

Opinión de Davara&Davara respecto al supuesto
práctico de la convocatoria TIC de 2010

Nuestra opinión respecto al supuesto práctico de la convocatoria TIC de 2010

En primer lugar, y respecto a la cesión de datos de carácter personal, es necesario partir de la base de lo dispuesto por la Ley Orgánica 15/1999¹ (en adelante, LOPD), en su artículo 11 que afirma que es necesario el consentimiento previo del interesado para una cesión o comunicación de datos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario. Sin embargo, entre las excepciones a la necesidad de contar con el consentimiento del interesado para la cesión de datos, en concreto en el apartado 2 letra d del citado artículo 11 se encuentra la siguiente: “ cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas”. Por tanto, comenzamos afirmando que la cesión del Ministerio del Interior a los Agentes facultados de las Fuerzas y Cuerpos de Seguridad del Estado se encuentra amparada tanto por el 11.2.d) de la LOPD como por el artículo 1 de la ley 25/2007 **siempre y cuando sea previa autorización judicial.**

10. En relación con la seguridad, conteste y justifique:

¿Qué nivel de seguridad aplicaría a los datos cedidos desde el punto de vista de la protección de datos personales? Indique la norma y artículo que lo determina.

¹ Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

A la hora de establecer el nivel de medidas de seguridad aplicable a los datos cedidos –esto es, los datos de tráfico de una operadora de comunicaciones- es necesario acudir al artículo 81 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (en adelante, RLOPD o el Reglamento), por cuanto establece los niveles de seguridad aplicables a los ficheros que contengan datos de carácter personal. En este sentido, en concreto el artículo 81.4 establece que “A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, **se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento**”. Por tanto, le es aplicable el nivel medio y tan sólo la medida de seguridad de nivel alto del artículo 103 del RLOPD correspondiente al registro de accesos.

¿En qué categoría clasificaría el Sistema de Información?

Respecto a la categorización de los sistemas de información, es necesario acudir a lo dispuesto en el Título X de Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS). En concreto, en su artículo 43.2 , establece un criterio objetivo para establecer una categoría para un Sistema de Información basado en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I donde establece el procedimiento para dicha categorización, haciendo referencia

en su apartado 1º a que tal perjuicio se valorará dicho impacto en base a la capacidad organizativa para: Alcanzar sus objetivos, proteger los activos a su cargo, cumplir sus obligaciones diarias de servicio, respetar la legalidad vigente y respetar los derechos de las personas. En este mismo sentido para determinar dicho impacto se deben tener en cuenta las siguientes dimensiones de seguridad que serán identificadas por sus iniciales en mayúsculas: Disponibilidad [D], Autenticidad [A], Integridad [I], Confidencialidad [C], Trazabilidad [T]. Ahora bien una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel, por tanto:

Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

- ◆ La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.
- ◆ El sufrimiento de un daño menor por los activos de la organización.
- ◆ El incumplimiento formal de alguna Ley o regulación, que tenga carácter de subsanable.
- ◆ Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.
- ◆ Otros de naturaleza análoga.

Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

- ◆ La reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.
- ◆ El sufrimiento de un daño significativo por los activos de la organización.
- ◆ El incumplimiento material de alguna Ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
- ◆ Causar un perjuicio significativo de difícil reparación a algún individuo.
- ◆ Otros de naturaleza análoga.

Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

- ◆ La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
- ◆ El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
- ◆ El incumplimiento grave de alguna Ley o regulación.

- ◆ Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
- ◆ Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

Una vez tengamos puntualizado lo antes indicado se procederá finalmente a determinar el sistema de información en tres categorías: Alta, Media y Básica. Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO. Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior. Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior. La determinación de la categoría de un sistema sobre la base de lo indicado anteriormente no implicará que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo.

¿Sería necesario realizar auditorías?

Respecto a la necesidad de someterse a auditorías, es necesario analizarlo desde una doble perspectiva: de un lado, en cuestión de protección de datos y, de otra, en relación con el Esquema Nacional de Seguridad.

