2025

TEMA 17.- MATERIAS TÉCNICO-CIENTÍFICAS

aspirantes.es

Temario de Ingreso al Cuerpo de la Guardia Civil. Edición de 15 de julio de 2024

Aspirantes.es
info@aspirantes.es

aspirantes.es

...por Anabel, Jorge, Cristina, Beli, Carmen, Juan, Pablo y Miguel. Por el tiempo que os he robado.

INTRODUCCIÓN AL CURSO DE INGRESO

Buenas aspirante, bienvenido a nuestro Curso de Ingreso a la Guardia Civil. Aspirantes.es es la primera plataforma de formación especializada en la preparación de las pruebas de Ingreso al Cuerpo.

Esta Guía de Estudio es solo uno de los elementos para poder afrontar la oposición. El curso para la preparación está compuesto por cuatro pilares fundamentales; el temario completo *(lo que incluye además de los temas gratuitos, los cuestionarios de psicotecnia y el manual de ortografía-gramática que te llegará a tu casa)*, los vídeos tutoriales, los Test de Verificación de Nivel y la tutorización.

Los más de 750 vídeos tutoriales, de entre 5 y 14 minutos, no solo te marcarán que es y que no es importante a efectos de centrar el estudio en la esencial del temario, sino que te explicarán los conceptos más difíciles o que tienen mayor interés. El comprender y conocer perfectamente cuál es la esencia de cada tema te facilitará sin duda el ingreso en un solo año, ya que podrás volcar el 100% de tu esfuerzo en ese 20% del temario de donde salen todos los años alrededor del 90% de las preguntas.

Los más de 12.000 Test de Verificación de Nivel que encontrarás en Aspirantes están perfectamente divididos por temas y subtemas y te facilitarán la consolidación progresiva del conocimiento.

Durante el curso encontrará textos que están subrayados y otros que no. El subrayado, si bien suele indicar importancia, no quiere decir que sea lo único que debes de saber. Ese subrayado trata de ubicar en la guía las explicaciones que se dan en los vídeos tutoriales. Por ello mucho cuidado con este concepto si decides estudiar por libre, ya que puedes dejar pasar conceptos fundamentales. Las actualizaciones del temario por cambios legislativos son comunicadas en nuestro Canal de Telegram.

En el momento que adquieras el curso, no solamente podrás acceder a los vídeos tutoriales y los test, sino que se te asignará un tutor personal. Este será en todo caso un miembro del Cuerpo en activo, con mando de unidad y especializado en la formación. A él podrás acudir directamente con todas las dudas que te surjan, a través de su teléfono personal y de su whatshapp.

El tutor estará a tu disposición en horario de mañana y de tarde todos los días de la semana. Él te facilitará la esquematización de conceptos y te orientará en todos los sentidos. Además, durante las primeras semanas *(se puede iniciar cualquier mes del año)*, te introducirá en el curso a través de video-llamadas individuales y te hará un seguimiento diario hasta que adquieras la dinámica a seguir.

Bueno aspirante, esto es todo por el momento. Si quieres contactar con Aspirantes para hacer alguna consulta pulsa aquí. Te deseamos mucha suerte y nos vemos en…

aspirantes.es

Ley 11/2022, de 28 de junio, General de Telecomunicaciones

Las telecomunicaciones constituyen uno de los sectores más dinámicos de la economía y uno de los que más pueden contribuir al crecimiento, la productividad, el empleo, y por tanto, al desarrollo económico y al bienestar social, afectando directamente al círculo de protección de los intereses generales.

Actualmente, la evolución tecnológica nos sitúa en una nueva etapa –la de extensión de las redes de nueva generación–, que obliga a los poderes públicos a reflexionar sobre la importancia de la función regulatoria.

El Título I, «Disposiciones generales», establece, entre otras cuestiones, el objeto de la Ley, que no se limita a la regulación de las «comunicaciones electrónicas», término que, de acuerdo con las Directivas comunitarias, engloba aspectos tales como la habilitación para actuar como operador, los derechos y obligaciones de operadores y usuarios, o el servicio universal, sino que aborda, de forma integral, el régimen de las «telecomunicaciones» al que se refiere el artículo 149.1.21.ª de la Constitución Española. Por ello, la presente Ley regula, asimismo, otras cuestiones como la instalación de equipos y sistemas, la interceptación legal de las telecomunicaciones, la conservación de datos, o la evaluación de conformidad de equipos y aparatos, temas que a nivel comunitario son objeto de normativa específica.

La Ley excluye expresamente de su regulación los contenidos difundidos a través de servicios de comunicación audiovisual, que constituyen parte del régimen de los medios de comunicación social, y que se caracterizan por ser transmitidos en un solo sentido de forma simultánea a una multiplicidad de usuarios. No obstante, las redes utilizadas como soporte de los servicios de radiodifusión sonora y televisiva y los recursos asociados sí son parte integrante de las comunicaciones electrónicas reguladas en la presente Ley.

Igualmente se excluye de su regulación la prestación de servicios sobre las redes de telecomunicaciones que no consistan principalmente en el transporte de señales a través de dichas redes. Estos últimos son objeto de regulación en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Asimismo, en este Título, se reordenan los objetivos y principios de la Ley, ya recogidos en la regulación anterior, incidiendo en la importancia de alcanzar un equilibrio entre el fomento de la innovación, el despliegue de nuevas redes, la prestación de nuevos servicios y la garantía de una competencia efectiva en los mercados de telecomunicaciones.

Procedamos al estudio de la materia objeto de examen

VER VÍDEO TEMA 17. PARTE 1ª

TÍTULO I

Disposiciones generales

Artículo 1. Objeto y ámbito de aplicación.

1. El objeto de esta ley es la regulación de las telecomunicaciones, que comprende la instalación y explotación de las redes de comunicaciones electrónicas, la 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 artículo 149.1.21.ª 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.

2. Quedan excluidos del ámbito de esta ley los servicios de comunicación audiovisual, los servicios de intercambio de vídeos a través de plataforma, los contenidos audiovisuales transmitidos a través de las redes, así como el 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 servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas, las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos y los 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.

Artículo 2. Las telecomunicaciones como servicios de interés general.

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

2. Sólo tienen la consideración de servicio público o están sometidos a obligaciones de servicio público los servicios regulados en el artículo 4 y en el título III, respectivamente.

Artículo 3. Objetivos y principios de la ley.

Los objetivos y principios de esta ley son los siguientes:

a) 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 bajada de los precios, calidad de los servicios, 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;

b) 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;

c) 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 conectividad, el acceso a las redes de muy alta capacidad, incluidas las redes fijas, móviles e inalámbricas y la interoperabilidad de extremo a extremo, en condiciones de igualdad y no discriminación;

d) 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 acceso funcional a internet, del teletrabajo, del

medioambiente, de la salud y la seguridad públicas y de la protección civil; así como cuando faciliten la vertebración y cohesión social y territorial o contribuyan a la sostenibilidad de la logística urbana.

e) promover el desarrollo de la ingeniería, así como de la industria de productos y equipos de telecomunicaciones;

f) 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;

g) 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;

h) 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;

i) fomentar la neutralidad tecnológica en la regulación;

j) 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;

k) 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. En la prestación de estos servicios deben salvaguardarse los imperativos constitucionales de no discriminación, de respeto a los derechos al honor y a la intimidad, la protección a la juventud y a la infancia, la protección a las personas con discapacidad, la protección de los datos personales y el secreto en las comunicaciones;

l) 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. En lo relativo al acceso a los servicios de comunicaciones electrónicas de las personas con discapacidad y personas en situación de dependencia, se fomentará el cumplimiento de las normas o las especificaciones pertinentes relativas a normalización técnica publicadas de acuerdo con la normativa comunitaria y se facilitará el acceso de los usuarios con discapacidad a los servicios de comunicaciones electrónicas y al uso de equipos terminales;

m) 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, especialmente en aquellas que necesitan de la instalación de redes de comunicaciones electrónicas y la mejora de las existentes para permitir impulsar distintas actividades económicas y sociales.

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

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

2. 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.

3. El Ministerio de Asuntos Económicos y Transformación Digital es el órgano de la Administración General del Estado con competencia, de conformidad con la legislación específica sobre la materia y lo establecido en esta ley, 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. Para el estudio e informe de estas materias, se constituirán los órganos interministeriales que se consideren adecuados, con la composición y competencia que se determinen mediante real decreto.

4. 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.

5. 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, dentro del ámbito de sus respectivas competencias. Estas medidas y sistemas deberán estar disponibles en las situaciones de normalidad o en las de crisis, así como en los supuestos contemplados en la Ley Orgánica 4/1981, de 1 de junio, reguladora de los Estados de Alarma, Excepción y Sitio, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas, la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil y el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

6. El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa de determinados servicios de comunicaciones electrónicas disponibles al público, distintos de los servicios de comunicaciones interpersonales, independientes de la numeración o de la explotación de ciertas redes públicas de comunicaciones electrónicas, para garantizar la seguridad pública y la seguridad nacional, en los términos en que dichas redes y servicios están definidos en el anexo II, excluyéndose en consecuencia las redes y servicios que se exploten o presten íntegramente en autoprestación. Esta facultad excepcional y transitoria de gestión directa podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer la seguridad pública y la seguridad nacional.

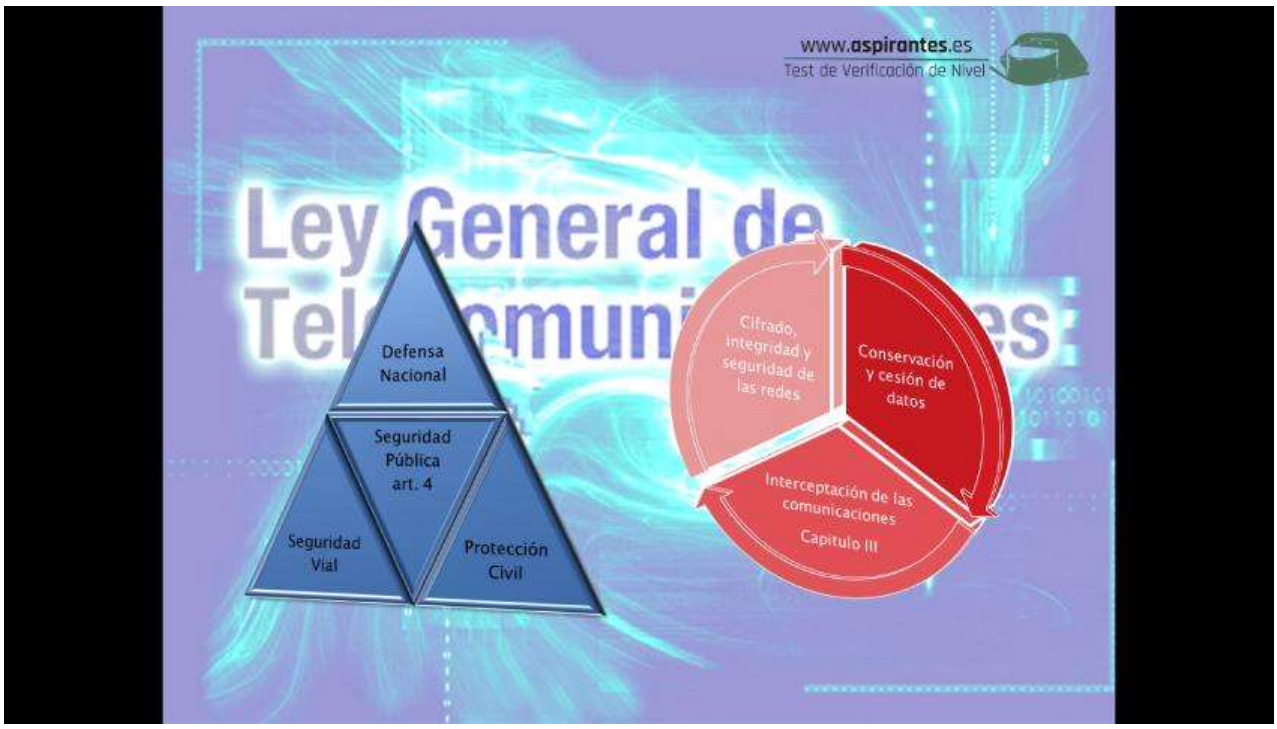
En ningún caso esta intervención podrá suponer una vulneración de los derechos fundamentales y libertades públicas reconocidas en el ordenamiento jurídico.

