servicio de emergencias a través de llamadas al 112,
ii. Afectación al servicio de alertas públicas,
iii. Afectación del servicio de atención al cliente,
iv. Otros operadores afectados,
v. Número de líneas o usuarios según el servicio afectado,
vi. Diferentes tipos de impacto (ej., interrupción del servicio telefónico, pérdida de conectividad, etc.).

c) Causas del incidente:

i. Análisis detallado de la causa del incidente.
ii. Descripción detallada de las posibles causas internas o externas: fallo en los sistemas, congestión de red, errores humanos, acciones maliciosas, fenómenos naturales, fallo de terceras partes como puede ser el suministro eléctrico, fuego provocado, robo del cable, terremoto o inundaciones, etc.

d) Medidas de contingencia adoptadas durante las dos horas siguientes al inicio del incidente:

i. Descripción de las medidas de contingencia realizadas para mitigar el incidente.
ii. Comunicación a las partes interesadas: Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, comunicación a los usuarios finales, otras autoridades como UME o protección civil.

e) Planes de recuperación:

i. Descripción de la evolución en la recuperación de cada uno de los servicios afectados como consecuencia de las acciones de contingencia realizadas para mitigar la avería.
ii. Medidas para evitar futuros incidentes similares.

f) Comunicación y persona de contacto:

i. Canales utilizados para informar sobre la interrupción o degradación del servicio ofrecido a través de infraestructuras digitales tanto a los usuarios como a la administración, protección civil y UME.
ii. Persona de Contacto: nombre, apellidos, correo electrónico y número de teléfono móvil.

g) Responsabilidad: posible responsabilidad del operador en el incidente.

h) Documentación justificativa.

2. Sin perjuicio de la información solicitada en el apartado anterior, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá confeccionar y remitir a los sujetos obligados un formulario específico de notificación durante el proceso de notificaciones iniciales, intermedias y finales requiriendo información específica y adicional adaptado al incidente de seguridad específico y según las necesidades y gravedad de afectación del servicio.

3. 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.

4. Los operadores comunicarán a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en el plazo de 3 meses desde la entrada en vigor de este Real Decreto, los datos de contacto del responsable o responsables de estas notificaciones con el fin de poder solicitar información adicional en caso de ser necesario. Los datos de contacto se actualizarán, al menos, una vez al año.

Artículo 13. Medidas paliativas.

La Secretaría Estado de Telecomunicaciones e Infraestructuras Digitales podrá 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. Dichas recomendaciones podrán hacerse públicas.

Artículo 14. Colaboración con otros Estados Miembros afectados.

1. Cuando proceda, y en particular si el incidente de seguridad en la red o prestación de los servicios de comunicaciones electrónicas o infraestructura digital pueda afectar a otro Estado Miembro, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, informará, sin demora debida, al otro Estado Miembro.

2. La información remitida al otro Estado Miembro incluirá la información recibida por los sujetos obligados preservando, de conformidad con el ordenamiento jurídico de la Unión Europea y nacional, los intereses comerciales de los sujetos obligados, así como la confidencialidad de la información facilitada.

Artículo 15. 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.

Los sujetos obligados comunicarán a las personas físicas y jurídicas destinatarias de los servicios de comunicaciones electrónicas, a la mayor brevedad, y en todo caso antes del plazo de 72 horas desde que se detectó el incidente de seguridad significativo, la afectación a la prestación de los servicios de comunicaciones electrónicas, así como las medidas o soluciones adoptadas para la pronta resolución de la incidencia.

Artículo 16. Notificaciones a otras autoridades competentes en el supuesto de incidentes de seguridad significativos que afectan a infraestructuras críticas y en materia de ciberseguridad.

1. En el supuesto de que un sujeto obligado sea titular de una infraestructura crítica en España, ante un incidente significativo de seguridad de la red o en la prestación de los servicios de comunicaciones electrónicas, deberá notificarlo, sin demora indebida, al Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, y el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), de conformidad con lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y su normativa de desarrollo.