En lo que respecta a la auditoría en protección de datos, la respuesta la encontramos en el artículo 96 del Reglamento de la LOPD que afirma que “a partir del nivel medio los sistemas de información e instalaciones de tratamiento

y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad correspondientes. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado anteriormente”. En este sentido, y tal y como hemos analizado en el primer apartado, los datos de tráfico de una operadora de comunicación, en base a lo dispuesto en el artículo 81.4 del RLOPD, han de considerarse de nivel medio, con la particularidad de la aplicación del artículo 103, medida de seguridad de nivel alto, plasmada en el Reglamento y, por tanto, han de someterse a la citada auditoría.

En todo caso, ha de tenerse en cuenta que el informe de auditoría en protección de datos deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas. Por tanto, en nuestro caso concreto, **deberá verificar el cumplimiento de todas las medidas de seguridad plasmadas en el Reglamento correspondientes al nivel medio de medidas de seguridad y la medida de seguridad de nivel alto del artículo 103 del citado Reglamento.**

Finalmente, simplemente destacar que los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Por lo que respecta a la auditoría que exige el Esquema Nacional de Seguridad, el Capítulo V del Real Decreto 3/2010 por el que se aprueba el Esquema Nacional de Seguridad está integrado por un único artículo, el 34, que bajo el epígrafe “auditoría de la seguridad” afirma:

1. Los sistemas de información a los que se refiere el presente real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

2. Esta auditoría se realizará en función de la categoría del sistema, determinada según lo dispuesto en el anexo I y de acuerdo con lo previsto en el anexo III.

3. En el marco de lo dispuesto en el artículo 39, de la ley 11/2007, de 22 de junio, la auditoría profundizará en los detalles del sistema hasta el nivel que considere que proporciona evidencia suficiente y relevante, dentro del alcance establecido para la auditoría.

4. En la realización de esta auditoría se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.

5. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del presente real decreto, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se

consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

6. Los informes de auditoría serán presentados al responsable del sistema y al responsable de seguridad competentes. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

7. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

8. Los informes de auditoría podrán ser requeridos por los responsables de cada organización con competencias sobre seguridad de las tecnologías de la información.

¿Sería obligatorio cifrar la base de datos?

En base al art. 104 del RLOPD, conforme al art. 81.3 de este reglamento, cuando se deban implantar las medidas de seguridad de nivel alto (en nuestro supuesto, tan sólo ha de aplicarse la medida plasmada en el artículo 103 del Reglamento), la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros. Esto quiere decir que se realizará cifrado de los datos en los siguientes supuestos:

- a. Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

- b. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- c. Aquéllos que contengan datos derivados de actos de violencia de género.

En este sentido, consideramos que nuestro supuesto se integra dentro de lo dispuesto en el apartado b) citado y, por tanto, la base de datos que contenga los datos de tráfico solicitados por las fuerzas y cuerpos de seguridad del Estado tendrá que ir cifrada.

¿Sería necesario implementar un registro de accesos?

Es obligatorio que se implemente un registro de accesos ya que a los datos de tráfico de una operadora de comunicaciones –como es nuestro supuesto- y conforme a lo dispuesto en el art. 81.4 del RLOPD se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 del citado Reglamento, Registro de accesos, que reza así:

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

- a) Que el responsable del fichero o del tratamiento sea una persona física.
- b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

¿Qué certificados utilizaría?

Con relación a la interoperabilidad de la identificación y autenticación por medio de certificados electrónicos, contempla la Ley de acceso (artículo 21) que los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por las Administraciones Públicas como válidos para relacionarse con las mismas, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones Públicas la información que sea precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas, añadiendo que los sistemas de firma electrónica utilizados o admitidos por alguna Administración Pública distintos de los basados en los certificados indicados, podrán ser, igualmente, admitidos por otras Administraciones, conforme a principios de reconocimiento mutuo y reciprocidad.

