Tema 23

Tecnologías de la información y la comunicación

DISPOSICIONES GENERALES (Tít. 1)

Objeto y ámbito de aplicación de la Ley (Art. 1)

El objeto de esta ley es la **regulación** de las **telecomunicaciones**, que comprende la [1]**instalación** y **explotación** de las **redes** de **comunicaciones electrónicas**, la [2]**prestación** de los **servicios** de **comunicaciones electrónicas**, sus **recursos** y **servicios asociados**, los **equipos radioeléctricos** y los **equipos terminales** de **telecomunicación**, de conformidad con el art. 149.1.21ª de la Constitución.

En particular, esta ley es de **aplicación** al **dominio público radioeléctrico utilizado** por parte de **todas** las **redes de comunicaciones electrónicas**, ya sean **públicas** o **no**, y con independencia del servicio que haga uso del mismo.

Quedan **excluidos** del ámbito de esta ley los [1]**servicios** de **comunicación audiovisual**, los [2]**servicios** de **intercambio de vídeos** a través de **plataforma**, los [3]**contenidos audiovisuales** transmitidos a través de las **redes**, así como el [4]**régimen básico** de los **medios de comunicación social** de **naturaleza audiovisual** a que se refiere el artículo 149.1.27.ª de la Constitución.

Asimismo, se **excluyen** del ámbito de esta ley los [5]**servicios** que **suministren contenidos** transmitidos mediante **redes** y **servicios** de **comunicaciones electrónicas**, las [6]**actividades** que consistan en el ejercicio del **control editorial** sobre dichos **contenidos** y los [7]**servicios** de la **Sociedad de la Información**, regulados en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en tanto en cuanto **no** sean asimismo **servicios** de **comunicaciones electrónicas**.

Las telecomunicaciones como servicios de interés general (Art. 2)

Las **telecomunicaciones** son **servicios** de **interés general** que se prestan en **régimen** de **libre competencia**.

Objetivos y principios de la ley (Art. 3)

Los **objetivos** y **principios** de esta ley son los siguientes:

- **Fomentar** la **competencia efectiva** y **sostenible** en los mercados de **telecomunicaciones** para **potenciar** al máximo los **intereses** y **beneficios** para las **empresas** y los **consumidores**, principalmente en términos de [1]**bajada** de los **precios**, [2]**calidad** de los **servicios**, [3]**variedad** de **elección** e **innovación**, teniendo debidamente **en cuenta** la variedad de **condiciones** en cuanto a la **competencia** y los **consumidores** que existen en las distintas **áreas geográficas**, y velando por que **no** exista **falseamiento** ni **restricción** de la competencia en la **explotación de redes** o en la prestación de **servicios de comunicaciones electrónicas**, incluida la transmisión de contenidos:
- **Desarrollar** la **economía** y el **empleo digital**, **promover** el **desarrollo** del sector de las **telecomunicaciones** y de todos los **nuevos servicios digitales** que las nuevas **redes** de alta y muy alta capacidad **permiten**, **impulsando** la **cohesión social** y **territorial**, mediante la **mejora** y **extensión** de las **redes**, especialmente las de **muy alta capacidad**, así como la **prestación** de los **servicios de comunicaciones electrónicas** y el **suministro** de los **recursos asociados** a ellas;
- **Promover**, en aras a la consecución del fin de interés general que supone, el **despliegue de redes** y la **prestación** de **servicios de comunicaciones electrónicas**, **fomentando** la [1]**conectividad**, el [2]**acceso** a las **redes** de **muy alta capacidad**, incluidas las **redes fijas**, **móviles** e **inalámbricas** y la [3]**interoperabilidad** de **extremo a extremo**, en condiciones de **igualdad** y **no discriminación**;
- **Impulsar** la **innovación** en el **despliegue de redes** y la **prestación** de **servicios de comunicaciones**, en aras a garantizar el **servicio universal** y la **reducción de la desigualdad** en el **acceso** a **internet** y las **Tecnologías de la Información y la Comunicación** (TIC), con especial consideración al **despliegue de redes** y **servicios a la ciudadanía** vinculados a la **mejora** del [1]**acceso funcional a internet**, del [2]**teletrabajo**, del [3]**medioambiente**, de la [4]**salud** y la **seguridad públicas** y de la [5]**protección civil**; así como cuando **faciliten** la **vertebración** y **cohesión social** y **territorial** o contribuyan a la **sostenibilidad** de la **logística urbana**.
- Promover el **desarrollo** de la **ingeniería**, así como de la **industria de productos** y **equipos de telecomunicaciones**;

- Contribuir al **desarrollo** del **mercado interior** de **servicios de comunicaciones electrónicas** en la **Unión Europea**, **facilitando** la convergencia de las condiciones que permitan la **inversión** en **redes de comunicaciones electrónicas** y en su **suministro**, en **servicios de comunicaciones electrónicas**, en **recursos asociados** y **servicios asociados** en toda la **Unión**;
- **Promover** la **inversión eficiente** en materia de **infraestructuras**, especialmente en las **redes** de **muy alta capacidad**, **incluyendo**, cuando proceda y con carácter prioritario, la **competencia** basada en **infraestructuras**, **reduciendo** progresivamente la **intervención ex ante** en los **mercados**, **posibilitando** la **coinversión** y el **uso compartido** y **fomentando** la **innovación**, teniendo debidamente en cuenta los riesgos en que incurren las empresas inversoras;
- Hacer posible el **uso eficaz** y **eficiente** de los **recursos limitados** de **telecomunicaciones**, como la **numeración** y el **espectro radioeléctrico**, la adecuada **protección** de este último, y el **acceso** a los **derechos de ocupación** de la **propiedad pública** y **privada**;
- **Fomentar** la **neutralidad tecnológica** en la regulación;
- **Garantizar** el **cumplimiento** de las obligaciones de **servicio público** en la **explotación de redes** y la **prestación** de **servicios** de **comunicaciones electrónicas** a las que se refiere el título III, en especial las de **servicio universal**;
- **Defender** los **intereses** de los **usuarios**, asegurando su **derecho** al **acceso** a los **servicios** de **comunicaciones electrónicas** en **condiciones** adecuadas de **elección**, **precio** y **buena calidad**, promoviendo la **capacidad** de los **usuarios finales** para **acceder** y **distribuir** la **información** o utilizar las aplicaciones y los servicios de su elección, en particular a través de un **acceso abierto** a **internet**.
- **Salvaguardar** y **proteger** en los **mercados** de telecomunicaciones la **satisfacción** de las **necesidades** de **grupos sociales específicos**, las **personas con discapacidad**, las **personas mayores**, las personas **en situación de dependencia** y usuarios **con necesidades sociales especiales**, atendiendo a los **principios** de **igualdad de oportunidades** y **no discriminación**.
- **Impulsar** la **universalización** del **acceso** a las **redes** y **servicios** de **comunicaciones electrónicas** de **banda ancha** y contribuir a alcanzar la **mayor vertebración territorial** y **social** posible mediante el **despliegue de redes** y la **prestación** de **servicios de comunicaciones electrónicas** en las distintas zonas del **territorio español**.

Servicios de telecomunicaciones para la seguridad nacional, la defensa nacional, la seguridad pública, la seguridad vial y la protección civil (Art. 4)

Sólo tienen la **consideración** de **servicio público** los **servicios** regulados en **este artículo**.

Las **redes**, **servicios**, **instalaciones** y **equipos de telecomunicaciones** que desarrollen **actividades esenciales** para la **seguridad** y **defensa nacionales** integran los medios destinados a éstas, se **reservan** al **Estado** y se **rigen** por su **normativa específica**.

El **Ministerio de Asuntos Económicos y Transformación Digital** es el **órgano** de la **Administración General del Estado** con competencia, para **ejecutar**, en la medida en que le afecte, la **política de defensa nacional** en el sector de las **telecomunicaciones**, con la debida **coordinación** con el **Ministerio de Defensa** y siguiendo los **criterios** fijados por éste.

En el marco de las **funciones** relacionadas con la **defensa civil**, **corresponde** al **Ministerio de Asuntos Económicos y Transformación Digital** **estudiar**, **planear**, **programar**, **proponer** y **ejecutar** cuantas **medidas** se relacionen con su aportación a la **defensa nacional** en el ámbito de las **telecomunicaciones**.

A tales efectos, los **Ministerios** de **Defensa** y de **Asuntos Económicos y Transformación Digital** **coordinarán** la **planificación** del **sistema de telecomunicaciones** de las **Fuerzas Armadas**, a fin de **asegurar**, en la medida de lo posible, su **compatibilidad** con los **servicios civiles**. Asimismo, **elaborarán** los **programas de coordinación tecnológica** precisos que faciliten la **armonización**, **homologación** y **utilización**, conjunta o indistinta, de los **medios**, **sistemas** y **redes civiles** y **militares** en el ámbito de las telecomunicaciones.

En los ámbitos del **orden público**, la **seguridad pública**, **seguridad vial** y de la **protección civil**, en su específica relación con el uso de las telecomunicaciones, el **Ministerio de Asuntos Económicos y Transformación Digital** **cooperará con** el **Ministerio del Interior** y con los **órganos responsables** de las **Comunidades Autónomas** con **competencias** sobre las citadas materias.

Los **bienes muebles** o **inmuebles vinculados** a los **centros**, **establecimientos** y **dependencias** afectos a la **instalación** y **explotación** de las **redes** y a la **prestación** de los **servicios de comunicaciones electrónicas** dispondrán de las **medidas** y **sistemas** de **seguridad**, **vigilancia**, **difusión de información**, **prevención de riesgos** y **protección** que se **determinen** por el **Gobierno**, a **propuesta** de los **Ministerios** de **Defensa**, del **Interior** o de **Asuntos Económicos y Transformación Digital**,

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 ningún caso esta **intervención** podrá suponer una **vulneración** de los **derechos fundamentales** y **libertades públicas** reconocidas en el **ordenamiento jurídico**.

Asimismo, en el caso de **incumplimiento** de las **obligaciones** de **servicio público** a las que se refiere el título 3, el **Gobierno**, previo **informe preceptivo** de la **Comisión Nacional de los Mercados** y la **Competencia**, e igualmente 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**.

Los **acuerdos** de [1]**asunción** de la **gestión directa** del **servicio** y de [2]**intervención** de este o los de [3]**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**.

La **regulación** contenida en esta **ley** 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**.

SALVAGUARDIA DE DERECHOS FUNDAMENTALES, SECRETO DE LAS COMUNICACIONES Y PROTECCIÓN DE LOS DATOS PERSONALES Y DERECHOS Y OBLIGACIONES DE CARÁCTER PÚBLICO VINCULADOS CON LAS REDES Y SERVICIOS DE COMUNICACIONES ELECTRÓNICAS. (Cap. 3)

Salvaguardia de derechos fundamentales (Art. 56)

Las **medidas** que se adopten en relación al **acceso** o al **uso** por parte de los **usuarios finales** de los **servicios** y las **aplicaciones** a través de redes de comunicaciones electrónicas **respetarán** los **derechos** y **libertades fundamentales**, como queda **garantizado** en el [1]**Convenio Europeo** para la **Protección de los Derechos Humanos** y de las **Libertades Fundamentales**, en la [2]**Carta de Derechos Fundamentales** de la Unión Europea, en los [3]**principios generales** del **Derecho comunitario** y en la **Constitución Española**.

