## 1. INTRODUCCIÓN:

El proceso de modernización de las Administraciones públicas debe ser considerado como un medio para impulsar España hacia la Sociedad de la Información, nunca por el mero hecho de modernizarlas en sí mismas. Esta concepción obliga a forzar un cambio cultural administrativo, lo que supone, entre otras medidas, priorizar los proyectos y los recursos públicos en función del impacto de futuro que tengan sobre la sociedad, buscando la generalización de usos y usuarios de Correo electrónico sobre X - 400, de EDI, la transferencia de ficheros, la videoconferencia, la digitalización de la información de interés público, la puesta a disposición a través de Bases de Datos multimedia, y el estímulo a la industria nacional de informática, telecomunicaciones y audiovisual, mediante especificaciones técnicas en los concursos públicos que les permitan desarrollar su potencial de innovación capacitándolas para competir fuera de nuestras fronteras.

Dentro de una política general de calidad en el Sector público, el uso y explotación de elementos tecnológicos facilita las tareas, otorgando al directivo una posición estratégica preeminente para una gestión de calidad. Este empeño provoca que a los directivos públicos se les exija, para cumplir más razonablemente su labor directiva, actitudes y aptitudes que lleven a la organización de la cual dependen a una mejora constante de sus resultados.

Ahora bien, para cumplir los objetivos expuestos, los gestores públicos necesitan cada vez no sólo una mayor cantidad de información, sino una serie de procedimientos que aseguren la fiabilidad, entendida en un sentido amplio, de la citada información.

## 2. ÁMBITO NORMATIVO GENERAL:

El legislador, consciente de la necesidad de dotar a los órganos administrativos de un desarrollo tecnológico que les dote de una mayor efectividad, dinámica y flexibilidad, publicó la Ley 30/1992, L.R.J. y P.A.C., que en su Exposición de Motivos (ap. 4) recoge que

*"Este planteamiento tan limitado ha dificultado el que la informatización, soporte y tejido nervioso de las relaciones sociales y económicas de nuestra época, haya*

*tenido hasta ahora incidencia sustantiva en el procedimiento administrativo, por falta de reconocimiento formal de la validez de documentos y comunicaciones emitidos por dicha vía. El extraordinario avance experimentado en nuestras Administraciones Públicas en la tecnificación de sus medios operativos, a través de su cada vez mayor parque informático y telemático, se ha limitado a funcionamiento interno, sin correspondencia relevante con la producción jurídica de su actividad relacionada con los ciudadanos. Las técnicas burocráticas formalistas, supuestamente garantistas, han caducado, por más que a algunos les parezcan inamovibles, y la Ley se abre decididamente a la tecnificación y modernización de la actuación administrativa en su vertiente de producción jurídica y a la adaptación permanente al ritmo de las innovaciones tecnológicas*."

Al hilo de lo anterior, el artículo 45.2 hace referencia a que los ciudadanos "podrán" relacionarse con la Administración a través de medios electrónicos, informáticos o telemáticos, regulación de la que se desprende que, dada la naturaleza de esta facultad u opción, la misma debe quedar reflejada expresamente a efectos de notificaciones, tal como se desprende, en el caso de la Administración General del Estado, del artículo 7.2 letra c) del R.D. 263/1996, de 16 de febrero.

Ahora bien, este tipo de comunicaciones estará en todo caso supeditada al hecho de su compatibilidad con los medios técnicos de los que dispongan las Administraciones Públicas, contando en todo caso con las garantías y requisitos previstos en cada procedimiento, que permitiendo la agilización procedimental mediante el empleo de las nuevas técnicas de transmisión de la información, salvaguarden necesariamente las garantías de autenticidad de la misma.

Ciñéndonos a la ya clásica categorización que establece la Organización Internacional de Normas (más conocida por sus siglas en inglés ISO, International Organization for Standardization) en su norma ISO/IEC 7498-2 (Arquitectura de Seguridad de OSI, Open Sistems Interconnection), los servicios de seguridad (entendiendo por tales aquellas funciones suministradas por una red de ordenadores para garantizar su seguridad y la de las transferencias de datos) son, entre otros, los de autenticidad, integridad, confidencialidad, no repudio y control de accesos.