Asimismo, en el caso de incumplimiento de las obligaciones de servicio público a las que se refiere el título III, 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 asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refieren los párrafos anteriores se adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración Pública competente. En este último caso, será preciso que la Administración Pública tenga competencias en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado, aquella tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final.

Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refiere este apartado deberán ser comunicados por el Gobierno en el plazo de veinticuatro horas al órgano jurisdiccional competente para que, en un plazo de cuarenta y ocho horas, establezca si los mismos resultan acordes con los derechos fundamentales y libertades públicas reconocidas en el ordenamiento jurídico, procediendo a su anulación en caso negativo.

7. La regulación contenida en 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.



TÍTULO III.- CAPÍTULO III

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

Artículo 56. Salvaguardia de derechos fundamentales.

1. 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 Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en la Carta de Derechos Fundamentales de la Unión Europea, en los principios generales del Derecho comunitario y en la Constitución Española.

2. 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 principio de presunción de inocencia, el derecho a la vida privada e intimidad, el derecho a la libertad de expresión e información y el derecho a la tutela judicial efectiva, a través de un procedimiento previo, justo e imparcial, que incluirá el derecho de los interesados a ser oídos, sin perjuicio de que concurran las condiciones y los requisitos procedimentales adecuados en los casos de urgencia debidamente justificados, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales y la Carta de los Derechos Fundamentales de la Unión Europea.

Artículo 57. Principio de no discriminación.

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 nacionalidad, el lugar de residencia o el lugar de establecimiento del usuario final, a menos que dicho trato diferente se justifique de forma objetiva.

Artículo 58. Secreto de las comunicaciones.

1. 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 artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. 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 de acuerdo con lo establecido en el capítulo V del título VIII del libro II de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. 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.

4. 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.

5. 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:

a) 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.

Si en una comunicación electrónica se asignaran identidades de carácter temporal al usuario, el sujeto obligado implementará, cuando técnicamente sea posible, las medidas de correlación necesarias para que en la información de la interceptación se faciliten las identidades permanentes que permitan la identificación inequívoca del usuario asignado, así como del dispositivo empleado en la comunicación.

b) identidad o identidades de las otras partes involucradas en la comunicación electrónica;

c) servicios básicos utilizados;

d) servicios suplementarios utilizados;

e) dirección de la comunicación;

f) indicación de respuesta;

g) causa de finalización;

h) marcas temporales;

i) información de localización;

j) información intercambiada a través del canal de control o señalización.

6. 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:

a) identificación de la persona física o jurídica;

b) 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:

c) número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado);

d) número de identificación del terminal;

e) número de cuenta asignada por el proveedor de servicios internet;

f) dirección de correo electrónico.

7. 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.

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

9. 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.

10. 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.

11. 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.

Artículo 59. Interceptación de las comunicaciones electrónicas por los servicios técnicos.

1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, 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:

a) 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;

b) 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.

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.

3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 85.

Artículo 60. Protección de los datos de carácter personal.

1. 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:

a) la garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley;

b) 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;

c) 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.

2. 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.

3. 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. Unas medidas de protección de estas características podrían ser aquellas que convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.

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 destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el 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 circunstancias en que se requiere que el operador notifique la violación de los datos personales, sobre el formato que debe adoptar dicha notificación y sobre la manera de llevarla a cabo, con pleno respeto a las disposiciones que en su caso sean adoptadas en esta materia por la Comisión Europea.

4. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y su normativa de desarrollo.

Artículo 61. Conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

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.

Artículo 62. Cifrado en las redes y servicios de comunicaciones electrónicas.

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

2. 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 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 obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente.

3. 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.

Artículo 63. Integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas.

1. 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.

2. 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.

3. 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:

a) el número de usuarios afectados por el incidente de seguridad;

b) la duración del incidente de seguridad;

c) el área geográfica afectada por el incidente de seguridad;

d) la medida en que se ha visto afectado el funcionamiento de la red o del servicio;

e) el alcance del impacto sobre las actividades económicas y sociales.

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.

4. 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.

5. 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:

a) 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;

b) 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.

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

7. El presente artículo se entiende sin perjuicio de lo establecido en el artículo 4.6.

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

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

Durante los últimos años hemos asistido a profundos cambios en la Administración en relación a la utilización de las tecnologías de la información y las comunicaciones (TIC). Cambios caracterizados, en una primera fase, por el uso de estas tecnologías en la automatización y mejora del funcionamiento de los procesos internos de la Administración, en el convencimiento de que el ahorro derivado de la mejora de la eficiencia se trasladaría a los ciudadanos. Posteriormente, por la universalización de Internet y de las tecnologías asociadas que ha propiciado el desarrollo de nuevos servicios y formas de relación con los ciudadanos y empresarios en un camino sin retorno hacía la Administración electrónica.

Precedamos al estudio de la materia objeto de examen.

CAPÍTULO I

Objeto y ámbito de aplicación

Artículo 1. Objeto.

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.

Este modelo de Gobernanza de las TIC incluirá, en todo caso, la definición e implementación de una estrategia global de transformación digital que garantice el uso adecuado de los recursos informáticos de acuerdo a las necesidades derivadas de la estrategia general del Gobierno, con el fin de mejorar la prestación de los servicios públicos al ciudadano.

Artículo 2. Ámbito de aplicación.

El ámbito de aplicación de este real decreto se extiende a la Administración General del Estado y sus Organismos Públicos previstos en el artículo 43 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

CAPÍTULO III

Modelo de gobernanza en el ámbito de las tecnologías de la información y las comunicaciones

Artículo 9. Estrategia en materia de tecnologías de la información y las comunicaciones.

El Gobierno, a iniciativa de la Comisión de Estrategia TIC, y a propuesta de los Ministros de la Presidencia, de Hacienda y Administraciones Públicas y de Industria, Consumo 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 ámbito temporal de la Estrategia TIC, así como su periodo de revisión.

Artículo 10. Medios y servicios compartidos.

1. 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.

2. 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 declaración de medio o servicio compartido habilitará a la Dirección de Tecnologías de la Información y las Comunicaciones para adoptar las medidas necesarias para su provisión compartida, bien directamente o a través de otras unidades TIC y, en su caso, para disponer tanto de los medios humanos y económicos como de las infraestructuras y resto de activos TIC que los ministerios y unidades dependientes venían dedicando a atender dichos servicios, entre los que se incluyen también ficheros electrónicos y licencias.

Dada la naturaleza funcional específica y régimen competencial singular de los servicios de Informática presupuestaria de la Intervención General de la Administración del Estado, lo establecido en este apartado 2 respecto a los servicios, recursos e infraestructuras TIC comunes y al catálogo de servicios TIC comunes, cuando pueda afectar a los sistemas de funcionalidad específica de Informática presupuestaria requerirá la previa aprobación de la Intervención General de la Administración del Estado.

3. 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.

4. 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.

5. 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.

6. 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 un 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.

7. La Dirección de Tecnologías de la Información y las Comunicaciones llevará un registro de los costes que son imputables a cada uno de los diferentes órganos y organismos usuarios, sin perjuicio de las competencias de otros órganos administrativos en materia de control de gasto.

8. La puesta a disposición común de los medios y servicios compartidos se hará de acuerdo con lo previsto en la normativa que resulte aplicable en cada ámbito en materia de personal, organización, presupuestos y patrimonial.

Artículo 11. Proyectos de interés prioritario.

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

La declaración de proyecto de interés prioritario se trasladará como recomendación al Ministerio de Hacienda y Administraciones Públicas y a la Comisión de Políticas de Gasto para que, en su caso, sea tenida en cuenta en la elaboración de los Presupuestos Generales del Estado.

Artículo 12. Unidades TIC.

1. 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.

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

a) Soporte, operación, implementación y/o gestión de sistemas informáticos corporativos o de redes de telecomunicaciones.

b) Desarrollo de aplicativos informáticos en entornos multiusuario.

c) Consultoría informática.

d) Seguridad de sistemas de información.

e) Atención técnica a usuarios.

f) Innovación en el ámbito de las TIC

g) Administración digital.

h) Conformar la voluntad de adquisición de bienes o servicios en el ámbito de las tecnologías de la información y las comunicaciones

i) Todas aquellas funciones no previstas expresamente en las letras anteriores, que sean relevantes en materia de tecnologías de la información y las comunicaciones.

3. 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.

Artículo 13. Cooperación interadministrativa.

1. La Dirección de Tecnologías de la Información y las Comunicaciones propondrá a la Secretaría de Estado de Administraciones Públicas las líneas de actuación, orientaciones comunes y la 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.

2. La Dirección de Tecnologías de la Información y las Comunicaciones propondrá al Secretario de Estado de Administraciones Públicas la designación de los representantes de la Administración General del Estado y sus Organismos Públicos en las comisiones o grupos que la Conferencia Sectorial de Administraciones Públicas cree en materia de tecnologías de la información y Administración digital.

FICHA CONTROL 1ª

	1ª vuelta	2ª vuelta	3ª vuelta	Total
Horas de Estudio				

Controle el tiempo real de estudio de forma precisa. La primera vuelta, al ser la que exige la realización de esquemas y resúmenes, será la que más tiempo necesite. Acceda a las baterías de Test a través de la plataforma Aspirantes. Al contestar los mismos, para un correcto análisis de sus resultados, deberá en todo caso responder a todas y cada una de las preguntas, incluso las dudosas.

Test de Verificación de Nivel	Resultado*	Observaciones*
Ley Telecomunicaciones y TIC núm. 1		
Ley Telecomunicaciones y TIC núm. 2		
Materias Técnico Científica núm. 1		**Al final del Tema**
Materias Técnico Científica núm. 2		**Al final del Tema**
Materias Técnico Científica núm. 3		**2ª Vuelta**
Materias Técnico Científica núm. 4		**3ª Vuelta**

Los posibles resultados son aprobado, insuficiente o suspenso. Anote en el recuadro de resultado el número de fallos que ha tenido. A continuación barra y número preguntas: 2/40

Tras la realización del Test de Verificación de Nivel, deberá de averiguar porque ha fallado en cada una de las preguntas, marcando en el temario si considera el concepto o datos relacionados de interés.

En el cuadro superior de observaciones debe dejar constancia del número de las preguntas falladas o erróneas, e incluso de aquellas que dudó aunque finalmente acertó. Una vez finalizado el temario, en una 2ª o 3ª vuelta del tema, deberá de contestar al menos aquellas que falló.

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

La presente Ley no realiza una regulación sistemática de los servicios electrónicos de confianza, que ya han sido legislados por el Reglamento (UE) 910/2014, el cual, por respeto al principio de primacía del Derecho de la Unión Europea, no debe reproducirse total o parcialmente. La función de esta Ley es, por lo tanto, complementar el Reglamento Europeo en aquellos aspectos concretos que no ha armonizado y cuyo desarrollo recae en los ordenamientos de los diferentes Estados miembros, cuyas disposiciones han de ser interpretadas de acuerdo con él. Anteriormente existía una directiva europea, lo que suponía que no existía un poder vinculante total a los estados miembros de la Unión. La elección de un Reglamento como instrumento legislativo por el legislador europeo, se fundamenta en que es de aplicación directa, reforzándose con ello la seguridad jurídica y terminando con la dispersión normativa provocada por las transposiciones de las anteriores Directivas de aplicación, que había provocado una importante fragmentación y contradicción en los distintos sistemas jurídicos nacionales dentro de la UE.

Así, mediante el Reglamento, que no tenemos que estudiar ya que no nos lo piden, pero si saber que es por lo que nace esta Ley, se persigue regular en un mismo instrumento normativo de aplicación directa en los Estados miembros dos realidades, la identificación y los servicios de confianza electrónicos en sentido amplio.

La aplicabilidad directa del Reglamento no priva a los Estados miembros de toda capacidad normativa sobre la materia regulada, es más, aquellos están obligados a adaptar los ordenamientos nacionales para garantizar que aquella cualidad se haga efectiva. Esta adaptación puede exigir tanto la modificación o derogación de normas existentes, como la adopción de nuevas disposiciones llamadas a completar la regulación europea. Prueba de lo anterior es la publicación en el año 2020 de esta Ley, que busca precisamente hace efectivo el Reglamento, de obligado cumplimiento por el ordenamiento jurídico español.

