>> Jorge Dávila

Los Esquemas Nacionales y el optimismo legislativo

Con el principio de este año, el Ministerio de la Presidencia nos ha agasajado con dos esquemas nacionales, uno de seguridad (ENS) y otro de interoperabilidad (ENI). Este hito es un paso más adelante en la dirección de una futura relación telemática universal entre Administración y ciudadanía. ¿Cómo se ha afrontado el escurridizo aspecto de la seguridad? ¿Cómo se piensan resolver las disyuntivas tecnológicas que tiene y tendrá delante la futura Administración Electrónica española? Todos estos temas ya empiezan a estar perfilados en estas dos últimas entregas legislativas, a las que merece la pena echar un vistazo.

El pasado 29 de enero, el BOE publicó en el Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica. El objetivo declarado de ese documento es, reconociendo que todo depende de la confianza que se genere en los ciudadanos, promover las condiciones necesarias para que la libertad e igualdad sean reales y efectivas en las relaciones telemáticas entre administrador y administrado, y también remover todos los obstáculos que impidan o dificulten su plenitud.

Este real decreto es un desarrollo del artículo 42.2 de la Ley 11/2007 de 22 de junio y persigue favorecer el uso de los medios electrónicos, garantizando la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. Esa seguridad serviría para probar que la administración electrónica custodia *"la información sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas"*. La idea es que cada sistema tenga un perímetro bien definido, unos responsables establecidos o conocidos, y además una coordinación real que evite la existencia de "tierras de nadie" y fracturas que pudieran dañar a la información o a los servicios prestados.

En este real decreto se hace referencia explícita a la utilización de estándares abiertos, lo cual es un gran avance que debería haberse dado hace tiempo, pero no cierra la puerta al *status quo* ya que, de forma complementaria, incluye otros estándares (no abiertos) de uso generalizado por los ciudadanos salvando con esa escusa a la industria informática actualmente establecida.

La seguridad como una actividad integral

Este real decreto se limita a establecer los principios básicos y requisitos mínimos, pero asume que la seguridad es una actividad integral, en la que de nada bueno sirven actuaciones puntuales o tratamientos coyunturales. El documento reconoce que la debilidad de un sistema la fija su punto más débil, y reconoce que muchas veces ese punto está en la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas. Lo que se pretende proteger es: *"el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos"* (Art 1.2), todas ellas cualidades y aspectos básicos en la seguridad de cualquier sistema.

Que en el artículo 5 se defienda que la seguridad es un proceso integral, quizás pueda parecer una obviedad, pero no está claro que lo sea si nos fijamos en todos los ámbitos de la administración, que son los que más van a verse afectados por este tipo de legislaciones. No son los departamentos más avanzados los que realmente van a poder medir el impacto de estos reales decretos, sino los ámbitos municipales y autonómicos que nunca han tenido nada que ver con la informatización masiva o la telemática. Es al menos satisfactorio que desde el principio quede claro que no basta con comprarle alguna *"solución"* al comercial más dicharachero, y que no hay *"soluciones mágicas"* ni soluciones particulares. Como bien sabemos, la seguridad es un proceso constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema.

El ENS no persigue ser especialmente innovador, ni arriesgado, por lo que recurre a la ortodoxia y al sentido común y llama a que la gestión de la seguridad esté dirigida por los riesgos que se corren. Ahora bien, los riesgos hay que identificarlos y medirlos, por lo que recomienda (exige) encarecidamente que cada organización desarrolle su propio análisis de riesgos como parte esencial del proceso de seguridad, y lo mantenga permanentemente actualizado.

Se persigue evitar la amenaza mediante la disuasión y la reducción de la exposición pero, en el caso de no haber tenido éxito, al menos mitigar sus efectos y repercusiones del ataque. Las medidas de recuperación deberán ser capaces de restaurar, con toda su integridad, la información y los servicios afectados. Para ello, los sistemas deberán garantizar la conservación de los datos e informaciones que existan en soporte electrónico, y que sean la base para la preservación del patrimonio digital.

En el artículo 8 se habla de las *"Líneas de defensa"* y se opta por la estrategia de establecer múltiples capas de seguridad de forma que, cuando una de ellas falle, se gane tiempo para tener una reacción adecuada, se reduzca la probabilidad de que el sistema sea globalmente comprometido, y se minimice el impacto final sobre el mismo.

