IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales»

ARTÍCULO

Las políticas públicas en materia de seguridad en la sociedad de la información

Ignacio Alamillo

Fecha de presentación: septiembre de 2009
Fecha de aceptación: noviembre de 2009
Fecha de publicación: diciembre de 2009

Resumen
La mayoría de los Estados se encuentran en el proceso de establecer una aproximación basada en múltiples participantes -aparte de los propios gobiernos- y una estructura de gobernanza de alto nivel para la implementación de políticas de alcance nacional.
En este sentido, estos Estados han hecho avances importantes en el desarrollo de marcos nacionales de políticas de seguridad, han aprobado medidas para combatir el cibercrimen y han establecido equipos de respuesta a incidencias de seguridad informática. Este artículo presenta las principales políticas y actuaciones públicas para la promoción de la seguridad de la información, y se centra específicamente en las actuaciones realizadas en Cataluña y en el Estado español en esta materia.

Palabras clave
políticas públicas de seguridad, cibercrimen, seguridad de la información

Tema
Protección de datos

Public Security Policies in the Information Society

Abstract
Most countries are in the process of reaching agreement among multiple participants - apart from the governments themselves - establishing a high level management structure for the implementation of national policies. Major advances have been made in the development of national frameworks for security policies, measures for combating cybercrime have been approved, and response teams for security issues have been established. This article presents the main public policies and legal proceedings for promoting information security, focussing specifically on legal proceedings which have been carried out in Catalonia and the rest of Spain.

Keywords
public security policies, cybercrime, information security

Subject
Data protection

1. Las políticas públicas de impulso genérico de la seguridad de la información

En esta sección presentamos las políticas públicas de seguridad de la información, desde una perspectiva genérica, común a toda la problemática de la seguridad de la información.

1.1. Estrategia global de seguridad de la información

El desarrollo de una estrategia global de seguridad de la información a nivel nacional empieza a ser una constante entre los Estados, una política habitualmente centrada en la necesidad de desarrollar herramientas de investigación y de concienciación del público en cuanto al número cada vez más importante de amenazas y vulnerabilidades de la seguridad en línea.

En algunos casos, se han desarrollado políticas nacionales para coordinar actuaciones previas individuales que perseguían objetivos muy concretos tratando de crear una política o estrategia global de seguridad, mientras que en otros casos las políticas nacionales se han dirigido a la implementación de políticas de administración electrónica e incluso de iniciativas singulares, como las firmas electrónicas o las tarjetas de ciudadanos.

La mayoría de los Estados se encuentran en fase de establecer algún tipo de estrategia global de la seguridad de la información, con dos rasgos característicos:

- Una aproximación multidisciplinar y con múltiples participantes.
- Una estructura de gobernanza de alto nivel.

Con respecto a la aproximación multidisciplinar y con múltiples participantes de las políticas nacionales de seguridad de la información, resulta interesante que la mayoría de las iniciativas constatan que la cultura de la seguridad no aparece sencillamente a partir de las soluciones tecnológicas.

Al contrario, se necesita una aproximación más amplia, que tome en consideración también los aspectos socioeconómicos y legales, lo que imprime una dimensión multidisciplinar a las políticas.

Además, se considera que los gobiernos, por sí solos, no pueden gestionar todos los retos y cuestiones de seguridad, lo que implica una necesidad de involucrar al sector privado y a la sociedad civil, efecto que se puede conseguir con diferentes instrumentos, como las asociaciones público-privadas, el desarrollo de mejores prácticas, el suministro de consejo y la participación en órganos comunes.

Resulta también frecuente que los gobiernos acudan al sector privado para recibir asesoría sobre desarrollos tecnológicos y de implementación global. Algunos Estados contratan a universidades y a expertos independientes para proporcionar ayuda en cuestiones de política, o crean la justificación necesaria para la implementación de una política concreta.

Como cuestión pendiente en la mayoría de los Estados, podemos encontrar la limitada participación de la sociedad civil en las cuestiones de seguridad de la información, lo que indica la necesidad de mejorar dicha participación.