Cualquiera de esas **medidas** relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas, que sea **susceptible** de **restringir** esos **derechos** y **libertades fundamentales** solo podrá **imponerse** si es **adecuada**, **necesaria** y **proporcionada** en una **sociedad democrática**, y su **aplicación** está **sujeta** a las **salvaguardias de procedimiento** apropiadas de conformidad con las normas mencionadas en el apartado anterior. Por tanto, dichas medidas **solo** podrán ser **adoptadas respetando** debidamente el [1]**principio** de **presunción de inocencia**, el [2]**derecho** a la **vida privada** e **intimidad**, el [3]**derecho** a la **libertad de expresión** e **información** y el [4]**derecho** a la **tutela judicial efectiva**,

Principio de no discriminación (Art. 57)

Los **operadores** que **instalen** o **exploten redes públicas** de comunicaciones electrónicas o que **presten servicios** de comunicaciones electrónicas disponibles al público **no aplicarán** a los **usuarios finales** ningún

requisito diferente ni **condiciones generales** de **acceso** o **uso** de redes o servicios ni de **utilización** de los mismos por **motivos** relacionados con la [1]**nacionalidad**, el [2]**lugar de residencia** o el [3]**lugar** de **establecimiento del usuario final**, a menos que dicho trato diferente se justifique de forma objetiva.

Secreto de las comunicaciones (Art. 58)

Los **operadores** que **suministren redes públicas** de **comunicaciones electrónicas** o que **presten servicios** de comunicaciones electrónicas disponibles al público deberán **garantizar** el **secreto de las comunicaciones** de conformidad con los art. 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

Los **operadores** que **suministren redes públicas** de comunicaciones electrónicas o que **presten servicios** de **comunicaciones interpersonales** basados en **numeración disponibles al público** o **servicios** de **acceso a internet** están **obligados** a realizar las **interceptaciones** que se autoricen judicialmente

La **interceptación** a que se refiere el apartado anterior deberá **facilitarse** para cualquier **comunicación** que tenga como origen o destino el **punto de terminación** de **red** o el **terminal específico** que se determine **a partir de** la **orden de interceptación legal**, **incluso** aunque esté **destinada** a **dispositivo de almacenamiento** o **procesamiento de la información**; asimismo, la **interceptación** podrá realizarse sobre un **terminal conocido** y con unos **datos de ubicación temporal** para comunicaciones desde locales públicos. Cuando **no** exista una **vinculación fija** entre el **sujeto** de la interceptación y el **terminal** utilizado, éste podrá ser **determinado** dinámicamente cuando el **sujeto** de la interceptación **lo active** para la comunicación mediante un **código de identificación personal**.

El **acceso** se facilitará para **todo tipo** de **comunicaciones electrónicas** disponibles al público **distintas** de las **comunicaciones interpersonales independientes** de la **numeración**, en particular, por su **penetración** y **cobertura**, para las que se realicen mediante **cualquier modalidad** de los servicios de **telefonía** y de **transmisión de datos**, se trate de comunicaciones de **vídeo**, **audio**, **intercambio** de **mensajes**, **ficheros** o de la **transmisión de facsímiles**.

El **acceso facilitado** servirá tanto para la **supervisión** como para la **transmisión** a los **centros de recepción** de las interceptaciones de la comunicación electrónica interceptada y la **información relativa** a la interceptación, y **permitirá obtener** la **señal** con la que se realiza la comunicación.

Los **sujetos obligados** deberán **facilitar** al **agente facultado**, salvo que por las características del servicio no estén a su disposición, los **datos** indicados en la **orden de interceptación legal**, de entre los que se relacionan a continuación:

- **Identidad** o identidades del **sujeto** objeto de la **medida** de la interceptación. Se entiende por **identidad**: **etiqueta técnica** que puede representar el **origen** o el **destino** de cualquier **tráfico** de comunicaciones electrónicas, en general **identificada** mediante un **número de identidad** de **comunicaciones electrónicas físico** (tal como un número de teléfono) o un **código de identidad** de **comunicaciones electrónicas lógico** o **virtual** (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

  Los **sujetos obligados proporcionarán**, cuando técnicamente sea posible, los **identificadores permanentes** que sean necesarios para la **atribución** de un **servicio** a un **usuario** determinado de forma inequívoca, así como los **identificadores** del **dispositivo empleado** para la **comunicación**. **Identidad** o identidades de las **otras partes** involucradas en la comunicación electrónica;

- **Servicios básicos** utilizados;
- **Servicios suplementarios** utilizados;
- **Dirección** de la **comunicación**;
- **Indicación** de **respuesta**;
- **Causa** de **finalización**;
- **Marcas temporales**;
- **Información** de **localización**;

- **Información intercambiada** a través del **canal de control** o **señalización**.

Además de la información relativa a la interceptación prevista en el apartado anterior, los **sujetos obligados** deberán **facilitar** al **agente facultado**, salvo que por las características del servicio no estén a su disposición, de **cualquiera** de las **partes** que **intervengan** en la comunicación que sean **clientes** del **sujeto obligado**, los siguientes **datos**:

- **Identificación** de la **persona física** o **jurídica**;
- **Domicilio** en el que el operador realiza las **notificaciones**; y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:
- **Número** de **titular** de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado);
- **Número** de identificación del **terminal**;
- **Número** de **cuenta** asignada por el proveedor de servicios internet;
- **Dirección** de **correo electrónico**.

Junto con los datos previstos en los apartados anteriores, los **sujetos obligados** deberán **facilitar**, salvo que por las características del servicio no esté a su disposición, **información** de la **situación geográfica** del **terminal** o **punto de terminación** de red **origen** de la llamada, y de la del **destino de la llamada**. En caso de **servicios móviles**, se proporcionará una **posición** lo **más exacta posible** del **punto de comunicación** y, en todo caso, la **identificación**, **localización** y **tipo** de la **estación base** afectada.

Los **sujetos obligados** deberán **facilitar** al agente facultado, de entre los datos previstos en los apdos. 5, 6 y 7 de este artículo, **sólo** aquéllos que estén **incluidos** en la **orden de interceptación legal**.

Con carácter **previo** a la **ejecución** de la **orden de interceptación legal**, los **sujetos** obligados deberán **facilitar** al **agente** facultado **información** sobre los **servicios** y **características** del **sistema de telecomunicación** que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes **nombres** de los **abonados** con sus **números** de **documento nacional de identidad**, **tarjeta de identidad de extranjero** o **pasaporte**, en el caso de personas físicas, o denominación y **número** de **identificación fiscal** en el caso de **personas jurídicas**.

Los **sujetos obligados** deberán tener en todo momento **preparadas una** o **más interfaces** a través de las cuales las **comunicaciones electrónicas interceptadas** y la **información** relativa a la interceptación se **transmitirán** a los **centros de recepción** de las **interceptaciones**. Las **características** de estas **interfaces** y el **formato** para la **transmisión** de las comunicaciones interceptadas a estos centros estarán **sujetas** a las **especificaciones técnicas** que se establezcan por el **Ministerio de Asuntos Económicos y Transformación** Digital.

En el caso de que los **sujetos obligados apliquen** a las comunicaciones objeto de interceptación legal algún **procedimiento** de **compresión**, **cifrado**, **digitalización** o cualquier **otro tipo** de codificación, deberán **entregar** aquellas **desprovistas** de los efectos de tales **procedimientos**, siempre que sean **reversibles**.

Las **comunicaciones interceptadas** deben proveerse al centro de recepción de las interceptaciones con una **calidad no inferior** a la que **obtiene** el **destinatario** de la **comunicación**.

Interceptación de las comunicaciones electrónicas por los servicios técnicos. (Art. 59)

Cuando para la **realización** de las tareas de **control** para la eficaz utilización del **dominio público radioeléctrico** o para la **localización** de **interferencias perjudiciales** sea necesaria la utilización de **equipos**, **infraestructuras** e **instalaciones técnicas** de **interceptación de señales** no dirigidas al público en general, será de **aplicación** lo siguiente:

- La **administración** de las telecomunicaciones deberá diseñar y establecer sus **sistemas técnicos** de **interceptación de señales** en forma tal que se **reduzca** al mínimo el **riesgo** de **afectar** a los **contenidos** de las comunicaciones;

- 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 concurran **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.

Cooperación interadministrativa (Art. 13)

La **Dirección de Tecnologías** de la Información y las Comunicaciones **propondrá** a la **Secretaría de Estado de Administraciones Públicas** las [1]**líneas de actuación**, [2]**orientaciones comunes** y la [3]**creación de órganos de cooperación** necesarios para favorecer el **intercambio** de **ideas**, **estándares**, **tecnología** y **proyectos** orientados a **garantizar** la **interoperabilidad** y **mejorar** la **eficacia** y **eficiencia** en la prestación de los **servicios públicos** de las distintas **Administraciones Públicas**, que serán **tratadas** en la **Conferencia Sectorial** de Administraciones Públicas, en cuyo seno se establecerán.

PRINCIPIOS Y RECOMENDACIONES BÁSICAS EN CIBERSEGURIDAD DEL CCNCERT

Sobre CNN-CERT (Nº 1)

El **CCN-CERT** es la **Capacidad de Respuesta a Incidentes de Seguridad de la Información** del **Centro Criptológic Nacional**. Este servicio **se creó** en el año **2006** como el **CERT Gubernamental/Nacional español** y sus **funciones** quedan recogidas en la **Ley 11/2002** reguladora del Centro Nacional de Inteligencia, el **RD 421/2004** regulador del CCN y en el **RD 3/2010**, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), **modificado** por el **RD 951/2015**, de 23 de octubre.

De acuerdo a todas ellas, es **competencia** del **CCN-CERT** la **gestión** de **ciberincidentes*** que **afecten** a [1]**sistemas** del **Sector público**, a [2]**empresas** y **organizaciones** de **interés estratégico** para el **país** y a cualquier [3]**sistema clasificado**.

Su **misión** es contribuir a la **mejora** de la **ciberseguridad** española, siendo el **centro de alerta** y **respuesta nacional** que coopere y ayude a **responder** de forma **rápida** y **eficiente** a los **ciberataques** y a **afrontar** de forma **activa** las **ciberamenazas**.

Introducción (Nº 2)

La **concienciación**, el **sentido común** y las **buenas prácticas** son las **mejores defensas** para **prevenir** y **detectar contratiempos** en la **utilización** de sistemas de las Tecnologías de la Información y la Comunicación (**TIC**).

Se puede decir que **no existe** un **Sistema** que **garantice** al **100**% la **seguridad** del **servicio** que presta y la **información** que maneja **debido**, en gran medida, a las [1]**vulnerabilidades** que presentan las **tecnologías** y lo que es más importante, la [2]**imposibilidad** de disponer de los suficientes **recursos** para hacerlas frente.

Por tanto, siempre hay que **aceptar** un riesgo; el conocido como **riesgo residual**, asumiendo un **compromiso** entre el **nivel de seguridad**, los **recursos disponibles** y la **funcionalidad deseada**.