De manera muy escueta, entenderemos por confidencialidad de los datos su protección de ataques pasivos, tratando de ocultarlos para prevenir su revelación no autorizada ; por integridad la garantía de la recepción de los mensajes sin alteraciones no autorizadas ; por

autenticación la acreditación fehaciente de los participantes en una comunicación ; y por no repudio la evitación de que el emisor o el receptor de un mensaje pueda renegar de su emisión o de su recepción respectivamente.

La correcta utilización de estos servicios debería bastar para eliminar los posibles problemas de seguridad que pudieran producirse en las comunicaciones telemáticas en las que sea parte la Administración, y en las que el concurso de los mecanismos expuestos permite confiar en la próxima puesta a punto de nuevas facilidades de relación con el administrado, que en el futuro cercano podrán desembocar en la teleadministración, una de las prioridades del Libro Blanco de la Comisión de la Unión Europea sobre Crecimiento, Competitividad y Empleo.

## 3. EL REQUISITO GENERAL DE LA INTEROPERABILIDAD DE SISTEMAS:

### 3.1. Transferencias de datos entre Administraciones Públicas.

La complementariedad entre los distintos sistemas de información supone el enriquecimiento de los instrumentos de gestión administrativa sin necesidad de ser redundantes en los tratamientos ni en la propia disponibilidad de la información. Este objetivo de “información compartible” puede incluso complementarse con la creación de bases de información común.

La seguridad y la confidencialidad de los datos que se transmiten mediante la utilización de los medios electrónicos, informáticos y telemáticos no están aseguradas, en razón a veces, de la insuficiencia de medios o de distintas calidades de transmisión de las diferentes redes. Debe existir por tanto una interoperabilidad entre los sistemas y redes de comunicaciones, en forma tecnológica, operativa y de armonización legislativa, actuando la misma como garantía de utilización de las comunicaciones telemáticas.

Dentro de este marco, y en el estricto ámbito de las relaciones interadministrativas, destaca el proyecto INDALO, que tiene como objetivo la elaboración de un modelo de datos común para las Administraciones Públicas en sus principales áreas de actividad.

De esta forma, se da respuesta a la existencia de un buen número de flujos de información “no reglados” que alimentan los fondos de información con datos no homogéneos, sobre todo en su perspectiva temporal, y se favorece la detección de redundancias e inconsistencias en

el tratamiento de una información antiguamente gestionada por una única Administración, y actualmente fragmentada en virtud de las modificaciones acaecidas en el marco competencial de las Comunidades Autónomas y Administraciones Locales.

La implantación de este sistema ha encontrado inconvenientes como el de no disponer de una clave única para identificar al ciudadano en las distintas bases de datos (la existencia de números duplicados y de errores en la grabación de los dígitos del D.N.I. hace imprescindible la rápida generalización del dígito de control en este número) ; la inexistencia en el Sector Público de Centros de Compensación de Datos (lo que dificulta el establecimiento de modelos racionales de circulación de datos entre las Administraciones Públicas) ; o la necesidad de creación de una estructura profesional, con representación paritaria de las distintas Administraciones, que asuma las competencias de mantenimiento, extensión y divulgación del Modelo de Datos (INDANOR o Instituto de Normalización de Datos de las Administraciones).

Técnicamente, las Tecnologías de la Información requieren el cumplimiento de unas reglas de juego, que pueden sintetizarse así:

- Definición de datos a transferir/intercambiar.
- Identificación conceptual de datos.
- Definición de formatos de intercambio.
- Coordinación de las estructuras de los registros de información.
- Establecimiento de protocolos de intercambio
  + Tipo de soporte
  + Periodicidad
  + Normas organizativas
  + Responsabilidades, etc.
- Transferencia sobre la calidad de la información de cada sistema.

En definitiva, se precisa que las organizaciones transformen su concepción de los sistemas informáticos como sistemas de datos hacia una consideración de los mismos como verdaderos sistemas de información.

3.2. Transferencias de datos entre la Administración y las Empresas.

Los flujos de información entre la Administración y la Empresa pueden clasificarse en servicios de información (servicios ASC II, videotex, referenciales - bibliográficos o directorios -, fuente - numéricos, textual numéricos, textuales, e icónicos - y mixtos), de comunicación (audiomáticos - pasivos, interactivos, de mensajería vocal, radiomensajería, y multiaudioconferencia -, y telemáticos - videotex, mensajería telemática, y EDI) e híbridos.