En tal sentido, busca la presente Ley es complementar el Reglamento (UE) 910/2014 en aquellos aspectos que este no ha armonizado y que se dejan al criterio de los Estados miembros. No obstante, la Ley se abstiene de reproducir las previsiones del Reglamento, abordando únicamente aquellas cuestiones que la norma europea remite a la decisión de los Estados miembros o que no se encuentran armonizadas, adquiriendo la regulación coherencia y sentido en el marco de la normativa europea.

VER VÍDEO TEMA 17. PARTE 2ª

TÍTULO I

Disposiciones generales

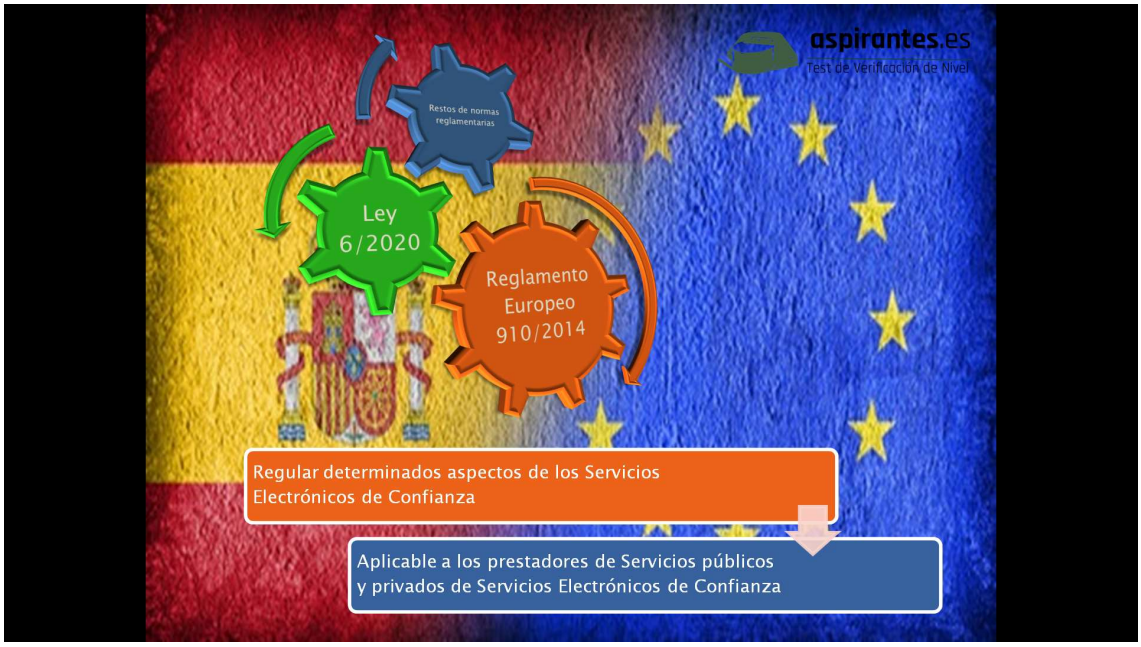
Artículo 1. Objeto de la Ley.

La presente Ley tiene por objeto regular determinados aspectos de los servicios electrónicos de confianza, como complemento del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

Artículo 2. Ámbito de aplicación.

Esta Ley se aplicará a los prestadores públicos y privados de servicios electrónicos de confianza establecidos en España.

Así mismo, se aplicará a los prestadores residentes o domiciliados en otro Estado que tengan un establecimiento permanente situado en España, siempre que ofrezcan servicios no supervisados por la autoridad competente de otro país de la Unión Europea.



Artículo 3. Efectos jurídicos de los documentos electrónicos.

1. Los documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

2. La prueba de los documentos electrónicos privados en los que se hubiese utilizado un servicio de confianza no cualificado se regirá por lo dispuesto en el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Si el servicio fuese cualificado, se estará a lo previsto en el apartado 4 del mismo precepto.

TÍTULO II

Certificados electrónicos

Artículo 4. Vigencia y caducidad de los certificados electrónicos.

1. Los certificados electrónicos se extinguen por caducidad a la expiración de su período de vigencia, o mediante revocación por los prestadores de servicios electrónicos de confianza en los supuestos previstos en el artículo siguiente.

2. El período de vigencia de los certificados cualificados no será superior a cinco años.

Dicho período se fijará en atención a las características y tecnología empleada para generar los datos de creación de firma, sello, o autenticación de sitio web.

Artículo 5. Revocación y suspensión de los certificados electrónicos.

1. Los prestadores de servicios electrónicos de confianza extinguirán la vigencia de los certificados electrónicos mediante revocación en los siguientes supuestos:

a) Solicitud formulada por el firmante, la persona física o jurídica representada por este, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web.

b) Violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del prestador de servicios de confianza, o de autenticación de sitio web, o utilización indebida de dichos datos por un tercero.

c) Resolución judicial o administrativa que lo ordene.

d) Fallecimiento del firmante; capacidad modificada judicialmente sobrevenida, total o parcial, del firmante; extinción de la personalidad jurídica o disolución del creador del sello en el caso de tratarse de una entidad sin personalidad jurídica, y cambio o pérdida de control sobre el nombre de dominio en el supuesto de un certificado de autenticación de sitio web.

e) Terminación de la representación en los certificados electrónicos con atributo de representante. En este caso, tanto el representante como la persona o entidad representada están obligados a solicitar la revocación de la vigencia del certificado en cuanto se produzca la modificación o extinción de la citada relación de representación.

f) Cese en la actividad del prestador de servicios de confianza salvo que la gestión de los certificados electrónicos expedidos por aquel sea transferida a otro prestador de servicios de confianza.

g) Descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo.

h) En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de los certificados no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

i) Cualquier otra causa lícita prevista en la declaración de prácticas del servicio de confianza.

2. Los prestadores de servicios de confianza suspenderán la vigencia de los certificados electrónicos en los supuestos previstos en las letras a), c) y h) del apartado anterior, así como en los casos de duda sobre la concurrencia de las circunstancias previstas en sus letras b) y g), siempre que sus declaraciones de prácticas de certificación prevean la posibilidad de suspender los certificados.

3. En su caso, y de manera previa o simultánea a la indicación de la revocación o suspensión de un certificado electrónico en el servicio de consulta sobre el estado de validez o revocación de los certificados por él expedidos, el prestador de servicios electrónicos de confianza comunicará al titular, por un medio que acredite la entrega y recepción efectiva siempre que sea factible, esta circunstancia, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

En los casos de suspensión, la vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el prestador no la hubiera levantado.

Artículo 6. Identidad y atributos de los titulares de certificados cualificados.

1. La identidad del titular en los certificados cualificados se consignará de la siguiente forma:

a) En el supuesto de certificados de firma electrónica y de autenticación de sitio web expedidos a personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, o a través de un pseudónimo que conste como tal de manera inequívoca. Los números anteriores podrán sustituirse por otro código o número identificativo únicamente en caso de que el titular carezca de todos ellos por causa lícita, siempre que le identifique de forma unívoca y permanente en el tiempo.

b) En el supuesto de certificados de sello electrónico y de autenticación de sitio web expedidos a personas jurídicas, por su denominación o razón social y su número de identificación fiscal. En defecto de este, deberá indicarse otro código identificativo que le identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.

2. Si los certificados admiten una relación de representación incluirán la identidad de la persona física o jurídica representada en las formas previstas en el apartado anterior, así como una indicación del documento, público si resulta exigible, que acredite de forma fehaciente las facultades del firmante para

actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

Artículo 7. Comprobación de la identidad y otras circunstancias de los solicitantes de un certificado cualificado.

1. La identificación de la persona física que solicite un certificado cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el Documento Nacional de Identidad, pasaporte u otros medios admitidos en Derecho. Podrá prescindirse de la personación de la persona física que solicite un certificado cualificado si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial.

2. Reglamentariamente, mediante Orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, se determinarán otras condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física según su evaluación por un organismo de evaluación de la conformidad. La determinación de dichas condiciones y requisitos técnicos se realizará a partir de los estándares que, en su caso, hayan sido determinados a nivel comunitario.

Serán considerados métodos de identificación reconocidos a escala nacional, a los efectos de lo previsto en el presente apartado, aquellos que aporten una seguridad equivalente en términos de fiabilidad a la presencia física y cuya equivalencia en el nivel de seguridad sea certificada por un organismo de evaluación de la conformidad, de acuerdo con lo previsto en la normativa en materia de servicios electrónicos de confianza.

3. La forma en que se ha procedido a identificar a la persona física solicitante podrá constar en el certificado. En otro caso, los prestadores de servicios de confianza deberán colaborar entre sí para determinar cuándo se produjo la última personación.

4. En el caso de certificados cualificados de sello electrónico y de firma electrónica con atributo de representante, los prestadores de servicios de confianza comprobarán, además de los datos señalados en los apartados anteriores, los datos relativos a la constitución y personalidad jurídica, y a la persona o entidad representada, respectivamente, así como la extensión y vigencia de las facultades de representación del solicitante mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. Esta comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

5. Cuando el certificado cualificado contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, estas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

6. Lo dispuesto en los apartados anteriores podrá no ser exigible cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de confianza en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubiese empleado el medio señalado en el apartado 1 y el período de tiempo transcurrido desde la identificación fuese menor de cinco años.

7. El Ministerio de Asuntos Económicos y Transformación Digital velará por que los prestadores cualificados de servicios electrónicos de confianza puedan contribuir a la elaboración de la norma reglamentaria prevista en el apartado 2 del presente artículo, de acuerdo con lo previsto en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

TÍTULO III

Obligaciones y responsabilidad de los prestadores de servicios electrónicos de confianza

Artículo 8. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios electrónicos de confianza para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta Ley se sujetará a lo dispuesto en la legislación aplicable en materia de protección de datos de carácter personal.

2. Los prestadores de servicios electrónicos de confianza que consignen un pseudónimo en un certificado electrónico deberán constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite.

3. Dichos prestadores de servicios de confianza estarán obligados a revelar la citada identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas en el ejercicio de funciones legalmente atribuidas, con sujeción a lo dispuesto en la legislación aplicable en materia de protección de datos personales.

Artículo 9. Obligaciones de los prestadores de servicios electrónicos de confianza.

1. Los prestadores de servicios electrónicos de confianza deberán:

a) Publicar información veraz y acorde con esta Ley y el Reglamento (UE) 910/2014.

b) No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.

En este caso, utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, y se aplicarán procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado. Además, deberán custodiar y proteger los datos de creación de firma, sello o autenticación de sitio web frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

2. Los prestadores de servicios de confianza que expidan certificados electrónicos deberán disponer de un servicio de consulta sobre el estado de validez o revocación de los certificados emitidos accesible al público.

3. Los prestadores cualificados de servicios electrónicos de confianza deberán cumplir las siguientes obligaciones adicionales:

a) El período de tiempo durante el que deberán conservar la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014, será de 15 años desde la extinción del certificado o la finalización del servicio prestado.

En caso de que expidan certificados cualificados de sello electrónico o autenticación de sitio web a personas jurídicas, los prestadores de servicios de confianza registrarán también la información que permita determinar la identidad de la persona física a la que se hayan entregado los citados certificados, para su identificación en procedimientos judiciales o administrativos.

b) Constituir un seguro de responsabilidad civil por importe mínimo de 1.500.000 euros, excepto si el prestador pertenece al sector público. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 500.000 euros más por cada tipo de servicio.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea coherente con lo dispuesto en el párrafo anterior.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.

c) El prestador cualificado que vaya a cesar en su actividad deberá comunicarlo a los clientes a los que preste sus servicios y al órgano de supervisión con una antelación mínima de dos meses al cese efectivo de la actividad, por un medio que acredite la entrega y recepción efectiva siempre que sea factible. El plan de cese del prestador de servicios puede incluir la transferencia de clientes, una vez acreditada la ausencia de oposición de los mismos, a otro prestador cualificado, el cual podrá conservar la información relativa a los servicios prestados hasta entonces.