La **implementación de seguridad** supone **planificar** y **tener en cuenta** los **elementos** siguientes:

- **Análisis de Riesgos**. **Estudiar** los **posibles riesgos** y **valorar** las **consecuencias** de los mismos sobre los **activos**. (Información y servicio)
- **Gestión de Riesgos**. **Valorar** las diferentes **medidas** de **protección** y **decidir** la **solución** que más se adecue a la entidad. (Determinación del riesgo residual).
- **Gobernanza**. **Adaptar** la **operativa habitual** de la **entidad** a las **medidas de seguridad**.
- **Vigilancia**. **Observación continua** de las **medidas de seguridad**, así como la **adecuación** de las mismas a la aparición de **nuevas tecnologías**.
- **Planes de Contingencia**. **Determinación** de las **medidas** a adoptar ante un **incidente** de **seguridad**. La **combinación** de estas prácticas ayuda a **proporcionar** el **nivel** de **protección mínima** para mantener los datos a salvo.

Factores de amenaza (Nº 3)

La **generalización** del **uso** de los **medios electrónicos** en el normal desenvolvimiento de la sociedad **ha incrementado** la superficie de **exposición a ataques** y, **en consecuencia**, los **beneficios potenciales** derivados, lo que **constituye** sin duda uno de los **mayores estímulos** para los **atacantes**.

En los **últimos años** se ha mantenido la tendencia, **incrementándose** el **número**, **tipología** y **gravedad** de los **ataques** contra los **sistemas de información** del Sector público, de las empresas e instituciones de interés estratégico o de aquellas poseedoras de importantes activos de propiedad intelectual e industrial y, en general, contra todo tipo de entidades y ciudadanos.

Siguen estando **presentes** las acciones de **Ciberespionaje**, consistente en **ciberataques** originados o patrocinados por **Estados** y perpetrados **por ellos mismos** o por otros **actores a sueldo**, y siempre con la **intención** de **apropiarse** de **información sensible** o **valiosa** desde los puntos de vista [1]**político**, [2]**estratégico**, de [3]**seguridad** o [4]**económico**. El **ciberespionaje** presenta las siguientes **características** generales:

- **Origen** en **Estados**, **industrias** o **empresas**.
- **Utilización**, generalmente, de **ataques dirigidos** (Amenazas Persistentes Avanzadas).
- **Realizado contra** los **sectores público** (información política o estratégica) y **privado** (información económicamente valiosa).
- Con una **enorme dificultad** de **atribución**.
- **Persiguiendo obtener ventajas políticas**, **económicas**, **estratégicas** o **sociales**.

La **seguridad** en sus **actividades** hace **más difícil analizar** estos **ataques**. De hecho, en los últimos años las **tácticas**, **técnicas** y **procedimientos** han **evidenciado** una creciente **profesionalización** mostrando con claridad un **nuevo tipo** de comportamiento **delictivo crime-as-a-service**. Este pone a disposición de terceros la **posibilidad** de desarrollar **ciberataques** de **alto impacto** y, generalmente, con el **objetivo** de obtener **beneficios económicos ilícitos**.

Otro elemento a tener en cuenta es la **utilización** del **ciberespacio** en la **denominada Guerra Híbrida**, que mediante la **combinación** de diferentes **tácticas** busca **desestabilizar** y **polarizar** la **sociedad** de los **estados evitando** el **conflicto armado**. A efectos de **categorizar** la **amenaza**, la figura siguiente muestra la **Pirámide del Daño**, atendiendo a la **mayor** o **menor peligrosidad** de las **ciberamenazas**, según sea su origen.

Los ataques (APT)

Los **ciberataques** se han convertido en una **alternativa real** a las **herramientas convencionales de inteligencia**, debido a su [1]**bajo coste**, a la [2]**dificultad de probar su autoría** y al importante [3]**volumen de información** que puede ser obtenido por esta vía.

Los **grupos APT*** **buscan recabar** la mayor cantidad de **información** posible y útil de la **víctima**, con el objetivo de **preparar** un **ataque** lo más efectivo posible.

Los **parámetros** que **caracterizan** las **APT** se basan en:

- **Capacidad de desarrollo**: **exploits*** y **vulnerabilidades** utilizadas.
- **Persistencia**: tras **reinicios**, **actualizaciones** e incluso actividades de **formateo**.
- **Cifrado**: **métodos de cifrado** y **fortaleza de claves** para intercambiar la información exfiltrada.
- **Técnicas exfiltración**: **protocolos** utilizados para la **extracción** de **información**.
- **Ocultación**: técnicas de **rootkit*** utilizadas para **ocultarse**.
- **Resistencia a ingeniería inversa**: **técnicas** que **dificultan** el **análisis** del **código**.

La **información exfiltrada**, en función de la **motivación** de los **atacantes**, puede ser de índole muy **variada**: **económica**, **sensible**, **propiedad intelectual**, **secretos industriales** o de **estado**, etc.

La internet profunda (Nº 4)

Internet se ha visto **dividida** en la Internet **profunda*** y la **superficial**. La [1]**superficial** se compone de **páginas estáticas** o **fijas**, mientras que la [2]**web profunda** está compuesta de **páginas dinámicas** donde el **contenido** se **coloca** en una **base** de **datos** que se **proporciona** a **petición** del **usuario**.

La **principal razón** de la **existencia** de la **Internet profunda** es la **imposibilidad** para los **motores de búsqueda** (**Google**, **Bing**, etc.) de **encontrar** gran parte de la **información** existente en ella.

Un **subconjunto** de la **Internet profunda** sólo es **accesible** utilizando **determinados navegadores** web. Además, los **usuarios** han de **conocer** previamente la **dirección** a la que han de dirigirse.

La red TOR

The Onion Router (**TOR**): es un **proyecto** diseñado e implementado por la **Marina** de los **EEUU** con el fin de **fortalecer** las **comunicaciones** por **Internet** y **garantizar** el **anonimato** y la **privacidad**.

TOR permite a los usuarios **navegar** por la **web** de forma **anónima**. Los **datos no viajan** de forma **directa** sino **a través** de **varios nodos** que **facilitan** el **anonimato** de las **comunicaciones**. Existe un **directorio** de **nodos intermedios** con las **claves públicas asociadas** para poder **establecer** la **comunicación cifrada**.

TOR se encarga de **crear circuitos virtuales compuestos** por **3 nodos aleatoriamente** escogidos de su **red**. De manera que la **comunicación** entre **origen**, nuestro **equipo** y el **destino**, por ejemplo, una web, ha de **recorrer** los **3 nodos asignados**, a través de los cuales la información se transmitirá de **forma cifrada**.

El **elemento origen cifra** la **comunicación** con la **clave pública** del **último nodo** de la **ruta elegida** para que de esta **forma** sea el **único elemento** que pueda **descifrar** el **mensaje** y las **instrucciones** (nodos intermedios y sus claves públicas asociadas) para **llegar al destino**.

Se **eligen rutas aleatorias** donde los **datos** se **cifran** en **capas** y una vez que la **última capa** es tratada por un **nodo de salida**, se lleva a cabo la **conexión** con la **página web destino**.

Bitcoin

El **bitcoin** es una **moneda electrónica cifrada**, **descentralizada**, de **ordenador a ordenador**, donde el **control** se realiza, de forma **indirecta**, por los propios **usuarios a través** de **intercambios P2P***.

En lugar de acuñar una **moneda** o imprimir un **billete**, se **utiliza** una **cadena** de **caracteres criptográficos** que se **intercambian** a través de **billeteras digitales** (wallets) entre el **usuario** y el **vendedor** (intercambios P2P), lo que hace que esté **fuera** del **control** de cualquier **gobierno**, **institución** o **entidad financiera**.

Cada **transacción** con bitcoins se **registra** en una **gran base de datos** llamada **"BlockChain"***. Los **datos** se **guardan** en **bloques** y **cada bloque** nuevo debe **contener** el **hash** del **bloque anterior**. Por lo tanto, **cada bloque nuevo** que se une a la cadena **posee todo** el **historial** de la **transacción**.

Este **protocolo** se **sustenta** sobre una **red** de "**mineros**" que **controlan** la **moneda**. Los **mineros ponen** a **disposición** de la **red recursos de cómputo** y como **recompensa**, **reciben bitcoins**. Estos **mineros protegen** al **sistema** para que **no** haya transacciones de **anulación** (devolución de dinero ya gastado).

Esta **moneda** es **internacional**, **fácil de utilizar**, permite transacciones de forma **anónima** y como **riesgos**, representa un **mecanismo** muy práctico para **blanquear dinero** y **evadir impuestos** (exención fiscal).

Aplicaciones (Nº 5)

La **instalación** de **programas** puede **afectar** al **rendimiento** y la **seguridad** de los **dispositivos/equipos**. Debe mantenerse la integridad de los mismos y siempre hay que **instalar software autorizado** y **proporcionado** directamente por el **fabricante**.

Hay que tener en cuenta lo siguiente para **garantizar** la **seguridad** de nuestras **aplicaciones**:

- El **empleo** de **software legal** ofrece **garantía** y **soporte**, con independencia de las implicaciones legales de utilizar software no legítimo.
- **Certificación** del **programa** para su **compatibilidad** con el **sistema operativo** y las demás aplicaciones.
- **Instalación** y **mantenimiento** de **parches** y **actualizaciones** de **seguridad**, con especial atención a aquellas de **carácter crítico** (en los últimos meses la no actualización de los programas ha provocado numerosas brechas de seguridad).

- **Considerar** la superficie de **exposición asociada** a los **sistemas heredados** (legacy), **especialmente** aquellos que tienen **más** de una **década** de **antigüedad** por su **extremada vulnerabilidad**.

Los usuarios deben ser conscientes de que la **introducción** de **software no autorizado** puede causar la **infección** del **sistema más protegido**. Como **buenas prácticas** se indica lo siguiente:

- **Trabajar** habitualmente en el sistema como **usuario sin privilegios**, **no** como "**administrador**".
- **No ejecutar** nunca **programas** de **origen dudoso** o **desconocido**.
- Si se **emplea** un paquete de **software ofimático** capaz de **ejecutar macros**, hay que **asegurarse** de que esté **desactivada** su **ejecución automática**.

En cuanto a la **impresión** de **documentos**, hay que ser conscientes de que los **documentos** y **transacciones impresas** son **susceptibles** de **violaciones** de la **seguridad**.

Por lo tanto, resulta **fundamental** emplear **buenas prácticas** para **cumplir** la **normativa** existente en cada entidad y que la **información impresa** sea **segura** y **no accesible** por **personal no autorizado**.

Cifrado de datos

Cifrar los **datos** significa **convertir texto plano** en **texto ilegible**, **denominado texto cifrado**, **evitando** que la **información** sea **accesible por terceros no autorizados**. Para lo cual, **se necesita** de un **algoritmo de cifrado** y la existencia de una **clave**, que **permite** realizar el proceso de **transformación** de los **datos** y que debe **mantenerse** en **secreto**.

Existen múltiples **soluciones comerciales** para **cifrar** los **equipos informáticos**, clasificables en **3 tipos** atendiendo al **nivel** en el que actúan en el **sistema de archivos**:

- **Cifrado** de **disco**: es una tecnología que **cifra** el **disco** por **completo**, de esta manera el **sistema operativo** se **encarga** de **descifrar** la **información** cuando el **usuario** la **solicita**.
- **Cifrado** de **carpetas**: el cifrado se realiza a **nivel** de **carpeta**. El **sistema de cifrado** se **encargará** de **cifrar** y **descifrar** la **información** cuando se **utiliza** la **carpeta protegida**.
- **Cifrado** de **documentos**: el **sistema** se encarga de **mostrar** y **permitir** el **acceso** al **documento** solo para los usuarios **autorizados**, haciendo **ilegible** el contenido a los **no autorizados**.

