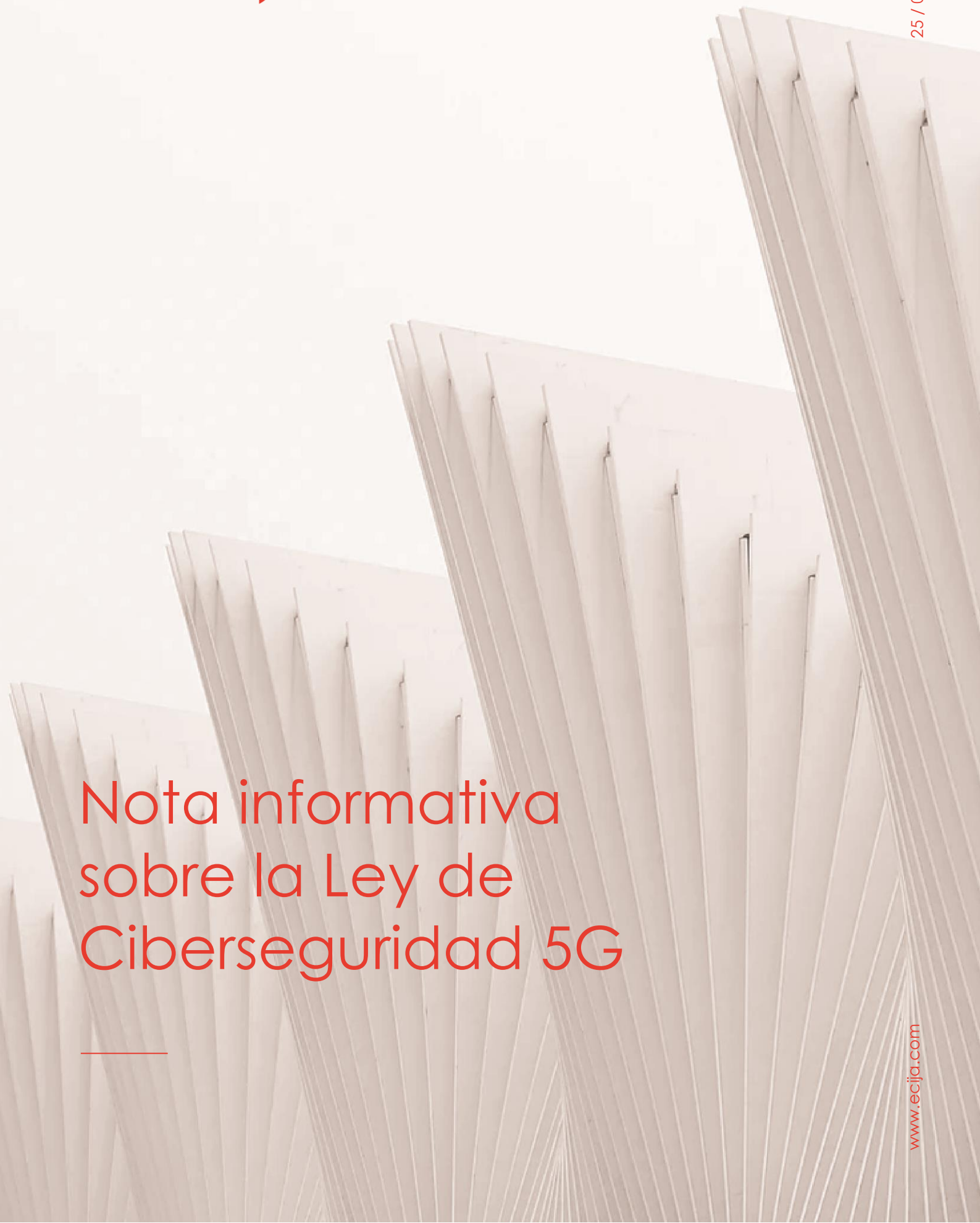
ECIJA

25 / 04 / 2022

Nota informativa sobre la Ley de Ciberseguridad 5G



www.ecija.com

ECIJA
Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa sobre la Ley de Ciberseguridad 5G

25 abril de 2022

El pasado 30 de marzo de 2022 el BOE publicaba 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 por medio del cuál se regulan nuevas obligaciones para los operadores 5G, para los suministradores 5G, y también para los usuarios corporativos 5G.

Este Real Decreto Ley entró en vigor al día siguiente de su publicación. No obstante, las obligaciones principales derivadas de la necesidad de gestionar la seguridad por estos sujetos obligados, entrará en vigor el 30 de abril de 2022.