2. En el caso de que el incidente sea de ciberseguridad que afecte a España, según el tipo de entidad y naturaleza del incidente, el sujeto obligado tendrá la obligación de notificarlo a las autoridades competentes establecidas para cada caso en la normativa vigente en materia de ciberseguridad.

Artículo 17. Notificaciones voluntarias de información pertinente.

1. Sin perjuicio de las notificaciones obligatorias recogidas en este real decreto, los sujetos obligados pueden notificar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, de forma voluntaria y en todo momento, cualquier otro tipo de incidente de seguridad, aunque no sea considerado como significativo, que afecte a la interrupción o degradación del servicio de comunicaciones electrónicas.

2. Las notificaciones obligatorias gozarán de prioridad sobre las voluntarias a los efectos de su gestión por los órganos competentes.

Artículo 18. Información de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales a los sujetos obligados.

La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, cuando así lo estime oportuno en función del número de sujetos obligados afectados, del tipo de incidente, sus repercusiones, 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

Comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas

Artículo 19. Obligación de los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas.

1. Los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas tienen la obligación de garantizar la seguridad y el encaminamiento de las llamadas 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 de llamadas de emergencias o a través de otro u otros proveedor o proveedores de servicios.

2. Las medidas adoptadas por parte de los centros de recepción de llamadas de emergencias a las que hace referencia el apartado anterior, serán 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.

3. Estas medidas adoptadas por los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas, los planes específicos adoptadas o planes de redundancia serán actualizados y remitidos a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales cada 2 años.

Artículo 20. Obligación de los sujetos obligados de garantizar el mantenimiento del servicio a los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas.

1. Los sujetos obligados tienen la obligación de presentar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en el plazo de 6 meses desde la entrada en vigor de este Real Decreto, un plan específico que incluya las medidas adoptadas para garantizar el mantenimiento del servicio y la transmisión de las comunicaciones de emergencia a los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas, incluyendo distintos mecanismos de redundancia u otras alternativas que garanticen la continuidad del servicio que puedan establecerse.

2. Este plan específico será actualizado y remitido a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, cada 2 años.

3. La Secretaría Estado de Telecomunicaciones e Infraestructuras Digitales analizará el Plan específico para el mantenimiento del servicio a los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas que presente cada sujeto obligado.

4. A la vista de dicho análisis, la Secretaría Estado de Telecomunicaciones e Infraestructuras Digitales podrá dictar instrucciones y directrices para que se proceda a la modificación de dicho Plan.

Artículo 21. Obligación de notificación en el supuesto de interrupción del servicio de llamadas al número de emergencias y sistema de alertas públicas.

1. En el supuesto de interrupción del servicio de encaminamiento de llamadas al número de emergencias, tanto los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas, como los sujetos obligados tienen la obligación de notificar dicho incidente a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, sin dilación alguna, en el plazo máximo de 1 hora desde que se obtuvo conocimiento de este suceso.

2. Con el fin de determinar la afectación de la interrupción del servicio de llamadas de emergencias y alertas públicas, se tendrá en cuenta los siguientes parámetros:

a) El número de usuarios afectados por la interrupción del servicio de llamadas de emergencias y/o alertas públicas.
b) La duración de la interrupción del servicio.
c) El área o áreas geográfica afectadas por la interrupción del servicio.
d) El alcance del impacto sobre la seguridad de la población.

3. Para la obligación de notificación de la interrupción de los servicios de llamadas de emergencias y/o alertas públicas, los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas y los sujetos obligados, al igual que lo señalado para los incidentes de seguridad, dispondrán de los medios materiales y humanos necesarios para cumplir con la obligación de notificación en caso de que se haya producido una interrupción del servicio de llamadas de emergencias y/o alertas públicas.

4. La interrupción del servicio de llamadas a números de emergencias es considerado como un incidente significativo.

En este sentido, los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas y los sujetos obligados que sufran una interrupción del servicio de llamadas a número de emergencia deberán notificar

a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, las siguientes notificaciones:

a) Notificación inicial.