Cortafuegos personales

Los **cortafuegos personales** son **programas** que **monitorizan** las **conexiones entrantes** y **salientes** del **equipo**. Están diseñados para **bloquear** el **acceso no autorizado** al mismo, pero **permitiendo** al mismo tiempo las **comunicaciones autorizadas**.

Lo **más complicado** de un **cortafuegos** es **configurarlo correctamente**, de modo que **no** se **bloqueen** las **conexiones legítimas** (navegación web, actualizaciones, correo electrónico, etc.).

Como criterio genérico, **no** se deben **permitir** las **conexiones** de fuentes **desconocidas**. Por tanto, deben **bloquear** todas las **conexiones entrantes** y sólo **permitir** aquellas que **se indiquen expresamente** sobre la base de un conjunto de normas y criterios establecidos. Un **cortafuegos** correctamente configurado **añade** una **protección** necesaria que **dificulta** los **movimientos laterales no autorizados** por la **red**, pero que **en ningún caso** debe **considerarse** como **suficiente**.

Aplicaciones antimalware

Entre las **acciones** que puede provocar un **código malicioso** o **malware** se encuentran: [1]**borrado** o [2]**alteración** de **archivos**, [3]**consumo** de **recursos** del equipo, [4]**acceso no autorizado** a archivos, [5]**infección remota** de los equipos, etc.

Las **funciones mínimas** que se pueden esperar en una herramienta **antimalware** (antivirus) son:

- **Filtrado entrante** y **saliente** de **contenidos maliciosos**.

- **Protección** en el **correo electrónico**, en la **navegación** y en las **conexiones** de todo tipo.
- **Analizar** los **ficheros** en **dispositivos removibles** como **discos externos** o **memorias USB**.
- Permitir **programar análisis exhaustivos** cada cierto tiempo.

Las **aplicaciones antimalware** deben disponer de **actualizaciones** y **ser productos** de **casas comerciales de confianza** que permitan una combinación de los siguientes **métodos**:

- Escáner de **acceso**: permite **examinar** los **archivos** cuando son **abiertos**.
- Escáner a **demanda**: **análisis** en base a un **calendario establecido**.
- Escáner de **correos electrónicos**: en dispositivos de **protección de perímetro** o **servidores de correo**.
- **Control de firmas**: permite **detectar cambios no legítimos** en el contenido de un **archivo**.
- **Métodos heurísticos**: **búsqueda** de **anomalías** en los **archivos** y **procesos** en base a experiencias previas de comportamiento del malware.

Pero una **aplicación antimalware** sola **no** es **suficiente**; hay que proporcionar un **enfoque centralizado** (cliente-servidor) para **proteger** todos los **puntos finales** (servidores, sobremesas, portátiles, teléfonos inteligentes, etc.) **conectados** a la **red**. Algunos **proveedores** ofrecen **sistemas** de **Endpoint Security*** que incluyen **antivirus**, **cortafuegos** y **otro software** de seguridad.

Borrado seguro de datos

Se puede pensar que un simple formateo del disco duro impedirá que los datos almacenados en el mismo puedan ser recuperados. Sin embargo, **hay aplicaciones** que **permiten deshacer** el **formateo** de una **unidad** existiendo **incluso métodos** para **recuperar** los **datos** de los **discos**, **aunque** estos hayan sido **sobrescritos**.

Si se quiere **garantizar** que **no** se está **distribuyendo información sensible**, se deben **sobrescribir** los **datos** siguiendo un método (**patrón de borrado**) que **no permita** su **recuperación** de modo alguno.

Para tal fin, es necesario **realizar diversas pasadas de escritura** sobre cada uno de los sectores **donde** se **almacena** la **información**.

En el caso de **fotografías digitales**, archivos de **audio** o **vídeo** y **documentos ofimáticos** existen **metadatos*** que pueden **almacenar información oculta** y **no visible usando** la configuración estándar de las **aplicaciones**, necesitando de una **configuración específica** o incluso un **software concreto** para **revelar** esos **datos**.

Estos **metadatos** son útiles ya que **facilitan** la **búsqueda** de **información**, **posibilitan** la **interoperabilidad** entre **organizaciones**, **proveen** la **identificación digital** y **dan soporte** a la **gestión** del ciclo de vida de los **documentos**.

Sin embargo, el **borrado** de **metadatos** o **datos ocultos** mediante **procedimientos** y **herramientas** de **revisión** y **limpieza** de **documentos/archivos** es fundamental para **minimizar** el **riesgo** de que se **revele información sensible** en el almacenamiento e intercambio de información.

Navegación segura (Nº 6)

La **comunicación** en **Internet** se sustenta en una **idea básica**: **clientes** (ordenadores, teléfonos, tabletas, ...) **llaman** a **servidores** (web, bases de datos...) que **proporcionan información**. Esta **comunicación** se lleva a cabo **a través** de un **protocolo** (**http**, **https**, **ftp**, etc.).

El **cliente** está **identificado** en la **red** a través de una **dirección IP** (TCP/IP) y cada vez que se **conecta** a un **sitio web**, éste **conoce automáticamente** la **dirección IP**, **nombre de máquina**, la **página de procedencia**, etc.

Se **produce** un **intercambio** de **información** que habitualmente **no** es **visible** donde el **navegador web** es el que **facilita** la mayoría de estos **datos**:

- Un alto porcentaje de los **usuarios no** es **consciente** de la cantidad de **información** que, de forma **inadvertida** e **involuntaria**, está **revelando** a **terceros** al hacer **uso** de **Internet**.

- Cada vez que se **visita** un **sitio web**, se **suministra** de forma rutinaria una **información** que puede ser **archivada** por el **administrador** del sitio.
- Al **sitio web** le resulta **trivial averiguar** la **dirección** de **Internet** de la [1]**máquina** desde la que se está accediendo, [2]**sistema operativo**, etc.
- Con ayuda de las "**cookies**" se puede **personalizar** aún más la **información** recabada acerca de los **visitantes**, **registrando** las **páginas más visitadas**, **preferencias**, **tiempo** de la visita, **software instalado**, etc.
- Un **navegador web**, en favor de la máxima usabilidad, **permite** que se **acceda** a **información** aparentemente **inofensiva**.
- La **dirección IP pública** con que se **conecta** el **usuario**.
  - Tu **dirección IP** es **xxx.xxx.xxx.xxx**.
  - Tu **navegador** está **utilizando 128 bits** de **clave secreta SSL**.
  - El **servidor** está **utilizando 1024 bits** de **clave pública SSL**.
- La **resolución** de la **pantalla**.
- Qué **páginas** se **leen** y cuáles no, qué **figuras** se **miran**, cuántas **páginas** se han **visitado**, cuál fue el **sitio** recientemente **visitado**.
- El **valor** del **campo** "**User-Agent**".
- El **idioma** y **zona GMT*** del **sistema operativo**.
- Si se **aceptan** o **no** "**cookies**".

Algunas **recomendaciones** para mantener una **navegación segura** son:

- **Acceder** únicamente a **sitios** de **confianza**.
- **Mantener actualizado** el **navegador** a la última versión disponible del fabricante.
- **Configurar** el **nivel** de **seguridad** del navegador **según** sus **preferencias**.
- **Descargar** los **programas** desde **sitios oficiales** para **evitar suplantaciones maliciosas**.
- **Configurar** el **navegador** para **evitar ventanas emergentes**.
- **Utilizar** un **usuario sin permisos** de "**Administrador**" para navegar por Internet e **impedir** la **instalación** de **programas** y **cambios** en los **valores** del **sistema**.
- **Borrar** las "**cookies**", los **ficheros temporales** y el **historial** cuando se **utilicen equipos ajenos** para **no dejar rastro** de la **navegación**.
- **Desactivar** la posibilidad "**script**" en navegadores web.
- En la medida de lo posible, **emplear máquinas virtuales** para **navegar** por **Internet**.

Además, hay que tener en cuenta que los **sistemas** de **navegación anónima permiten** el **uso** de algunos servicios de **Internet** de forma **desvinculada** de la **dirección IP origen** de la comunicación.

- **Anonimizadores**: actúan como un **filtro** entre el **navegador** y **sitio web** que se desea visitar o al conectarse al anonimizador, se **introduce** la **URL** a **visitar** y entonces éste **se adentra** en la **red filtrando cookies**, **javascripts**, etc.
- **Servidores Proxy**: actúa de **pasarela** entre la **máquina cliente** e **Internet**, actúa de **intermediario**, se encarga de **recuperar** las **páginas web en lugar** del **usuario** que navega.
- **Túneles de Cifrado** (TOR): por las cuales los **datos de navegación**, debidamente **cifrados**, **atraviesan múltiples nodos hasta** llegar a su **destino**.

Correo electrónico (Nº 7)

Actualmente el **correo electrónico** sigue siendo una de las **herramientas más utilizadas** por cualquier entorno corporativo para el **intercambio** de **información** a pesar de que en los últimos años han surgido multitud de tecnologías y herramientas colaborativas para facilitar la comunicación y el intercambio de ficheros.

El **incremento** y **efectividad** de la **ingeniería social** para **engañar** a los **usuarios** por medio de **correos electrónicos** ha **modificado** el paradigma de la **seguridad corporativa**.

Actualmente los **cortafuegos perimetrales*** y la **securización** de los **servicios** expuestos a **Internet no** son **contramedidas suficientes** para **proteger** una organización de **ataques externos**.

Algunas **recomendaciones** para utilizar el **correo electrónico** de forma segura:

- **No abrir** ningún **enlace ni descargar** ningún **fichero adjunto** procedente de un **correo** electrónico que presente cualquier **indicio** o **patrón fuera** de lo **habitual**.
- **No confiar** únicamente en el **nombre** del **remitente**. El **usuario** deberá **comprobar** que el propio **dominio** del **correo** recibido es de confianza.
- **Antes** de **abrir** cualquier **fichero descargado** desde el **correo**, hay que **asegurarse** de la **extensión** y **no fiarse** del **icono** asociado al mismo.
- **No** hacer **clic** en ningún **enlace** que **solicite datos personales** o **bancarios**.
- **Tener** siempre **actualizado** el **sistema operativo**, las **aplicaciones ofimáticas** y el **navegador**.
- **Utilizar herramientas de seguridad** para mitigar virus de manera **complementaria** al software **antivirus**.
- **Evitar** hacer **clic** directamente en cualquier **enlace** desde el propio cliente de **correo**.
- **Utilizar contraseñas robustas** para el acceso al correo electrónico. Las contraseñas deberán ser **periódicamente renovadas** y si es posible utilizar **doble autenticación**.
- **Cifrar** los **mensajes** de **correo** que contengan **información sensible**.

Virtualización (Nº 8)

La **virtualización** es la **recreación** de un **recurso físico** (hardware) o **lógico** (software), por **medio** de un **hipervisor*** que **permite** su **ejecución** por **más** de un **entorno** al **mismo tiempo**.