Siguiendo con la ortodoxia, el real decreto opta por los triunviratos y diferencia el responsable de la información del responsable del servicio y del responsable de la seguridad (Art 10), y a la hora de marcar los mínimos, éstos se plasman en la necesaria existencia de una Política de Seguridad (Art. 11). En esta política se han de satisfacer diecisiete requisitos mínimos y se obliga (Art. 24) a disponer de un sistema de detección y reacción frente a código dañino, así como a registrar los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Lo que no se dice en ningún sitio es qué clasificación tendrán esos incidentes, ¿serán información pública, confidencial o secreta?

A la hora de tratar la gestión del personal (Art. 14), se indica

A la hora de tratar la gestión del personal, en el ENS se indica que para corregir o exigir responsabilidades, cada usuario con acceso al sistema debe estar identificado "de forma única", de modo que siempre se sepa quién hace el qué. Sin embargo, para esa finalidad habría que exigir la capacidad de no-repudio, ya que un nombre de usuario y una palabra clave pueden ser una identificación única, y no por ello ser prueba suficiente, ya que además del usuario hay otros que conocen sus credenciales de acceso (el sistema, por ejemplo). Esto tiene mucho que ver con obligar en el ENS al registro y trazabilidad de actividades de los usuarios dentro de los sistemas informáticos.

expresamente que para corregir o exigir responsabilidades, cada usuario con acceso al sistema debe estar identificado "*de forma única*", de modo que siempre se sepa quién hace el qué. Sin embargo, para esa finalidad habría que exigir la capacidad de no-repudio, ya que un nombre de usuario y una palabra clave pueden ser una identificación única, y no por ello ser prueba suficiente, ya que además del usuario hay otros que conocen sus credenciales de acceso (el sistema, por ejemplo). Esto tiene mucho que ver con obligar en el ENS al registro y trazabilidad de actividades de los usuarios dentro de los sistemas informáticos [1].

El delicado tema de los proveedores de tecnología

En el artículo 18 se toca el delicado tema de los proveedores de tecnología y se queda corto estableciendo que se "*valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición*"; pero no se exige ningún tipo de certificación internacional, sino que deja al **Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información** que determine el criterio a cumplir en cada caso y en función del uso previsto del producto.

En el artículo 19 se apela a la "*Seguridad por defecto*" y, muy acertadamente, se exige que los sistemas deben diseñarse y configurarse de forma que garanticen la mínima funcionalidad requerida tanto en operación como en administración y registro, a la vez que se eliminen y desactiven por configuración todas aquellas funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue. Por último, se obliga a que el uso ordinario del sistema sea sencillo y seguro, de forma que su uso inseguro requiera un acto consciente por parte del usuario. Aunque todas estas exigencias son encomiables, sin embargo, anular funcionalidades peligrosas mediante la gestión de la configuración entra en cierto conflicto con los demás principios y puede suponer una inconsistencia interna.

Como era deseable, el real decreto se preocupa de la seguridad de la información, tanto cuando es transmitida como cuando se almacena, y en su artículo 21 presta especial atención a la información en entornos inseguros como lo son los equipos portátiles, las PDAs y *smartphones*, las memorias USB, las comunicaciones sobre redes abiertas o con cifrado débil, etc.

En el artículo 36 del ENS se nombra al **Centro Criptológico Nacional** (CCN) como el encargado de dar respuesta a los incidentes de seguridad con su CCN-CERT, que actuará con independencia de otras capacidades.

La categoría de un sistema viene determinada por el impacto que tendría un incidente que afectara a la seguridad de la información o de los sistemas, y que afectase a su capacidad para alcanzar sus objetivos, proteger sus activos, cumplir sus obligaciones diarias de servicio, respetar la legalidad vigente y los derechos de las personas. Para definir esa categoría, se proponen las siguientes dimensiones de la seguridad: Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad, que, por otra parte, son las clásicas.

Tanto si es para reponerse de un fallo o ataque, como si se trata de preservar el patrimonio digital del Estado, el ENS recuerda que forman parte importante de la seguridad los procedimientos de recuperación y conservación a largo plazo de los documentos electrónicos producidos. Para ello se tendrá que definir una política de gestión de documentos a utilizar, así como incluir los expedientes en un Índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del expediente electrónico. La existencia de ese Índice otorgará una identificación única e inequívoca (metadatos) a cada documento y con ello podrán ser clasificados, recuperados y citados, cosa que actualmente es muy difícil, si no imposible.

Tanto si es para reponerse de un fallo o ataque, como si se trata de preservar el patrimonio digital del Estado, el ENS recuerda en ese mismo artículo (Art 21) que forman parte importante de la seguridad los procedimientos de recuperación y conservación a largo plazo de los documentos electrónicos producidos por la Administración.