La notificación inicial se remitirá en todo caso por los centros de recepción de llamadas de emergencias y/o alertas públicas, así como por los sujetos obligados, ante cualquier interrupción del servicio de llamadas de emergencias y/o alertas públicas.

Esta notificación se llevará a cabo, por correo electrónico, a la Secretaría de Estado de Telecomunicaciones e infraestructuras digitales, en el plazo máximo de 1 hora desde que el sujeto obligado tuvo conocimiento del suceso.

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.

b) Notificaciones intermedias.

Si transcurrida 1 hora desde la notificación inicial no se hubiera reestablecido el servicio de llamada al número de emergencias y/o alertas públicas, tanto los centros de recepción de llamadas al número de emergencias como los sujetos obligados por este Real Decreto, tendrán que remitir, cada hora, a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, por correo electrónico, todas aquellas notificaciones intermedias necesarias para actualizar la información incorporada a la notificación inicial y aportar la información adicional que demande la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales en tiempo y forma indicados.

Las notificaciones intermedias se irán remitiendo cada hora, por medio de correo electrónico, hasta que se lleve a cabo la notificación final sin perjuicio de que la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales pueda modificar este periodo de tiempo en función de la afectación y gravedad del incidente de seguridad producido.

En las notificaciones intermedias que se realicen a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales se proporcionará con más detalle la información reportada en la notificación inicial. Se remitirá una descripción detallada 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.

c) Notificación final.

Tan pronto como tenga conocimiento del restablecimiento del servicio de llamadas de emergencias y/o alertas públicas, los centros de recepción de llamadas de emergencias y los sujetos obligados de este Real Decreto lo notificarán a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales por medio de correo electrónico.

Sin perjuicio de lo anterior, en el plazo máximo de 24 horas desde la notificación de finalización del suceso, los sujetos obligados identificados remitirán 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.

d) Informe detallado.

El informe detallado se remitirá por correo electrónico a la Secretaría de Estado de Infraestructuras Digitales en el plazo máximo de 5 días hábiles desde la notificación de la restauración del servicio de llamadas al número de emergencias y/o alertas públicas.

El informe detallado contendrá, como mínimo, la siguiente información:

i) Descripción detallada sobre el incidente:

   a. Hora de inicio y fin del incidente. Duración total del incidente.
   b. Tipo de incidente (ej. fallo de red, interrupción del servicio, caída del servidor, CPDs, etc.).
   c. Área geográfica afectada.

ii) Impacto del incidente:

   a. Afectación al servicio de emergencias ofrecidos a través del 112.
   b. Afectación al servicio de alertas públicas.
   c. Otros operadores afectados.
   d. Número de líneas o usuarios afectados.

iii) Causas del incidente:

   a. Análisis detallado de la causa del incidente.

b. Descripción detallada de las posibles causas internas o externas: Falo en los sistemas, congestión de red, errores humanos, acciones maliciosas, fenómenos naturales, fallo de terceras partes como puede ser el suministro eléctrico, fuego provocado, robo del cable, terremoto o inundaciones, etc.

iv) Medidas de contingencia adoptadas durante las dos horas siguientes al inicio del incidente:

a. Descripción de las medidas de contingencia realizadas para mitigar el incidente del servicio de llamadas a números de emergencias y/o alertas públicas.
b. Comunicación a las partes interesadas: Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, comunicación a los usuarios finales, otras autoridades como UME o protección civil.

v) Planes de recuperación:

a. Descripción de la evolución en la recuperación de cada uno de los servicios afectados como consecuencia de las acciones de contingencia realizadas para mitigar el incidente.
b. Medidas para evitar futuros incidentes similares.

vi) Comunicación y persona de contacto:

a. Canales utilizados para informar sobre la interrupción del servicio de llamadas a número de emergencias y/o alertas públicas tanto a los usuarios como a la administración, protección civil y UME.
b. Persona de Contacto: Nombre, apellidos, correo electrónico y número de teléfono móvil.

vii) Responsabilidad: Posible responsabilidad del sujeto obligado en el incidente.

viii) Documentación justificativa.

5. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá confeccionar y remitir un formulario específico de notificación durante el proceso de notificaciones iniciales, intermedias y finales durante la interrupción del servicio de llamadas de emergencias y/o alertas públicas requiriendo información específica y adicional adaptado a las necesidades y gravedad de afectación del servicio.

6. Los centros de recepción de comunicaciones de emergencia a través del número de emergencia 112 y alertas públicas y 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 de este real decreto, los datos de contacto del responsable de estas notificaciones con el fin de poder solicitar información adicional en caso de ser necesario. Los datos de contacto deberán actualizarse una vez al año.

CAPÍTULO V

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.

Artículo 22. Asunción 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.

1. En virtud de lo dispuesto en el artículo 4.6 de la Ley General de Telecomunicaciones, el Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa de determinados servicios de comunicaciones electrónicas disponibles al público, distintos de los servicios de comunicaciones interpersonales, independientes de la numeración o de la explotación de ciertas redes públicas de comunicaciones electrónicas, para garantizar la seguridad pública y la seguridad nacional, en los términos en que dichas redes y servicios están definidos en el anexo II de la Ley General de Telecomunicaciones, excluyéndose las redes y servicios que se exploten o presten íntegramente en autoprestación.

2. Esta facultad excepcional y transitoria de gestión directa podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer la seguridad pública y la seguridad nacional sin que, en ningún caso, esta intervención pueda suponer una vulneración de los derechos fundamentales y libertades públicas reconocidas en el ordenamiento jurídico.

3. En el caso de incumplimiento de las obligaciones de servicio público, de conformidad con lo establecido en la Ley General de Telecomunicaciones, el Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa de los correspondientes servicios o de la explotación de las correspondientes redes. En este último caso, podrá, con las mismas condiciones, intervenir la prestación de los servicios de comunicaciones electrónicas.

4. Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refieren los párrafos anteriores se

adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración Pública competente. En este último caso, será preciso que la Administración Pública tenga competencias en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas.

5. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado, aquella tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final.

6. Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refiere este apartado 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 resultan acordes con los derechos fundamentales y libertades públicas reconocidas en el ordenamiento jurídico, procediendo a su anulación en caso negativo.

7. La regulación contenida en este artículo se entiende sin perjuicio de lo previsto en la normativa específica sobre las telecomunicaciones relacionadas con el orden público, la seguridad pública, la defensa nacional y la seguridad nacional.

CAPÍTULO VI

Supervisión y cooperación

Artículo 23. Supervisión y ejecución de las obligaciones de seguridad y resiliencia de la redes y servicios de comunicaciones electrónicas y de determinadas infraestructuras digitales.

1. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, ejercerá como autoridad competente en España en la recepción de las notificaciones a que se refiere el capítulo III de este real decreto así como en la supervisión de las obligaciones de seguridad y resiliencia de la redes y servicios de comunicaciones electrónicas y de determinadas infraestructuras digitales y adoptará las medidas necesarias para garantizar el cumplimiento de las obligaciones recogidas en este Real Decreto. En la adopción de estas medidas, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá establecer metodologías de supervisión que permitan priorizar dichas funciones aplicando un enfoque basado en el riesgo.

2. En particular, la actuación de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, como autoridad competente, tiene por objeto controlar y verificar el cumplimiento de las obligaciones de los sujetos obligados establecidas en este Real Decreto, entre otros, en la presentación de los planes generales de

operador, los específicos por servicios, y obligaciones de notificación de incidentes de seguridad de la red y servicios de comunicaciones electrónicas y de determinadas infraestructuras digitales, así como, cualquier otra obligación que se imponga por parte de la Secretaría de Estado en virtud del presente Real Decreto.

