

REDES SEGURAS

Una garantía para la Administración electrónica



Carlos Delso

Director general de Enterasys

Los constantes avances en Tecnologías de la Información hacen posible que las iniciativas que las diferentes Administraciones Públicas y organismos dependientes de ellas están poniendo en marcha sean cada vez más ambiciosas, tanto por el ámbito y alcance de las mismas como por su escala.

Este avance se debe en gran medida a la expansión de las redes de comunicación, en concreto de Internet, una infraestructura sobre la cual están basadas un elevado porcentaje de las iniciativas de “e-goverment”. Por ello, no es exagerado decir que las infraestructuras y tecnologías de red se han convertido en la piedra angular de los proyectos de Administración Electrónica.

Sin embargo, encontramos que en España se ha producido un desarrollo muy dispar de las diferentes infraestructuras necesarias para proyectos de “e-administración”. Mientras que la inversión en aplicaciones y el desarrollo de interfaces ha alcanzado unos niveles muy altos, la inversión en infraestructuras de red que soporten dichas aplicaciones no ha alcanzado el nivel suficiente. Este desequilibrio puede hacer que más de un proyecto fracase, debido a que los ciudadanos necesitan redes seguras y con

suficiente capacidad para poder acceder a los diferentes servicios que la Administración les ofrece “on-line”. Sin ellas, muchas iniciativas de Administración Electrónica simplemente fracasarán.

Esta opinión la confirman estudios de diferentes consultoras han situado algunos de los servicios prestados “on-line” en España a la cabeza de Europa en grado de desarrollo y nivel de interacción con el ciudadano. Pero estos estudios se centran exclusivamente en analizar aplicaciones e interfaces web, sin prestar atención a si las infraestructuras de red que los soportan son las adecuadas.

REDES SEGURAS, REQUISITO IMPRESCINDIBLE PARA LA ADMINISTRACIÓN ELECTRÓNICA

La relación Administración-Ciudadano podría equipararse a la que mantiene cualquier organización con sus clientes y proveedores. Es una forma de “e-commerce” en la que una de las partes ofrece una serie de servicios que en numerosas ocasiones son de “adquisición obligatoria” por parte del cliente, en este caso empresas y ciudadanos.

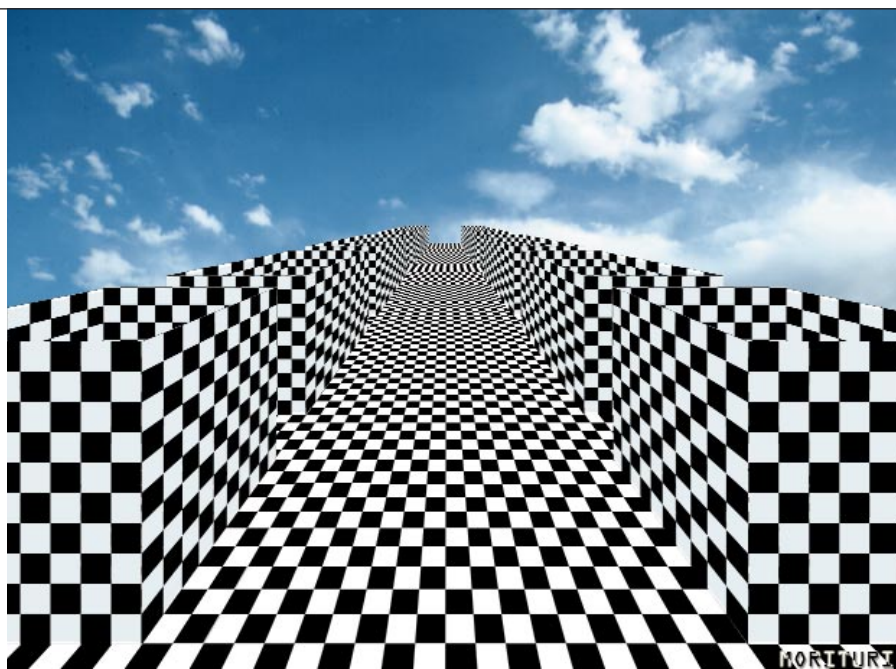
Dado que las transacciones pueden ser equivalentes en muchos as-

pectos, no es de extrañar que los requisitos que se exijan a una infraestructura de red que vaya a soportar servicios públicos sean como mínimo los mismos que se exigen a una red corporativa, es decir, **seguridad**, para proteger los sistemas de información de amenazas y usos inadecuados, y asegurar la privacidad e integridad de las transacciones por un lado, y **continuidad**, de manera que los servicios puedan estar disponibles para el ciudadano en cualquier momento, asegurando además una calidad de servicio.

