

- Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los **soportes** en los que éstos aparezcan deberán ser **custodiados hasta la finalización**, en su caso, del **expediente sancionador** que hubiera lugar o, en otro caso, **destruidos** inmediatamente. En ninguna circunstancia podrán ser objeto de divulgación.

Protección de los datos de carácter personal (Art. 60)

Los **operadores** que **suministren redes públicas** de comunicaciones electrónicas o que **presten servicios** de comunicaciones electrónicas disponibles **al público**, incluidas las **redes públicas** de comunicaciones que **den soporte a dispositivos de identificación y recopilación de datos**, deberán **adoptar las medidas técnicas y de gestión** adecuadas para **preservar la seguridad** en el **suministro** de su **red** o en la **prestación** de sus **servicios**, con el fin de garantizar la protección de los datos de carácter personal. Dichas **medidas** incluirán, como mínimo:

- La **garantía** de que **sólo el personal autorizado** tenga **acceso** a los **datos personales** para fines autorizados por la ley;
- La **protección** de los **datos personales almacenados o transmitidos** de la **destrucción accidental o ilícita**, la **pérdida o alteración accidentales** o el **almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos**;
- La **garantía** de la aplicación efectiva de una **política de seguridad** con respecto al **tratamiento de datos personales**.

La **Agencia Española de Protección de Datos**, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá **examinar las medidas adoptadas** por los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y podrá **formular recomendaciones** sobre las **mejores prácticas** con respecto al **nivel de seguridad** que debería **conseguirse** con estas medidas.

En caso de que exista un **riesgo particular de violación de la seguridad** de la **red pública** o del **servicio de comunicaciones electrónicas**, el **operador** que suministre dicha red o preste el servicio de comunicaciones electrónicas **informará** a los **abonados** sobre dicho **riesgo** y sobre las **medidas** a adoptar.

En caso de **violación** de los **datos personales**, el **operador** de servicios de comunicaciones electrónicas disponibles al público **notificará sin dilaciones** indebidas dicha violación a la **Agencia Española de Protección de Datos**. Si la **violación** de los datos pudiera **afectar negativamente** a la **intimidad** o a los **datos personales** de un abonado o particular, el operador notificará **también** la violación al **abonado o particular sin dilaciones** indebidas.

La **notificación** de una **violación** de los datos personales a un **abonado o particular** afectado **no** será **necesaria** si el **operador ha probado a satisfacción** de la **Agencia Española de Protección de Datos** que ha aplicado las **medidas de protección tecnológica** convenientes y que estas medidas **se han aplicado** a los **datos afectados** por la violación de seguridad

Sin perjuicio de la obligación del operador de informar a los abonados o particulares afectados, si el **operador no** ha **notificado ya** al **abonado** o al **particular** la violación de los datos personales, la **Agencia Española de Protección de Datos** podrá **exigirle** que lo haga, una vez **evaluados** los posibles **efectos adversos** de la violación.

En la **notificación** al **abonado** o al **particular** se **describirá** al menos la **naturaleza** de la **violación** de los **datos personales** y los **puntos de contacto** donde puede **obtenerse más información** y se recomendarán **medidas** para **atenuar** los posibles **efectos adversos** de dicha violación. En la notificación a la **Agencia Española de Protección de Datos** se **describirán** además las **consecuencias** de la **violación** y las **medidas propuestas o adoptadas** por el **operador** respecto a la violación de los datos personales.

Los **operadores** deberán llevar un **inventario** de las **violaciones** de los datos personales, **incluidos** los **hechos relacionados** con tales infracciones, sus **efectos** y las **medidas adoptadas** al respecto, que resulte suficiente para **permitir** a la **Agencia Española de Protección de Datos** **verificar** el cumplimiento de las **obligaciones**

de notificación reguladas en este apartado. Mediante **real decreto** podrá establecerse el **formato** y **contenido** del inventario.

A los efectos establecidos en este artículo, **se entenderá** como **violación** de los **datos personales** la **violación** de la **seguridad** que **provoque** la ¹**destrucción**, accidental o ilícita, la ²**pérdida**, la ³**alteración**, la ⁴**revelación** o el ⁵**acceso no autorizados**, de **datos personales transmitidos, almacenados o tratados de otro modo** en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público.

La **Agencia Española de Protección de Datos** podrá **adoptar directrices** y, en caso necesario, **dictar instrucciones** sobre las ¹**circunstancias** en que se requiere que el **operador notifique** la **violación** de los **datos personales**, sobre el ²**formato** que debe adoptar dicha **notificación** y sobre la ³**manera** de **llevarla a cabo**, con pleno **respeto** a las **disposiciones** que en su caso sean adoptadas en esta materia por la **Comisión Europea**.

Conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (Art. 61)

La **conservación** y **cesión** de los **datos** generados o tratados en el marco de la prestación de **servicios de comunicaciones electrónicas** o de **redes públicas** de comunicación a los **agentes facultados** a través de la correspondiente **autorización judicial** con fines de **detección, investigación y enjuiciamiento** de **delitos graves** contemplados en el Código Penal o en las leyes penales especiales **se rige por** lo establecido en la **Ley 25/2007**, de 18 de octubre, de **conservación de datos** relativos a las **comunicaciones electrónicas** y a las **redes públicas** de comunicaciones.

Cifrado en las redes y servicios de comunicaciones electrónicas (Art. 62)

Cualquier tipo de **información** que se **transmita** por **redes** de **comunicaciones electrónicas** podrá ser **protegida** mediante **procedimientos** de **cifrado**.

El **cifrado** es un **instrumento de seguridad** de la **información**. Entre sus condiciones de uso, cuando se utilice para **proteger** la **confidencialidad** de la información, se podrá imponer la ¹**obligación** de **facilitar** a un **órgano** de la **Administración General del Estado** o a un **organismo público**, los **algoritmos** o cualquier **procedimiento de cifrado** utilizado, en casos justificados de **protección** de los **intereses** esenciales de **seguridad** del **Estado** y la **seguridad pública**, y para **permitir** la **investigación**, la **detección** y el **enjuiciamiento** de **delitos**, así como la ²**obligación** de **facilitar** sin coste alguno los **aparatos de cifra** a efectos de su **control** de acuerdo con la normativa vigente.

Toda **información obtenida** por parte de la Administración General del Estado o cualquier organismo público a **través** de los **preceptos** incluidos en el apartado 2 de este artículo deberá ser **tratada** con la **máxima confidencialidad** y **destruida** una vez que se **resuelva** la **amenaza** para la **seguridad del Estado** y la **seguridad pública** o se haya dictado **sentencia firme** sobre el **delito** en cuestión.

Integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas (Art. 63)

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 **evitar** o **reducir** al mínimo el **impacto** de los **incidentes de seguridad** en los **usuarios** y en **otras redes y servicios**, para lo cual deberán **adoptar** las **medidas técnicas** y **organizativas** adecuadas, que deberán ser **proporcionadas** y **en línea** con el **estado de la técnica**, pudiendo incluir el **cifrado**.

Asimismo, los **operadores** de redes públicas de comunicaciones electrónicas **garantizarán** la **integridad** de las mismas a fin de **asegurar** la **continuidad** en la prestación de los **servicios** que utilizan dichas redes.

Los **operadores** que suministren redes públicas o presten servicios de comunicaciones electrónicas disponibles al público **notificarán** al **Ministerio de Asuntos Económicos y Transformación Digital** los **incidentes de seguridad** que hayan tenido un **impacto significativo** en el **suministro** de las **redes** o los **servicios**.

Con el fin de **determinar** la **importancia** del impacto de un **incidente de seguridad** se tendrán en cuenta, en particular, los **parámetros** siguientes, cuando se disponga de ellos:

- El **número** de **usuarios afectados** por el incidente de seguridad;
- La **duración** del **incidente** de seguridad;
- El **área geográfica afectada** por el incidente de seguridad;
- La **medida** en que se ha visto **afectado** el **funcionamiento** de la red o del servicio;
- El **alcance del impacto** sobre las **actividades económicas y sociales**.

Cuando proceda, el **Ministerio informará** a las **autoridades nacionales** competentes **de otros Estados miembros** y a la **Agencia Europea de Seguridad en las Redes y la Información** (ENISA). Asimismo, 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**. **Una vez al año**, el **Ministerio presentará** a la **Comisión** y a la **ENISA** un **informe resumido** sobre las **notificaciones** recibidas y las **medidas** adoptadas de conformidad con este apartado.

Del mismo modo, el **Ministerio 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. También el **Ministerio comunicará** a la **Comisión Nacional de los Mercados y la Competencia** los **incidentes de seguridad** a que se refiere este apartado que **afecten** o **puedan afectar** a las **obligaciones** específicas **impuestas** por dicha Comisión en los **mercados de referencia**.

En caso de que exista una **amenaza particular y significativa** de **incidente de seguridad** en las redes públicas de comunicaciones electrónicas o en los servicios de comunicaciones electrónicas disponibles para el público, los **operadores** deberán **informar** a sus **usuarios** que pudieran **verse afectados** por dicha amenaza sobre las posibles **medidas de protección** o **soluciones** que pueden adoptar los usuarios. Cuando proceda, los operadores también **informarán** a sus **usuarios** sobre la **propia amenaza**.