Por lo que respecta a la estructura de gobernanza, la mayoría de los Estados posiciona su estructura de gobernanza de la seguridad al más alto nivel. En muchas ocasiones, encontramos una dependencia de esta estructura de seguridad de la oficina del Gobierno o del primer ministro y, de manera más escasa, como parece ser el caso del Estado español, esta responsabilidad se encuentra repartida entre diferentes departamentos ministeriales.

En todos los casos, es preciso indicar que una aproximación jerárquica, de arriba abajo, no resulta suficiente, también es necesaria la cooperación próxima de la industria y de todos los actores de la sociedad de la información, con el Gobierno como coordinador de los esfuerzos y actividades requeridas.

Más allá de las fronteras nacionales, se necesita la colaboración con las organizaciones internacionales y el resto de gobiernos para conseguir el objetivo de la seguridad, ya que la actividad individual de los Estados no puede dar respuesta al reto global de la seguridad de Internet, que no conoce fronteras.

En el Estado español, el Plan Avanza, liderado por el Ministerio de Industria, Turismo y Comercio, mediante la Secretaría de Estado de Telecomunicaciones y Sociedad de la Información, ha sido uno de los instrumentos importantes en relación con la estrategia global española de

seguridad de la información, de la que ha surgido una línea relevante de servicios a los ciudadanos y a las empresas, ofrecidos por el INTECO.

También es preciso referirse a la actuación del Centro Nacional de Inteligencia/Centro Criptológico Nacional, dependiente del Ministerio de Defensa, en relación con la política de seguridad de información clasificada en el ámbito de la defensa y la seguridad nacional, que incluye la participación en la OTAN, y la operación del Esquema nacional de evaluación y certificación de la seguridad de la información, orientado a la seguridad de los productos, tanto de ámbito militar como civil, y que se presenta posteriormente.

Finalmente, en el ámbito catalán, es necesario referirse al Plan nacional de seguridad de la información de Cataluña, aprobado por acuerdo del Gobierno de la Generalitat de Cataluña de 17 de marzo del 2009.

1.2. Concienciación y formación sobre la seguridad de la información

Una de las políticas públicas genéricas más importante es aquella que se orienta a incrementar los niveles de conciencia sobre la necesidad de la seguridad de la información, que la OCDE denomina la «cultura de la seguridad».

A este aspecto se han dedicado las importantes Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de la seguridad, del año 2002, que sustituyen a las directrices de seguridad de los sistemas de información del año 1992.

Las directrices parten de la noción de un importante cambio en la computación, que ha pasado de sistemas aislados y redes privadas a un entorno basado en ordenadores personales, tecnologías convergentes, el uso masivo de redes públicas como Internet y la interconexión de sistemas abiertos. En este nuevo contexto, Internet se ha convertido en parte de las infraestructuras operativas de sectores estratégicos como la energía, los transportes y las finanzas, y se encuentra en la base del comercio y el gobierno electrónicos, además de permitir nuevas posibilidades a los ciudadanos.

Como contrapartida, han surgido nuevas vulnerabilidades y amenazas a la seguridad de la información y las comunicaciones, que es preciso tratar adecuadamente, comenzando por un nivel suficiente de conocimiento de los nuevos retos de seguridad, para llegar a una cultura de la seguridad que abarque a todos los participantes en la sociedad de la información.

Los propósitos de las directrices son los siguientes:

- Promover una cultura de seguridad entre todos los participantes como medio para proteger los sistemas y redes de información.
- Incrementar la concienciación sobre el riesgo de los sistemas y redes de información sobre las políticas, prácticas, medidas y procedimientos disponibles para poder hacer frente a estos riesgos, así como sobre la necesidad de adoptarlos y ejecutarlos.
- Motivar entre todos los participantes una mayor confianza en los sistemas y redes de información, así como en su forma de operación y de uso.
- Crear un marco general de referencia que ayude a los participantes en la comprensión de los aspectos de seguridad y con respecto a los valores éticos en el desarrollo y la ejecución de políticas coherentes, así como de prácticas, medidas y procedimientos para la seguridad de sistemas y redes de información.
- Suscitar entre todos los participantes, cuando sea posible, la cooperación y el intercambio de información sobre el desarrollo y la ejecución de políticas de seguridad, así como de prácticas, medidas y procedimientos.
- Promover el conocimiento en materia de seguridad como un objetivo importante que se debe alcanzar entre todos los participantes involucrados en el desarrollo y la ejecución de normas técnicas.

