TECNIMAP2010 - Comunicaciones

Autor: Ramón Miralles
Cargo: Coordinador de Auditoria y Seguridad de la Información
Entidad: Agencia Catalana de Protección de Datos

Título: **Esquema Nacional de Seguridad y protección de datos personales.**

La reciente entrada en vigor del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, supone un cambio radical en cuanto a la manera en que el sector público venia organizando y desplegando la protección de los medios electrónicos utilizados para el ejercicio de sus competencias y la prestación de servicios.

¿Por qué podemos calificar de radical el cambio? Pues porque implica la ordenación, o normalización si se quiere, en base a unos principios básicos y requisitos mínimos de seguridad, de los controles o medidas de seguridad que deben ser implantados en los sistemas de información de las administraciones públicas, cuestión que hasta ahora quedaba a discreción de cada administración, todo y que ciertamente en relación a los datos de carácter personal ya se disponía de un marco común de protección de la información.

Y esa es la cuestión principal de esta comunicación, abordar de qué manera el modelo de seguridad planteado por el ENS se integra de manera colaborativa, o sumatoria, en el conjunto de medidas de seguridad ya previstas en el contexto de la protección de datos de carácter personal.

Algunas consideraciones generales

Como del contenido de la comunicación se podría desprender, en algunos supuestos, una visión crítica de aspectos de la regulación material del ENS, vaya por delante que conceptualmente el hecho de disponer de un marco común para la protección de los sistemas de información relacionados con la actividad del sector público, es no solo una buena iniciativa, si no algo absolutamente imprescindible para el uso eficaz y eficiente de los medios electrónicos por parte de las administraciones públicas, y especialmente cuando se trata de utilizarlos para las relaciones con ciudadanos, empresas y entre las propias administraciones.

La necesaria confianza que debe generarse en relación al uso de los medios electrónicos obliga a disponer de unas pautes comunes de protección de la información.

La exposición de motivos del Real Decreto 3/2010 incide en esa necesidad de generar confianza, como resultado de la exigencia de una aplicación segura de las tecnologías de la información y la comunicación (TIC), así la finalidad principal del ENS es crear las condiciones necesarias de confianza en el uso de los medios electrónicos.

La generación de confianza no resulta una tarea fácil, la arquitectura y características propias de las redes públicas de comunicaciones, especialmente las basadas en Internet, que van a ser el principal canal por el que los ciudadanos accederán a los servicios electrónicos de las administraciones públicas, favorecen la aparición de fenómenos suficientemente conocidos y en los que aquí no corresponde ahondar, que podemos concentrar en el concepto genérico de incidentes de seguridad, donde la gran dificultad estriba en que el usuario realmente sea consciente de que se encuentra ante una situación de riesgo.

La determinación o la percepción de "peligro" no resulta evidente, por tanto la articulación de mecanismos que favorezcan un clima de confianza, no vinculado a conocimientos expertos en materia de la seguridad de la información por parte de los ciudadanos, resulta un reto complicado de abordar, en esta línea el ENS puede aportar al menos la garantía de que el sector público actúa según unas pautas comunes y aplicando unos mecanismos mínimos de seguridad que tienen por objetivo reducir o eliminar esos posibles incidentes en la relación con los ciudadanos por medios electrónicos.

Tal y como recoge la exposición de motivos las medidas de seguridad deben garantizar el ejercicio de derechos y cumplimento de deberes a través de esos medios electrónicos, de manera que se pueda confiar en que los sistemas de información:

- Prestaran los servicios i custodiaran la información según lo previsto y sin interrupciones (disponibilidad)
- Sin modificaciones fuera de control (integridad)
- Sin que la información pueda llegar al conocimiento de personas no autorizadas (confidencialidad)

El ENS se desarrolla según lo previsto en el art. 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, que establece su objeto y contenido.

El ENS tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Dos enfoques para una misma cuestión

Una parte importante del contenido del derecho fundamental a la protección de datos de carácter personal está constituida por la implantación de medidas de seguridad, tanto técnicas como organizativas, en los ficheros y tratamientos de datos personales.

La derogada Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD), preveía su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas que garantizaran la seguridad de los datos de carácter personal y evitaran su alteración, pérdida, tratamiento o acceso no autorizado, según el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que pudieran estar expuestos, tanto si esos riesgos provenían de la acción humana o del medio físico o natural.

Por tanto el hecho de contar con una regulación más o menos exhaustiva, de carácter común y obligatorio para el sector público en materia de seguridad de la información, no es una novedad, todo y que la protección se centre en aquella información relacionada con el tratamiento de datos de carácter personal, que en el caso de las administraciones públicas implica hablar casi del 100% de la información que utiliza para el desarrollo de las actividades que les son propias.

