



¿QUÉ PREOCUPA?

EL DNI ELECTRÓNICO E INTERNET: ¿FIN DE LA CIBERDELINCUENCIA Y AUMENTO DEL NEGOCIO EN RED?

Somos conscientes de la situación de necesidad que tienen las “operaciones de confianza” por Internet para un normal desarrollo del comercio en línea, así como de la profunda utilización en servicios administrativos, consultas, bases de datos y, en general, un aprovechamiento real de las posibilidades que tenemos hoy en día, para facilitar la vida y ahorrar tiempo y dinero.

Las políticas y procesos de seguridad han ido mejorando en estos últimos años pero también lo han hecho los sistemas y actividades que intentan vulnerarlos, o simplemente la “sensación” de estar vigilado, de estar controlado o de que nos van a quitar algo que nos pertenece.

Para empezar debemos resolver dos problemas: el legal y el técnico. Por la parte legal, ya se están dando los primeros pasos, incluso incluyendo en el último borrador de la propuesta de modificación del Código Penal, el delito de intrusión, además de los daños ocasionados, entre otras posibles modificaciones. En el técnico tenemos ya muchas soluciones: software

importante la “sensación de seguridad” y de control como disponer de medidas tecnológicas y procesos “invulnerables”.

Pero, por otro lado, tenemos una realidad internacional, empezando por la europea, es decir, dentro de nuestras fronteras interiores comunitarias. No disponemos de DNIs en otros estados, no son electrónicos, no son compatibles, o no los hemos hecho aún compatibles. Esto limita mucho las actividades por la Red. Es preferible ser pioneros, mejorar la situación y progreso nacional; pero el crecimiento global sigue limitado.

Coordinación Administración-Empresas

Por tanto, respecto al DNI electrónico, debemos conformarnos por el momento, y no es poco, con obtener una alta rentabilidad de nuestra nueva identificación digital. Para ello hay que adaptar los sistemas y recursos de las empresas, y quizás hay que dar un paso más: facilitar a los usuarios que lo deseen la posibilidad de entrar en los que

posteriores (con la consiguiente repercusión predelito) con el DNI electrónico habrá que considerar exclusivamente portales que admitan el mismo, incluyendo aquí los correspondientes a la administración local, autonómica o nacional, además de las empresas que ya están trabajando en ello. Por lo demás son mejoras, sin duda, pero no garantizan nada si consideramos la globalidad de Internet.

Autodisciplina de seguridad

Lo más importante es que nos acostumbremos a disponer de medidas de seguridad en Internet. No debemos navegar sin precauciones. En estos momentos que se valoran tanto las medidas preventivas en la seguridad (pensemos en las extremas medidas de prevención en la circulación vial recientes, en alarmas en nuestros domicilios o vehículos, en seguros,...) no podemos permitir que un medio ya imprescindible, además de útil y con futuro claro, como es Internet, sea desprestigiado o minusvalorado por no tener claro conceptos de uso como:

- Protección del entorno y control (acceso: cortafuegos, identificadores y antivirus, al menos).
- Aseguramiento de identidad (para las comunicaciones en las que se necesite).
- Información de uso.
- Apoyo legal y conservar datos para investigaciones.

Las empresas están facilitando cada vez más comunicaciones y servicios crecientemente seguros, pero ello no evita tomar medidas en el nivel del cliente final. Muchos ya tienen esa sensibilidad y quieren conocer las medidas que se le ofrecen en la seguridad de los servicios, otros necesitan medidas e informaciones más transparentes y sencillas.

Concluyendo, debemos reducir riesgos y dar confianza, y el DNI electrónico es una herramienta muy útil en este sentido, aunque no la única. Debemos trabajar para que pueda ser utilizada en los medios que se pueda, y avanzar en otros sistemas de seguridad para aquellos en los que no tenga opciones, aunque con un concepto de posible convergencia para un futuro próximo. ■

Debemos conformarnos por el momento –y no es poco– con obtener una alta rentabilidad de nuestra nueva identificación digital. Para ello es necesario adaptar los sistemas y recursos de las organizaciones, y quizás, también, dar un paso más: facilitar a los usuarios que lo deseen la posibilidad de entrar en “entornos globales seguros”, esto es, identificarse con el DNI electrónico.

de identificación y autenticación, certificación digital, firma digital, llaves y otros sistemas de hardware de seguridad, compatibles en mayor o menor medida, pero a las que se añade una solución con una pretensión global y sobre todo sencilla y fiable: el DNI electrónico.

Éste tiene la ventaja añadida de que los poseedores del documento de identidad están familiarizados con él, con la necesidad de portarlo y con su fiabilidad, incluso como documento de viaje, y dispone de una certera autenticación.

Desarrollo digital nacional vs. mundial

Ahora tenemos que pensar en dos mundos distintos, aunque no excluyentes: uno es el exclusivamente interior, donde las empresas y los usuarios debemos apoyar la utilización del DNI electrónico promovido por la Administración. Y más en un entorno donde sabemos que es tan

podemos denominar “entornos globales seguros”, esto es, identificarse con el DNI electrónico (u otro sistema de identificación) y acceder a webs diferentes en los que el cliente tenga intereses, a modo de identidad federada. La Administración debe apoyar proactivamente este proceso.

Para el resto de servicios externos seguiremos trabajando en medidas de seguridad lo más cercanas y sencillas para el usuario.

Formación e Información

Otra necesidad es la formación e información del usuario. Hay que aclarar que el uso de este documento de identidad electrónico no es obligatorio, y solamente cuando se quiera disponer de ese entorno seguro para realizar alguna operación de compra o consulta se trabajará con el DNI. En el resto nada impide la navegación anónima.

El caso es que para acabar con la ciberdelincuencia o al menos facilitar las investigaciones



Bernardino Cortijo
Director de Seguridad
en Internet

TELEFÓNICA, S.A.