Dentro de los servicios de información, destacan especialmente la mensajería telemática (el auténtico correo electrónico o “buzón electrónico” de almacenamiento y retransmisión, en el que destaca el X- 400, que asegura la compatibilidad entre los correos electrónicos privados, así como su interconexión internacional) y los servicios EDI, o transmisión electrónica de datos entre ordenadores, sin intervención manual.

Mediante EDI (Electronic Data Interchange) se sustituye el soporte físico - papel (desmaterialización de documentos) de los documentos administrativos más habituales que intercambian las Empresas con la Administración, por transacciones electrónicas entre sus respectivos ordenadores, una vez fijados los formatos para cada tipo de documento, transmitiendo electrónicamente su contenido de acuerdo con el formato y sintaxis fijados de antemano (interoperabilidad).

Sin embargo, con los sistemas de intercambio tradicionales llega un momento en que no es viable la conexión directa entre todos los elementos, puesto que el gran número de empresas involucradas generarían un excesivo número de líneas de comunicaciones, con diferentes protocolos y diferentes formatos, en función de las aplicaciones particulares de cada empresa. La solución se consigue mediante un Centro de Compensación intermedio, en el que cada empresa tenga asignado un “buzón”, evitando que el envío y la recepción coincidan en el tiempo.

Es una primera etapa quizás fuera conveniente la implantación del sistema EDI sobre un equipo frontal autónomo, que actuara inicialmente como puente entre el sistema informático actual y el mundo EDI exterior al mismo ; este hecho da lugar a la Estación de Trabajo EDI (“Work Station EDI”, o W.S.E). No obstante, conforme los requerimientos del EDI se estabilicen, las interfaces de usuario se hagan más complejas y la integración con el resto de aplicaciones informáticas convencionales se vaya extendiendo, las aplicaciones del EDI deberían abandonar el protegido entorno de la W.S.E. y desplazarse al centro de los sistemas informáticos corporativos.

El sistema EDI constituye por otro lado una red cerrada, a la que sólo tienen acceso los usuarios autorizados por las empresas de telecomunicación, de forma que proporciona un grado satisfactorio de control por parte de dichas empresas y, por tanto, de fiabilidad.

Algunos de los problemas que la Administración tradicionalmente se ha venido encontrando para realizar el intercambio de información con el Sector Privado son de carácter organizativo, que arrancan del ya mencionado bajo nivel de estándares de información dentro de la

Administración y a la concepción de una tendencia posesiva de los datos a nivel departamental (aparición de “fenómenos inducidos de acaparación”, recelo psicológico con aparición de servidumbres, etc.); de carácter tecnológico, que parten de la también mencionada ausencia de estándares en sistemas y comunicaciones, dado que la transportabilidad de la información parte de una gran multiplicidad de sistemas y estándares de información corporativos ; y de carácter jurídico, que se han visto considerablemente reducidos gracias a una novedosa normativa (pendiente aún de un mayor desarrollo), cuyo mayor o menor grado de acierto está aún por constatar, y que a continuación pasaremos a analizar.

# 4. MARCO NORMATIVO ESPECÍFICO DE SEGURIDAD.

## 4.1. Las Medidas de Seguridad.

Hay que ser conscientes de las limitaciones que la administración de los sistemas distribuidos objetivamente comporta, frente a una mayor inaccesibilidad de la anterior arquitectura informática de carácter centralizado, siendo preciso establecer por tanto medidas tanto técnicas como organizativas de los recursos al servicio de la nueva arquitectura de los sistemas de información.

En virtud de lo expuesto, los proyectos informáticos, desde su comienzo, desde la fase funcional o de prototipado, tienen que contemplar el nuevo Reglamento de medidas de seguridad, el Real Decreto 994/1999, de 11 de junio, publicado en el BOE núm. 151, de 25 de junio, que venía a desarrollar los artículos 9 y 44 de la ya derogada LORTAD, y que, según se indica en la disposición transitoria tercera de la nueva Ley de Protección de Datos, subsistirá en su vigencia hasta tanto se lleven a efecto las previsiones de la disposición final primera de dicha norma, y en cuanto no se opongan a lo dispuesto en esa Ley (incluyendo aquí el giro experimentado en cuanto al ámbito de aplicación de la LOPD mediante la supresión del término “automatizado” de su ámbito de aplicación).