PROTECCIÓN DE DATOS

Sin embargo, la relación Administración-Ciudadano presenta peculiaridades que exigen un plus en determinados aspectos, como la seguridad. La naturaleza de la información que se maneja en estas transacciones, y la trascendencia de los negocios jurídicos que se realizan con la Administración hacen necesario que la red ofrezca unas garantías de seguridad reforzadas.

La Ley Orgánica de Protección de Datos, que exige a las empresas cumplir con una serie de requisitos relativos a la confidencialidad de datos de clientes, cobra más importancia si cabe cuando hablamos de



Administraciones Públicas, debido a la cantidad y calidad de datos que manejan sobre el ciudadano.

El nuevo DNI digital, que se encuentra en fase de desarrollo en la actualidad, no sólo servirá para identificarnos con él, sino que le añadirá una nueva capacidad, la de poder firmar digitalmente con él, ya que incluirá firma electrónica, que servirá para dar validez a cualquier transacción electrónica que se realice. Este nuevo DNI incorporará todos los datos relativos a la filiación del individuo y datos biométricos, como la huella dactilar. Todo ello protegido por un sistema de doble clave.

En este contexto, la protección de las redes necesita ir más allá de los tradicionales sistemas de seguridad y protección. Las tecnologías de encriptación, autenticación de usuarios, sistemas de protección perimetral, etc., aún siendo necesarias son insuficientes para garantizar la seguridad de las redes en sentido amplio: no sólo la protección y confidencialidad de los datos, sino también su disponibilidad para el uso al que están destinadas, asegurando la continuidad del servicio. Un enfoque basado en políticas de usuario permite dotar de este nivel de

seguridad sin sacrificar el rendimiento y la gestionabilidad de la infraestructura.

CIUDADES DIGITALES

Las entidades locales juegan un papel fundamental en la creación de lo que se ha venido en llamar “ciudades digitales”. Las ciudades locales son algo más que un conjunto de servicios públicos ofrecidos por Internet, sino que se trata de una verdadera ciudad virtual en la que entidades públicas, empresas y ciudadanos se relacionan y realizan multitud de actividades, desde el pago de un impuesto a reuniones virtuales de padres de alumnos.

En las ciudades digitales las infraestructuras de red juegan de nuevo un papel fundamental. Vienen a ser las “calles virtuales” por donde todo el tráfico de la ciudad concurre y el medio de acceder a los diferentes “sitios”, ya sea al Ayuntamiento, al colegio o al centro de salud. Todos los expertos coinciden en que la planificación es esencial en el desarrollo de ciudades digitales y si es el Ayuntamiento el que tiene la iniciativa de esa planificación estratégica debe prestar especial atención a la infraestructura de

red, sobre la cual se va a construir todo lo demás.

En definitiva, la apuesta de la Administración Pública por las nuevas tecnologías es imprescindible. A fin de cuentas, todas las Administraciones son actores, y no poco importantes en el conjunto global de la economía, y es fundamental que optimicen sus procesos aprovechando las nuevas tecnologías. Por otro lado, todo esfuerzo que se realice para facilitar al ciudadano sus trámites administrativos redundará en beneficio de todos, ciudadanos, empresas y Administración.

Una red que soporte servicios de Administración Electrónica debe incorporar:

Contexto. La red debe ser capaz de reconocer no sólo quién accede, sino en que momento accede, desde dónde y con qué fin, es decir, debe ser capaz de contextualizar y gestionar el uso de la misma de forma inteligente

Control sobre quien accede a los servicios, garantizando no sólo la autenticación del usuario (certificados digitales, firma digital) sino también la autorización, es decir a qué recursos y aplicaciones está autorizado a acceder

Cumplimiento. Debe garantizar la seguridad e integridad de los datos de manera que se pueda cumplir con la legislación vigente en materia de privacidad de la información del ciudadano

Continuidad de los servicios, que sólo se puede asegurar a través de mecanismos de seguridad de red que permitan un control granular sobre el usuario y dispositivo que accede a la red.

Consolidación. La red debe permitir integrar comunicaciones heterogéneas y procedentes de diferentes dispositivos sin comprometer el funcionamiento de los diferentes servicios y aplicaciones