

DAVID BLANCO GIRÓ DIRECTOR GENERAL DE TRACTIS (PLATAFORMA DE VERIFICACIÓN DE LA IDENTIDAD Y CONTRATACIÓN ELECTRÓNICA)

“Ausencia total de estrategia de implantación”

E.F.

David Blanco Giró (Valladolid, 1973) conoce de primera mano cómo se gestó el proyecto del DNI-e en nuestro país. La empresa que dirige, Tractis, ha desarrollado una de las plataformas de verificación de identidad y contratación electrónica más potentes a nivel nacional y fue contratada por el Ministerio de Industria para realizar el primer reparto masivo de lectores DNI-e.

¿Qué ha fallado en el proyecto del DNI-e?
Todos los errores por los que no ha cumplido sus expectativas podrían resumirse en uno: la ausencia total, en el momento de inicio del despliegue del plan, de una estrategia de implantación y difusión del DNI-e en el sector privado.

¿Cuál ha sido el papel de la DGP?
La Dirección General de la Policía, responsable de la implantación del proyecto del DNI-e, se centró desde el principio en crear una herramienta de verificación de la identidad que resolviera sus necesidades. Lógicamente, su preocupación fue siempre la seguridad y no la usabilidad de aplicaciones para el DNI-e en el sector privado, porque la seguridad es su principal cometido y por eso le pagan. ¿Significa eso afirmación que la DGP tiene la culpa del fracaso del DNI-e? Ni mucho menos. Es culpa de quien decidió que la encargada de la implantación del DNI-e fuera la DGP.

¿Cuándo apareció Red.es?
Con el paso del tiempo y al hacerse evidente el problema de difusión del DNI-e en el

sector privado, se transfirieron competencias a la Entidad Pública Empresarial adscrita al Ministerio de Industria, Red.es, cuyo objetivo principal es promover la presencia digital en internet entre ciudadanos y empresas. Sin embargo, Red.es no disponía de las herramientas necesarias para mejorar las cosas, pues el control del proyecto seguía correspondiendo a la DGP.

¿Cómo debería haberse diseñado el DNI-e?
En mi opinión, podría haberse creado un ente autónomo encargado de la difusión del DNI-e, del cual habría ‘colgado’ un comité conjunto DGP-Red.es. A este comité conjunto habría que haberle dotado de continuidad en el tiempo, con reuniones periódicas de revisión y áreas de actuación coordinadas, pero independientes. En la actualidad, Red.es depende de la DGP para cualquier cambio importante que desee plantear, aunque los objetivos de la DGP no tengan nada que ver con los Red.es. Así que la DGP ha hecho una labor encomiable (para lo que son sus objetivos) y Red.es ha hecho un trabajo extraordinario (para el grado de libertad con el que cuenta).

¿Qué tal un despliegue masivo de lectores?
Sería fundamental, no necesariamente gratis, pero sí facilitando su adquisición. Una opción dura sería obligar a los fabricantes de ordenadores a incluir lectores de serie en España (en plan: “es como la tecla ñ: o la pones o no vendes”). Otra estrategia más suave y de menor confrontación sería crear un sello de “ordenador compatible con DNI-e” y, a continuación, publicitar: “no comprés ningún ordenador sin este sello”.



David Blanco Giró. TRACTIS.COM

¿Y qué haríamos con las normativas?
Habría que publicar un reglamento que desarrollara la Ley de Medidas de Impulso a la Sociedad de la Información. Por esta ley, por ejemplo, todas las empresas de banca, seguros, teleco, energía, transportes, etc. que tuvieran más de 100 trabajadores o que facturaran más de 6 millones €/año (Telefónica, Vodafone, France Telecom, Jazztel, Gas Natural, Iberdrola, Santander, BBVA, Caja Madrid, Bankinter, ING Direct, etc.) estarían obligadas a soportar el DNI-e en las relaciones y contrataciones con sus clientes (altas, bajas,

portabilidades, renovaciones...). Y deberían hacerlo, por ejemplo, antes de diciembre de 2011. Si todas ellas cumplieran la ley, el ciudadano percibiría muchísimo valor en utilizar su DNI-e, pues habría centenares de gestiones valiosas que podría realizar desde casa, en segundos, a cualquier hora.

¿Como podría presionar el ciudadano?
Probablemente, en la situación de crisis actual, el gobierno no considera que sea buena idea pedir a estas empresas este tipo de gasto. Así que la solución sería que los ciudadanos se acercaran a las oficinas del consumidor y denunciasen a todas las empresas de banca, seguros, teleco, etc. por incumplimiento masivo de la legislación y su consiguiente pérdida de derechos.

¿Y los otros certificados digitales?
Habría que exigir ‘ya’ la normativa europea, que sólo reconoce como “firma electrónica cualificada” la que está creada con un dispositivo seguro, es decir, con el DNI-e o una tarjeta criptográfica (con chip). Traducido al cristiano y de manera menos política: habría que prohibir el certificado Ceres de *software* (el que se almacena en una memoria USB) para hacer la declaración del IRPF y admitir sólo Ceres en tarjeta criptográfica.