El Real Decreto 994/1999 (ya derogado), de 11 de junio, que aprobó el Reglamento de medidas de seguridad para los ficheros automatizados que contuvieran datos de carácter personal desarrollaba el mencionado art. 9 de la LORTAD.

La LORTAD vino a ser substituida por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), como resultado de la transposición de la Directiva Europea 95/46, que mantuvo la vigencia del mencionado reglamento de medidas de seguridad de 1999, hasta la publicación del Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que dedica su Título VIII a las medidas de seguridad en el tratamiento de datos de carácter personal, sea cual sea el sistema de tratamiento de esos datos.

En definitiva la necesidad y obligación de proteger la información y los sistemas que le sirven de soporte tiene ya un cierto recorrido normativo, no entraré a valorar aquí cual es la situación y las dificultades de cumplimiento de la normativa de protección de datos en este aspecto concreto, por ser suficientemente conocidas, el INTECO tiene publicados unos estudios más que reveladores de esta cuestión.

Como no podía ser de otra manera el ENS no es ajeno a la existencia de unas obligaciones en materia de seguridad de la información derivadas del tratamiento de datos de carácter personal, así en la exposición de motivos al explicar la concepción de actividad integral de la seguridad se añade que la información tratada en los sistemas electrónicos a los que se refiere el ENS estará protegida teniendo en cuenta los criterios establecidos en la LOPD, y ya en la parte dispositiva, el art. 27.2 establece que cuando un sistema de información maneje datos de carácter personal le será de aplicación lo dispuesto en la LOPD y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el ENS.

Lo que si se plantea es una diferente manera de abordar la implantación de las medidas de seguridad, mientras para la LOPD lo importante es el dato, por tanto la protección siempre gira entorno a proteger la información personal, en cambio para el ENS la seguridad se aplica a la utilización de los medios electrónicos, una perspectiva más amplia, si se quiere, que incluye como objeto de protección los datos, las informaciones y los sistemas, por tanto a lo largo de su desarrollo se evidencia que lo importante a proteger es el uso de los sistemas de información.

La definición de sistema de información que se hace en uno y otro responde a esa diferente concepción, mientras la LOPD define como sistema de información el “conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal”, para el ENS se trata de un “conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir”, el ENS pone el énfasis de la seguridad en el uso del sistema de información y la LOPD en los propios recursos utilizados, incluida la información.

Una diferente visión que en la práctica no tiene porque dar resultados divergentes o contradictorios, pero si que es indudable que aportará una mayor complejidad a la gestión de la seguridad de la información, por ejemplo, esa diferente manera de abordar o definir la seguridad puede dar lugar a la paradoja de que unos datos a los que según la LOPD se le deban aplicar medidas de seguridad de nivel básico, en cambio por aplicación del ENS, al

determinar la categoría del sistema que los soporta, se concluya que debe ser calificado de categoría alta.

El ENS de seguridad busca la alineación de la seguridad con los objetivos de las organizaciones, por tanto un elemento esencial es garantizar el uso de esos sistemas en condiciones óptimas de seguridad, de manera que cuando el anexo I del ENS aborda la cuestión de la determinación de la categoría de los sistemas lo fundamenta en la repercusión que el incidente de seguridad pueda tener en elementos tan críticos para las organizaciones como el hecho de alcanzar sus objetivos, proteger los activos a su cargo o cumplir con las obligaciones diarias de servicio.

Hay que señalar que también se fundamenta esa determinación de la categoría de los sistemas de información en cuestiones directamente relacionada con el derecho fundamental a la protección de datos de carácter personal, como son el respeto a la legalidad vigente o el respeto a los derechos de las personas.

En definitiva en el ENS las medidas de seguridad a implantar se vinculan a la categoría del sistema de información, mientras que en la LOPD se vincula al tipo de datos tratados.

El ENS aporta una visión amplia de la seguridad de la información, de ahí que en la práctica esté planteando la implantación de un sistema de gestión de la seguridad de la información, con muchos elementos en común con la UNE-ISO/IEC 27001 y los controles previstos ISO/IEC 27002.

Algunas cuestiones concretas

Sin animo de ser exhaustivo, se pueden identificar claramente toda una serie de cuestiones que revelan las dificultades con las que los responsables de ficheros o tratamientos de datos de carácter personal del sector público se pueden encontrar a la hora de concretar la mejor manera de adecuar sus sistemas de información a las previsiones del ENS, teniendo en cuenta que ya disponen de toda una serie de medidas de seguridad desplegadas, con mayor o menor intensidad, como consecuencia de la aplicación de la LOPD y su normativa de desarrollo.