3. En el ejercicio de estas funciones, se podrá requerir a los sujetos obligados que proporcionen toda la información pertinente que resulte necesaria para evaluar la seguridad de las redes y servicios de comunicaciones electrónicas.

4. También se podrá solicitar a los sujetos obligados que realicen, a su coste, una auditoría externa sobre el cumplimiento de las obligaciones recogidas en el presente Real Decreto.

5. Los sujetos obligados colaborarán en dicha supervisión, facilitando las actuaciones de inspección, proporcionando toda la información que a tal efecto se les requiera, y aplicando las órdenes o instrucciones dictadas, en su caso, para la subsanación de las deficiencias observadas.

6. Las medidas de supervisión o ejecución impuestas por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales en relación con el cumplimiento por parte de los sujetos obligados de las obligaciones que le vienen impuestas en este Real Decreto serán efectivas, proporcionadas y disuasorias, teniendo en cuenta las circunstancias de cada caso.

7. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, como autoridad competente en el ejercicio de sus funciones de supervisión, podrán adoptar, al menos, las siguientes medidas en relación con los sujetos obligados:

a) Inspecciones in situ y supervisión a distancia, que podrán incluir controles aleatorios realizados por profesionales cualificados.
b) Auditorías de seguridad periódicas y específicas llevadas a cabo, cuando resulte de aplicación, por un tercero independiente, conforme a los procedimientos y con la periodicidad que determine la autoridad competente. Dichas auditorías de seguridad se basarán en evaluaciones del riesgo, sus resultados se comunicarán a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, y sus costes serán sufragados por la entidad auditada.
c) Auditorías extraordinarias, en particular cuando así lo justifique un incidente significativo o cuando se disponga de pruebas, indicios o información de incumplimiento por parte de un sujeto obligado.
d) Análisis de seguridad basados en criterios de evaluación del riesgo objetivos, no discriminatorios, justos y transparentes, con la cooperación de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales cuando sea necesario.
e) Solicitudes de información necesaria para evaluar las medidas adoptadas por el sujeto obligado con relación al cumplimiento de la obligación de presentar información a la autoridad de control.

f) Solicitudes de acceso a datos, documentos e información necesaria para el desempeño de sus funciones de supervisión.

8. En el ejercicio de sus facultades de ejecución, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá, al menos:

a) Advertir por incumplimiento a los sujetos obligados.
b) Adoptar instrucciones vinculantes, que deberán recoger las medidas necesarias para prevenir o subsanar un incidente, los plazos para ejecutar esas medidas y notificar su aplicación, o una orden de requerimiento para que los sujetos obligados subsanen las deficiencias o los incumplimientos detectados.
c) Exigir, en su caso, a los sujetos obligados que pongan fin a las conductas que infrinjan esta norma y que se abstengan de repetirlas.
d) Exigir a los sujetos obligados que garanticen el cumplimiento de las obligaciones impuestas en este Real Decreto, entre ellas, las obligaciones de presentar sus planes generales por operador y específico por servicios, así como, la obligación de notificación de incidentes de seguridad señalados en el artículo 12 en los plazos señalados.
e) Ordenar a los sujetos obligados que informen, en los supuestos determinados en este Real Decreto, a las personas físicas o jurídicas a las que prestan servicios o realizan actividades, de las interrupción o degradación del servicio de comunicaciones electrónicas que le prestan, así como sobre cualquier medida adoptada para la pronta recuperación del servicio.
f) Ordenar a los sujetos obligados que apliquen las medidas correctoras, y/o recomendaciones formuladas en el plazo fijado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
g) Designar un responsable de supervisión para que supervise, durante el periodo que se determine, el cumplimiento por parte de los sujetos obligados de sus obligaciones.
h) Ordenar a los sujetos obligados que hagan públicos determinados aspectos del incumplimiento de una manera específica.
i) Ejercer la potestad sancionadora en los casos y términos previstos en el presente Real Decreto, así como tramitar en todo caso los procedimientos administrativos.