La LFE avanza y profundiza en el tema, distinguiendo entre firma electrónica, firma electrónica avanzada y firma electrónica reconocida. De esta forma, indica

la LFE que una firma electrónica avanzada², que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá³ respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel⁴.

Y a esta firma electrónica avanzada, a la que le otorga todos los efectos jurídicos, la denomina firma electrónica reconocida por estar basada en un certificado electrónico reconocido. Se introduce aquí un nuevo concepto que es el que otorga la máxima validez jurídica a la firma electrónica llegando a tener el mismo valor que la firma manuscrita; y este nuevo concepto es el de certificado electrónico. Y no solamente el concepto de certificado, sino que tiene que ser un certificado electrónico “reconocido”.

Pues hablemos, por tanto, de certificados electrónicos reconocidos para llegar a conocer la firma electrónica reconocida. Partiremos en primer lugar del concepto de certificado electrónico que nos llevará al de prestador de servicios de certificación.

Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Luego un certificado electrónico es un documento que vincula la clave pública (datos de verificación de firma), con una persona, confirmando su identidad. Esta persona, que es el firmante tiene que poseer un dispositivo de creación de firma y, a partir de sus datos de creación de firma (clave privada), haber podido firmar un documento.

² Entendiendo por tal aquella firma electrónica que permite la identificación del signatario y que está vinculada únicamente al mismo de forma que sea detectable cualquier modificación posterior de los datos a los que se refiere.

³ Artículo 3, apartado cuarto.

⁴ En este sentido, indica el Considerando (20) de la Directiva 1999/93/CE, que las firmas electrónicas avanzadas basadas en un certificado reconocido pretenden lograr un mayor nivel de seguridad, pero, las firmas electrónicas avanzadas relacionadas con un certificado reconocido y creadas mediante un dispositivo seguro de creación de firma únicamente pueden considerarse jurídicamente equivalentes a las firmas manuscritas si se cumplen los requisitos aplicables a las firmas manuscritas.

Para comprobar la identidad del firmante se hace a través de la clave pública de forma que el certificado electrónico que se emita vincule la clave pública a esa persona confirmando así su identidad.

Surgen así los denominados prestadores de servicios de certificación que la LFE en su Exposición de Motivos califica como *“los sujetos que hacen posible el empleo de la firma electrónica”*. Y ¿qué hacen estos prestadores de servicios de certificación? Pues, en principio, lo que hacen es emitir certificados electrónicos consistentes en documentos electrónicos que *“relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal”*⁵.

Al emitir certificados electrónicos que van a ser la base para garantizar la identidad de la persona firmante de un documento electrónico, la LFE les obliga a efectuar una tutela y gestión permanente de los certificados que expiden. Hasta tal punto es así que les obliga a hacer una declaración de prácticas de certificación extensa y exigente en la que se deben especificar las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos y, además, deben mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse actualizadamente si los certificados están vigentes o si su vigencia ha sido suspendida o extinguida.

Indica a este respecto la LFE en su artículo 19, bajo el epígrafe de “declaración de prácticas de certificación”, que todos los prestadores de servicios de certificación deberán formular una declaración de prácticas de certificación en la que detallarán las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma; esto es, la gestión de la clave privada (datos de creación de firma) y de la clave pública (datos de verificación de firma).

⁵ Tercer párrafo, del apartado II de la Exposición de Motivos de la LFE.

También deberán detallar las obligaciones relativas a la gestión de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso, la existencia de procedimientos de coordinación con los Registros públicos⁶ correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

Esta declaración de prácticas de certificación deberá estar disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita y, además, tendrá la consideración de documento de seguridad a los efectos previstos en el artículo 9 de la Ley de Protección de datos y en el Título VIII de su Reglamento de desarrollo, por lo que deberán contener todos los requisitos exigidos para el documento de seguridad en el referido reglamento.