Es en el artículo 28 donde se aplica el principio de agregación de infraestructuras y servicios que serían de uso común para facilitar el cumplimiento del ENS en condiciones de mayor eficacia, aunque es en el Esquema Nacional de Interoperabilidad donde se trata más claramente el tema. Lo que sí es específico del ENS es indicar cuáles son las condiciones técnicas de seguridad en las comunicaciones respecto a la constancia de la transmisión y recepción (notificaciones electrónicas, Art. 32), de la fecha en la que ocurre, de su integridad y de la identificación cierta de los comunicantes.

El Esquema Nacional de Interoperabilidad (ENI)

El Esquema Nacional de Interoperabilidad aparece simultáneamente con el de seguridad y pretende ser su complemento natural. Aquél, como éste, persigue promover las condiciones para que la libertad e igualdad sean reales y efectivas pero, además, dice defender plenamente el principio de neutralidad tecnológica, haciendo que todo el sistema sea independiente de la tecnología por la que opten los ciudadanos. Para ello, este real decreto pretende garantizar el nivel suficiente de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones utilizados por las Administraciones Públicas,

Para ello el ENI propugna el uso de estándares abiertos, de sistemas con fuentes abiertas, y también opta por la reutilización, operados en aras a la interoperabilidad (Art. 5) y, para empezar, tendrán que publicar todo lo referente a condiciones de acceso, utilización de servicios, datos y documentos electrónicos que pongan a disposición de otras administraciones, las modalidades de consumo, consulta o interacción, tipos de usuarios autorizados, requisitos técnicos, condiciones de seguridad, etc. (Art. 8). Para ayudar más en ello, se propone el establecimiento y uso de "nodos de interoperabilidad" que faciliten completamente el cumplimiento de estos requisitos. Estos nodos serán especialmente atractivos para aquellos municipios pequeños, con poco presupuesto, que también representan a ciudadanos *peer-two-peer* con los de las urbes más potentes.

Otra novedad es la de los **Inventarios de Información Administrativa** en los que se podrá saber qué conoce exactamente cada administración, y qué procedimientos ofrece y realiza, así como cuáles son sus oficinas y sedes de registro y atención al ciudadano.

Dado que hablando no

[1] Artículo 23: …*"reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa".*

siempre se entiende la gente, también es necesario observar la dimensión semántica de la información (Art. 10). Para ello hay que tener publicados los modelos de datos de intercambio y decir cómo deben interpretarse exactamente cada uno de ellos, de modo que no haya malos entendidos cuando los reciba la administración receptora de los mismos. Todo ello se publicará a través del **Centro de Interoperabilidad Semántica de la Administración** (Art. 16).

Es en el artículo 11 donde el ENI se decanta claramente hacia el uso de estándares abiertos, aunque reconoce que pueden ser complementados por "*estándares que sean de uso generalizado por los ciudadanos*", con lo que salva a los productos Microsoft y muchos otros, prácticamente todos, los que constituyen la industria TI nacional y extranjera. No es conveniente que este proceder realista reste empuje a la necesidad de que la Administración pública utilice estándares y códigos abiertos.

Es este artículo el que debería desterrar el triste hecho de que las *webs* de la Administración española, sus sedes electrónicas, están siempre diseñadas para funcionar con el Internet Explorer y no suelen ser compatibles con cualquier otro navegador. Que esto lo haga el sector privado, ya se lo premiará o demandará el mercado, pero en el caso de los servicios públicos ese control no es posible, y deberá ser el cumplimiento del ENI el que ponga fin a esta inconfesada tendencia a favor de los más grandes y poderosos.

En el artículo 12 se trata otro tema que es importante, y no es otro que el relativo a la centralización de infraestructuras y servicios dentro de la Administración. Ambos modelos de organización de los recursos informáticos, el "*centralizado*" y el "*inter pares*", tienen sus ventajas e inconvenientes. Por el momento, cada ministerio, cada comunidad, cada ayuntamiento grande, etc., tiene su propio sistema informático y sus aplicaciones, y se enlazan entre sí a través de las *Red de comunicaciones de las Administraciones públicas españolas* (Art.13).

En el artículo 16 del ENI se descarta la posibilidad de que las Administraciones puedan cobrar por las aplicaciones y los servicios e informaciones, ya que el bien defendido debe ser el del "*aprovechamiento y la reutilización, así como la protección contra su apropiación en exclusiva por parte de terceros*". Asimismo, se opta por el uso de la Licencia Pública de la Unión Europea u otras del todo equivalentes.