En el entorno de **máquinas virtuales**, el **hipervisor** permite el **uso simultáneo** del **hardware** en **más** de un **sistema operativo**.

El **apogeo** de la **virtualización** ha llegado con la **utilización** de la **nube**, donde este **sistema** de **reparto** de los **recursos** se hace casi **indispensable**.

La **seguridad** en la **virtualización** tiene la misma premisa que cualquier otro sistema, que es la **minimización** de la **superficie** de **ataque**.

Como norma general, es conveniente **seguir** las siguientes **indicaciones** a la hora de **configurar** un **host*** de máquinas virtuales:

- **Tener instaladas** en el sistema operativo las **últimas actualizaciones de seguridad**.
- **Tener** la **última reversión disponible** del programa de virtualización.
- Si es posible, **tener** al menos **1 adaptador de red** en exclusiva para la infraestructura de virtualización.
- **Crear** un **entorno** de **laboratorio aislado** del entorno de producción.
- **Disponer** de un **grupo de seguridad** para gestionar la plataforma de seguridad.
- **Proteger** los **dispositivos de almacenamiento** en los que guardan los archivos de recursos y de definición de la máquina virtual.

- **Mantener estancos** a los **administradores** de los **guest*** **respecto** a los de **host**.

Para la **creación** de **guest**, se recomienda seguir las siguientes **normas**:

- **Hacer** un **esquema previo** de lo que será la **infraestructura** de **virtualización**.
- **Dimensionar** la creación de **máquinas virtuales** a las **necesidades** reales y a los recursos de **hardware** disponibles en el host.
- **Cifrar** los **ficheros** de **máquinas virtuales**, **instantáneas** y **discos duros virtuales** destinados al **almacenamiento** de la plataforma de virtualización.
- **Instalar** las **últimas actualizaciones de seguridad** en cada sistema operativo guest.
- **Valorar** la **instalación** de los **agentes de hipervisor**, tipo **Guest Additions**, y en caso de hacerlo, mantenerlos **actualizados**.
- **Asegurar** con **antimalware** y **firewalls** todos los sistemas operativos invitados.
- **Conectar DVD**, **CD** y **medios de almacenamiento externos solo** cuando sea **necesario** y **desactivar** tras su uso.
- **Mantener activas** solamente las **máquinas virtuales imprescindibles**.
- **Usar** para la **conexión** con la **red corporativa** o con **Internet** una **interfaz** de **red virtual diferenciada** que se deberá **desactivar** cuando **no** se vaya a **utilizar**.
- **Cifrar** los medios de **almacenamiento externos** que contengan **ficheros de virtualización de respaldo** y custodiarlos convenientemente.

Seguridad en dispositivos móviles y redes inalámbricas (Nº 9)

El **incremento** de **posibilidades** y **capacidades** que llevan asociados los **dispositivos móviles** en la actualidad **implica** igualmente **mayores riesgos** para la **seguridad** de los mismos.

Se deben tener en cuenta los siguientes **aspectos** a la hora de usar **dispositivos móviles** para **garantizar** la **seguridad**:

- **Establecer** un **método seguro** para **desbloquear** el **terminal**.
- Es recomendable **eliminar** las **previsualizaciones** de los **mensajes** y extremar las **medidas** cuando **no** se disponga del **teléfono al alcance**.
- **Deshabilitar** las **conexiones inalámbricas** (WiFi, Bluetooth, etc.) y todas aquellas innecesarias mientras **no** vayan a **utilizarse**.
- Mantener **actualizado** el **software** del dispositivo y **utilizar** una **configuración de seguridad aprobada** por el **responsable TIC** de la entidad.
- Tener **cuidado** con el **acceso** y las **solicitudes de permisos** de las **aplicaciones** que se ejecuten en el **teléfono**.
- **Ignorar** y **borrar mensajes** (SMS, MMS u otros) de **origen desconocido** que invitan a descargar contenidos o acceder a sitios web.
- **Activar** el **acceso** mediante **PIN** a las conexiones **Bluetooth** y configurar el **dispositivo** en **modo oculto**. **No aceptar conexiones** de **dispositivos no conocidos**.
- **Descargar aplicaciones** únicamente desde las **tiendas oficiales**. **En ningún caso**, descargar software de sitios **poco fiables** y en todo caso **solicitar** al **responsable TIC** de la entidad las **aplicaciones necesarias**.
- **Utilizar** una **red privada virtual** (VPN16) para **proteger** el **tráfico de datos** desde el **dispositivo** móvil **hasta** la infraestructura de la **entidad**. Siempre es una buena práctica para **evitar** la posible **monitorización*** por parte de intrusos.
- **Evitar** en lo posible el **uso** de **impresoras**, **faxes** o **redes WiFi públicas**, como las ofrecidas en hoteles o aeropuertos, **salvo** que se disponga de las **herramientas** necesarias para **asegurar** sus **comunicaciones**.
- **Limitar** la **compartición** de las **imágenes** en la **red** o bien **utilizar aplicaciones** que **eliminen** dicha **información**.

- **Separar** las **comunicaciones personales** de las **profesionales** es una buena práctica de seguridad.
- **Implementar** la **gestión centralizada** de dispositivos **móviles** mediante el **empleo** de **agentes MDM** (Mobile Device Management)*.
- Para manejar información sensible, **utilizar** únicamente **soluciones aprobadas** por el **responsable** de **seguridad TIC** de la entidad.

Seguridad en redes inalámbricas (Nº 10)

Si se **trabaja** con una **red inalámbrica**, para **maximizar** la **seguridad** en la red **WiFi** es necesario prestar atención a las **siguientes recomendaciones**:

- **Cambiar** la **contraseña** de **acceso** por **defecto** para la administración del Punto de Acceso.
- **Modificar** el **SSID*** **configurado** por **defecto no** empleando **nombres** que pudieran **identificar** a la **entidad** y que permitan pasar **desapercibidos** con el entorno.
- **Ocultar** el identificador **SSID** al **exterior dificulta obtener** el **nombre de la red**, aunque la **trazabilidad** de los clientes sigue siendo **posible** con independencia de la **ocultación** del **SSID**.
- **Activar** el **filtrado** de **direcciones MAC*** de los dispositivos **WiFi** para **permitir** que se **conecten** a la **red** los **dispositivos** con las **direcciones MAC especificadas**.
- **Configurar WPA2-AES** en el **modo** de **confidencialidad** de datos, **obteniendo autenticación** y **cifrado** de datos robusto.
- **Limitar** la **cobertura WLAN**. Una **antena multidireccional** ubicada en el **centro** de la **casa**/**oficina** es la opción más común.
- **Desconectar** la **red** cuando **no** se **utilice**. Si bien **no** es **práctico** hacerlo **diariamente**, es muy **recomendable** durante **largos períodos** de **inactividad**.
- **Desactivar UPnP** (Universal Plug and Play)* cuando su uso no sea necesario, para **evitar** que un **código dañino** de la propia red **lo utilice** para **abrir** una **brecha** en el **cortafuegos** del **router** y **permitir** así que otros atacantes **accedan a él**.
- **Actualizar** el "**firmware**" del **router** periódicamente, pues muchas de las actualizaciones y parches que se van incorporando afectan a la seguridad.
- **Usar** direcciones **IP estáticas** o **limitar** el número de **direcciones reservadas** (DHCP) cuando sea posible, para **evitar** que **usuarios no autorizados** puedan **obtener** una **dirección IP** de la **red local**.
- **Activar** el **cortafuegos** del **router**, para que sólo los usuarios y los servicios autorizados puedan tener acceso a la red.
- **Activar** la opción de **registro** (login) para el **router** y **analizar** periódicamente el **historial de accesos**.
- Es recomendable **cambiar** el **DNS** que por **defecto** trae configurado el router por otro que **preserve** la **privacidad** del **usuario** y **mejore** su **seguridad**, por ejemplo, **DNSCrypt**.

Mensajería instantánea (Nº 11)

Las **aplicaciones** de **mensajería instantánea** permiten enviar **mensajes de texto mediante** la conexión a **Internet** (**WhatsApp** y **Telegram** son las más conocidas).

Además, el **uso compartido** de la **información personal** y la **escasa percepción** de **riesgo** que los usuarios tienen con la seguridad las han convertido en un **entorno atractivo** para **intrusos** y **ciberatacantes** que **intentan obtener datos** e **información** de sus **usuarios**.

Uno de los **fallos** más comunes en las aplicaciones de mensajería es la **forma** que utilizan para **borrar** las **conversaciones almacenadas** en el **teléfono** ya que **no** implica la **eliminación directa** de los **mensajes**, sino que estos quedan **marcados** como **libres**, de tal forma que **puedan ser sobrescritos** por **nuevas conversaciones** o **datos** cuando sea necesario siendo **accesible** por **técnicas forenses**.

Además, hay que tener en cuenta las **implicaciones** cuando se tenga **activa** la **opción** de **copia de seguridad** (almacenando una posible conversación ya borrada) que **podría ser recuperada** en un futuro.

Durante el establecimiento de **conexión** con los **servidores**, se puede **intercambiar** en texto claro **información sensible** acerca del usuario quedando **expuesta** a cualquiera en el caso de **utilizar** redes **WiFi públicas** o de **dudosa procedencia**:

- **Sistema operativo** del cliente.
- **Versión de la aplicación** en uso.
- **Número de teléfono** registrado.

Al **utilizar** una conexión basada en **redes privadas virtuales** (VPN), todos los **datos enviados** y **recibidos** pasan **cifrados** entre el **emisor** y el **receptor**, **añadiendo** una **nueva capa de seguridad** para **evitar** posibles **atacantes** que estén interceptando el tráfico de red.

Por otro lado, la **base de datos** de **conversaciones**, **ficheros**, **mensajes**, así como otros datos que manejan este tipo de aplicaciones **se almacena** de **forma local dentro** del **teléfono** y existen multitud de aplicaciones que por ejemplo para WhatsApp **permiten** de una forma sencilla el **descifrado** de la **información** contenida.

Aunque la **información** se **almacena cifrada** en **local**, **existen** multitud de **aplicaciones** que por ejemplo para WhatsApp **permiten** de una forma sencilla el **descifrado** de la **información** contenida, tanto en **versión local** para un equipo, como **a través** de una **aplicación** en el teléfono o **interfaz web**.

Para **evitar** que un **atacante** pueda tener **acceso** a toda la **información privada** que se **almacena** en el **teléfono** hay que prestar especial **atención** a qué [1]**aplicaciones** de terceros se **instalan**, así como el [2]**acceso físico** de otra persona **al terminal**.

En el caso de **intercambio** de **datos** con **redes sociales**, como WhatsApp y Facebook, y **a pesar** de que los **mensajes**, **fotos** e información de **perfil no** serán **objetivos a compartir**, otra información como **número de teléfono**, **contactos**, **hora** de última **conexión**, así como tus **hábitos de uso** de la aplicación pueden ser **compartidos**.