Concluyendo diremos que es necesaria una firma electrónica reconocida, basada en un certificado reconocido y que haya sido creada por un dispositivo seguro de creación de firma, para que tenga el mismo valor jurídico que la firma manuscrita y sea admitida como prueba en juicio y, todo ello, con la participación de los prestadores de servicios de certificación que emitirán certificados electrónicos reconocidos que garanticen la identidad del firmante en la forma ya expresada.

Una vez hechas estas consideraciones, creemos que bastará con hacer uso de certificados electrónicos de firma electrónica avanzada, si bien se podría contemplar la posibilidad de usar certificados basados en firma electrónica reconocida puesto que la seguridad es máxima.

⁶ En este sentido, el último párrafo, del apartado III, de la Exposición de Motivos de nuestra vigente Ley de Firma Electrónica, indica que “debe destacarse que la ley permite que los prestadores de servicios de certificación podrán, con el objetivo de mejorar la confianza en sus servicios, establecer mecanismos de coordinación con los datos que preceptivamente deban obrar en los Registros públicos, en particular, mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de estos. Dichos mecanismos de coordinación también podrán contemplar la notificación telemática por parte de los registros a los prestadores de servicios de certificación de las variaciones registrales posteriores”.

¿Sería necesario declarar este fichero ante la Agencia Española de Protección de Datos?

Sí, tal y como establece el artículo 26 de la LOPD en su primer apartado “Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos”, y a su vez el Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. Deberá inscribir el fichero de los datos de tráfico que conserva la operadora y ha de hacerlo mediante el programa NOTA de inscripción de ficheros de manera electrónica a través del sitio web de la Agencia Española de Protección de Datos (www.agpd.es), indicando el nombre del fichero, responsable del fichero, dirección, teléfono, datos, nivel de medidas de seguridad, cesiones de datos, transferencia internacional de datos y demás apartados que le requiera el formulario.

¿Y publicarlo en el Boletín Oficial del Estado (BOE)?

No es necesario publicar la inscripción del fichero en el Boletín Oficial del Estado por cuanto se trata de una inscripción de un fichero de titularidad privada y, como tal, no ha de notificarse en el BOE. Esta obligación es únicamente exigible a los ficheros de datos de carácter personal de titularidad pública, tal y como exige el artículo 20 de la LOPD , en lo que se refiere a los ficheros de titularidad pública, afirma que “La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente”.

Indique dónde aplica el Esquema Nacional de Interoperabilidad (ENI) en el sistema. Justifique su respuesta.

El Preámbulo del Real Decreto 4/2010 por el que se aprueba el Esquema Nacional de Interoperabilidad afirma que su finalidad 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 redunde en beneficio de la eficacia y la eficiencia.

Por interoperabilidad entiende el Real Decreto 4/2010, la 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.

La interoperabilidad es absolutamente necesaria, entre otras cuestiones, para la cooperación, el desarrollo, la integración y la prestación de servicios conjuntos por las Administraciones Públicas, facilitando el desarrollo de la Administración electrónica y de la Sociedad de la Información.

Esta interoperabilidad abarca a distintas actuaciones que se interrelacionan para poder operar en la Administración electrónica y que, como es natural, se han tenido en cuenta, en el momento de desarrollar la regulación del ENI; desde lo contemplado en la propia Ley de acceso a la consideración de otras acciones necesarias para completar la seguridad de acceso del ciudadano electrónicamente a los servicios públicos, como pueden ser el derecho fundamental a la protección de datos, recogido en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y su normativa de desarrollo, hasta la identificación y autenticación electrónica tanto de los ciudadanos como de la propia Administración y, en particular, todo lo relativo a la normativa sobre

firma electrónica y Documento Nacional de Identidad electrónico, centrado en la Ley 59/2003 de firma electrónica, contando también con su normativa de desarrollo, pasando por cuestiones de accesibilidad, uso de lenguas oficiales, reutilización de la información en el sector público y órganos colegiados responsables de la Administración electrónica.