9. Cuando las medidas de ejecución adoptadas resulten ineficaces para alcanzar los fines previstos por las mismas, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales fijará un plazo para que los sujetos obligados adopten las medidas necesarias para subsanar las deficiencias o cumplir los requisitos, sin perjuicio de las responsabilidades que puedan exigirse. Si estas medidas no se adoptan dentro del plazo establecido, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales estará facultada para:

a) Suspender temporalmente o solicitar a los organismos competentes, de conformidad con la normativa vigente, para que suspenda temporalmente

la autorización referente a una parte o la totalidad de los servicios o actividades de que se trate prestados por el sujeto obligado.

b) Solicitar que los organismos competentes, de acuerdo con el ordenamiento jurídico, para que prohíban temporalmente a cualquier persona que ejerza responsabilidades de dirección a nivel de director general o de representante legal en dicha entidad esencial ejercer funciones de dirección.

Las suspensiones o las prohibiciones temporales que se impongan se aplicarán únicamente hasta que los sujetos obligados adopten las medidas necesarias para subsanar las deficiencias o cumplir los requisitos establecidos por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales. La imposición de tales suspensiones o prohibiciones temporales estará sujeta a las garantías adecuadas conforme a los principios generales del ordenamiento jurídico.

10. De forma adicional, en lo no regulado expresamente en este artículo, resultarán de aplicación as medidas de supervisión y ejecución reguladas en la normativa nacional y europea en materia de coordinación y gobernanza de la ciberseguridad y sobre la resiliencia de las entidades críticas.

Artículo 24. Cooperación nacional.

1. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales ejercerá los siguientes cometidos en materia de cooperación nacional:

a) Con objeto de garantizar el cumplimiento efectivo de sus funciones y obligaciones, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales cooperará y colaborará con los órganos y organismos públicos con competencias en materia de Seguridad Nacional, Defensa Nacional, seguridad pública, seguridad ciudadana, administración digital, protección de datos de carácter personal, así como con cualquier entidad con competencias dentro de su ámbito de aplicación en lo referente a la seguridad de redes y servicios de comunicaciones electrónicas.

b) Cooperará e intercambiará periódicamente información con las autoridades competentes designadas conforme a la normativa sobre identificación de entidades críticas, los riesgos, las ciberamenazas y los incidentes relacionados con las TIC, así como sobre los riesgos, las amenazas y los incidentes no cibernéticos que afecten a entidades esenciales identificadas como entidades críticas, y sobre las medidas adoptadas en respuesta a los mismos. También intercambiará información en relación con los incidentes relacionados con las TIC y ciberamenazas con las autoridades competentes en materia de identificación electrónica y los servicios de confianza para las

transacciones electrónicas en el mercado interior, resiliencia operativa digital del sector financiero, y comunicaciones electrónicas.

c) Cooperará con las autoridades competentes en los sectores sometidos a la normativa específica en materia de ciberseguridad con la finalidad de armonizar la normativa.

2. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales comunicará a la Secretaría de Estado de Seguridad del Ministerio del Interior aquellos incidentes que afectando a los operadores estratégicos nacionales sean de interés para la mejora de la protección de infraestructuras críticas, en el marco de la Ley 8/2011, de 28 de abril, reguladora de las mismas.

3. También la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales comunicará a la Comisión Nacional de los Mercados y la Competencia los incidentes de seguridad que afecten o puedan afectar a las obligaciones específicas impuestas por dicha Comisión en los mercados de referencia.

Artículo 25. Cooperación con las Comunidades Autónomas.

1. 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 en aras de lograr la mejor coordinación 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.

2. En particular, 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.

3. Asimismo, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales 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.

Artículo 26. Cooperación en el ámbito de la Unión Europea.

1. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales cooperará en el ámbito de la Unión Europea asumiendo la representación nacional en los foros y los grupos de trabajo de nivel político-estratégico sobre seguridad de la red y servicios de comunicaciones electrónicas e infraestructuras digitales.