El **Ministerio de Asuntos Económicos y Transformación Digital** establecerá los mecanismos para **supervisar** el cumplimiento de las **obligaciones** anteriores y, en su caso, **dictará** las **instrucciones** correspondientes, que serán **vinculantes** para los **operadores**, incluidas las relativas a las medidas necesarias adicionales a las identificadas por los operadores para solventar incidentes de seguridad, o impedir que ocurran cuando se haya observado una amenaza significativa, e incumplimientos de las fechas límite de aplicación. Entre las **medidas relativas** a la **integridad** y **seguridad** de redes y servicios de comunicaciones electrónicas que se puedan **exigir** a los **operadores**, podrá **imponer**:

- La obligación 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**;
- La obligación de **someterse** a una **auditoría de seguridad** realizada por un **organismo independiente** o por una **autoridad** competente, y de poner el **resultado** a disposición del **Ministerio de Asuntos Económicos y Transformación Digital**. El **coste** de la auditoría será sufragado por el **operador**.

REAL DECRETO 806/2014, DE 19 DE SEPTIEMBRE, SOBRE ORGANIZACIÓN E INSTRUMENTOS OPERATIVOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN LA ADMINISTRACIÓN GENERAL DEL ESTADO Y SUS ORGANISMOS PÚBLICOS.

OBJETO Y ÁMBITO DE APLICACIÓN (Cap. 1)

Objeto (Art. 1)

El **objeto** de este real decreto es el **desarrollo** y **ejecución** de un **modelo común** de **gobernanza** de las **Tecnologías de la Información y las Comunicaciones (TIC)** en la Administración General del **Estado** y sus **Organismos Públicos**.

Ámbito de aplicación (Art. 2)

El **ámbito de aplicación** de este real decreto se extiende a la **Administración General del Estado** y sus **Organismos**

MODELO DE GOBERNANZA EN EL ÁMBITO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (Cap. 3)

Estrategia en materia de tecnologías de la información y las comunicaciones (Art. 9)

El **Gobierno**, a iniciativa de la **Comisión de Estrategia TIC**, y a **propuesta** de los **ministros** de la ¹**Presidencia**, de ²**Hacienda** y **Administraciones Públicas** y de ³**Industria, Energía y Turismo**, **aprobará** la Estrategia en materia de tecnologías de la información y las comunicaciones (en adelante **Estrategia TIC**), así como las **revisiones** de la misma.

La **Estrategia TIC** **determinará** los **objetivos, principios y acciones** para el desarrollo de la **administración digital** y la **transformación digital** de la Administración General del Estado y sus Organismos Públicos y servirá de **base** para la elaboración por los distintos ministerios de sus **planes de acción** para la transformación digital.

La **Comisión de Estrategia TIC** **determinará** el ¹**ámbito temporal** de la Estrategia TIC, así como su ²**periodo de revisión**.

Medios y servicios compartidos (Art. 10)

Los **medios y servicios TIC** de la Administración General del **Estado** y sus **Organismos Públicos** serán declarados de **uso compartido** cuando, en razón de su **naturaleza** o del **interés común**, **respondan** a necesidades transversales de un **número significativo** de **unidades administrativas**.

A los efectos de este real decreto, se entenderá por «**medios y servicios**» todas las **actividades, infraestructuras técnicas, instalaciones, aplicaciones, equipos, inmuebles, redes, ficheros electrónicos, licencias y demás activos** que **dan soporte** a los **sistemas de información**.

Los **activos TIC** afectos a la prestación de servicios sectoriales se podrán **mantener** en sus **ámbitos específicos** en razón de la **singularidad competencial y funcional** que atienden y **no** tendrán, por tanto, la **consideración** de **medios y servicios compartidos**.

La **responsabilidad** sobre la **gestión** de estos medios **corresponderá** a los **departamentos ministeriales y organismos adscritos** desarrollada **a través** de las respectivas **unidades TIC** con el **apoyo y supervisión** de la **Dirección de Tecnologías de la Información y las Comunicaciones**.

La **declaración** de **medios y servicios compartidos** necesarios para la ejecución y desarrollo de la Estrategia TIC **aprobada** por el **Gobierno**, **corresponderá** a la **Comisión de Estrategia TIC a propuesta** de la **Dirección de Tecnologías de la Información y las Comunicaciones**.

Cuando concurren **razones económicas, técnicas** o de **oportunidad** sobrevenidas, la **Comisión de Estrategia TIC** podrá **autorizar** al **Director de Tecnologías de la Información y las Comunicaciones** a acordar **excepciones** a la **declaración de medio o servicio de uso compartido**, de las que se dará **traslado** a los miembros de la **Comisión de Estrategia TIC**.