En el marco de estos objetivos generales, se proponen nueve principios, complementarios entre sí, de interés político y técnico, con indicación expresa de que los esfuerzos por fortalecer la seguridad de los sistemas y redes de información deben respetar los valores democráticos y, en particular, garantizar tanto flujos de comunicación libres y abiertos como la protección de los datos de carácter personal:

1. Concienciación. Los participantes deben ser conscientes de la necesidad de disponer de sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.

2. Responsabilidad. Todos los participantes son responsables de la seguridad de los sistemas y redes de información.

3. Respuesta. Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten a la seguridad.

4. Ética. Los participantes deben respetar los intereses legítimos de terceros.

5. Democracia. La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.

6. Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo.

7. Diseño y realización de la seguridad. Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.

8. Gestión de la seguridad. Los participantes deben adoptar una visión integral de la administración de la seguridad.

9. Evaluación continua. Los participantes deben revisar y evaluar periódicamente la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

Continuando con su actividad de promoción de la cultura de la seguridad, la OCDE preparó en el año 2003 un plan de implementación que identifica aspectos importantes con respecto a los diferentes roles o funciones de los participantes, sobre la base de la necesidad de una cooperación continuada entre los gobiernos, las empresas y la sociedad civil.

En opinión de la OCDE, los gobiernos tienen la responsabilidad de emprender el liderazgo del desarrollo de la cultura de la seguridad, mediante las diferentes funciones que cumple en relación con los sistemas y redes de la información (desarrollador de políticas públicas, propietario y operador de sistemas y redes).

Durante el proceso de desarrollo de políticas públicas, los gobiernos deben promover la seguridad de las redes y los sistemas de información para generar confianza en su uso y asegurar mejor la seguridad global. A pesar de ser un proceso propio, los gobiernos deberían desarrollar estas políticas públicas de manera transparente, mediante consultas con otros gobiernos y con otros interesados.

Los gobiernos también deben desarrollar políticas públicas nacionales o regionales sobre seguridad de la información y certificar la cooperación internacional para promover esta cultura global de la seguridad mediante instrumentos como los siguientes:

- Medidas legales y técnicas para combatir la ciberdelincuencia, coincidentes con la Convención del Consejo de Europa, que presentaremos posteriormente.
- Equipos y recursos personales altamente cualificados para proporcionar soporte a la lucha coordinada contra el fraude informático.
- Instituciones preparadas para responder a ataques y emergencias informáticas, así como para intercambiar información al respecto, por ejemplo, los denominados CERT.
- Mecanismos de cooperación con el sector privado para combatir con mayor efectividad los problemas de seguridad.
- Apoyo a la investigación y el desarrollo en el campo de la seguridad de las tecnologías de la información.
- Actividades de concienciación pública, de formación y educación del público.
- Suministro de recursos de información al público sobre la seguridad de los sistemas y redes de información.

Como propietarios y operadores de sistemas y redes de información, los gobiernos comparten papel con las empresas, otras organizaciones y los individuos en cuanto a asegurar el uso correcto de los sistemas y las redes, dentro de la cultura de la seguridad.

En general, debido al volumen de los sistemas de los gobiernos en relación con el territorio nacional, éstos deberían ser un modelo y ejemplo de operación segura, para guiar al resto de organizaciones y ciudadanos mediante el establecimiento de mejores prácticas y otras técnicas de mejora organizativa; mientras que, en particular, es necesario considerar la capacidad de adquisición de tecnología que tienen los gobiernos como un mecanismo para influir en la mejora de la seguridad de los productos ofrecidos en el mercado.

El análisis realizado por la OCDE a finales del 2004 sobre las actividades gubernamentales, en relación con la seguridad de la información y, en particular, sobre el marco normativo en apoyo de la seguridad, ha mostrado que una serie importante de Estados identifican la firma electrónica y la certificación digital como aspecto esencial de su estrategia legal en apoyo de la seguridad.

Adicionalmente, se identifican como elementos importantes la protección de datos personales y las medidas de inspección y control sobre las comunicaciones electrónicas.