Igualmente, comunicará al órgano de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

d) Enviar el informe de evaluación de la conformidad al Ministerio de Asuntos Económicos y Transformación Digital en los términos previstos en el artículo 20.1 del Reglamento (UE) 910/2014. El incumplimiento de esta obligación conllevará la retirada de la cualificación al prestador y al servicio que este presta, y su eliminación de la lista de confianza prevista en el artículo 22 del citado Reglamento, previo requerimiento al prestador del servicio para que cese en el citado incumplimiento.

Artículo 10. Responsabilidad de los prestadores de servicios electrónicos de confianza.

Los prestadores de servicios electrónicos de confianza asumirán toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios electrónicos de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

Artículo 11. Limitaciones de responsabilidad de los prestadores de servicios electrónicos de confianza.

1. El prestador de servicios electrónicos de confianza no será responsable de los daños y perjuicios ocasionados a la persona a la que ha prestado sus servicios o a terceros de buena fe, si esta incurre en alguno de los supuestos previstos en el Reglamento (UE) 910/2014 o en los siguientes:

a) No haber proporcionado al prestador de servicios de confianza información veraz, completa y exacta para la prestación del servicio de confianza, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada, actuando con la debida diligencia, por el prestador de servicios.

b) La falta de comunicación sin demora indebida al prestador de servicios de cualquier modificación de las circunstancias que incidan en la prestación del servicio de confianza, en particular, aquellas reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, sello o autenticación de sitio web, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de estos o, en su caso, de los medios que den acceso a ellos.

d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma, sello o autenticación de sitio web o, en su caso, de los medios que den acceso a ellos.

e) Utilizar los datos de creación de firma, sello o autenticación de sitio web cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de confianza le notifique la extinción o suspensión de su vigencia.

2. El prestador de servicios de confianza tampoco será responsable por los daños y perjuicios si el destinatario actúa de forma negligente. Se entenderá que el destinatario actúa de forma negligente cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico, o cuando no verifique la firma o sello electrónico.

3. El prestador de servicios de confianza no será responsable por los daños y perjuicios en caso de inexactitud de los datos que consten en el certificado electrónico si estos le han sido acreditados mediante documento público u oficial, inscrito en un registro público si así resulta exigible.

Artículo 12. Inicio de la prestación de servicios electrónicos de confianza no cualificados.

Los prestadores de servicios de confianza no cualificados no necesitan verificación administrativa previa de cumplimiento de requisitos para iniciar su actividad, pero deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses desde que la inicien, que publicará en su página web el listado de prestadores de servicios de confianza no cualificados en una lista diferente a la de los prestadores de servicios de confianza cualificados, con la descripción detallada y clara de las características propias y diferenciales de los prestadores cualificados y de los prestadores no cualificados.

En el mismo plazo deberán comunicar la modificación de los datos inicialmente transmitidos y el cese de su actividad.

Artículo 13. Obligaciones de seguridad de la información.

1. Los prestadores cualificados y no cualificados de servicios electrónicos de confianza notificarán al Ministerio de Asuntos Económicos y Transformación Digital las violaciones de seguridad o pérdidas de la integridad señaladas en el artículo 19.2 del Reglamento (UE) 910/2014, sin perjuicio de su notificación a la Agencia Española de Protección de Datos, a otros organismos relevantes o a las personas afectadas.

2. Los prestadores de servicios tienen la obligación de tomar las medidas necesarias para resolver los incidentes de seguridad que les afecten.

3. Los prestadores de servicios ampliarán, en un plazo máximo de un mes tras la notificación del incidente y, de haber tenido lugar, tras su resolución, la información suministrada en la notificación inicial con arreglo a las directrices y formularios que pueda establecer el Ministerio de Asuntos Económicos y Transformación Digital.

Disposición adicional tercera. Documento Nacional de Identidad y sus certificados electrónicos.

1. El Documento Nacional de Identidad electrónico es el Documento Nacional de Identidad que permite acreditar electrónicamente la identidad personal de su titular, en los términos establecidos en el artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, así como la firma electrónica de documentos.

2. Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del Documento Nacional de Identidad para acreditar la identidad y los demás datos personales del titular que consten en el mismo, así como la identidad del firmante y la integridad de los documentos firmados con sus certificados electrónicos.

3. Los órganos competentes del Ministerio del Interior para la expedición del Documento Nacional de Identidad cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios electrónicos de confianza que expidan certificados cualificados.

4. Sin perjuicio de la aplicación de la normativa vigente en materia del Documento Nacional de Identidad en todo aquello que se adecúe a sus características particulares, el Documento Nacional de Identidad se regirá por su normativa específica.

ADEMÁS DE ATENDER A LAS EXPLICACIONES DE LOS VÍDEOS, DEBES SEGUIR LAS ORIENTACIONES SOBRE EL MATERIAL ESENCIAL A ESTUDIAR

FICHA CONTROL 2ª

	1ª vuelta	2ª vuelta	3ª vuelta	Total
Horas de Estudio				

Controle el tiempo real de estudio de forma precisa. La primera vuelta, al ser la que exige la realización de esquemas y resúmenes, será la que más tiempo necesite. Acceda a las baterías de Test a través de la plataforma Aspirantes. Al contestar los mismos, para un correcto análisis de sus resultados, deberá en todo caso responder a todas y cada una de las preguntas, incluso las dudosas.

Test de Verificación de Nivel	Resultado*	Observaciones*
Sede Electrónica de Confianza núm. 1		
Sede Electrónica de Confianza núm. 2		
Materias Técnico Científica núm. 1		**Al final del Tema**
Materias Técnico Científica núm. 2		**Al final del Tema**
Materias Técnico Científica núm. 3		**2ª Vuelta**
Materias Técnico Científica núm. 4		**3ª Vuelta**

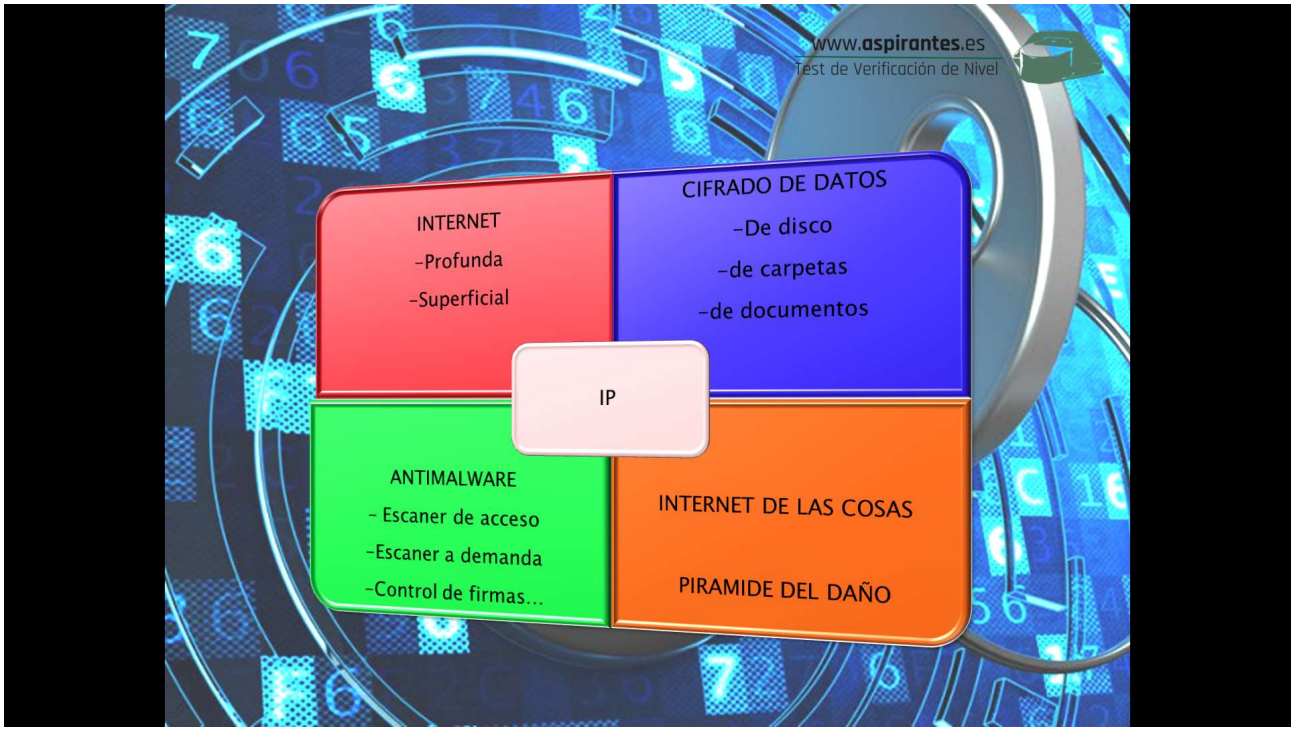
Los posibles resultados son aprobado, insuficiente o suspenso. Anote en el recuadro de resultado el número de fallos que ha tenido. A continuación barra y número preguntas: 2/40

Tras la realización del Test de Verificación de Nivel, deberá de averiguar porque ha fallado en cada una de las preguntas, marcando en el temario si considera el concepto o datos relacionados de interés.

En el cuadro superior de observaciones debe dejar constancia del número de las preguntas falladas o erróneas, e incluso de aquellas que dudó aunque finalmente acertó. Una vez finalizado el temario, en una 2ª o 3ª vuelta del tema, deberá de contestar al menos aquellas que falló.

Principios y recomendaciones básicas de Ciberseguridad del CCN-CERT

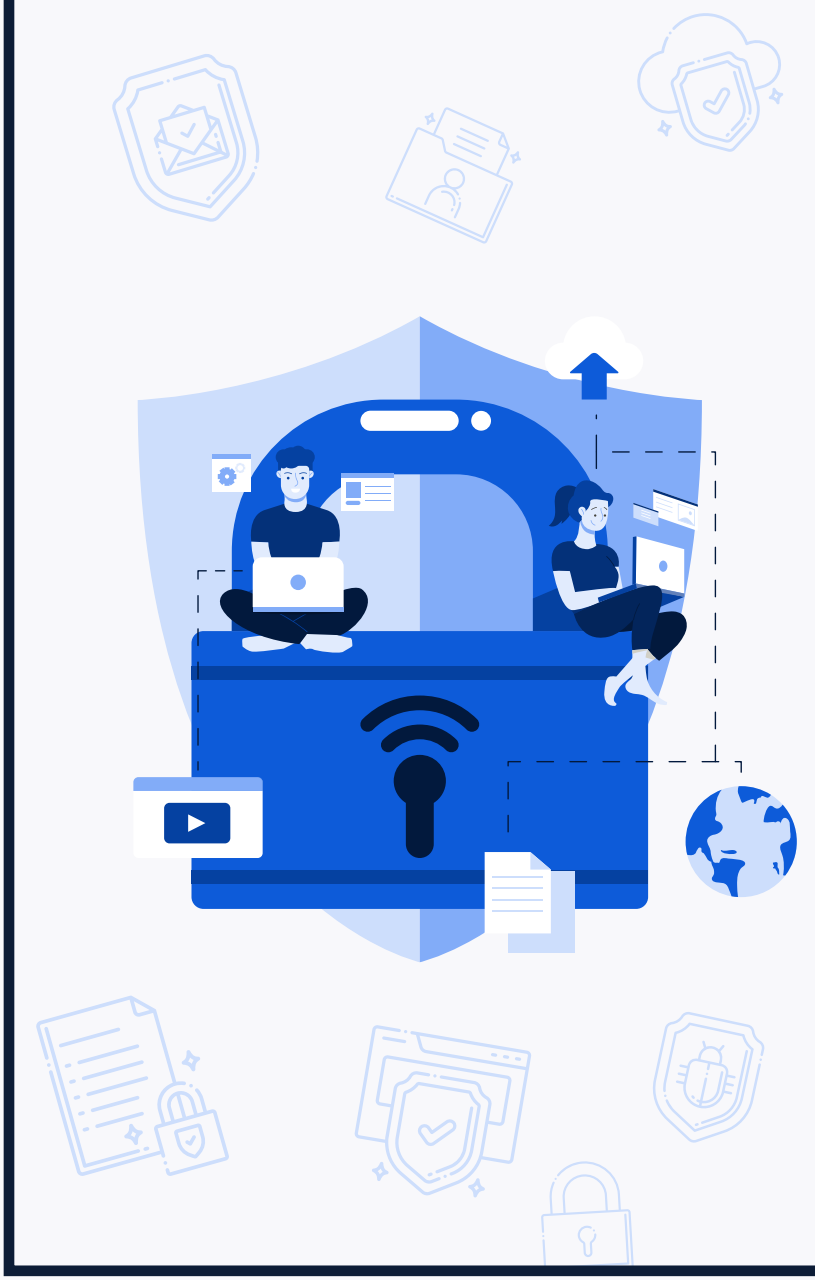
VER VÍDEO TEMA 17. PARTE 3ª



A continuación procedemos a incluir el dossier informativo del Centro Criptológico Nacional donde encontraremos las principales amenazas y recomendaciones para prevenir los ataques del ciberespacio.