Insistiendo en las recomendaciones indicadas para dispositivos móviles, será necesario adoptar determinadas **precauciones** en el uso de **aplicaciones** de **mensajería instantánea** como:

- **Mantener** el **teléfono bloqueado**. De esta forma, se reducirá el riesgo si el dispositivo cae en las manos equivocadas.
- Sería recomendable **eliminar** las **previsualizaciones** de los **mensajes** y extremar las **medidas** cuando **no** se disponga del **teléfono** al **alcance**.
- En la medida de lo posible, se **recomienda** la **configuración** de las aplicaciones para **solo recibir mensajes** de **personas autorizadas**.
- **Desactivar** la **conectividad adicional** del teléfono cuando no se vaya a utilizar, como podría ser la conexión WiFi o Bluetooth, ya que además de reducir el consumo de batería, reduce la posible superficie de ataque sobre el dispositivo.
- **Utilizar aplicaciones** de mensajería instantánea cuyo **código fuente** esté [1]**abierto** a la comunidad y haya sido [2]**revisado**.

Redes sociales (Nº 12)

Comunicarse, **compartir información**, mantener un **contacto** por interés o afinidad, **relacionarse**, formar una **identidad** y **reputación**, **reivindicarse**, **protestar**, **manipular**... son múltiples los **objetivos** buscados a la hora de **utilizar** una u otra **red social**.

No obstante, el **éxito** alcanzado, las enormes **posibilidades** que brindan y su **uso masivo**, han hecho situarse a las redes sociales en el **punto de mira** de los **ciberatacantes** que **no dudan** en **explotar** los **riesgos** y **vulnerabilidades** que tienen.

Una vez más, el **eslabón más débil** de esta cadena vuelve a ser el **factor humano** por su **escasa concienciación** y su **exceso de confianza** a la hora de emplear estas redes.

En general, los **riesgos** asociados a las redes sociales son los mismos que los del resto de actividades y/o servicios en Internet: grandes [1]**dificultades** para **eliminar** la **información subida**, el [2]**acceso futuro** por **terceros** (el derecho a cambiar de opinión es nulo y será muy difícil borrar cualquier opinión, fotografía o vídeo subido a la red) y la [3]**dificultad** de **discernir** entre **información veraz** y **propaganda** o **manipulación**.

A continuación, se indican los principales **consejos** que se pueden dar como buenas prácticas en el **uso** de **redes sociales**:

- **Creación cuidadosa** del **perfil** y la **configuración** de **privacidad**. No basarse en la configuración por defecto que proporcionan las plataformas.
- **Reflexión** sobre todo **lo que se publica** y **emplear** un **pseudónimo**. Dar por sentado que todo lo que se sube en una red social es **permanente**, aunque se elimine la cuenta.
- **Escoger cuidadosamente** a nuestros **amigos**.
- Para **evitar revelar** las direcciones de **correo** de sus **amigos**, **no permita** que los **servicios de redes sociales examinen** su **libreta** de direcciones de **correo**.
- **Prestar atención** a los **servicios** basados en la **localización** y la **información** del **teléfono móvil**.
- **Precaución** con los **enlaces**. **Evitar** hacer clic en **hipervínculos** o **enlaces** de procedencia **dudosa**.
- **Escribir directamente** la **dirección** de su **sitio** de **redes sociales** en el **navegador** para evitar que un sitio falso pueda robar su información personal.
- **Tener precaución** al **instalar elementos adicionales** en su sitio ya que, en ocasiones, se usan estas aplicaciones para robar información personal.
- **Revisar** la **información publicada**. **Eludir dar excesiva información** sobre **uno mismo** entre otras cosas para evitar que puedan entrar en su cuenta al responder a preguntas del tipo su cumpleaños, su ciudad natal, clase del instituto, etc.
- **Seguridad** de las contraseñas, **utilice contraseñas complejas** que incluyan **números**, **símbolos** y **signos de puntuación**. Es importante no compartir la misma contraseña para todas las redes sociales ni para el resto de servicios que se utilizan en Internet.
- **Incrementar** la **seguridad** en el **acceso** a la **cuenta añadiendo** un **segundo factor** de **autenticación** (2FA) que impida a un potencial atacante que se haya hecho con la contraseña acceder al servicio.

Internet de las cosas IoT (Nº 13)

En esencia, **IOT** (Internet of Things) se refiere a **redes** de **objetos físicos**, **artefactos**, **vehículos**, **edificios**, **electrodomésticos**, **atuendos**, **implantes**, etc. que **llevan** en su seno **componentes electrónicos**, **software**, **sensores con conectividad** en red que les **permite recolectar información** para lograr una contextualización de la situación **mediante técnicas** de **Big Data*** imposible de realizar por otros medios.

Se trata de una **red** que **interconecta** miles de **objetos físicos ofreciendo datos** en **tiempo real**, convirtiéndose en los sensores del mundo físico. En este punto hay que considerar el **cambio cultural** que suponen ya que la tecnología **influye** en nuestra **forma** de **tomar** las **decisiones** y ello **afecta** a la **capacidad de acción**, **privacidad** y **autonomía** de las personas.

La **Iot** es la **primera evolución real** de **Internet**, un salto que podría llevar a **aplicaciones revolucionarias** con capacidad para **modificar** de forma dramática **la forma** en la que **vivimos, aprendemos**, **trabajamos** y nos **entretenemos** o **relacionamos socialmente**.

Los **artículos** de **uso diario** han **dejado de ser** elementos **aislados**, dispositivos que a su vez pueden estar conectados a otros dispositivos. La **pesadilla** de los **expertos** en **ciberseguridad** puede convertirse en **ejércitos** de "**botnets**" **utilizando** las **tostadoras inteligentes** para desarrollar **ataques DDoS*** o para **esconder información** y ejecutables lejos de la vista de los investigadores.

En la **Iot** hay que considerar **aspectos** de **vital importancia** como la **seguridad**, la **interoperabilidad** y **manejabilidad** de dichos **sistemas**:

- **Interfaz Web**.
- **Mecanismos** de **autenticación**.
- **Servicios** de **red**.
- **Transporte no cifrado**.
- **Protección** de la **intimidad**.
- **Configuración** de **seguridad**.
- **Integridad software/firmware**.
- **Seguridad física** de los **dispositivos**.
- El **reto** se reduce a establecer una base de **monitorización** y **control** para **reducir** la **exposición** al **riesgo** y **aplicar técnicas inteligentes** a la creciente población de dispositivos Iot.
- **Cambiar** las **contraseñas** por **defecto** de los dispositivos y **utilizar contraseñas** realmente **robustas**.
- **Mantener actualizados** los **dispositivos** con las **últimas versiones** disponibles de **software** y **firmware**.
- **Desactivar** toda **conectividad remota** (con Internet) de los dispositivos cuando no sea estrictamente necesaria.
- **Mantener abiertos** solo aquellos **puertos de comunicación** que sean realmente **necesarios** y **modificar** los **puertos de escucha** si es posible.
- Si los **dispositivos Iot no permiten** la **configuración** de su **seguridad**, **operar** con ellos siempre en una **red de área local** (**LAN**) detrás de un **dispositivo** (enrutador) correctamente configurado que **sí provea** esa **seguridad**.
- En la medida de lo posible, **asegurar** la **autenticidad**, **confidencialidad** e **integridad** en todas las **comunicaciones locales** (**LAN**), especialmente si estas se realizan por enlaces radio (WiFi, Bluetooth, etc.).
- **Comprobar** periódicamente la **configuración** de **seguridad** de todos los **elementos** de la arquitectura **Iot** y su **comunicación** con el **exterior**.
- **Mantener deshabilitados** los **componentes no necesarios** como pueden ser, según el caso, micrófonos, cámaras de vídeo, etc...
- **Comprobar** la **visibilidad** de los **dispositivos** propios en **buscadores** de **dispositivos Iot** como **Shodan**.

REAL DECRETO 4/2010, DE 8 DE ENERO, POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE INTEROPERABILIDAD EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA.

DISPOSICIONES GENERALES (Cap. 1)

Objeto (Art. 1)

El presente **real decreto** tiene por objeto **regular** el **Esquema Nacional de Interoperabilidad** establecido en el artículo 42 de la Ley 11/2007, de 22 de junio.

El **Esquema Nacional de Interoperabilidad** comprenderá los **criterios** y **recomendaciones** de [1]**seguridad**, [2]**normalización** y [3]**conservación** de la **información**, de los **formatos** y de las **aplicaciones** que deberán ser tenidos en cuenta por las Administraciones públicas para **asegurar** un adecuado nivel de **interoperabilidad** **organizativa**, **semántica** y **técnica** de los **datos**, **informaciones** y **servicios** que gestionen en el ejercicio de sus competencias y para **evitar** la **discriminación** a los **ciudadanos** por razón de su elección tecnológica.

Ámbito de aplicación (Art. 3)

El **Esquema Nacional de Interoperabilidad** y sus normas de desarrollo, **prevalecerán** sobre cualquier **otro criterio** en materia de **política** de **interoperabilidad** en la utilización de medios electrónicos para el acceso de los ciudadanos a los servicios públicos.

PRINCIPIOS BÁSICOS (Cap. 2)

Principios básicos del Esquema Nacional de Interoperabilidad (Art. 4)

La **aplicación** del **Esquema Nacional de Interoperabilidad** se desarrollará de acuerdo con los principios generales establecidos en el artículo 4 de la Ley 11/2007, de 22 de junio, y con los siguientes **principios específicos** de la interoperabilidad:

- La interoperabilidad como **cualidad integral**.
- **Carácter multidimensional** de la interoperabilidad.
- **Enfoque** de **soluciones multilaterales**.

La interoperabilidad como cualidad integral (Art. 5)

La **interoperabilidad** se tendrá presente de **forma integral** desde la **concepción** de los **servicios** y **sistemas** y **a lo largo** de su **ciclo de vida**: [1]**planificación**, [2]**diseño**, [3]**adquisición**, [4]**construcción**, [5]**despliegue**, [6]**explotación**, [7]**publicación**, [8]**conservación** y [9]**acceso** o [10]**interconexión** con los mismos.

Carácter multidimensional de la interoperabilidad (Art. 6)

La **interoperabilidad** se entenderá contemplando sus **dimensiones organizativa**, **semántica** y **técnica**. La **cadena** de **interoperabilidad** se **manifiesta** en la práctica en los [1]**acuerdos interadministrativos**, en el despliegue de los [2]**sistemas** y **servicios**, en la determinación y uso de [3]**estándares**, en las [4]**infraestructuras** y **servicios básicos** de las Administraciones públicas y en la publicación y reutilización de las [5]**aplicaciones** de las Administraciones públicas, de la documentación asociada y de otros objetos de información

Enfoque de soluciones multilaterales (Art. 7)

Se **favorecerá** la aproximación **multilateral** a la **interoperabilidad** de forma que se puedan obtener las **ventajas** derivadas del [1]**escalado**, de la aplicación de las [2]**arquitecturas modulares** y **multiplataforma**, de [3]**compartir**, de [4]**reutilizar** y de [5]**colaborar**.