El ámbito de aplicación del Real Decreto es, al igual que el de la Ley de acceso, tanto las Administraciones Públicas en general -entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de Derecho Público vinculadas o dependientes de las mismas-, como los ciudadanos en sus relaciones con las Administraciones Públicas y las relaciones entre ellas, no siendo de aplicación a las Administraciones Públicas en las actividades que desarrollen en régimen de derecho privado.

La aplicación del ENI, señala el artículo 4 del Real Decreto que se desarrollará de acuerdo con los siguientes principios específicos de la interoperabilidad: a) La interoperabilidad como cualidad integral. b) Carácter multidimensional de la interoperabilidad y c) Enfoque de soluciones multilaterales.

Respecto a la interoperabilidad como cualidad integral señala que 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.

Con relación al carácter multidimensional de la interoperabilidad, ésta se entenderá contemplando sus dimensiones organizativa, semántica y técnica.

Respecto a la interoperabilidad semántica, que ya hemos indicado se centra en las cuestiones necesarias para que los sistemas de información puedan leer y entender la información que intercambian, establece el Real Decreto 4/2010, bajo el epígrafe de “activos semánticos”, que 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, añadiendo que 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.

Estos modelos de datos se ajustarán a lo previsto en el propio Real Decreto sobre estándares aplicables y a los que hacemos referencia al tratar sobre la interoperabilidad técnica.

Respecto a la utilización de la firma electrónica para la identificación, y en su caso, autenticación, del ciudadano y de la Administración - con todas sus posibilidades y el potencial que comporta cada uno de los diferentes tipos o formas de firma que se pueden adoptar, desde la que podemos llamar firma electrónica “a secas”, a la firma electrónica reconocida, basada en un certificado reconocido, pasando por la firma electrónica avanzada con la utilización de la seguridad que otorga la criptografía de clave asimétrica -, puede tornarse en un auténtico caos de incompatibilidad y, consecuentemente, de falta de interoperabilidad si no se siguen unos estándares que orienten o guíen en un camino determinado que permita optimizar los recursos, por un lado de la Administración General del Estado y por otro, cuando se considere conveniente por los distintos órganos, de las diferentes Administraciones Autonómicas o Locales.

Es así que la Administración General del Estado deberá fijar una política de firma electrónica y de certificados que, tal y como señala el artículo 18 del ENI,

sirva de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación. Pero esto no significa en absoluto que se establezca un coto cerrado en la Administración General del Estado sino, por el contrario, el camino debe quedar abierto para que esta política pueda ser adoptada y utilizadas sus ventajas por el resto de las Administraciones que así lo decidan.

Con relación a los documentos electrónicos, se deben adoptar medidas uniformes, tanto técnicas como organizativas, con el fin de garantizar su interoperabilidad a lo largo del ciclo de vida del propio documento, a cuyos efectos establece el apartado segundo del artículo 21 del ENI que 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 referidos documentos electrónicos.

**ALGUNOS ASPECTOS DEL REAL DECRETO 424/2005 QUE
CONVIENE TENER EN CUENTA**

Artículo 17. Condiciones generales

Las condiciones generales que deben cumplir todos los operadores, con independencia de la red o servicio que pretendan explotar o prestar, y sin perjuicio de otras que resulten exigibles conforme a los artículos siguientes de este capítulo, serán las siguientes:

h) Ejecutar las órdenes de interceptación legal que emanen de la autoridad competente, conforme a la Ley de Enjuiciamiento Criminal y a la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, de acuerdo con lo establecido en el artículo 33 de la Ley 32/2003, de 3 de noviembre, y en el título V de este Reglamento.

i) Cumplir, cuando así venga establecido en la normativa vigente, las resoluciones de las autoridades adoptadas por razones de interés público, de seguridad pública y de defensa nacional.