CCN-CERT

BP/01



Principios y recomendaciones básicas en Ciberseguridad

INFORME DE BUENAS PRÁCTICAS

MARZO **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edita:

Centro Criptológico Nacional, 2021

Fecha de Edición: marzo de 2021

Índice

1. Sobre CCN-CERT

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional.

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). 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 **sistemas del Sector Público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. Su misión, por tanto, 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.

2. Introducción

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).

La concienciación, el sentido común y las buenas prácticas son las mejores defensas.

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 vulnerabilidades que presentan las tecnologías y lo que es más importante, la 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 mínimo para mantener los datos a salvo.

3. Factores de la amenaza

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**, consistentes 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 político, estratégico, de seguridad o económico.

A modo de resumen, podemos decir que el ciberespionaje presenta las siguientes características generales:

- **Origen en Estados, industrias o empresas.**
- **Utilización, generalmente, de ataques dirigidos (Amenazas Persistentes Avanzadas).**
- **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, al que podríamos denominar *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, pero a la vez consiguiendo que dichas acciones aparezcan como deliberadamente ambiguas.

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.

La Guerra Híbrida busca desestabilizar y polarizar la sociedad de los Estados.

Nivel de Peligrosidad y Amenazas

Figura 1. Pirámide del Daño

3.1 Ataques dirigidos (APT)

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

En este sentido, los grupos APT[1] (Advanced Persistent Threat) buscan recabar la mayor cantidad de información posible y útil de la víctima, con el objetivo de preparar un ataque lo más efectivo posible.

Figura 2.- Fases de una APT

1. Amenazas Persistentes Avanzadas.

3. Factores de la amenaza

Los parámetros que caracterizan las técnicas del ataque (APT) se basan en:

Capacidad de desarrollo

Exploits[2] 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*[3], *bootkit* 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.

2. Programa o código que se aprovecha de una vulnerabilidad en una aplicación o sistema para provocar un comportamiento no deseado o imprevisto.
3. Herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo.

4. La internet profunda

Internet se ha visto dividida en la Internet profunda y la superficial.

La superficial se compone de páginas estáticas o fijas, mientras que la 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, Yahoo!, Bing, etc.) de encontrar o indexar gran parte de la información existente en ella.

Un subconjunto de la Internet profunda solo es accesible utilizando determinados navegadores web. Es el caso, por ejemplo, de la red *TOR*, donde los usuarios han de disponer del software de navegación adecuado para poder acceder a dominios que son inaccesibles desde un navegador convencional.

Además, los usuarios han de conocer previamente la dirección a la que han de dirigirse.

Existen listados con algunos dominios públicos de la red TOR que los usuarios pueden consultar (The Hidden Wiki, Silk Road, Agora, Evolution, Middle-Earth, etc…) y buscadores como "*Grams*" (el Google de la *dark web*).

4.1 La red TOR

The Onion Router **(TOR) fue un proyecto diseñado e implementado por la Marina de los Estados Unidos, lanzado en 2002, con el fin de fortalecer las comunicaciones por Internet y garantizar el anonimato y la privacidad.**

A diferencia de los navegadores de Internet convencionales, *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 tres (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 tres (3) nodos asignados, a través de los cuales la información se transmitirá de forma cifrada.

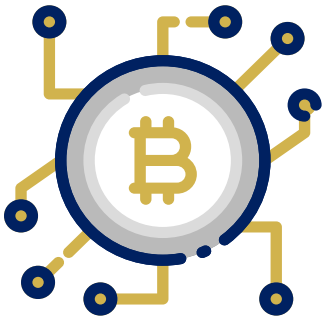
El elemento origen cifra la comunicación con la clave pública del último nodo de la ruta elegida para que de esta forma sea el único elemento que pueda descifrar el mensaje y las instrucciones (nodos intermedios y sus claves públicas asociadas) para llegar al destino.

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.

A diferencia de los navegadores de Internet convencionales, TOR permite a los usuarios navegar por la web de forma anónima.

4.2 Bitcoins

Se utiliza una cadena de caracteres criptográficos que se intercambian a través de billeteras digitales entre el usuario y el vendedor, lo que hace que esté fuera del control de cualquier gobierno, institución o entidad financiera.



Bitcoin **es una moneda electrónica cifrada, descentralizada, de ordenador a ordenador (peer-to-peer) 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.

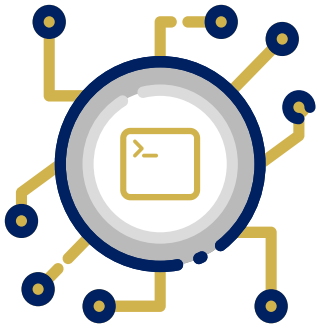
Cada transacción con bitcoins se registra en una gran base de datos llamada "*BlockChain*". Los datos se guardan en bloques y cada bloque nuevo debe contener el hash del bloque anterior. Por lo tanto, cada bloque nuevo que se une a la cadena posee todo el historial de la transacción.

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, existen cajeros automáticos y cada vez hay más vendedores/comercios que la aceptan. Como riesgos, representa un mecanismo muy práctico para blanquear dinero y evadir impuestos (exención fiscal).

5. Aplicaciones

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.



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.

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.

5. Aplicaciones

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.

> **La introducción de software no autorizado puede causar la infección del sistema más protegido.**

5.1 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[4] para cifrar los equipos informáticos, clasificables en tres (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.

Cifrar los datos significa convertir texto plano en texto ilegible, denominado texto cifrado, evitando que la información sea accesible por terceros no autorizados.

4. Véase **Guía CCN-STIC-955B Recomendaciones de empleo de GPG** (https://www.ccn-cert.cni.es/series-ccn-stic/900-informes-tecnicos/1816-ccn-stic-955b-recomendaciones-de-empleo-de-gpg/file.html)

5.2 Cortafuegos personales

Los cortafuegos[5] personales o *firewalls* 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 solo 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.

5. Véase **Guía CCN-STIC-408 Seguridad Perimetral-Cortafuegos** (https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html)

5.3 Aplicaciones antimalware

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

Las funciones mínimas que se pueden esperar en una buena **herramienta antimalware**[6] (más conocidas por **antivirus**) son las de filtrado entrante y saliente de contenidos maliciosos, protección en el correo electrónico, en la navegación y en las conexiones de todo tipo en redes profesionales o domésticas. También deben ser capaces de analizar los ficheros en dispositivos removibles como discos externos o memorias USB y permitir programar análisis exhaustivos cada cierto tiempo.

Las aplicaciones antimalware deben disponer de actualizaciones regulares (últimas definiciones y motores de búsqueda) 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.

---

6. El CCN-CERT tiene disponible para los usuarios registrados de su portal la **plataforma multiantivirus MARIA** para el análisis estático de código dañino a través de múltiples motores antivirus y antimalware para plataformas Windows y Linux (https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/maria-publico.html)

5.4 Borrado seguro de datos[7]

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. Para simplificar la tarea, lo más sencillo es utilizar alguna aplicación especializada que permita eliminar la información de forma sencilla.

En el caso de fotografías digitales, archivos de audio o vídeo y documentos ofimáticos, existen metadatos[8] 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.

7. Véase **Guía CCN-STIC-305 Destrucción y sanitización de soportes informáticos** (https://www.ccn-cert.cni.es/series-ccn-stic/300-instrucciones-tecnicas/60-ccn-stic-305-destruccion-y-sanitizacion-de-soportes-informaticos/file.html)
8. Véase **Guía CCN-STIC-835 Borrado de Metadatos en el marco del ENS** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2031-ccn-stic-835-borrado-de-metadatos-en-el-marco-del-ens/file.html)

6. Navegación segura

La comunicación en Internet se sustenta en una idea básica: clientes (ordenadores, teléfonos, tabletas, …) llaman a servidores (web, bases de datos…) que proporcionan (sirven) información. Esta comunicación se lleva a cabo a través de un protocolo (http, https[9] , 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.

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 máquina desde la que se está accediendo, 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.

---

9. Véase **Informe de Buenas Prácticas CCN-CERT BP-01/17 Recomendaciones implementación HTTPS** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html)

6. Navegación segura

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 "*Referer*".
- El valor del campo "*User-Agent*".
  - Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
- El idioma y zona GMT del sistema operativo.
- Si se aceptan o no "*cookies*".
- Las fuentes cargadas en el sistema o *plugins* instalados y activados.

Algunas **recomendaciones** para mantener una **navegación segura**[10] 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.

10. Véase **Informe de Buenas Prácticas CCN-CERT BP-06/16 Navegación segura** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1801-ccn-cert-bp-06-16-navegadores-web/file.html)

6. Navegación segura

- 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, como Firefox (NoScript) o Chrome (NotScript), para prevenir la ejecución de los mismos por parte de dominios desconocidos.
- Se recomienda hacer uso de HTTPS (SSL/TLS) frente a HTTP incluso para aquellos servicios que no manejen información sensible. Algunas funcionalidades como HSTS y extensiones como *HTTPS Everywhere* servirán de gran ayuda para garantizar el uso preferente de HTTPS sobre HTTP durante la navegación 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, principalmente los basados en navegación web (http/https), 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.

  Al conectarse al anonimizador, se introduce la URL a visitar y entonces éste se adentra en la red filtrando cookies, javascripts, etc.

- **Servidores Proxy**

  Un servidor proxy actúa de pasarela entre la máquina cliente e Internet.

  El servidor proxy actúa de intermediario, se encarga de recuperar las páginas web en lugar del usuario que navega.

- **Túneles de Cifrado (TOR, VPS y Darknets)**

  Red de "túneles" por las cuales los datos de navegación, debidamente cifrados, atraviesan múltiples nodos hasta llegar a su destino.

7. Correo electrónico

Actualmente el correo electrónico[11] 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**[12] 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. Si un correo procedente de un contacto conocido solicita información inusual, contacte con el mismo por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.**
- **Antes de abrir cualquier fichero descargado desde el correo, hay que asegurarse de la extensión y no fiarse del icono asociado al mismo.**
- **No habilitar las macros de los documentos ofimáticos incluso si el propio fichero así lo solicita.**

---

11. Véase **Guía CCN-STIC-814 Seguridad en correo electrónico** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/524-ccn-stic-814-seguridad-en-servicio-de-correo/file.html)
12. Véase **Informe de Buenas Prácticas CCN-CERT BP-02/16 Correo electrónico** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-16-correo-electronico/file.html)

7. Correo electrónico

- **No hacer clic en ningún enlace que solicite datos personales o bancarios.**
- **Tener siempre actualizado el sistema operativo, las aplicaciones ofimáticas y el navegador (incluyendo los *plugins*/extensiones instaladas).**
- **Utilizar herramientas de seguridad para mitigar exploits de manera complementaria al software antivirus.**
- **Evitar hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido, es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.**
- **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.**

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.

8. Virtualización

La virtualización se entiende como la recreación de un recurso físico (hardware) o lógico (software), por medio de un hipervisor (hypervisor) 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**[13] , donde este sistema de reparto de los recursos se hace casi indispensable. Aunque ya existían múltiples sistemas de muchos fabricantes, el desarrollo y avances de los mismos se han incrementado de una forma exponencial. Actualmente se puede optar, entre otros, por XenServer de Citrix, VMware ESXi de Dell, VirtualBox de Oracle, Oracle VM Server e Hyper-V de Microsoft.

La seguridad en la virtualización tiene la misma premisa que cualquier otro sistema, que es la *minimización de la superficie de ataque*. No obstante, cuenta con particularidades que hacen que la aseguración sea más difícil como, por ejemplo, la multitud de recursos compartidos o los sistemas operativos que funcionan simultáneamente con sus propias aplicaciones sobre una misma máquina física.