A modo de resumen, clasificaremos la seguridad de la información en diferentes tipos. Así, la seguridad física hace referencia a las medidas de externas a los Centros de Proceso de Datos establecidas para la protección de éstos y de su entorno de amenazas físicas exteriores ; la seguridad lógica pretende proteger el patrimonio informacional de las aplicaciones informáticas y del contenido de las bases de datos y ficheros ; la seguridad organizativo -

administrativa complementa a las anteriores con políticas de seguridad, de personal, de contratación, análisis de riesgos (destacaremos en este punto el sistema M.A.G.E.R.I.T. o Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas, creado en el seno del S.S.I.T.A.D.), o planes de contingencia ; la seguridad jurídica pretende, a través de las normas legales, fijar el marco jurídico necesario para proteger los bienes informáticos. Es en este último apartado donde podríamos encuadrar al Reglamento de medidas de seguridad, que pese a la discutible oportunidad del momento de su publicación (hubiera sido más coherente haber esperado a la publicación de la Ley Orgánica de Protección de Datos de Carácter Personal y haber adecuado con carácter previo su articulado al contenido de ésta), no deja de ser un acierto en aras de la seguridad jurídica en esta materia.

4.2. La Firma Electrónica.

Siguiendo la Propuesta de Directiva del Parlamento Europeo y del Consejo (PDIR), por la que se establece un marco común para la firma electrónica, el Real Decreto Ley 14/1999, de 17 de septiembre, regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación, desvinculando el problema de la validez y efectos del documento electrónico.

La firma electrónica avanzada (que permite la identificación del signatario, habiendo sido creada por medios que éste maneja bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, permitiendo detectar cualquier modificación ulterior de éstos), siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

Incluso a aquella firma electrónica que no reúna todos los requisitos apuntados (como por ejemplo las firmas electrónicas respaldadas por un sistema voluntario de acreditación), no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica.

Hasta este momento, la doctrina y la jurisprudencia admiten el documento electrónico como fuente de prueba y lo hacen genéricamente. Esto es, cualquier documento electrónico despliega un potencial probatorio, que es canalizado a través del medio de prueba del reconocimiento

judicial o pericial (cfr. STS 30 - 11 - 1992). Sin importar sus condiciones técnicas de seguridad, el documento electrónico es admisible en juicio; postura ésta que coincide con la defendida por la mayoría de la doctrina. Ahora bien, después del Real Decreto Ley encontramos un nuevo tipo de documentos ("avalados") que ofrecen condiciones de seguridad y fiabilidad muy superiores a las ofrecidas por el documento electrónico tradicional (incluso, muy superiores a las que ofrece un documento privado escrito). Si esto es así, no parecería muy lógico mantener a este nuevo tipo de documento sujeto a la servidumbre del reconocimiento judicial o pericial. Más bien parecería adecuado equiparar plenamente su eficacia probatoria al documento privado tradicional y, por tanto, incluirlo dentro del trámite de prueba documental.

Por lo que respecta a aquellos documentos electrónicos no avalados, resultaría conveniente mantener la situación actual, admitiendo por tanto su eficacia procesal, pero reconducida al medio de prueba del reconocimiento judicial y pericial.

Tanto del espíritu como de la letra de la citada norma, se colige una clara intención del legislador de atribuir efectos a la firma y al documento electrónicos. Esa atribución de efectos se realiza, además, por referencia a sus congéneres escritos. Ello supone que la norma no pretende generar "nuevos" efectos jurídicos para la firma y el documento electrónicos; la asignación de efectos jurídicos se realiza entonces por asimilación o equiparación. Esta cuestión es la que Martínez Nadal engloba bajo la denominación de equivalencia o "regla del equivalente funcional".

Conforme a los requisitos expuestos, determinadas clases de firmas electrónicas reúnen iguales, si no superiores, condiciones de seguridad que la firma manuscrita. Mediante ellas quedan adecuadamente garantizados los requisitos de autenticidad, integridad, y no rechazo de origen.

En el caso específico de las Administraciones Públicas, la normativa estatal o autonómica pueden supeditar el uso de la firma electrónica en su seno y en las relaciones que con cualquiera de ellas mantengan los particulares, a las condiciones adicionales que se consideren necesarias (que en todo caso serán objetivas, razonables, y no discriminatorias, no obstaculizando la prestación de servicios al ciudadano cuando intervengan otras Administraciones, y garantizando el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992), para salvaguardar las garantías de cada procedimiento, entre las que pueden incluirse medidas como la prestación de un servicio de consignación de fecha y hora ("time stamping")

respecto a los documentos electrónicos integrados en un expediente administrativo.