En el articulo 21 se habla de las condiciones para la recuperación y conservación de los documentos, y con ello plantea el tema de los futuros registros documentales digitales de la Administración. Para ello se tendrá que definir una política de gestión de documentos a utilizar en la formación y gestión de documentos y expedientes, así como incluir los expedientes de un **Índice electrónico firmado** por el órgano o entidad actuante que garantice la integridad del expediente electrónico. La existencia de ese Índice otorgará una identificación única e inequívoca

pueden ser muy lentos si los comparamos con lo rápido y fácilmente que se puede arruinar y volver inservible un sistema digital de almacenamiento de la información.

Es en este artículo donde muy sigilosamente se pretende **resolver el problema de las firmas digitales longevas,** optando porque la autenticidad y el carácter de evidencia de los documentos sobrevivan a la validez de sus firmas digitales, y que ambas emanen de su historial de conservación y custodia en los repositorios y archivos electrónicos.

Es en el artículo 22 del ENI donde muy sigilosamente se pretende resolver el problema de las firmas digitales longevas, optando porque la autenticidad y el carácter de evidencia de los documentos sobrevivan a la validez de sus firmas digitales, y que ambas emanen de su historial de conservación y custodia en los repositorios y archivos electrónicos.

Aplicaciones, recuperación y conservación de los documentos

Las aplicaciones de la Administración deberán aparecer (art. 17) en **Directorios de aplicaciones reutilizables** para su libre uso, y se podrá acceder a ellas a través del **Centro de Transferencia de Tecnología**. De hecho, las Administraciones públicas deberán tener en cuenta esas soluciones disponibles a la hora de planificar sus adquisiciones o desarrollos. El objetivo no es sólo poner a disposición de los demás entes la aplicación, sino incluso su mismo código, tanto si están en desarrollo como si están finalizadas, lo cual es muy recomendable.

En lo enrevesado de los artículos relativos a la firma electrónica y a los certificados de identidad digital (Arts. 18-20) se ve que ese tema no está claro en el ENI y puede que traiga problemas a la larga. Dado que las PKIs no terminan de cuajar, realmente será mejor, por el momento, dejar a un lado estos temas.

(**metadatos**) a cada documento, y con ello podrán ser clasificados, recuperados y citados, cosa que actualmente es muy difícil, si no imposible.

En este artículo se hace mención explícita a proporcionar la capacidad de "*copia o descarga en línea en los formatos originales y la impresión a papel*". Esta exigencia tiene sentido en un periodo de transición, pero decaerá en el momento en el que los documentos no hayan tenido nunca un origen distinto al digital. Sin embargo, esta cautela hace recordar que muchas **veces la información de los documentos no sólo está en lo que está escrito, sino también en cómo está impreso e, incluso, en el estado de conservación del documento** para la determinación de su autenticidad. En el mundo digital todo esto ya no va a ser posible.

En el artículo 22 se plantea la seguridad necesaria para la conservación[2] de los documentos electrónicos en lo que se refiere a los medios y soportes en los que se almacenen dichos documentos, y según sea la categoría de los sistemas que los cobijan, y para ello hay que poner en pie una **Política de Protección Documental** global. Si los archivos clásicos tienen como enemigos el fuego, el agua, los roedores y los ácaros, entre otros, éstos

Mientras que el Esquema Nacional de Seguridad se mantiene dentro de la ortodoxia de la seguridad en los sistemas TIC y que su cumplimiento sería un hito memorable, además de un avance considerable respecto a la seguridad actual en las Administraciones, el Esquema Nacional de Interoperabilidad es algo novedoso y loable, ya que pretende aprovechar el paso a las tecnologías digitales para poner un poco de orden en los procedimientos burocráticos.

Las nuevas tecnologías no dejan lugar para antiguas actitudes y es de esperar que terminen enterrando (mejor aún, incinerando) el concepto de póliza, redonda o no, que tan insidiosamente ha martirizado a generaciones y generaciones de españoles. Somos libres, como comunidad, como país, como Administración, de desaprovechar esta oportunidad, pero las consecuencias de hacerlo nos pueden enviar de nuevo al "segundo mundo" del que no hace tanto tiempo salimos. ■

Jorge Dávila Muro
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[2] Lo que se pretende es *"garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios, y se realizarán atendiendo a los riesgos a los que puedan estar expuestos y a los plazos durante los cuales deban conservarse los documentos".*