(I) Antecedentes

No cabe duda de que la quinta generación de redes móviles (5G) van a suponer una revolución en las comunicaciones en los próximos 5 a 10 años que van a permitir nuevos servicios de valor añadido dirigidos a la sociedad, en ámbitos como medicina, logística, redes sociales, debido principalmente a su velocidad y baja latencia. Sin embargo, debido a las características propias de estas redes, que implementan en muchas ocasiones computación en el borde (edge computing), esto es, capacidad de computación cercana al usuario para reducir la latencia, así como virtualización múltiple de redes (network slicing) y computación en la nube, deben tenerse en cuenta y gestionarse nuevos riesgos que no eran habituales en generaciones previas de las redes móviles.

El despliegue de estas redes es clave en la estrategia digital, y de hecho, la aprobación de la conocida como Ley de Ciberseguridad 5G es una de las reformas previstas en el Plan de Recuperación, Transformación y Resiliencia, en el apartado dedicado a «Conectividad digital, impulso de la ciberseguridad y despliegue del 5G».

Una de las características principales de las redes 5G es la adopción de arquitecturas descentralizadas, donde entran en juego nuevos suministradores de tecnología de los que los operadores 5G previsiblemente serán dependientes, y cuyos riesgos también deben ser gestionados, no solo a nivel de infraestructura, sino también debido a aspectos estratégicos o geopolíticos, en tanto en cuanto estos suministradores puedan estar expuestos a injerencias de terceros países, circunstancia que se ha incrementado notablemente con la reciente guerra de Ucrania.

(II) Objeto y sujetos obligados

Esta ley tiene como **objeto** establecer requisitos de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología de quinta generación (5G).

Los **sujetos obligados** que deberán cumplir con las obligaciones de esta ley son:

a) Los operadores 5G: Persona física o jurídica que instala, despliega o explota redes públicas 5G o presta servicios 5G disponibles al público a través, total o parcialmente, de las redes 5G, disponga de red 5G propia o no, y ha notificado al Registro de operadores el inicio de su actividad o está inscrita en el Registro de operadores

b) Los suministradores 5G: El fabricante, el representante autorizado, el importador, el distribuidor, el prestador de servicios logísticos o cualquier otra persona física o jurídica sujeta a obligaciones en relación con la fabricación de productos, su comercialización o su puesta en servicio en materia de equipos de telecomunicación, los suministradores de hardware y software y los proveedores de servicios auxiliares que intervengan en el funcionamiento u operación de redes 5G o en la prestación de servicios 5G.

c) Los usuarios corporativos 5G: La persona física o jurídica que instala, despliega o explota redes privadas 5G o presta servicios 5G a través, total o parcialmente, de las redes 5G, para fines profesionales o en autoprestación. que tengan otorgados derechos de uso del dominio público radioeléctrico para estas actividades.

(III) Obligaciones

Todos los sujetos obligados deberán realizar tratamiento integral de la seguridad de las redes, elementos, infraestructuras, recursos, facilidades y servicios de los que sean responsables. Deberán:

- Realizar análisis de vulnerabilidades, amenazas y riesgos de forma holística.
- Gestionar de manera adecuada e integral dichos riesgos para lograr su mitigación o eliminación.
- Cumplimiento de lo dispuesto en la Ley de ciberseguridad 5G, a lo que se establezca en el Esquema Nacional de Seguridad de redes y servicios 5G (no publicado aún) y a los actos que se dicten en ejecución de ambas disposiciones.
- Proporcionar la información que sea necesaria en la Ley de ciberseguridad 5G o en el Esquema Nacional de Seguridad de redes y servicios 5G o la que le sea requerida por el Ministerio de Asuntos Económicos y Transformación Digital (en adelante, MINECO).

(III.A) Análisis de riesgos:

Todos los sujetos obligados tiene la obligación de realizar un análisis de riesgos cuyo contenido dependerá del tipo de sujeto obligado:

- **Operadores 5G:** Se requiere la realización de un estudio pormenorizado e individualizado cada dos años, que deberá ser remitido al MINECO, sobre las amenazas y vulnerabilidades que afecten, al menos, a los siguientes elementos, infraestructuras y recursos de una red pública 5G:

  - Los relativos a las funciones del núcleo de la red (considerado como un elemento crítico).
  - Las funciones de transporte y transmisión.
  - La red de acceso (considerado como un elemento crítico).
  - Los sistemas de control y gestión y los servicios de apoyo (considerado como un elemento crítico).
  - Las funciones de computación en el borde, virtualización de red y gestión de sus componentes.
  - Los relativos a intercambios de tráfico con redes externas e Internet.
  - Otros componentes y funciones que, a tal efecto, se determinen en el Esquema Nacional de Seguridad de redes y servicios 5G.