### 4.3. El Cifrado Electrónico.

El cifrado es una de las pocas herramientas de la tecnología moderna de naturaleza enteramente defensiva: protege la información y la intimidad, proporcionando el refuerzo necesario para las transacciones electrónicas seguras, la confidencialidad de las comunicaciones, la intimidad de los individuos, y la autenticidad del receptor.

Los algoritmos de cifrado permiten transformar un mensaje escrito en claro, en un mensaje cifrado denominado criptograma. Este resultado es obtenido por medio de una transformación utilizando una o varias claves. Los servidores Web actualmente incluyen servicios de encriptación y autentificación del mensaje, de modo que los usuarios puedan enviar y recibir datos de forma segura.

Los algoritmos utilizan un sistema de claves generadas por el propio usuario o por una entidad independiente. Este procedimiento se puede combinar con la presencia de un tercero de confianza que certifique que la clave es correcta y proceda a contestar o dar por concluido el mensaje.

Podemos clasificar los algoritmos según sean de clave privada o simétrica, DES, (con una clave única y secreta que sólo el emisor y el receptor conocen), o de clave asimétrica, RSA (que utilizan dos claves para cada participante, sirviendo una en general para la operación de cifrado, que es pública; mientras que la otra clave, la de descifrado, es secreta y es la única que puede recuperar la información cifrada), pudiendo ser combinados ambos sistemas entre sí.

En base a la variedad de situaciones a las que puede afectar el cifrado y criptoanálisis de la información y las comunicaciones, así como la complejidad tecnológica y jurídica, unido a los controles que necesita por la alta sensibilidad de los temas a que se refiere, tal vez sería aconsejable una regulación específica, completa y sistemática del cifrado y criptoanálisis de la información y las comunicaciones.

### 4.4. Especial referencia al régimen de las notificaciones administrativas.

El proceso de evolución de la regulación de los medios para practicar las notificaciones se ha caracterizado por la progresiva aceptación por parte de la Administración de nuevos medios de notificación, como respuesta al crecimiento de la actividad administrativa y fruto de la aplicación de las nuevas técnicas de comunicación entre Administración y administrados. Técnicas que permiten una mayor facilidad y rapidez en la práctica de notificaciones y, por ende, en las relaciones entre Administración y administrado.

Sin embargo la realidad diaria nos permite constatar la escasa utilización de los medios telemáticos al objeto de la práctica de notificaciones. Las causas podrían resumirse en dos: la falta de aceptación social (Administración y ciudadanos) de la transmisión telemática de documentos; y en segundo lugar la ausencia de normas jurídicas que habiliten dichas prácticas en cada sector de la Administración, privándose así a la Administración y los administrados de materializar una posibilidad hasta ahora sólo genérica de acudir a las mismas.

El artículo 45.2 de la Ley 30/1992 hace referencia a que los ciudadanos “podrán” relacionarse con la Administración a través de medios electrónicos, informáticos o telemáticos; de donde se desprende que se trata de una facultad u opción de éstos, que debe quedar reflejada expresamente a efectos de notificaciones, tal como se deduce del artículo 7.2 c) del R.D. 263/1996, de 16 de febrero. Esto significa que no serán válidas las notificaciones por vía telemática si el ciudadano no ha señalado dicho medio a estos efectos.

En cualquier caso, debe tenerse en cuenta lo dispuesto en el artículo 7.3 del R.D. 263/1996, a tenor del cual “en las actuaciones o procedimientos que se desarrollen íntegramente en soportes electrónicos, informáticos y telemáticos, en los que se produzcan comunicaciones caracterizadas por su regularidad, número, y volumen entre órganos y entidades del ámbito de la Administración General del Estado y determinadas personas físicas o jurídicas, éstas comunicarán la forma y el código de accesos a sus sistemas de comunicación. Dichos sistemas se entenderán señalados con carácter general como preferentes para la recepción y transmisión de comunicaciones y notificaciones en las actuaciones a que se refiere este apartado.”

La única obligatoriedad en la elección de los medios de notificación vendría dada por la necesidad de elección por el administrado de un medio compatible con los medios técnicos de que dispongan las Administraciones.