INTEROPERABILIDAD ORGANIZATIVA (Cap. 3)

Servicios de las Administraciones públicas disponibles por medios electrónicos (Art. 8)

Las **Administraciones públicas** establecerán y publicarán las **condiciones** de **acceso** y **utilización** de los **servicios**, **datos** y **documentos** en formato **electrónico** que pongan a disposición del resto de Administraciones **especificando** las [1]**finalidades**, las [2]**modalidades de consumo**, [3]**consulta** o [4]**interacción**, los [5]**requisitos** que deben satisfacer los posibles **usuarios** de los mismos, los [6]**perfiles** de los **participantes** implicados en la utilización de los servicios, los [7]**protocolos** y **criterios funcionales** o **técnicos** necesarios para **acceder** a dichos **servicios**, los necesarios [8]**mecanismos de gobierno** de los **sistemas interoperables**, así como las [9]**condiciones de seguridad** aplicables. Estas **condiciones** deberán en todo caso resultar **conformes** a los principios, derechos y obligaciones contenidos en la **Ley Orgánica 15/1999** de 13 de diciembre, de [1]**Protección de Datos de Carácter Personal** y su normativa de desarrollo, así como a lo dispuesto en el [2]**Esquema Nacional de Seguridad**, y los instrumentos jurídicos que deberán suscribir las Administraciones públicas requeridoras de dichos servicios, datos y documentos.

Se **potenciará** el establecimiento de **convenios** entre las **Administraciones públicas** emisoras y receptoras y, en particular, con los **nodos de interoperabilidad** previstos en el apdo. 3 de este artículo, con el objetivo de **simplificar** la **complejidad organizativa** sin menoscabo de las garantías jurídicas.

Al objeto de dar cumplimiento de manera eficaz a lo establecido en el artículo 9 de la Ley 11/2007, de 22 de junio, en el **Comité Sectorial de Administración electrónica** se **identificarán**, **catalogarán** y **priorizarán** los **servicios de interoperabilidad** que deberán prestar las diferentes Administraciones públicas.

Las **Administraciones públicas** **publicarán** aquellos **servicios** que pongan a disposición de las demás administraciones **a través** de la **Red de comunicaciones** de las Administraciones públicas españolas, o de

cualquier **otra** red **equivalente** o **conectada** a la misma que **garantice** el **acceso seguro** al resto de administraciones.

Las **Administraciones públicas** podrán **utilizar nodos de interoperabilidad**, entendidos como **entidades** a las cuales se les **encomienda** la **gestión** de apartados **globales** o **parciales** de la **interoperabilidad organizativa**, **semántica** o **técnica**.

Inventarios de información administrativa (Art. 9)

Cada **Administración Pública** mantendrá **actualizado** el conjunto de sus **inventarios de información administrativa** que incluirá, al menos:

- La relación de los **procedimientos administrativos** y **servicios** prestados de forma **clasificada** y **estructurada**.

  Las Administraciones Públicas **conectarán electrónicamente** sus **inventarios** con el **Sistema de Información Administrativa** gestionado por el **Ministerio de Política Territorial y Función Pública** en **colaboración** con el **Ministerio de Asuntos Económicos y Transformación Digital**.

- La relación de sus **órganos administrativos** y **oficinas orientadas al público** y sus relaciones entre ellos. Dicho inventario se **conectará electrónicamente** con el **Directorio Común de Unidades Orgánicas y Oficinas**, gestionado por el **Ministerio de Asuntos Económicos y Transformación Digital**, en **colaboración** con el **Ministerio de Política Territorial y Función Pública**, que proveerá una **codificación unívoca**.

INTEROPERABILIDAD SEMÁNTICA (Cap. 4)

Activos semánticos (Art. 10)

Se establecerá y mantendrá **actualizada** la **Relación de modelos** de **datos de intercambio** que tengan el **carácter** de **comunes**, que serán de preferente **aplicación** para los **intercambios** de **información** en las **Administraciones públicas**, de acuerdo con el procedimiento establecido en disposición adicional primera.

Los órganos de la **Administración pública** o **Entidades de Derecho Público** vinculadas o dependientes de aquélla, titulares de competencias en materias sujetas a **intercambio** de **información** con los **ciudadanos** y con **otras Administraciones públicas**, así como en materia de **infraestructuras**, **servicios** y **herramientas comunes**, establecerán y publicarán los correspondientes **modelos de datos de intercambio** que serán de obligatoria aplicación para los intercambios de información en las Administraciones públicas.

Los **modelos de datos** a los que se refieren los apartados 1 y 2, se ajustarán a lo previsto sobre estándares en el artículo 11 y **se publicarán**, junto con las **definiciones** y **codificaciones** asociadas, **a través** del **Centro de Interoperabilidad Semántica** de la **Administración**, según las condiciones de licenciamiento previstas en el artículo 16.

INTEROPERABILIDAD TÉCNICA (Cap. 5)

Estándares aplicables (Art. 11)

Las **Administraciones públicas** usarán **estándares abiertos**, así como, en su caso y de **forma complementaria**, **estándares** que sean de **uso generalizado** por los **ciudadanos**, al objeto de **garantizar** la **independencia** en la **elección** de alternativas **tecnológicas** por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología y, de forma que:

- Los **documentos** y **servicios** de **administración electrónica** que los órganos o Entidades de Derecho Público emisores pongan a disposición de los ciudadanos o de otras Administraciones públicas se encontrarán, como mínimo, **disponibles** mediante **estándares abiertos**.
- Los **documentos**, **servicios electrónicos** y **aplicaciones** puestos por las Administraciones públicas a disposición de los ciudadanos o de otras Administraciones públicas serán, según corresponda, **visualizables**, **accesibles** y **funcionalmente operables** en condiciones que permitan **satisfacer** el

principio de **neutralidad tecnológica** y **eviten** la **discriminación** a los **ciudadanos** por razón de su **elección tecnológica**.

En las **relaciones** con los **ciudadanos** y con **otras Administraciones públicas**, el **uso** en exclusiva de un **estándar no abierto sin** que se ofrezca una alternativa basada en un **estándar abierto** se **limitará** a aquellas **circunstancias** en las que **no** se **disponga** de un **estándar abierto** que satisfaga la **funcionalidad satisfecha** por el estándar **no abierto** en **cuestión** y sólo mientras dicha disponibilidad no se produzca. Las **Administraciones públicas** promoverán las **actividades** de **normalización** con el fin de **facilitar** la **disponibilidad** de los **estándares abiertos relevantes** para sus necesidades.

Para la **selección** de **estándares**, en general y, para el **establecimiento** del **catálogo** de estándares, en particular, se atenderá a los siguientes **criterios**:

- El **uso** de las **especificaciones técnicas** de las **TIC** en la **contratación pública** junto con las definiciones de **norma** y **especificación técnica** establecidos en el **Reglamento** Nº **1025/2012**, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.
- La definición de **estándar abierto** establecida en la **Ley 11/2007**, de 22 de junio, anexo, letra k).
- Carácter de **especificación formalizada**.
- Definición de «**coste** que **no** suponga una **dificultad de acceso**», establecida en el anexo de este real decreto.
- **Consideraciones adicionales** referidas a la **adecuación** del estándar a las **necesidades** y **funcionalidad** requeridas

En cualquier caso los **ciudadanos** podrán **elegir** las **aplicaciones** o **sistemas** para **relacionarse** con las **Administraciones públicas**, o dirigirse a las mismas, siempre y cuando **utilicen** [1]**estándares abiertos** o, en su caso, aquellos otros que sean de [2]**uso generalizado** por los **ciudadanos**.

Para **facilitar** la **interoperabilidad** con las Administraciones públicas el **catálogo de estándares contendrá** una relación de **estándares abiertos** y en su caso **complementarios** aplicables.

INFRAESTRUCTURAS Y SERVICIOS COMUNES (Cap. 6)

Uso de infraestructuras y servicios comunes y herramientas genéricas (Art. 12)

Las **Administraciones públicas enlazarán** aquellas **infraestructuras** y **servicios** que puedan implantar en su ámbito de actuación con las infraestructuras y servicios comunes que proporcione la Administración General del Estado para **facilitar** la **interoperabilidad** y la **relación multilateral** en el **intercambio** de **información** y de **servicios** entre todas las Administraciones públicas.

COMUNICACIONES DE LAS ADMINISTRACIONES PÚBLICAS (Cap. 7)

Red de comunicaciones de las Administraciones públicas españolas (Art. 13)

Al objeto de satisfacer lo previsto en el artículo 43 de la Ley 11/2007, de 22 de junio, las Administraciones públicas utilizarán **preferentemente** la **Red de comunicaciones de las Administraciones públicas españolas** para **comunicarse entre sí**, para lo cual **conectarán** a la misma, bien **sus** respectivas [1]**redes**, bien sus [2]**nodos de interoperabilidad**, de forma que se facilite el **intercambio** de **información** y de **servicios** entre las mismas, así como la interconexión con las [3]**redes** de las **Instituciones** de la **Unión Europea** y de **otros Estados miembros**.

La **Red Sara*** **prestará** la citada **Red de comunicaciones** de las **Administraciones públicas españolas**.

Plan de direccionamiento de la Administración (Art. 14)

Las **Administraciones Públicas** aplicarán el **Plan de direccionamiento e interconexión de redes** en la Administración, desarrollado en la **norma técnica de interoperabilidad** correspondiente, para su **interconexión** a través de las **redes de comunicaciones**.

Hora oficial (Art. 15)

Los **sistemas** o **aplicaciones** implicados en la provisión de un servicio público por vía electrónica se **sincronizarán** con la **hora oficial**, con una **precisión** y **desfase** que **garanticen** la certidumbre de los **plazos** establecidos en el **trámite administrativo** que satisfacen.

La **sincronización** de la **fecha** y la **hora** se **realizará** con el **Real Instituto y Observatorio de la Armada**, de conformidad con lo previsto sobre la hora legal en el **Real Decreto 1308/1992**, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como **laboratorio depositario** del **patrón nacional de Tiempo** y laboratorio **asociado** al **Centro Español de Metrología** y, cuando sea posible, con la **hora oficial** a **nivel europeo**.

REUTILIZACIÓN Y TRANSFERENCIA DE TECNOLOGÍA (Cap. 8)

Condiciones de licenciamiento aplicables (Art. 16)

Las **condiciones** de **licenciamiento** de las **aplicaciones informáticas**, **documentación asociada**, y cualquier **otro** objeto de información cuya **titularidad** de los derechos de la **propiedad intelectual** sea de una **Administración Pública** y permita su **puesta a disposición** de **otra Administración** y de los **ciudadanos** tendrán en cuenta los siguientes **aspectos**:

- El fin perseguido es el **aprovechamiento** y la **reutilización** de **recursos públicos**.
- La completa **protección** contra su **apropiación** exclusiva o parcial por parte de **terceros**.
- La **exención** de **responsabilidad** del **cedente** por el posible **mal uso** por parte del **cesionario**.
- La **no obligación** de **asistencia técnica** o de **mantenimiento** por parte del **cedente**.
- La **ausencia total** de **responsabilidad** por parte del **cedente** con respecto al cesionario en caso de **errores** o **mal funcionamiento** de la aplicación.
- El **licenciamiento** se realizará por defecto **sin contraprestación** y **sin necesidad** de establecer **convenio** alguno. Sólo se podrá acordar la **repercusión parcial** del **coste** de **adquisición** o **desarrollo** de las aplicaciones cedidas en aquellos casos en los que este **pago repercuta** directamente en el **incremento** de **funcionalidades** del activo cedido, incluya **adaptaciones concretas** para su **uso** en el **organismo cesionario**, o impliquen el **suministro** de servicios de **asistencia** o **soporte** para su **reutilización** en el organismo cesionario.