  Este análisis de riesgos deberá considerar los siguientes elementos:

  - Parametrización y configuración de elementos y funciones de red.
  - Políticas de integridad y actualización de los programas informáticos.
  - Estrategias de permisos de acceso a activos físicos y lógicos.
  - Dependencias de determinados suministradores en elementos críticos de la red 5G.
  - Agentes externos, incluyendo grupos organizados con capacidad para atacar la red.
  - Equipos terminales y dispositivos conectados a la red.
  - Elementos de usuarios corporativos y redes externas conectadas a la red 5G.
  - La interrelación con otros servicios esenciales para la sociedad.

  El análisis de riesgos debe priorizar y jerarquizar los riesgos en función de los siguientes parámetros:

  - Afectación a un elemento crítico de la red pública 5G.
  - Tipo de recurso, infraestructura y servicio que pueda verse afectado.
  - Afectación a la integridad y mantenimiento técnico de la red o a la continuidad del servicio.
  - Capacidad de detección y recuperación.
  - Número y tipo de usuarios afectados.
  - Tipo de información cuya integridad haya podido verse comprometida.

El Operador 5G tendrá que recabar de sus suministradores las prácticas y medidas de seguridad adoptadas en los productos y servicios que les han suministrado para la realización del análisis de riesgos, teniendo en cuenta los factores indicados anteriormente y el perfil de riesgo del suministrador.

Importante: Los operadores 5G deberán remitir antes del 30 de septiembre de 2022 al MINECO, un análisis de riesgos de sus redes y servicios 5G o de los que vayan a desplegar en los próximos dos años y un informe de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos

- **Suministradores 5G:** Deberán analizar los riesgos de los equipos de telecomunicación, hardware y software y servicios auxiliares que intervengan en el funcionamiento u operación de redes 5G o en la prestación de servicios 5G, detectando vulnerabilidades y amenazas que le afecten tanto a la gestión de la empresa como a dichos equipos. Deberá ser remitido al MINECO cuando le sea requerido.

  Si el suministrador 5G es calificado como de alto riesgo o de riesgo medio, tendrá la obligación de remitir el análisis de riesgos al MINECO en el plazo de 6 meses desde que sea calificado como tal. Adicionalmente deberán realizar un nuevo análisis cada dos años y remitirlo al Ministerio.

- **Usuarios Corporativos 5G:** Deberán analizar los riesgos de las redes y servicios 5G, detectando vulnerabilidades y amenazas que afecten a los elementos de red, infraestructuras, recursos, facilidades y servicios que empleen o provean en la instalación, despliegue y explotación de redes privadas 5G o en la prestación de servicios 5G en autoprestación. Deberá ser remitido al MINECO cuando le sea requerido.

Todos los análisis de riesgos mencionados tendrán la consideración de **información confidencial** y no podrán ser utilizados para otras finalidades.

(III.B) Gestión de los riesgos:

Todos los sujetos obligados deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G, que sean acordes con lo establecido en la Ley de Ciberseguridad 5G, el Esquema Nacional de Seguridad 5G y otros actos de ejecución que puedan publicarse.

No obstante, esta gestión tendrá particularidades según el sujeto obligado que corresponda:

- **Operadores 5G:** Deberán cumplir con las siguientes medidas para mitigar riesgos:

    - Adoptar medidas técnicas y operativas para garantizar la integridad física y lógica de las redes 5G o cualesquiera de sus elementos, infraestructuras y recursos, así como la continuidad en la prestación de servicios 5G.
    - Adoptar planes y medidas de contingencia específicas para asegurar la continuidad de otros servicios esenciales para la sociedad que dependan de las redes y servicios 5G.
    - Seleccionar e identificar a las personas que puedan acceder a los activos físicos y lógicos de la red, y realizar el mantenimiento de registros de acceso.
    - Mantener las credenciales de usuario para el acceso a la red en posesión del operador.
    - Utilizar únicamente productos, recursos, servicios o sistemas certificados para la operación de las redes 5G, o en alguna de sus partes o elementos.
    - Cumplir las normas o especificaciones técnicas aplicables a redes y sistemas de información.
    - Cumplir con los esquemas europeos de certificación de productos, servicios o sistemas, sean o no específicos de la tecnología 5G, que se empleen en la operación o explotación de redes y servicios 5G.
    - Someterse, a su costa, a una auditoría de seguridad realizada por una entidad pública o una entidad privada acreditada a estos efectos.
    - Exigir a sus suministradores el cumplimiento de estándares de seguridad, desde el diseño de los productos y servicios hasta su puesta en funcionamiento.
    - Controlar su propia cadena de suministro y la estrategia de diversificación que haya diseñado.

Adicionalmente deberán remitir al MINECO cada dos años una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos.

Por último, si los operadores 5G cuentan con suministradores que en un determinado momento sean calificados de alto riesgo, dispondrán de un plazo de cinco años a contar desde la calificación para llevar a cabo la sustitución en los elementos críticos de red relativos a las funciones del núcleo de la red y a los sistemas de control y gestión y los servicios de apoyo, así como de un plazo de dos años para llevar a cabo dicha sustitución en los elementos críticos de red relativos a la red de acceso en zonas geográficas y ubicaciones.