Capítulo II

La interceptación legal de las comunicaciones

Sección I

Disposiciones generales

Artículo 83. Objeto

Es objeto de este capítulo el establecimiento del procedimiento que debe seguirse y las medidas que deberán adoptar, de conformidad con el artículo 33 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, los operadores que presten o estén en condiciones de prestar servicios de comunicaciones electrónicas disponibles al público o de establecer o explotar redes públicas de comunicaciones electrónicas.

Las únicas interceptaciones que estarán obligados a realizar los sujetos a los que se refiere el artículo 85 son las dispuestas en el artículo 579 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.

Artículo 84. Definiciones

A los efectos de lo dispuesto en este capítulo, los términos definidos en este artículo tendrán el significado siguiente:

a) Interceptación legal: medida establecida por ley y adoptada por una autoridad judicial que acuerda o autoriza el acceso o la transmisión de las comunicaciones electrónicas de una persona, y la información relativa a la interceptación, a los agentes facultados, sin perjuicio de lo establecido en el artículo 579.4 de la Ley de Enjuiciamiento Criminal.

b) Interfaz de interceptación: localización física o lógica dentro de las instalaciones de los sujetos obligados en la que se proporcionan las comunicaciones electrónicas interceptadas y la Real Decreto 424/2005, de 15 de abril, Reglamento sobre condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

información relativa a la interceptación a los agentes facultados. La interfaz de interceptación no es necesariamente un único punto fijo.

c) Orden de interceptación legal: resolución acordada por una autoridad judicial por la que se acuerda o autoriza la adopción de una medida de interceptación legal o se ordena lo necesario para su ejecución técnica a los sujetos obligados o un agente facultado.

d) Sujeto a la interceptación: la persona o las personas designadas, o bien incluidas de forma individualizadas, en la orden de interceptación legal cuyas comunicaciones electrónicas son objeto de la medida.

e) Agente facultado: policía judicial o personal del Centro Nacional de Inteligencia habilitado por una autoridad judicial para materializar una interceptación legal.

f) Autoridad judicial: autoridad a la que la ley faculta para acordar o autorizar la adopción y ordenar la ejecución técnica de una medida de interceptación legal.

g) Centro de recepción de las interceptaciones: instalación de los agentes facultados que recibe las comunicaciones electrónicas interceptadas y la información relativa a la interceptación de un determinado sujeto sometido a interceptación.

h) Itinerancia: situación en la que se presta un servicio de comunicaciones electrónicas por una red distinta de la local en la que está inscrito el usuario.

i) 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.

Artículo 85. Sujetos obligados y obligación de colaborar

1. **Estarán obligados a seguir los procedimientos y adoptar las medidas a las que se refiere el artículo 83 los operadores que presten o estén en condiciones de prestar servicios de comunicaciones electrónicas disponibles al público o de establecer o explotar redes públicas de comunicaciones en España, con independencia de la naturaleza, ámbito territorial y momento en que tuvo efecto su habilitación.**

Los operadores a los que se refiere el párrafo anterior estarán obligados a cumplir lo establecido en este capítulo, aun en el caso de que sólo presten en España acceso a una red pública de comunicaciones electrónicas, y todo aquel equipamiento susceptible de emplearse para realizar la interceptación se encuentre bajo la jurisdicción de otro Estado.

2. Cualquier operador de red que ponga ésta a disposición de un proveedor de servicios de comunicaciones electrónicas deberá colaborar con él en el cumplimiento de los requisitos de este capítulo.

Asimismo, cualquier otro proveedor de servicios de comunicaciones electrónicas disponibles al público que acuerde facilitar servicio de itinerancia con un proveedor principal estará obligado a colaborar con éste en el cumplimiento de los requisitos de este capítulo.