2. Una vez al año, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales presentará a la Comisión y a la ENISA un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de conformidad con este real decreto.

Artículo 27. Cooperación en lo relativo a los incidentes que afecten a datos personales.

1. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales cooperará estrechamente con la Agencia Española de Protección de Datos y, en su caso, con las autoridades independientes de control de las Comunidades Autónomas, para hacer frente a los incidentes que produzcan violaciones de la seguridad de datos personales, y les informará sobre aquellos incidentes que puedan comprometer la seguridad de los datos personales que deban ser objeto de notificación, y su evolución.

2. Todo ello sin perjuicio de las funciones que tienen asignadas los responsables de tratamiento en relación con las notificaciones de las posibles brechas de protección de datos personales conforme a lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales así como, en su caso, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

3. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales y su normativa de desarrollo.

Artículo 28. Autorización para la cesión de datos personales.

1. Si para realizar notificación de incidentes o su gestión, análisis o resolución es necesario comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso.

2. Su cesión para estos fines únicamente se entenderá autorizada en los siguientes casos:

a) De los sujetos obligados a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales u organismos designados por ésta para ejercer funciones de control y ejecución.
b) Entre la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y los organismos designados por ésta para ejercer funciones de control y ejecución.
c) Entre la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y las Autoridades Nacionales de Reglamentación Europeas o Internacionales.
d) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.

CAPÍTULO VII

Inspección y régimen sancionador en materia de seguridad y continuidad de las redes y servicios de comunicaciones electrónicas e infraestructuras digitales

Artículo 29. Función de inspección.

La función de inspección en materia de seguridad de redes y servicios de comunicaciones electrónicas e infraestructuras digitales corresponde al Ministerio para la Transformación Digital y de la Función Pública, que se llevará a cabo a través de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Artículo 30. Facultad de inspección.

1. Los Servicios de Inspección de la Secretaría Estado de Telecomunicaciones e Infraestructuras Digitales, podrán realizar las inspecciones que consideren necesarias al objeto de verificar el cumplimiento de las obligaciones establecidas a los sujetos obligados en este Real Decreto. A tal efecto, dichos Servicios de Inspección 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.

2. Los sujetos obligados tendrán la obligación de poner a disposición del personal de inspección cuantos libros, registros y documentos, sea cual fuere su forma y soporte, y medios técnicos este considere precisos, incluidos el software, los programas informáticos y los archivos magnéticos, ópticos o de cualquier otra clase, pudiendo al efecto el personal de inspección hacer u obtener copias de ellos.

3. Asimismo, deberán facilitarles, a su petición, cualquier tipo de documentación que el personal de la inspección les exija para la determinación de la titularidad de los

equipos o la autoría de emisiones, actividades o de los contenidos o servicios que se presten a través de las redes de comunicaciones electrónicas.

4. Los sujetos obligados tendrán la obligación de someterse a las inspecciones que efectúe el personal de inspección. La negativa u obstrucción para comparecer a los actos de inspección a los cuales haya sido citados, a la realización de las pruebas técnicas o actuaciones complementarias requeridas o a facilitar la información o documentación requerida será sancionada, conforme a los artículos siguientes de este título, como obstrucción a la labor inspectora.

5. El personal de inspección, a los efectos del cumplimiento de las funciones previstas en este artículo, tendrá acceso gratuito a todo registro público, en particular, en los Registros de la Propiedad y Mercantiles. El acceso a la información registral se realizará por medios electrónicos, en la forma determinada en su normativa reguladora.

Artículo 31. Responsabilidad por las infracciones.

La responsabilidad administrativa por la infracción de los preceptos contenidos en el presente Real Decreto será exigible a la persona física o jurídica que desarrolle la actividad.

Artículo 32. Infracciones graves.