13. Véase **Guía CCN-STIC-823 Seguridad en entornos Cloud** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html)

8. Virtualización

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 un 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*.**

8. Virtualización

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.**

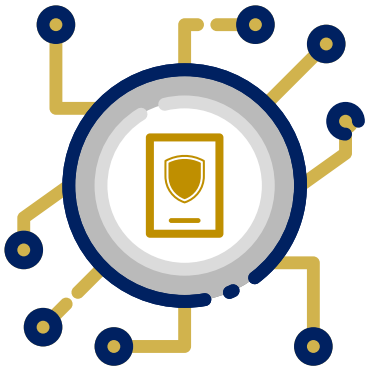
9. Seguridad en dispositivos móviles

El incremento de posibilidades y capacidades que llevan asociados los dispositivos móviles[14] en la actualidad implica igualmente mayores riesgos para la seguridad de los mismos.

Es muy importante que los usuarios sean conscientes de la importancia de la seguridad en los aparatos móviles y los peligros que pueden llevar consigo su mal uso.

Es conveniente seguir los siguientes **consejos**[15] :

El incremento de posibilidades y capacidades que llevan asociados los dispositivos móviles[14] en la actualidad implica igualmente mayores riesgos para la seguridad de los mismos.



- **Establecer un método seguro para desbloquear el terminal, por ejemplo, utilizando una *passphrase* robusta.**
- **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.**

14. Véase diversas **Guías CCN-STIC 450-451-452-453-454 y 455 Seguridad en dispositivos móviles** (https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6-ccn-stic-450-seguridad-en-dispositivos-moviles/file.html)
15. Véase **Informe de Buenas Prácticas CCN-CERT BP-03/16 Dispositivos móviles** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1807-ccn-cert-bp-03-16-dispositivos-moviles-1/file.html)

9. Seguridad en dispositivos móviles

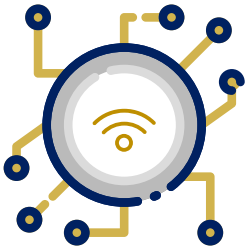
- **Mantener actualizado el software del dispositivo y utilizar una configuración de seguridad aprobada por el responsable TIC de la entidad.**
- **Tener cuidado con el acceso y las solicitudes de permisos de las aplicaciones que se ejecuten en el teléfono.**
- **Ignorar y borrar mensajes (SMS, MMS u 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.**
- **Evitar realizar *jailbreaking* o *rooting* del terminal, ya que puede comprometer y reducir considerablemente la seguridad del teléfono a pesar de ser tentador para acceder a aplicaciones o servicios específicos.**
- **Utilizar una red privada virtual (VPN[16]) 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.**
- **Muchos teléfonos móviles y cámaras digitales añaden las coordenadas GPS en la información de las imágenes tomadas, por lo que es oportuno 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. Disponer de compartimentos estancos en un solo dispositivo aumentará la 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.**

---

16. Véase **Guía CCN-STIC-836 Seguridad en redes privadas virtuales (VPN)** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html)

10. Seguridad en redes inalámbricas

Si se trabaja con una red inalámbrica, para maximizar la seguridad en la red WiFi es necesario prestar atención a las siguientes **recomendaciones**[17]:



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.

---

17. Véase **Guía CCN-STIC-816 Seguridad en Redes Inalámbricas** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html)

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 solo 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*.

11. Mensajería instantánea

Las aplicaciones de mensajería instantánea permiten enviar mensajes de texto mediante la conexión a Internet (WhatsApp[18] y Telegram[19] son las más conocidas).

En el caso de WhatsApp, lanzada al mercado en el año 2009, por ejemplo, gestiona actualmente alrededor de cien mil millones de mensajes al día.

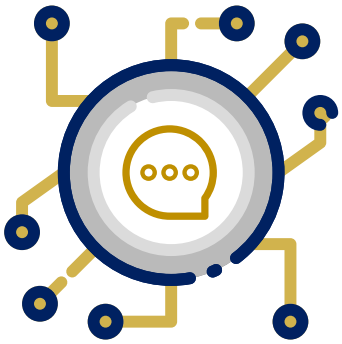
Se trata de plataformas que al poder tener un comportamiento semejante al de una red social convencional son propensas a su expansión. Además, el uso compartido de la información personal y la escasa percepción de riesgo que los usuarios tienen con la seguridad las han convertido en un entorno atractivo 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.

El uso compartido de información personal y la escasa percepción de riesgo que los usuarios tienen han convertido a las aplicaciones de mensajería instantánea en un entorno atractivo para los ciberatacantes.



18. Véase **CCN-CERT IA-21/16 Riesgos de uso de WhatsApp** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1746-ccn-cert-ia-21-16-riesgos-de-uso-de-whatsapp/file.html)
19. Véase **CCN-CERT IA-23/17 Riesgos de uso de Telegram** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2443-ccn-cert-ia-23-17-riesgos-de-uso-de-telegram-1/file.html)

11. Mensajería instantánea

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 (*man-in-the-middle*).

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, con independencia de que se tenga la opción de "*backup*" en la nube activada en el dispositivo.

Aunque la información se almacena cifrada en local, existen multitud de aplicaciones[20] 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 aplicaciones de terceros se instalan, así como el 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.

20. WhatCrypt: http://whatcrypt.com/

11. Mensajería instantánea

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 abierto a la comunidad y haya sido revisado. En ese sentido existen alternativas que, además, aseguran la confidencialidad en las comunicaciones, cifrando el tráfico extremo a extremo (e2e), un ejemplo es *Signal*.**

12. Redes sociales

Las redes sociales no solo han cambiado la manera en que los ciudadanos se informan y se comunican entre sí, sino también la manera en que los Gobiernos y organizaciones transmiten sus mensajes a los ciudadanos y la forma en que estos responden.

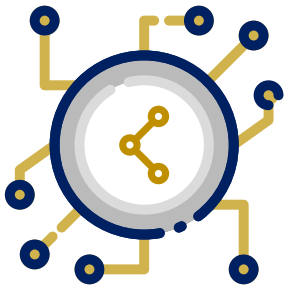
Comunicarse, compartir información, mantener un contacto por interés o afinidad, relacionarse, formar una identidad y reputación, reivindicarse, protestar, manipular… son múltiples los objetivos buscados a la hora de utilizar una u otra red social.

No obstante, el éxito alcanzado, las enormes posibilidades que brindan y su uso masivo las han hecho situarse en el punto de mira de los ciberatacantes, que no dudan en explotar los riesgos y vulnerabilidades que tienen tanto las plataformas que sustentan estas redes sociales como las personas u organizaciones que las utilizan.

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 dificultades para eliminar la información subida, el 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 dificultad de discernir entre información veraz y propaganda o manipulación.

En este punto hay que recordar la importancia que tiene la configuración de seguridad del dispositivo (sistema operativo y navegador) utilizado para conectarse a Internet y, de esta manera, acceder a las redes sociales.



No obstante, el éxito alcanzado, las enormes posibilidades que brindan y su uso masivo las han hecho situarse en el punto de mira de los ciberatacantes.

12. Redes sociales

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, como su cumpleaños, su ciudad natal, clase del instituto, etc., para evitar que puedan entrar en su cuenta.**
- **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 (empleo de gestores de contraseñas tipo *keepass*).**
- **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.**

13. Internet de las cosas (IoT)

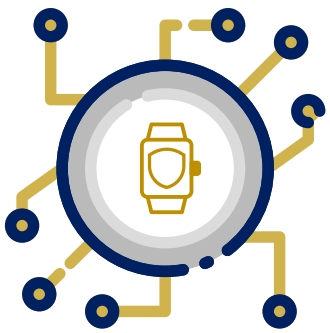
En esencia, IoT[21] (*Internet of Things*) se refiere a redes de objetos físicos, artefactos, vehículos, edificios, electrodomésticos, atuendos, implantes, etc. que llevan en su seno componentes electrónicos, software, sensores con conectividad en red que les permite recolectar información para lograr 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, 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.

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, nos entretenemos o relacionamos socialmente.



21. Véase **Informe de Buenas Prácticas CCN-CERT BP-05/16 Internet de las Cosas** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2258-ccn-cert-bp-05-16-internet-de-las-cosas/file.html)

13. Internet de las cosas (IoT)

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.

13. Internet de las cosas (IoT)

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.**

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

FICHA CONTROL 3ª

	1ª vuelta	2ª vuelta	3ª vuelta	Total
Horas de Estudio				

Controle el tiempo real de estudio de forma precisa. La primera vuelta, al ser la que exige la realización de esquemas y resúmenes, será la que más tiempo necesite. Acceda a las baterías de Test a través de la plataforma Aspirantes. Al contestar los mismos, para un correcto análisis de sus resultados, deberá en todo caso responder a todas y cada una de las preguntas, incluso las dudosas.

Test de Verificación de Nivel	Resultado*	Observaciones*
Recomendaciones Ciberseguridad núm. 1		
Recomendaciones Ciberseguridad núm. 2		
Recomendaciones Ciberseguridad núm. 3		
Materias Técnico Científica núm. 1		**Al final del Tema**
Materias Técnico Científica núm. 2		**Al final del Tema**
Materias Técnico Científica núm. 3		**2ª Vuelta**
Materias Técnico Científica núm. 4		**3ª Vuelta**

Los posibles resultados son aprobado, insuficiente o suspenso. Anote en el recuadro de resultado el número de fallos que ha tenido. A continuación barra y número preguntas: 2/40

Tras la realización del Test de Verificación de Nivel, deberá de averiguar porque ha fallado en cada una de las preguntas, marcando en el temario si considera el concepto o datos relacionados de interés.

En el cuadro superior de observaciones debe dejar constancia del número de las preguntas falladas o erróneas, e incluso de aquellas que dudó aunque finalmente acertó. Una vez finalizado el temario, en una 2ª o 3ª vuelta del tema, deberá de contestar al menos aquellas que falló.

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

Este real decreto se limita a establecer los criterios y recomendaciones, junto con los principios específicos necesarios, que permitan y favorezcan el desarrollo de la interoperabilidad en las Administraciones públicas desde una perspectiva global y no fragmentaria, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, en el ámbito de la Ley 11/2007, de 22 de junio, al objeto de conseguir un común denominador normativo.

La finalidad del Esquema Nacional de Interoperabilidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

En esta norma se hace referencia a la interoperabilidad como un proceso integral, en el que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

El Esquema Nacional de Interoperabilidad se remite al Esquema Nacional de Seguridad para las cuestiones relativas en materia de seguridad que vayan más allá de los aspectos necesarios para garantizar la interoperabilidad.

VER VÍDEO TEMA 17. PARTE 4ª

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

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.

2. El Esquema Nacional de Interoperabilidad comprenderá los criterios y recomendaciones de seguridad, normalización y 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.

Artículo 2. Definiciones.

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos se entenderán en el sentido indicado en el Glosario de Términos incluido en el anexo.

Artículo 3. Ámbito de aplicación.

1. El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.

2. 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.

CAPÍTULO II

Principios básicos

Artículo 4. Principios básicos del Esquema Nacional de Interoperabilidad.

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:

a) La interoperabilidad como cualidad integral.

b) Carácter multidimensional de la interoperabilidad.

c) Enfoque de soluciones multilaterales.

Artículo 5. La interoperabilidad como cualidad integral.

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: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos.

Artículo 6. Carácter multidimensional de la interoperabilidad.

La interoperabilidad se entenderá contemplando sus dimensiones organizativa, semántica y técnica. La cadena de interoperabilidad se manifiesta en la práctica en los acuerdos interadministrativos, en el despliegue de los sistemas y servicios, en la determinación y uso de estándares, en las infraestructuras y servicios básicos de las Administraciones públicas y en la publicación y reutilización de las aplicaciones de las Administraciones públicas, de la documentación asociada y de otros objetos de información. Todo ello sin olvidar la dimensión temporal que ha de garantizar el acceso a la información a lo largo del tiempo.

Artículo 7. Enfoque de soluciones multilaterales.

Se favorecerá la aproximación multilateral a la interoperabilidad de forma que se puedan obtener las ventajas derivadas del escalado, de la aplicación de las arquitecturas modulares y multiplataforma, de compartir, de reutilizar y de colaborar.