La **utilización** de los **medios y servicios compartidos** será de **carácter obligatorio** y **sustitutivo** respecto a los **medios y servicios** particulares empleados por las distintas **unidades**.

La **Dirección de Tecnologías de la Información y las Comunicaciones** **establecerá** un **Catálogo de Servicios Comunes** del que formarán parte los medios y servicios compartidos, así como aquellas infraestructuras técnicas o aplicaciones desarrolladas por la Dirección de Tecnologías de la Información y las Comunicaciones cuya **provisión** de manera compartida **facilite** la aplicación de **economías** de escala y **contribuya** a la **racionalización y simplificación** de la **actuación administrativa**.

Dentro de **este Catálogo** figurarán **servicios de administración digital** orientados a **integrar** todas las **relaciones** de las **Administraciones públicas** con el **ciudadano**, mediante la provisión compartida, que le permita tener una visión integral de sus relaciones con las Administraciones públicas y acceso a todos los servicios on-line.

La **provisión, explotación y gestión** de los **medios y servicios compartidos** será realizada por la **Dirección de Tecnologías de la Información y las Comunicaciones**, **salvo** los que correspondan a los **servicios de**

informática presupuestaria de la **Intervención General de la Administración del Estado**. Las eficiencias que se produzcan en estos procesos se dedicarán preferentemente a potenciar los servicios sectoriales.

Las **CMAD*** y las **unidades TIC sectoriales** velarán por el **uso** de los **medios** y **servicios compartidos**. En este sentido, cuando las **necesidades** puedan ser **comunes** a **más de 1 área funcional** o **unidad**, del mismo o de distinto ministerio, se **escogerá** la **alternativa** que permita **compartir** el **servicio** entre dichas áreas, **salvo autorización expresa** de la **Dirección de Tecnologías** de la Información y las Comunicaciones.

Proyectos de interés prioritario (Art. 11)

El **Comité de Estrategia TIC** podrá **declarar** como **proyectos** de **interés prioritario** aquellos que tengan una ¹**singular relevancia** y, especialmente, aquellos que tengan como objetivo la ²**colaboración** y **cooperación** con las **comunidades autónomas** y los **entes** que integran la **Administración local** y la **Unión Europea** en materia de **Administración digital**.

Unidades TIC (Art. 12)

Son **unidades TIC** aquellas **unidades administrativas** cuya **función** sea la **provisión** de **servicios** en materia de **Tecnologías de la Información y Comunicaciones** a **sí mismas** o a **otras unidades** administrativas.

Las **unidades TIC**, bajo la dirección de los órganos superiores o directivos a los que se encuentren adscritas, se configuran como **instrumentos fundamentales** para la **implementación** y **desarrollo** de la **Estrategia TIC** y del proceso de **transformación digital** de los ámbitos sectoriales de la Administración General del Estado y sus Organismos Públicos bajo la **coordinación** y **supervisión** de la **Dirección de Tecnologías** de la **Información** y las **Comunicaciones**.

Se entenderá por provisión de **servicios TIC** la **realización** de una o varias de las siguientes **funciones**:

- **Soporte, operación, implementación** y/o **gestión** de **sistemas informáticos corporativos** o de **redes de telecomunicaciones**.
- **Desarrollo** de **aplicativos informáticos** en **entornos multiusuario***.
- **Consultoría informática**.
- **Seguridad** de **sistemas de información**.
- **Atención técnica** a **usuarios**.
- **Innovación** en el **ámbito** de las **TIC**.
- **Administración digital**.
- **Conformar** la **voluntad** de **adquisición** de **bienes** o **servicios** en el ámbito de las tecnologías de la información y las comunicaciones.
- Todas aquellas funciones **no previstas** expresamente en las letras anteriores, que sean **relevantes** en materia de **tecnologías de la información y las comunicaciones**.

Las **unidades TIC adscritas** a los **departamentos** ministeriales o a sus **organismos** adscritos, **impulsarán**, en el marco de la CMAD, la **transformación digital** de los **servicios sectoriales en sus ámbitos**.

La **Dirección de Tecnologías de la Información** y las **Comunicaciones** **propondrá** a los **órganos competentes**, las **áreas administrativas** que **deban ser atendidas** por las **unidades TIC** de manera que **se adapten** a las **nuevas necesidades** derivadas de la declaración de medios o servicios compartidos con el fin de **mejorar** la **eficiencia** y **operatividad** en la **prestación** de sus **servicios**.

Las **unidades TIC** deberán llevar a cabo dicha transformación **identificando** las **oportunidades** que les **permitan sacar** el **máximo rendimiento** a las TIC de acuerdo a las necesidades funcionales determinadas por las áreas administrativas a las que prestan sus servicios.