Artículo 86. Requisitos generales

1. **Los sujetos obligados deberán tener sus equipos configurados de forma que puedan facilitar el acceso de los agentes facultados a todas las comunicaciones transmitidas, generadas para su transmisión o recibidas por el sujeto de una interceptación legal y los datos de tráfico asociados a dicha comunicación.** Junto con las comunicaciones deberán poder facilitar la información relativa a la interceptación que se enumera en el artículo 88, aun cuando la comunicación quede en mero intento por no llegar a establecerse. La correspondencia entre una comunicación y la información relativa a dicha interceptación se hará de tal manera que se pueda establecer entre ambos una correlación inequívoca, siempre que sea técnicamente posible.

2. 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, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

3. Los sujetos obligados a los que hacen referencia los apartados anteriores deberán disponer de los medios técnicos y humanos que permitan el cumplimiento de las obligaciones establecidas en este reglamento.

Artículo 87. Acceso a las comunicaciones electrónicas

1. El acceso a una comunicación electrónica por el sujeto obligado se hará excluyendo cualquier otra comunicación que no se incluya en el ámbito de aplicación de la orden de interceptación legal.

2. **El acceso se facilitará para todo tipo de comunicaciones electrónicas, 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 facsímil.**

3. 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.

4. El acceso a las comunicaciones se facilitará aun cuando el sujeto de la interceptación utilice procedimientos para desviar las llamadas a otros servicios de comunicaciones electrónicas o a otros puntos de terminación de red, o a otros terminales, y aun cuando las llamadas sean procesadas por proveedores de servicios de comunicaciones electrónicas distintos de aquel al que se dirige la orden de interceptación, siempre que se pueda discernir la comunicación que es objeto de la orden de interceptación.

Artículo 88. Información relativa a la interceptación

1. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

- a) Identidad o identidades -en la acepción definida en el artículo 84.i- del sujeto objeto de la medida de la interceptación.
- b) Identidad o identidades -en la acepción definida en el artículo 84.i- 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. Real Decreto 424/2005, de 15 de abril, Reglamento sobre condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

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

2. 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 y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, 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 proveedor realiza las notificaciones.

Domicilio en el que el proveedor realiza las notificaciones:

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.

3. 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.

Sección II

Requisitos operacionales

Artículo 89. Información previa a la interceptación

1. En el marco de la investigación legal a requerimiento de la autoridad judicial o cuando así lo determine una norma con rango legal, los sujetos obligados conforme al artículo 85 pondrán a disposición de la autoridad que lleve a cabo dicha investigación, con carácter previo a la interceptación legal, información actualizada relativa a los datos a que hace referencia el artículo 90.

2. 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 residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

3. Los sujetos obligados conforme al artículo 85 deben tener dispuesta la organización necesaria que garantice el cumplimiento de la orden de interceptación legal en los términos establecidos en el artículo 99. Para ello, deberán identificar la unidad habilitada para recibir una orden de interceptación que les sea notificada y establecer los procedimientos internos para dar soporte a las actuaciones necesarias.

Artículo 90. Información para la interceptación.

La interceptación se llevará a efecto si en la orden de interceptación legal se incluye, al menos, uno de los datos siguientes:

- a) La identificación del abonado o usuario sujeto a la interceptación
- b) La ubicación donde se encuentre un punto de terminación de red al que el operador da servicio.
- c) Un identificador de punto de terminación de red (dirección), o de terminal, al que el proveedor de servicios de comunicaciones electrónicas da servicio.
- d) El código de identificación en caso de que sea el usuario el que active el terminal para la comunicación.
- e) Cualquier otra identidad -en la acepción definida en el artículo 84.i- que corresponda al sujeto especificado en la orden de interceptación legal.

Artículo 91. Lugares para la interceptación

Para delimitar las responsabilidades y asegurar mejor el secreto de las telecomunicaciones frente a terceras partes ajenas, su interceptación se realizará preferentemente en salas con acceso restringido que garantice la confidencialidad en los términos del artículo 92. En cualquier caso, se deberá garantizar el secreto de las comunicaciones, para lo que deberán adoptarse las medidas técnicas necesarias.