Las **Administraciones Públicas** utilizarán para las **aplicaciones informáticas**, **documentación asociada**, y cualquier **otro** objeto de información **declarados** como de **fuentes abiertas** aquellas **licencias** que **aseguren** que los programas, datos o información **cumplen** los siguientes **requisitos**:

- Pueden **ejecutarse** para **cualquier propósito**.
- Permiten **conocer** su **código fuente**.
- Pueden **modificarse** o **mejorarse**.
- Pueden **redistribuirse** a **otros usuarios** con o sin cambios **siempre** que la **obra** derivada **mantenga** estas cuatro **garantías**.

Para este fin se **procurará** la aplicación de la **Licencia Pública de la Unión Europea**, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.

A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las **Administraciones Públicas incluirán** en los **pliegos de cláusulas técnicas** de aquellos **contratos** que tengan por finalidad el desarrollo de **nuevas aplicaciones informáticas**, los siguientes **aspectos**:

- Que la **Administración** contratante **adquiera** los **derechos completos** de **propiedad intelectual** de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato.
- Que en el caso de **reutilizar activos** previamente existentes, la **Administración** contratante **reciba** un **producto** que **pueda ofrecer** para su reutilización posterior a **otras Administraciones Públicas**. Además, en

el caso de partir de productos de fuentes abiertas, que sea posible declarar como de fuentes abiertas la futura aplicación desarrollada.

Directorios de aplicaciones reutilizables (Art. 17)

La **Administración General del Estado** mantendrá el **Directorio general de aplicaciones** para su **libre reutilización**, de acuerdo al artículo 158 de la **Ley 40/2015**, de 1 octubre, a través del **Centro de Transferencia de Tecnología**. Este directorio **podrá** ser **utilizado** por **otras Administraciones** Públicas. En el caso de disponer de un **directorio propio**, deberá garantizar que las aplicaciones disponibles en ese directorio propio se pueden **consultar** también **a través** del **Centro de Transferencia de Tecnología**.

Las **Administraciones Públicas conectarán** los **directorios de aplicaciones** para su libre **reutilización** entre sí; y con **instrumentos equivalentes** del ámbito de la **Unión Europea**.

Las **Administraciones Públicas publicarán** las **aplicaciones reutilizables**, en **modo producto** o en modo **servicio**, en los directorios de aplicaciones para su libre reutilización, con al menos el siguiente **contenido**:

- **Código fuente** de las **aplicaciones finalizadas**, en el caso de ser **reutilizables** en modo **producto** y haber sido declaradas de **fuentes abiertas**.
- **Documentación asociada**.
- **Condiciones de licenciamiento** de todos los **activos**, en el caso de ser **reutilizables** en modo **producto**, o nivel de **servicio** ofrecido, en el caso de ser reutilizables en modo servicio.
- Los **costes** asociados a su **reutilización**, en el caso de que existieran.

FIRMA ELECTRÓNICA Y CERTIFICADOS (Cap. 9)

Interoperabilidad en la política de firma electrónica y de certificados (Art. 18)

La **Administración General del Estado** definirá una **política** de **firma electrónica** y de **certificados** que servirá de **marco general de interoperabilidad** para el **reconocimiento mutuo** de las **firmas electrónicas** basadas en **certificados de documentos administrativos** en las Administraciones Públicas.

Todos los **organismos** y **entidades de derecho público** de la Administración General del Estado **aplicarán** la **política** de firma electrónica y de certificados a que se refiere el párrafo anterior. La **no aplicación** de dicha **política** deberá ser **justificada** por el órgano u **organismo competente** y **autorizada** por la **Secretaría General de Administración Digital**.

Sin perjuicio de lo expuesto en el apartado anterior, las **Administraciones Públicas** podrán aprobar **otras políticas** de **firma electrónica** dentro de sus respectivos ámbitos competenciales.

Plataformas de validación de certificados electrónicos y de firma electrónica (Art. 20)

Las **plataformas de validación** de certificados electrónicos y de firma electrónica **proporcionarán servicios de confianza** a las **aplicaciones usuarias** o **consumidoras** de los servicios de **certificación** y **firma**, proporcionando servicios de **validación** de los **certificados** y **firmas** generadas y admitidas en diversos ámbitos de las Administraciones públicas.

Proporcionarán, en un único punto de llamada, todos los elementos de **confianza** y de **interoperabilidad organizativa**, **semántica** y **técnica** necesarios para **integrar** los distintos **certificados** reconocidos y **firmas** que pueden encontrase en los **dominios** de **2 administraciones** diferentes.

RECUPERACIÓN Y CONSERVACIÓN DEL DOCUMENTO ELECTRÓNICO (Cap. 10)

Condiciones para la recuperación y conservación de documentos (Art. 21)

Las **Administraciones públicas** adoptarán las **medidas organizativas** y **técnicas** necesarias con el fin de **garantizar** la **interoperabilidad** en relación con la **recuperación** y **conservación** de los **documentos electrónicos** a lo largo de su ciclo de vida. Tales **medidas** incluirán:

- La **definición** de una **política** de **gestión** de **documentos** en cuanto al **tratamiento**, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.
- La **inclusión** en los **expedientes** de un **índice electrónico firmado** por el **órgano** o entidad **actuante** que garantice la integridad del expediente electrónico y permita su recuperación.
- La **identificación única** e **inequívoca** de cada **documento** por **medio** de **convenciones** adecuadas, que **permitan clasificarlo**, **recuperarlo** y **referirse** al mismo con facilidad.
- La **asociación** de los **metadatos mínimos obligatorios** y, en su caso, **complementarios**, asociados al documento electrónico, a lo largo de su ciclo de vida, e **incorporación** al **esquema de metadatos**.
- La **clasificación**, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de cada una de las **Administraciones públicas** y de las **Entidades de Derecho Público** vinculadas o dependientes de aquéllas.
- El **período de conservación** de los **documentos**, **establecido** por las **comisiones calificadoras** que correspondan, de acuerdo con la legislación en vigor, las normas administrativas y obligaciones jurídicas que resulten de aplicación en cada caso.
- El **acceso completo** e **inmediato** a los **documentos a través** de métodos de **consulta en línea** que **permitan** la **visualización** de los documentos con todo el detalle de su **contenido**, la **recuperación exhaustiva** y **pertinente** de los documentos, la **copia** o **descarga** en línea en los **formatos originales** y la **impresión a papel** de aquellos documentos que sean necesarios.
  El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento.
- La adopción de **medidas** para **asegurar** la **conservación** de los **documentos electrónicos** a lo largo de su ciclo de vida, de acuerdo con lo previsto en el artículo 22, de forma que se pueda asegurar su **recuperación** de acuerdo con el **plazo mínimo** de **conservación determinado** por las **normas administrativas** y **obligaciones jurídicas**,
- La **coordinación horizontal entre** el **responsable de gestión** de documentos y los **restantes servicios** interesados en materia de archivos.
- **Transferencia**, en su caso, de los **expedientes** entre los diferentes **repositorios electrónicos** a **efectos** de **conservación**, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y **recuperación** a **medio** y **largo plazo**.
- Si el resultado del procedimiento de evaluación documental así lo establece, **borrado** de la **información**, o en su caso, **destrucción física** de los **soportes**, de acuerdo con la legislación que resulte de aplicación, dejando **registro** de su eliminación.
- La **formación tecnológica** del **personal responsable** de la ejecución y del control de la **gestión** de **documentos**, como de su **tratamiento** y **conservación** en **archivos** o **repositorios** electrónicos.
- La **documentación** de los **procedimientos** que garanticen la interoperabilidad a medio y largo plazo, así como las **medidas** de **identificación**, **recuperación**, **control** y **tratamiento** de los documentos electrónicos.

Seguridad (Art. 22)

Para asegurar la **conservación** de los **documentos electrónicos** se aplicará lo previsto en el **Esquema Nacional de Seguridad** en cuanto al cumplimento de los [1]**principios básicos** y de los [2]**requisitos mínimos de seguridad** mediante la aplicación de las **medidas de seguridad** adecuadas a los **medios** y **soportes** en los que se almacenen los **documentos**, **de acuerdo** con la **categorización** de los **sistemas**.

Estas **medidas** se aplicarán con el fin de **garantizar** la **integridad**, **autenticidad**, **confidencialidad**, **disponibilidad**, **trazabilidad**, **calidad**, **protección**, **recuperación** y **conservación física** y **lógica** de los **documentos electrónicos**, sus **soportes** y **medios**, y se realizarán atendiendo a los **riesgos** a los que puedan estar expuestos y a los **plazos** durante los cuales deban conservarse los documentos.

Los **aspectos relativos** a la **firma electrónica** en la **conservación** del **documento electrónico** se **establecerán** en la **Política** de **firma electrónica** y de **certificados**, y **a través** del **uso** de **formatos** de **firma longeva** que **preserven** la **conservación** de las **firmas** a lo largo del tiempo.

Cuando la **firma** y los **certificados** **no** puedan **garantizar** la **autenticidad** y la **evidencia** de los **documentos electrónicos** a lo largo del tiempo, éstas les **sobrevendrán** a través de su conservación y custodia en los [1]**repositorios** y [2]**archivos electrónicos**, así como de los [3]**metadatos** de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

Formatos de los documentos (Art. 23)

Con el fin de garantizar la conservación, el **documento** se **conservará** en el **formato** en que haya sido **elaborado**, **enviado** o **recibido**, y **preferentemente** en un formato correspondiente a un **estándar abierto** que **preserve** a lo largo del tiempo la **integridad** del [1]**contenido** del documento, de la [2]**firma electrónica** y de los [3]**metadatos** que lo acompañan.

Cuando exista **riesgo** de **obsolescencia** del formato o bien **deje de figurar** entre los **admitidos** en el presente **Esquema Nacional de Interoperabilidad**, se aplicarán **procedimientos normalizados** de **copiado auténtico** de los documentos con cambio de formato, de etiquetado con información del formato utilizado y, en su caso, de las migraciones o conversiones de formatos.

Digitalización de documentos en soporte papel (Art. 24)

La **digitalización** de **documentos** en soporte **papel** por parte de las Administraciones públicas se realizará de acuerdo con lo indicado en la **norma técnica de interoperabilidad** correspondiente en relación con los siguientes **aspectos**:

- **Formatos estándares** de **uso común** para la digitalización de documentos en soporte papel y técnica de compresión empleada, de acuerdo con lo previsto en el artículo 11.
- **Nivel de resolución**.
- **Garantía de imagen fiel** e **íntegra**.
- **Metadatos mínimos obligatorios** y **complementarios**, asociados al proceso de digitalización.

La **gestión** y **conservación** del **documento electrónico digitalizado** atenderá a la posible **existencia** del mismo en **otro soporte**.

ACTUALIZACIÓN (Cap. 12)

Actualización permanente (Art. 29)

El **Esquema Nacional de Interoperabilidad** se deberá mantener **actualizado** de **manera permanente**. Se **desarrollará** y **perfeccionará** a lo largo del tiempo, **en paralelo** al [1]**progreso** de los servicios de **Administración Electrónica**, de la [2]**evolución tecnológica** y a medida que vayan consolidándose las [3]**infraestructuras** que le apoyan.