De acuerdo con lo dispuesto en los artículos 45.2 y 59.1 de la Ley 31/1992, las notificaciones practicadas por vía telemática son admisibles siempre y cuando permitan

tener constancia de la recepción, fecha, identidad del interesado o su representante y del contenido del acto notificado, gozando en tal caso de la validez y eficacia jurídica de documento original, en tanto que se garantice su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, en los términos recogidos en las leyes (destacando en este punto la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal), pudiendo incluso ser admitidos como prueba en los procesos judiciales.

Podemos diferenciar dos clases de notificaciones telemáticas que puede practicar la Administración, a saber: las basadas en EDI (se trata de una red cerrada, a la que sólo tienen acceso los usuarios autorizados por las empresas de telecomunicación, de forma que proporciona un grado satisfactorio de control por parte de tales empresas, y por tanto, de fiabilidad), y las efectuadas a través de Internet (se trata de una red telemática pública y abierta, disponiendo de servicios como el correo electrónico, la transferencia de ficheros, la conexión remota a otros ordenadores, los grupos de debate, y la World Wide Web o telaraña de ámbito mundial).

Respecto a esta última modalidad de notificación telemática, destaca el denominado proyecto CERES, creado con el objetivo general de facilitar la comunicación vía Internet entre la Administración y sus administrados, así como las comunicaciones entre los distintos Órganos de la Administración.

De hecho, el proyecto CERES se planteó con un objetivo doble: establecer por un lado la infraestructura técnica necesaria para garantizar la seguridad en cuanto a autenticidad, integridad, confidencialidad y no repudio de las transacciones electrónicas realizadas en el ámbito administrativo entre ciudadanos y empresas con las Administraciones Públicas o de éstas entre sí; y, por otro, proponer la reglamentación necesaria para otorgar validez a los actos administrativos que se produzcan por esa vía.

Las posibilidades que este proyecto ofrece son enormes, posibilitando a las Administraciones la prestación de servicios públicos a través de Internet con garantías legales y de seguridad (facturación telemática, pago de impuestos, solicitud y gestión de certificados, renovación de documentos, presentación de reclamaciones, etc.). A través de iniciativas como CERES, el e-government en España comienza a ser una realidad.

## 5. CONCLUSIONES.

La Administración informatizada presenta notables ventajas como la racionalización, simplificación, celeridad y seguridad de las prácticas administrativas, las cuales redundan en una mayor eficacia y transparencia (mediante la difusión informativa) de la entera actividad administrativa, constituyendo este proceso de renovación administrativa una exigencia del Estado Social, que requiere de instrumentos eficaces para la puntual y cumplida satisfacción de las demandas sociales, y a este fin coadyuva positivamente la implantación de aquellas.

No obstante, la aplicación de las modernas tecnologías en el seno de la Administración también ofrece riesgos a tener en cuenta, como entre otros, la ruptura del equilibrio de poderes de la sociedad (la Administración se convierte en una “casa de cristal” y, por efecto reflejo, los ciudadanos se sienten “personas de cristal”, sufriendo el denominado “síndrome de pez”), y la potenciación de una determinada clase de formalismo (el ordenador se convierte en el verdadero “interlocutor” en las relaciones Administración - ciudadano).

Para conseguir al unísono una plena y segura explotación de estas técnicas, resulta preciso seguir potenciando iniciativas (INDALO, MAGERIT, CERES, etc.) a todos los niveles (servicios) de seguridad aludidos en el presente estudio (interoperabilidad, autenticidad, integridad, confidencialidad, no repudio, y control de accesos), utilizando para ello el soporte jurídico que la novedosa normativa en la materia (firma electrónica, protección de datos de carácter personal, etc.) nos aporta.

El siguiente paso hacia la teleadministración necesariamente pasará por complementar el marco normativo actual con normas jurídicas específicas que habiliten la práctica de notificaciones telemáticas en todos y cada uno de los sectores administrativos; dotar a la Administración de medios informáticos compatibles que aseguren tanto la interoperabilidad y la seguridad de los sistemas de comunicación, como la accesibilidad de los ciudadanos a los mismos; y por último realizar campañas de información y formación tanto en el seno de las propias Administraciones (para evitar recelos psicológicos y la aparición de fenómenos inducidos de acaparación) como en el conjunto de la sociedad.