Artículo 92. Personal autorizado

Sin perjuicio de lo establecido en la legislación sobre protección de materias clasificadas, el sujeto obligado será responsable de que sólo el personal que haya sido expresamente autorizado pueda acceder a los mecanismos de interceptación.

Artículo 93. Confidencialidad

1. Todo documento relativo a las operaciones de interceptación, al igual que cualquier información relativa a procedimientos de interceptación, será de circulación restringida a las personas autorizadas de acuerdo con lo establecido en el artículo anterior y sin perjuicio de lo establecido en la legislación sobre materias clasificadas.

2. La interceptación se efectuará de manera que ni el sujeto a la interceptación, ni ninguna persona no autorizada, pueda tener conocimiento de ella. En particular, las prestaciones del servicio deben ser las mismas que en ausencia de interceptación, y ninguna alteración de éste puede permitir sospechar que se está realizando una interceptación.

Artículo 94. Acceso en tiempo real

La interceptación se realizará en tiempo real, sin más retardo que el mínimo imprescindible para realizar el encaminamiento y transmisión, e ininterrumpidamente durante el plazo establecido en la orden de interceptación legal. Si no se pudiera facilitar la información relativa a la interceptación a la que se refiere el artículo 88 en tiempo real por causa de fuerza mayor, se efectuará al finalizar la conexión y, en todo caso, lo antes posible.

Artículo 95. Interfaces de interceptación

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 reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.

Artículo 96. Señal en claro y calidad de la señal entregada

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 97. Secreto de las comunicaciones

Las comunicaciones y la información relativa a la interceptación sólo se facilitarán al agente facultado. Para ello, los sujetos a los que se refiere el artículo 85 pondrán todos los medios necesarios para impedir la manipulación de los mecanismos de interceptación, y para garantizar la autenticidad, confidencialidad e integridad de la información obtenida con la interceptación.

Artículo 98. Interceptaciones múltiples y simultáneas

1. Los sujetos obligados garantizarán que pueda llevarse a cabo de forma múltiple más de una interceptación legal en relación con una línea, un usuario o abonado.
2. El número máximo de interceptaciones simultáneas que ha de ser capaz de proveer un operador de red o proveedor de servicio se establecerá mediante orden ministerial.

Artículo 99. Plazo de ejecución de la interceptación

1. El plazo de ejecución de una orden de interceptación legal será el fijado en ella. Cuando no se establezca plazo, las órdenes se ejecutarán antes de las 12:00 horas del día laborable siguiente al que el sujeto obligado reciba la orden de interceptación legal.

2. Cuando la orden de interceptación legal establezca la urgencia de su ejecución, los sujetos obligados deberán ejecutarla con la mayor brevedad posible teniendo en cuenta lo dispuesto en la orden de interceptación.

3. La activación del mecanismo de interceptación será notificada al agente facultado por el medio que se acuerde entre dicho agente y el sujeto obligado.

Artículo 100. Abono del coste de la interceptación

El operador o proveedor de servicios de comunicaciones electrónicas que haya realizado una interceptación legal tendrá derecho a que se le abonen las cantidades en que haya incurrido por el uso de canales de comunicación, temporales o permanentes, que establezca de modo específico para facilitar la transmisión de las comunicaciones electrónicas interceptadas y la información relativa a la interceptación a los agentes facultados, teniendo en cuenta los precios que se apliquen en cada caso. En ningún caso serán objeto de compensación los gastos relativos a equipamientos específicos para la

interceptación de que, en su caso, tuviera que dotarse, toda vez que constituyen una carga accesoria a los deberes de la habilitación correspondiente.

Artículo 101. Infracciones

1. Sin perjuicio de la responsabilidad penal en que pueda incurrirse en la ejecución de las interceptaciones, el incumplimiento de las órdenes de interceptación legal será constitutivo de una infracción sancionable de acuerdo con las previsiones del título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. En la imposición de la sanción se valorará el retraso en la ejecución de la interceptación y otros perjuicios causados por el incumplimiento