Menudas medidas de ‘guerrilla’...
Así es, pero provocarían: (1) que los fabricantes incluyeran lectores en sus ordenadores; (2) que las grandes empresas ofreciesen servicios de valor con el DNI-e (no la tontería de la autenticación); y (3) que los ciudadanos se acostumbraran al uso del DNI-e.

JULIÁN INZA ALDAZ PRESIDENTE DEL GRUPO INTERACTIVA (ALBALIA.COM)

“Un círculo vicioso entre aplicaciones y certificados”

E.F.

Julián Inza Aldaz (Pamplona, 1961) es pionero en el desarrollo de la firma y la banca electrónica en España. Trabajó desde los inicios con prototipos del DNI electrónico para la implantación de un sistema de firma digital en móviles y preside uno de los grupos de empresas más prestigiosos especializado en firma electrónica, el Grupo Interactiva. Ha realizado múltiples seminarios y cursos online sobre el DNI-e para Inteco (Instituto Nacional de Tecnologías de la Comunicación) y ha sido seleccionado por Red.es como entidad promotora del DNI-e.

¿Cómo describiría la situación del DNI-e?
Afortunadamente, en España las cosas están empezando a cambiar. El bajo uso del DNI-e ha sido esencial para romper el círculo vicioso en el que nos encontrábamos inmersos y que se describiría así: “Como hay pocos certificados electrónicos no merece la pena desarrollar servicios y aplicaciones que saquen partido de ellos. Como no hay aplicaciones que requieran certificados, no merece la pena obtenerlos”.

¿Cuáles han sido los principales errores?
La doble certificación que incluye el DNI-e (autenticación y firma) es, a mi juicio, innecesaria. Además, el hecho de que se exija continuamente el PIN lo hace inusable. También considero trabas: la limitación a 30 meses de la validez de los dos certificados del DNI-e, la excesiva normativa sobre firma electrónica -dispersa y contradictoria-, la dejadez de los organismos públicos o el secretismo sobre cierta información técnica.



Julián Inza Aldaz. ATENEAINTERACTIVA.COM

¿Cómo se daría un giro a la situación?
Creo que la cualidad más importante de los certificados digitales es la interoperabilidad, es decir, la capacidad para intercambiar procesos o datos entre diferentes sistemas. Por ello, habría que tratar al DNI-e igual que al resto de los certificados cualificados: unificar los interfaces de acceso, suprimir el PIN y dotar a sus certificados de la misma duración que el propio soporte: 10 años. Por último, habría que simplificar la normativa sobre firma digital, con un sólo concepto y una fuente única de derecho.

CARLOS JIMÉNEZ SUÁREZ PRESIDENTE DE SECUWARE (SEGURIDAD TIC)

“La usabilidad es una cuestión imprescindible”

E.F.

Carlos Jiménez Suárez (Madrid, 1966) es una autoridad mundial en seguridad informática. Experto en ciberterrorismo y reconocido por organizaciones como la OTAN, el Ministerio de Defensa o el CNI, con tan solo 20 años inventó el primer antivirus de la historia para el *Viernes 13*. Preside Secuware, la empresa que él mismo fundó, y acaba de presentar su último proyecto conjunto con Telefónica-Movistar para llevar el DNI-e al móvil. El proyecto fue anunciado a mediados de febrero en el Mobile World Congress de Barcelona.

¿Cómo se mejora el DNI-e?
Hay que considerar la usabilidad. Por un lado, pienso en el PIN. Aunque en un futuro no muy lejano, se ha previsto eliminar el PIN del certificado de identidad, creo que esta supresión, en lugar de arreglar el problema, creará uno nuevo de seguridad. El 90% del código que maneja el DNI-e estaba formado por componentes de Microsoft y, desde el principio, Microsoft asumía que un certificado digital no estaba protegido por PIN. Sin embargo, se incluyó por exigencias de la Agencia de Protección de Datos. Por otro lado, si el DNI-e no puede utilizarse en el móvil y necesitamos siempre un ordenador, su uso se reducirá muchísimo.

¿Por qué no ha cumplido las expectativas?
Para utilizar el DNI-e, el usuario tiene que superar una carrera de obstáculos. (1) hay que tener un lector y que los *drivers* funcionen; (2) hay que instalar el Mó-



Carlos Jiménez Suárez. SECUWARE.COM

dulo Criptográfico de la DGP; (3) hay que conocer el PIN, -probablemente el inhibidor mayor, ya que menos de un 5% de los usuarios lo conocen. Y una vez llegados ahí, el DNI-e es muy incómodo de usar, porque el PIN se solicita muchísimas veces.

¿Qué futuro le augura al DNI-e?
Los españoles tenemos una llave de seguridad perfecta para realizar gestiones, a cualquier hora, desde cualquier sitio. Indudablemente, a medio plazo, existirán muchas más aplicaciones de uso sencillo.