- **Operadores 5G que sean titulares o exploten elementos críticos** de una red pública 5G tienen adicionalmente las siguientes obligaciones:

    - Deberán diseñar una estrategia de diversificación en la cadena de suministro de los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales en una red pública 5G, de forma que dichos equipos, sistemas o recursos sean proporcionados, como mínimo, por dos suministradores diferentes. No se considerarán diferentes si pertenecen al mismo grupo de empresas. Si no se puede cumplir, deberá comunicarse al Ministerio quien decidirá si resulta posible mantener un suministrador único.
      IMPORTANTE: Deberán remitir al MINECO la estrategia de diversificación en la cadena de suministro antes del 30 de septiembre de 2022.
    - No podrán utilizar en los elementos críticos de red equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo.
    - No podrán utilizar en la red de acceso de una red pública 5G equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo, en aquellas estaciones radioeléctricas con las que se proporcione cobertura a centrales nucleares, centros vinculados a la Defensa Nacional y las ubicaciones determinadas por el Consejo de Seguridad Nacional.
    - Deberán ubicar los elementos críticos de una red pública 5G dentro del territorio nacional.

- **Suministradores 5G:** Deberán cumplir con las siguientes medidas que serán concretas en el ENS 5G:

    - Cumplir estándares de seguridad desde el diseño de los equipos, productos y servicios hasta su puesta en funcionamiento.
    - Reforzar la integridad del software, actualización y gestión de parches.
    - Acreditar la certificación de productos y servicios de tecnologías de la información que se usen en las redes y servicios 5G.
    - Garantizar la aplicación de medidas de seguridad técnicas y organizativas estándar a través de un sistema de certificación.
    - Efectuar una auditoría de seguridad de sus equipos, productos y servicios.
    - Proporcionar información sobre posibles injerencias de terceros en el diseño, operación y funcionamiento de sus equipos, productos y servicios.

- Colaborar con los operadores 5G y usuarios corporativos 5G proporcionando información y acreditando el cumplimiento de estándares de seguridad de equipos, productos y servicios que suministren.

Adicionalmente deberán aportar al MINECO una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos, cuando sean requeridos para ello.

Si el suministrador 5G ha sido calificado por el Consejo de Ministros como de alto riesgo o de riesgo medio deberá remitir al MINECO un informe de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos en el plazo de seis meses a contar desde que haya sido calificado, y posteriormente cada dos años.

La ley prevé que antes del 30 de junio de 2022, el Consejo de Ministros calificará como de alto riesgo a determinados suministradores 5G.

- **Usuarios Corporativos 5G:** deberán garantizar la instalación, despliegue y explotación seguros de redes privadas 5G y prestación segura de servicios 5G en autoprestación mediante la aplicación de técnicas y procedimientos de operación y supervisión que garanticen la seguridad de las redes y servicios 5G, y aportarán al MINECO una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos, cuando sean requeridos para ello.

(III.C) ENS 5G:

Todos los sujetos obligados, así como los fabricantes, importadores, distribuidores y quienes pongan en el mercado y comercialicen equipos terminales y dispositivos para conectarse a una red 5G y poder prestar servicios 5G deberán prestar la colaboración y remitir la información que le sea requerida para la elaboración, aprobación y ejecución del Esquema Nacional de Seguridad de redes y servicios 5G. Los requerimientos de información deberán ser contestados en el plazo de 15 días.

(IV) Inspecciones, infracciones y Sanciones

La facultad de supervisión e inspección corresponde al MINECO, mientras que la sancionadora corresponde a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

En cuanto a las infracciones, podemos distinguir 3 tipos:

- **Muy graves:** Con una sanción cuyo importe podrá ser hasta al quíntuplo del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción, o 20 millones de euros si no se puede calcular la cantidad anterior. Además puede proceder inhabilitación de hasta 5 años.
- **Graves:** Con una sanción cuyo importe será el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable hasta 2 millones de euros.
- **Leves:** Hasta 50.000 euros.

Además, en caso de que el sujeto obligado sea una persona jurídica, se podrá sancionar con hasta 60.000 € a sus representantes legales o a las personas que integran los órganos directivos que hayan intervenido en el acuerdo o decisión.

Área de Ciberseguridad de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60

ECIJA

Most recognized Spanish firm in LATAM and Best European TMT Firm

34 practices globally recognized in 10 jurisdictions

Best Technology Firm

Amongst most innovative European Firms

Best European TMT Firm

Most innovative project, Best Digital Economy Firm

Torre de Cristal
Pº de la Castellana, 259C
28046 Madrid