CAPÍTULO III

Interoperabilidad organizativa

Artículo 8. Servicios de las Administraciones públicas disponibles por medios electrónicos.

1. 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 finalidades, las modalidades de consumo, consulta o interacción, los requisitos que deben satisfacer los posibles usuarios de los mismos, los perfiles de los participantes implicados en la utilización de los servicios, los protocolos y criterios funcionales o técnicos necesarios para acceder a dichos servicios, los necesarios mecanismos de gobierno de los sistemas interoperables, así como las 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 Protección de Datos de Carácter Personal y su normativa de desarrollo, así como a lo dispuesto en el 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 apartado 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.

2. 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.

3. 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.

Artículo 9. Inventarios de información administrativa.

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

a) 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 n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea

b) 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.

2. Cada Administración Pública regulará la creación y mantenimiento de estos dos inventarios, en las condiciones que se determinen, con carácter general, por las normas técnicas de interoperabilidad correspondientes; en su caso, las Administraciones Públicas podrán hacer uso de los citados Sistema de Información Administrativa y Directorio Común de Unidades Orgánicas y Oficinas para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.

CAPÍTULO IV

Interoperabilidad semántica

Artículo 10. Activos semánticos.

1. 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.

2. 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.

3. 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.

4. Las definiciones y codificaciones empleadas en los modelos de datos a los que se refieren los apartados anteriores tendrán en cuenta lo dispuesto en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y el resto de disposiciones que regulan la función estadística.

CAPÍTULO V

Interoperabilidad técnica

Artículo 11. Estándares aplicables.

1. 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:

a) 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.

b) 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.

2. 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.

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

a) Las definiciones de norma y especificación técnica establecidas en la Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998 por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas.

b) La definición de estándar abierto establecida en la Ley 11/2007, de 22 de junio, anexo, letra k).

c) Carácter de especificación formalizada.

d) Definición de «coste que no suponga una dificultad de acceso», establecida en el anexo de este real decreto.

e) Consideraciones adicionales referidas a la adecuación del estándar a las necesidades y funcionalidad requeridas; a las condiciones relativas a su desarrollo, uso o implementación, documentación disponible y completa, publicación, y gobernanza del estándar; a las condiciones relativas a la madurez, apoyo y adopción del mismo por parte del mercado, a su potencial de reutilización, a la aplicabilidad multiplataforma y multicanal y a su implementación bajo diversos modelos de desarrollo de aplicaciones.

4. Para el uso de los estándares complementarios a la selección indicada en el apartado anterior, se tendrá en cuenta la definición de «uso generalizado por los ciudadanos» establecida en el anexo del presente real decreto.

5. 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 estándares abiertos o, en su caso, aquellos otros que sean de 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.

CAPÍTULO VI

Infraestructuras y servicios comunes

Artículo 12. Uso de infraestructuras y servicios comunes y herramientas genéricas.

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.

CAPÍTULO VII

Comunicaciones de las Administraciones públicas

Artículo 13. Red de comunicaciones de las Administraciones públicas españolas.

1. 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 redes, bien sus nodos de interoperabilidad, de forma que se facilite el intercambio de información y de servicios entre las mismas, así como la interconexión con las 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.

2. Para la conexión a la Red de comunicaciones de las Administraciones públicas españolas serán de aplicación los requisitos previstos en la disposición adicional primera.

Artículo 14. Plan de direccionamiento de la Administración.

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.

Artículo 15. Hora oficial.

1. 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.

2. 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.

CAPÍTULO VIII

Reutilización y transferencia de tecnología

Artículo 16. Condiciones de licenciamiento aplicables.

1. 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:

a) El fin perseguido es el aprovechamiento y la reutilización de recursos públicos.

b) La completa protección contra su apropiación exclusiva o parcial por parte de terceros.

c) La exención de responsabilidad del cedente por el posible mal uso por parte del cesionario.

d) La no obligación de asistencia técnica o de mantenimiento por parte del cedente.

e) La ausencia total de responsabilidad por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.

f) 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.

2. 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:

a) Pueden ejecutarse para cualquier propósito.

b) Permiten conocer su código fuente.

c) Pueden modificarse o mejorarse.

d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas cuatro garantías.

3. 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.

4. 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:

a) 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.

b) 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.

Artículo 17. Directorios de aplicaciones reutilizables.

1. 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.

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

3. 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:

a) Código fuente de las aplicaciones finalizadas, en el caso de ser reutilizables en modo producto y haber sido declaradas de fuentes abiertas.

b) Documentación asociada.

c) 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.

d) Los costes asociados a su reutilización, en el caso de que existieran.

4. Las Administraciones procurarán la incorporación a la aplicación original de aquellas modificaciones o adaptaciones realizadas sobre cualquier aplicación que se haya obtenido desde un directorio de aplicaciones reutilizables.

CAPÍTULO IX

Firma electrónica y certificados

Artículo 18. Interoperabilidad en la política de firma electrónica y de certificados.

1. 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.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. 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.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las reglas de creación y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.

Artículo 19. Suprimido.

Artículo 20. Plataformas de validación de certificados electrónicos y de firma electrónica.

1. 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.

2. 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 dos administraciones diferentes.

3. Potenciarán la armonización técnica y la utilización común de formatos, estándares y políticas de firma electrónica y de certificados para las firmas electrónicas entre las aplicaciones usuarias, y de otros elementos de interoperabilidad relacionados con los certificados, tales como el análisis de los campos y extracción univoca de la información pertinente. En particular, se tendrán en cuenta los estándares europeos de las Organizaciones Europeas de Estandarización en el campo de las Tecnologías de Información y Comunicación aplicadas a la firma electrónica.

4. Incorporarán las listas de confianza de los certificados interoperables entre las distintas Administraciones públicas nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza.

CAPÍTULO X

Recuperación y conservación del documento electrónico

Artículo 21. Condiciones para la recuperación y conservación de documentos.

1. 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:

a) 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.

b) 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.

c) La identificación única e inequívoca de cada documento por medio de convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.

d) 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.

e) 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.

f) 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.

g) 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.

h) 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, se garantice su conservación a largo plazo, se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

i) La coordinación horizontal entre el responsable de gestión de documentos y los restantes servicios interesados en materia de archivos.

j) 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.

k) 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.

l) 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.

m) 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.

2. A los efectos de lo dispuesto en el apartado 1, las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

Artículo 22. Seguridad.

1. Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimento de los principios básicos y de los 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.

2. Cuando los citados documentos electrónicos contengan datos de carácter personal les será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.

3. 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.

4. 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 repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros

metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

Artículo 23. Formatos de los documentos.

1. 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 contenido del documento, de la firma electrónica y de los metadatos que lo acompañan.

2. La elección de formatos de documento electrónico normalizados y perdurables para asegurar la independencia de los datos de sus soportes se realizará de acuerdo con lo previsto en el artículo 11.

3. 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.

Artículo 24. Digitalización de documentos en soporte papel.

1. 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:

a) 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.

b) Nivel de resolución.

c) Garantía de imagen fiel e íntegra.

d) Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización.

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

CAPÍTULO XI

Normas de conformidad

Artículo 25. Sedes y registros electrónicos.

La interoperabilidad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos, se regirán por lo establecido en el Esquema Nacional de Interoperabilidad.

Artículo 26. Ciclo de vida de servicios y sistemas.

La conformidad con el Esquema Nacional de Interoperabilidad se incluirá en el ciclo de vida de los servicios y sistemas, acompañada de los correspondientes procedimientos de control.

Artículo 27. Mecanismo de control.

Cada órgano o Entidad de Derecho Público establecerá sus mecanismos de control para garantizar, de forma efectiva, el cumplimiento del Esquema Nacional de Interoperabilidad.

Artículo 28. Publicación de conformidad.

Los órganos y Entidades de Derecho Público de las Administraciones públicas darán publicidad, en las correspondientes sedes electrónicas, a las declaraciones de conformidad y a otros posibles distintivos de interoperabilidad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Interoperabilidad.

CAPÍTULO XII

Actualización

Artículo 29. Actualización permanente.

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

Disposición adicional primera. Desarrollo del Esquema Nacional de Interoperabilidad.

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas:

a) Norma Técnica de Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

b) Norma Técnica de Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.

c) Norma Técnica de Digitalización de documentos: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

d) Norma Técnica de Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) Norma Técnica de Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones Públicas.

f) Norma Técnica de Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones Públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

g) Norma Técnica de Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras Administraciones.

h) Norma Técnica de Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones Públicas y por los organismos públicos y entidades de derecho público vinculados o dependientes de aquéllas.

i) Norma Técnica de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.

j) Norma Técnica de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) Norma Técnica de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.

l) Norma Técnica de Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

m) Norma Técnica de interoperabilidad de inventario y codificación de objetos administrativos: tratará las reglas relativas a la codificación de objetos administrativos, así como la conexión entre los inventarios correspondientes, incluyendo, por un lado, las unidades orgánicas y oficinas de la Administración, y, por otro lado, la información administrativa de procedimientos y servicios.

n) Norma Técnica de Interoperabilidad de Transferencia e Ingreso de documentos y expedientes electrónicos: tratará los requisitos y condiciones relativos a la transferencia de agrupaciones documentales en formato electrónico, documentos y expedientes electrónicos, junto con los metadatos asociados, entre sistemas de gestión de documentos electrónicos y sistemas de archivo electrónico.

ñ) Norma Técnica de Interoperabilidad de Valoración y Eliminación de documentos y expedientes electrónicos: tratará las condiciones y requisitos relativos a la valoración de los documentos y expedientes electrónicos para establecimiento de plazos de conservación, transferencia y acceso o, en su caso, eliminación total o parcial.

o) Norma Técnica de Interoperabilidad de preservación de documentación electrónica: tratará las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los documentos y su contexto.

p) Norma Técnica de Interoperabilidad de tratamiento y preservación de bases de datos: tratará las condiciones y requisitos relativos a la conservación de las bases de datos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los datos y su contexto.

q) Norma Técnica de Interoperabilidad de Plan de Direccionamiento: tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas.

r) Norma Técnica de Interoperabilidad de reutilización de activos en modo producto y en modo servicio: tratará los requisitos y condiciones para facilitar la reutilización de activos tanto en modo producto como en modo servicio por las Administraciones Públicas españolas.

s) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros de funcionarios habilitados: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de funcionarios habilitados pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas.

t) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros electrónicos de apoderamientos: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, A los registros mercantiles, de la propiedad, y a los protocolos notariales.

u) Norma Técnica de Interoperabilidad de Sistema de Referencia de documentos y repositorios de confianza: tratará los requisitos técnicos que deberán cumplir las referencias a documentos al ser intercambiadas, de forma que se evite trasladar documentación de forma innecesaria.

v) Norma Técnica de Política de firma electrónica y de certificados en el ámbito estatal: tratará las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, organizadas alrededor de los conceptos de generación y validación de firma e incluirá los perfiles interoperables de los medios de identificación de las Administraciones Públicas previstos en Ley 40/2015, de 1 de octubre.

2. El Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica prevista en la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aprobará las normas técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

3. Para la redacción y actualización de las normas técnicas de interoperabilidad indicadas en el apartado 1 y las futuras que pueda aprobar el Ministerio de Asuntos Económicos y Transformación Digital que sean necesarias para garantizar el adecuado nivel de interoperabilidad como consecuencia del nivel de desarrollo tecnológico, los compromisos internacionales o el marco normativo aplicable, se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de Administración electrónica.

Para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del 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, el órgano competente será el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia.

4. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Sistema de Información Administrativa: Inventario de procedimientos administrativos, servicios prestados y otras actuaciones administrativas que generen documentación pública, conteniendo información de los mismos clasificada por funciones y con indicación de su nivel de informatización, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: Almacenará, publicará y difundirá los modelos de datos de los servicios de interoperabilidad entre Administraciones Públicas y de estas con los ciudadanos, tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, además de las especificaciones semánticas y codificaciones relacionadas. Su propósito es facilitar la comprensión semántica de los servicios de intercambio de datos de las Administraciones y maximizar la reutilización de activos semánticos en la construcción de éstos. Se conectará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Centro de Transferencia de Tecnología: Directorio de aplicaciones para su libre reutilización que contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

d) Directorio Común de Unidades Orgánicas y Oficinas de las Administraciones Públicas: Instrumento que permitirá la sincronización de los sistemas que traten la información de inventariado, codificación y evolución de unidades orgánicas y oficinas en diferentes modalidades de integración para garantizar la flexibilidad tanto en el consumo como en la provisión de información relacionada.