Antes de abordar esas cuestiones hay que evidenciar un hecho importante, como es que el ENS no se aplica exclusivamente a los sistemas de información orientados a la relación “externa”, ya sea con ciudadanos o empresas, o para el caso de las relaciones inter-administrativas, ya que es de aplicación a los medios electrónicos que las administraciones

públicas gestionen en el ejercicio de sus competencias, de manera que el art. 1.1 al definir el objeto del real decreto, y referirse a los medios electrónicos a los que se refiere la Ley 11/2007, esta en su art. 3.5 concreta como una de las finalidades de la ley contribuir a la mejora del funcionamiento interno de las AAPP, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones.

Esa idea de aplicación a todos los sistemas de información viene reforzada cuando en el anexo I especifica que cuando se determina la categoría de un sistema esta será de aplicación a todos los sistemas empleados para la prestación de los servicios de Administración electrónica y para los empleados en el soporte del procedimiento administrativo general.

Hay un elemento esencial en todo el ENS, la política de seguridad (art. 1.1, objeto del ENS "determinar la política de seguridad"), que en ningún caso debe confundirse con el documento de seguridad, en el que la legislación sobre protección de datos obliga a documentar todas las medidas de seguridad desplegadas para proteger una fichero o tratamiento de datos de carácter personal, la política de seguridad tiene un alcance mayor, pero eso si, deberá referenciar y ser coherente con lo establecido en el documento de seguridad LOPD (apartado 3.1 del marco organizativo del anexo II del ENS).

Para el ENS la política de seguridad es el conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos, según eso el documento de seguridad LOPD seria una de esas directrices.

El ENS plantea por otra parte como principio básico la seguridad como función diferenciada, de manera que la responsabilidad de la seguridad de la información debe estar diferenciada de la responsabilidad sobre la prestación de los servicios, es en la política de seguridad de la organización donde deberán detallarse las atribuciones de responsabilidad y los mecanismos de coordinación y resolución de conflictos.

El art. 10 recoge la necesidad de diferenciar entre el responsable de la información, el responsable del servicio y el responsable de seguridad, añadiendo además a lo largo del ENS otra figura adicional, el responsable del sistema de información.

Obviamente las dificultades de aplicación de esa segregación de funciones en ciertas administraciones públicas, especialmente las administraciones locales de tamaño medio o

pequeño son más que evidentes, todo y que el ENS prevé un cierto recurso a entidades u organismos supra-municipales para el desarrollo de ciertos aspectos del ENS.

Incluye el ENS un práctica que se hecha de menos en el modelo de seguridad LOPD, como es la realización de análisis de riegos y la gestión de estos, todo y que en función de la categoría del sistema, el nivel de exigencia y formalización puede variar substancialmente.

Uno de los elementos que van a exigir una mayor sincronización va a ser el de las auditorias de seguridad, que al igual que en el contexto de la LOPD deben realizarse cada 2 años; a fin de evitar una doble auditoria sobre los mismos elementos es imprescindible adecuar las guías de auditoria para que con un solo proceso sea posible dar respuesta a los requerimientos de verificación del ENS y de la normativa de protección de datos de carácter personal.

Concluyendo

Estas son solo algunas de las cuestiones mas relevantes en cuanto a la sincronización de los dos modelos de seguridad, otro tipo de análisis más detallado tendría que ver con las medidas de seguridad concretas, todo el anexo II del ENS se dedica a ellas, y será necesario por parte de responsables de seguridad LOPD proceder a mapear que controles de los que planeta el ENS ya están implantados como exigencia LOPD, y si su configuración y alcance se corresponden.

En definitiva al reto del uso de los medios electrónicos y el acceso electrónico de los ciudadanos a los servicios de las administraciones públicas, se añade la imprescindible seguridad, pero también la necesaria sincronización de las medidas de seguridad LOPD, de manera que se evite la duplicación de procesos, la interferencia de medidas de seguridad, la repetición de funciones o roles en materia de seguridad de la información y cualquier otro efecto negativo de la concurrencia de los dos modelos de seguridad en los mismos sistemas de información.

Urge, por el valor que pueden aportar, disponer de instrumentos de ayuda y soporte a la adecuación al ENS, que por otra parte anuncia el propio decreto, y también que las autoridades de control en materia de protección de datos de carácter personal se posicionen al respecto, aportando criterios claros en cuanto a la coincidencia de las medidas de seguridad técnicas y organizativas previstas en el ENS y en el Real Decreto 1720/2007.

No quisiera finalizar si hacer un breve apunte sobre una modificación del reglamento de desarrollo de la LOPD, que inluye la Disposición adicional cuarta del Real Decreto 3/2010. Concretamente modifica la letra b del art. 81.5 del Real Decreto1720/2007, que pasa a tener la siguiente redacción:

“b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad”

Regula la excepción de aplicación de las medidas de seguridad de nivel alto todo y que puedan llegar a tratarse datos sensibles, al aparecer estos de forma incidental, antes solo se aplicaba la excepción a los tratamientos no automatizados, ahora a la excepción podrá aplicarse a cualquier tipo de tratamiento.