La infracción de cualesquiera de las obligaciones recogidas en este Real Decreto por parte de los sujetos obligados será considerada como grave en virtud del artículo 107.22 de la Ley General de Telecomunicaciones.

Artículo 33. Sanciones.

1. Por la comisión de las infracciones graves se impondrá al infractor multa por importe de hasta dos millones de euros, de conformidad con el artículo 109 de la Ley General de Telecomunicaciones.

2. Además de la sanción que corresponda imponer a los infractores, 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. Quedan 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.

3. A los efectos de lo establecido en este real decreto, 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.

Artículo 34. Criterios para la determinación de la cuantía de la sanción.

1. La cuantía de la sanción que se imponga se graduará teniendo en cuenta, además de lo previsto en el artículo 29 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, lo siguiente:

a) la gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona;
b) el daño causado, como la producción de la degradación del servicio y su reparación;
c) el cumplimiento voluntario de las medidas cautelares que, en su caso, se impongan en el procedimiento sancionador;
d) la negativa u obstrucción al acceso a la información o documentación requerida;
e) el cese de la actividad infractora, previamente o durante la tramitación del expediente sancionador;
f) la afectación a bienes jurídicos protegidos relativos el orden público, la seguridad pública y la seguridad nacional o los derechos de los usuarios;
g) la colaboración activa y efectiva con la autoridad competente en la detección o prueba de la actividad infractora.

2. 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, entre otros criterios, el perjuicio causado a la competencia, a los usuarios o a la Administración pública.

Artículo 35. Medidas cautelares.

La Secretaría de Estado para la Transformación Digital y de la Función Pública podrá adoptar medidas cautelares si el incumplimiento de las obligaciones establecidas en este Real Decreto esté perjudicando la integridad de la red o afectando a la continuidad de los servicios de comunicaciones electrónicas.

Artículo 36. Prescripción.

1. Las infracciones graves prescribirán a los dos años de conformidad con el artículo 113 de la Ley General de Telecomunicaciones.

El plazo de prescripción de las infracciones comenzará a computarse desde el día en que se hubieran cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador. 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.

2. 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.

Artículo 37. Competencia sancionadora.

La competencia sancionadora por el cumplimiento de las obligaciones recogidas en este Real Decreto corresponde a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales de conformidad con el artículo 114 de la Ley General de Telecomunicaciones.

Disposición adicional primera. Normativa relativa a la coordinación y gobernanza de ciberseguridad y sobre la resiliencia de las entidades críticas.

1. El presente 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.

2. Sin perjuicio de lo anterior, a los sujetos obligados en este Real Decreto 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.

1. 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.

2. La Mesa de coordinación de seguridad y resiliencia de redes y servicios de comunicaciones electrónicas 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.

3. La Mesa de coordinación de seguridad y resiliencia de redes y servicios de comunicaciones electrónicas aprobará su reglamento de organización y funcionamiento.

4. La Mesa 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 única. Derogación normativa.

1. Queda derogado el Capítulo VI 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 telecomunicaciones, relativo a los sucesos que lleven una degradación importante de la calidad del servicio.

2. Asimismo, quedan derogadas las disposiciones de igual o inferior rango a este real decreto que se opongan a lo dispuesto en ella.

Disposición final primera. Título competencial.

Este 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.

Disposición final segunda. Desarrollo reglamentario y aplicación.

1. La persona titular del Ministerio para la Transformación Digital y de la Función Pública dictará, en el ámbito de sus competencias, cuantas disposiciones sean necesarias para el desarrollo de lo establecido en el este Real Decreto.

2. La persona titular del Ministerio para la Transformación Digital y de la Función Pública y la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales aprobarán, en el ámbito de sus competencias, cuantas medidas sean necesarias para la aplicación de lo establecido en el este Real Decreto.

Disposición final tercera. Entrada en vigor.

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

En Madrid a xx de xxxx de 2025

El Ministro para la Transformación Digital
y de la Función Pública

ÓSCAR LÓPEZ ÁGUEDA