Disposición adicional segunda. Formación.

El personal de las Administraciones públicas recibirá la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Interoperabilidad, a cuyo fin los órganos responsables dispondrán lo necesario para que esta formación sea una realidad efectiva.

Disposición adicional tercera. Suprimido

Disposición adicional cuarta. Suprimido

Disposición adicional quinta. Normativa técnica relativa a la reutilización de recursos de información.

La normativa relativa a la reutilización de recursos de información deberá estar aprobada a más tardar el 1 de junio de 2012.

ANEXO

Glosario de términos

Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.

Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

Cadena de interoperabilidad: Expresión de la interoperabilidad en el despliegue de los sistemas y los servicios como una sucesión de elementos enlazados e interconectados, de forma dinámica, a través de interfaces y con proyección a las dimensiones técnica, semántica y organizativa.

Ciclo de vida de un documento electrónico: Conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de documentos, hasta su selección para conservación permanente, de acuerdo con la legislación sobre Archivos de aplicación en cada caso, o para su destrucción reglamentaria.

Coste que no suponga una dificultad de acceso: Precio del estándar que, por estar vinculado al coste de distribución y no a su valor, no impide conseguir su posesión o uso.

Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.

Digitalización: El proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Especificación técnica: Una especificación que figura en un documento en el que se definen las características requeridas de un producto, tales como los niveles de calidad, el uso específico, la seguridad o las dimensiones, incluidas las prescripciones aplicables al producto en lo referente a la denominación de venta, la terminología, los símbolos, los ensayos y métodos de ensayo, el envasado, el marcado y el etiquetado, así como los procedimientos de evaluación de la conformidad.

Especificación formalizada: Aquellas especificaciones que o bien son normas en el sentido de la Directiva 98/34 o bien proceden de consorcios de la industria u otros foros de normalización.

Esquema de metadatos: Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su ciclo de vida.

Estándar: Véase norma.

Estándar abierto: Aquél que reúne las siguientes condiciones:

a) Que sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

b) Que su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

Ficheros de implementación de las políticas de firma: Son la representación en lenguaje formal (XML o ASN.1) de las condiciones establecidas en la política de firma, acorde a las normas técnicas establecidas por los organismos de estandarización.

Firma electrónica: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Formato: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria.

Herramientas genéricas: Instrumentos y programas de referencia, compartidos, de colaboración o componentes comunes y módulos similares reutilizables que satisfacen las necesidades comunes en los distintos ámbitos administrativos.

Imagen electrónica: Resultado de aplicar un proceso de digitalización a un documento.

Índice electrónico: Relación de documentos electrónicos de un expediente electrónico, firmada por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

Infraestructura o servicio común: capacidad organizativa y técnica que satisface necesidades comunes de los usuarios en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.

Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Interoperabilidad organizativa: Es aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.

Interoperabilidad semántica: Es aquella dimensión de la interoperabilidad relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.

Interoperabilidad técnica: Es aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.

Interoperabilidad en el tiempo: Es aquella dimensión de la interoperabilidad relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas; se manifiesta especialmente en la conservación de la información en soporte electrónico.

Licencia Pública de la Unión Europea («European Union Public Licence-EUPL»): Licencia adoptada oficialmente por la Comisión Europea en las 22 lenguas oficiales comunitarias para reforzar la interoperabilidad de carácter legal mediante un marco colectivo para la puesta en común de las aplicaciones del sector público.

Lista de servicios de confianza (TSL): Lista de acceso público que recoge información precisa y actualizada de aquellos servicios de certificación y firma electrónica que se consideran aptos para su empleo en un marco de interoperabilidad de las Administraciones públicas españolas y europeas.

Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

Modelo de datos: Conjunto de definiciones (modelo conceptual), interrelaciones (modelo lógico) y reglas y convenciones (modelo físico) que permiten describir los datos para su intercambio.

Nivel de resolución: Resolución espacial de la imagen obtenida como resultado de un proceso de digitalización.

Nodo de interoperabilidad: Organismo que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que éstas fijen.

Norma: Especificación técnica aprobada por un organismo de normalización reconocido para una aplicación repetida o continuada cuyo cumplimiento no sea obligatorio y que esté incluida en una de las categorías siguientes:

a) norma internacional: norma adoptada por una organización internacional de normalización y puesta a disposición del público,

b) norma europea: norma adoptada por un organismo europeo de normalización y puesta a disposición del público,

c) norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público.

Política de firma electrónica: Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

Procedimiento administrativo: Proceso formal regulado jurídicamente para la toma de decisiones por parte de las Administraciones públicas para garantizar la legalidad, eficacia, eficiencia, calidad, derechos e intereses presentes, que termina con una resolución en la que se recoge un acto administrativo; este proceso formal jurídicamente regulado se implementa en la práctica mediante un proceso operativo que coincide en mayor o menor medida con el formal.

Proceso operativo: Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Repositorio electrónico: Archivo centralizado donde se almacenan y administran datos y documentos electrónicos, y sus metadatos.

Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Servicio de interoperabilidad: Cualquier mecanismo que permita a las Administraciones públicas compartir datos e intercambiar información mediante el uso de las tecnologías de la información.

Soporte: Objeto sobre el cual o en el cual es posible grabar y recuperar datos.

Trámite: Cada uno de los estados y diligencias que hay que recorrer en un negocio hasta su conclusión.

Uso generalizado por los ciudadanos: Usado por casi todas las personas físicas, personas jurídicas y entes sin personalidad que se relacionen o sean susceptibles de relacionarse con las Administraciones públicas españolas.

Política de firma electrónica: Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

Procedimiento administrativo: Proceso formal regulado jurídicamente para la toma de decisiones por parte de las Administraciones públicas para garantizar la legalidad, eficacia, eficiencia, calidad, derechos e intereses presentes, que termina con una resolución en la que se recoge un acto administrativo; este proceso formal jurídicamente regulado se implementa en la práctica mediante un proceso operativo que coincide en mayor o menor medida con el formal.

Proceso operativo: Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Repositorio electrónico: Archivo centralizado donde se almacenan y administran datos y documentos electrónicos, y sus metadatos.

Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Servicio de interoperabilidad: Cualquier mecanismo que permita a las Administraciones públicas compartir datos e intercambiar información mediante el uso de las tecnologías de la información.

Soporte: Objeto sobre el cual o en el cual es posible grabar y recuperar datos.

Trámite: Cada uno de los estados y diligencias que hay que recorrer en un negocio hasta su conclusión.

Uso generalizado por los ciudadanos: Usado por casi todas las personas físicas, personas jurídicas y entes sin personalidad que se relacionen o sean susceptibles de relacionarse con las Administraciones públicas españolas.

FICHA CONTROL 4ª

	1ª vuelta	2ª vuelta	3ª vuelta	Total
Horas de Estudio				

Controle el tiempo real de estudio de forma precisa. La primera vuelta, al ser la que exige la realización de esquemas y resúmenes, será la que más tiempo necesite. Acceda a las baterías de Test a través de la plataforma Aspirantes. Al contestar los mismos, para un correcto análisis de sus resultados, deberá en todo caso responder a todas y cada una de las preguntas, incluso las dudosas.

Test de Verificación de Nivel	Resultado*	Observaciones*
Sistemas Informáticos núm. 1		
Sistemas Informáticos núm. 2		
Sistemas Informáticos núm. 3		
Materias Técnico Científica núm. 1		**Al final del Tema**
Materias Técnico Científica núm. 2		**Al final del Tema**
Materias Técnico Científica núm. 3		**2ª Vuelta**
Materias Técnico Científica núm. 4		**3ª Vuelta**

Los posibles resultados son aprobado, insuficiente o suspenso. Anote en el recuadro de resultado el número de fallos que ha tenido. A continuación barra y número preguntas: 2/40

Tras la realización del Test de Verificación de Nivel, deberá de averiguar porque ha fallado en cada una de las preguntas, marcando en el temario si considera el concepto o datos relacionados de interés.

En el cuadro superior de observaciones debe dejar constancia del número de las preguntas falladas o erróneas, e incluso de aquellas que dudó aunque finalmente acertó. Una vez finalizado el temario, en una 2ª o 3ª vuelta del tema, deberá de contestar al menos aquellas que falló.

FICHA CONTROL FINAL

	1ª vuelta	2ª vuelta	3ª vuelta	Total
Horas de Estudio				

Controle el tiempo real de estudio de forma precisa. La primera vuelta, al ser la que exige la realización de esquemas y resúmenes, será la que más tiempo necesite. Acceda a las baterías de Test a través de la plataforma Aspirantes. Al contestar los mismos, para un correcto análisis de sus resultados, deberá en todo caso responder a todas y cada una de las preguntas, incluso las dudosas.

Test de Verificación de Nivel	Resultado*	Observaciones*
Materias Técnico Científica núm. 1		
Materias Técnico Científica núm. 2		
Materias Técnico Científica núm. 3		2ª Vuelta
Materias Técnico Científica núm. 4		3ª Vuelta

Los posibles resultados son aprobado, insuficiente o suspenso. Anote en el recuadro de resultado el número de fallos que ha tenido. A continuación barra y número preguntas: 2/40

Tras la realización del Test de Verificación de Nivel, deberá de averiguar porque ha fallado en cada una de las preguntas, marcando en el temario si considera el concepto o datos relacionados de interés.

En el cuadro superior de observaciones debe dejar constancia del número de las preguntas falladas o erróneas, e incluso de aquellas que dudó aunque finalmente acertó. Una vez finalizado el temario, en una 2ª o 3ª vuelta del tema, deberá de contestar al menos aquellas que falló.

ANTES DE HACER TEST FINALES VER VÍDEOS DE REFUERZO SI LOS HAY

CONOCIMIENTOS Guardia Civil

Parte I

249 €

TEMARIO, TUTORIALES Y TEST

TUTOR PERSONAL

✔ Temas 1 al 4

ACCEDER

CONOCIMIENTOS Guardia Civil

Parte II

249 €

TEMARIO, TUTORIALES Y TEST

TUTOR PERSONAL

✔ Temas 5 al 9

ACCEDER

CONOCIMIENTOS Guardia Civil

Parte III

249 €

TEMARIO, TUTORIALES Y TEST

TUTOR PERSONAL

✔ Temas 10 al 14

ACCEDER

CONOCIMIENTOS Guardia Civil

Parte IV

249 €

TEMARIO, TUTORIALES Y TEST

TUTOR PERSONAL

✔ Temas 15 al 19

ACCEDER

CONOCIMIENTOS Guardia Civil

Parte V

249 €

TEMARIO, TUTORIALES Y TEST

TUTOR PERSONAL

✔ Temas 20 al 23 y finales

ACCEDER

CONOCIMIENTOS Guardia Civil

Completo

950 €

+ GRAMAT-ORTOG-PSICO

TUTOR PERSONAL

✔ Ahorras un 40%

ACCEDER

GRAMÁTICA ORTOGRAFÍA

Guardia Civil

99 €

TEMARIO, TUTORIALES Y TEST

TUTOR PERSONAL

✔ Ejercicios Prácticos

ACCEDER

GRAMÁTICA INGLESA

Guardia Civil

50 - 240 €

Solo para inscritos en Curso Completo

TUTOR PERSONAL

✔ Ejercicios Prácticos

INFORMACIÓN

PSICOTÉCNICOS Guardia Civil

PRÁCTICO

99 €

TEMARIO, TUTORIALES Y TEST

TUTOR PERSONAL

✔ Ejercicios Prácticos

ACCEDER

CONOCIMIENTOS Guardia Civil

"PERMANENTE"

2.400 €

Hasta 3 convocatorias

TUTOR PERSONAL

✔ 3 años

INFORMACIÓN

ENTREVISTA Guardia Civil

SIMULACRO REAL

150 - 200 €

VARIAS SEDES A NIVEL NACIONAL

POR MANDOS DEL CUERPO

✔ Preparación indivudalizada

INFORMACIÓN

Canal de Información para Opositores

GRUPOS DE WHATSHAPP PARA OPOSITORES POR CCAA

...en Aspirantes tú marcas el ritmo

(pulsa en el ICONO al que te interese acceder)

aspirantes.es