Con respecto a los programas de sensibilización sobre la seguridad de la información, ENISA ha publicado un interesante documento, dirigido a ayudar a los Estados miembros de la Unión a preparar este tipo de programa, en el que expone sus beneficios principales:

1. Representar un punto de referencia y un motor para una serie de actividades de sensibilización, formación y educación relacionadas con la seguridad de la información, de las que ya existen algunas, pero que posiblemente deban ser objeto de una mayor coordinación y optimización.

2. Transmitir las directrices o prácticas recomendadas importantes que sean necesarias para proteger los recursos de información.

3. Facilitar información general y específica sobre los riesgos y controles de la seguridad de la información a las personas que deban conocerla.

4. Informar a las personas de sus responsabilidades en relación con la seguridad de la información.

5. Estimular a las personas a adoptar las directrices o prácticas recomendadas.

6. Crear una cultura de seguridad más arraigada, con una comprensión y un compromiso de amplio alcance respecto a la seguridad de la información.

7. Contribuir a potenciar la coherencia y eficacia de los controles de la seguridad de la información y fomentar la adopción de controles efectivos con respecto a su coste.

8. Favorecer la reducción del número y el alcance de las infracciones de la seguridad, para disminuir así el coste directamente (por ejemplo, daños producidos por virus) e indirectamente (por ejemplo, reducción de la necesidad de investigar y solucionar las infracciones). Éstas son las principales ventajas financieras del programa.

Los últimos estudios muestran que los Estados ya se encuentran activamente involucrados en iniciativas para incrementar la concienciación pública en relación con la cultura de la seguridad, iniciativas que incluyen presentaciones públicas y la distribución de materiales informativos.

Por ejemplo, en el Estado español se pueden mencionar varias iniciativas en este sentido, que incluyen el proyecto de divulgación del estado de la seguridad FARO, de ASIMELEC; el *road-show* EXPOSEC para presentar aspectos de seguridad, también realizado por ASIMELEC en colaboración con el Ministerio de Industria, Turismo y Comercio; la constante tarea divulgadora de las cámaras de comercio, en particular de Camerfirma; o la actuación de la sociedad civil, por ejemplo, mediante el Foro de las evidencias electrónicas, que genera discusión en línea y reuniones periódicas con todos los actores en torno a aspectos relativos a la seguridad de la información, como la generación de pruebas electrónicas con reconocimiento judicial.

Los actos públicos tratan una importante variedad de temas de seguridad, cuestiones muy generales o más específicas como la gestión de riesgo, la autenticación electrónica, las firmas electrónicas o las infraestructuras de clave pública (PKI). El público destinatario de estos acontecimientos también resulta variable, desde el público en general hasta expertos que trabajan en el sector privado y el sector público. En particular, muchos gobiernos llevan a cabo de manera regular actuaciones internas para formar a su personal (por ejemplo, el Centro Criptológico Nacional tiene una importante actividad en éste sentido), con una incipiente tendencia a abrir estos actos al sector privado y a los ciudadanos, que puede ser un modo más efectivo de llegar a estos destinatarios.

Por otra parte, la preparación y distribución gratuita de recomendaciones, mejores prácticas y guías generales es una manera muy importante de vehicular las políticas de concienciación de la seguridad.

Además, en varios Estados existe la tendencia a redactar mejores prácticas y guías en cuestiones técnicas y operativas, como la autenticación en línea, las firmas electrónicas, las redes sin hilos, las redes entre iguales (*peer-to-peer*), la gestión del riesgo y la respuesta a incidentes.

1.3. Análisis y gestión de riesgo

El análisis y la gestión de riesgo es también una política genérica importante en varios Estados, entre los que se incluye el español.

Las iniciativas relacionadas con el análisis y la gestión de riesgo incluyen casos como el desarrollo de metodologías (Francia, con EBIOS, o España, con MAGERIT), o normas y guías (Noruega, Japón o EE. UU.). Algunas iniciativas se completan con una red específica de usuarios, como sucede en Francia, para el intercambio de información y para continuar el desarrollo de la metodología.

Otras iniciativas incluyen la creación y el suministro de herramientas automáticas para asistir en la realización de los análisis de riesgo, como es el caso de la herramienta PILAR del Centro Criptológico Nacional o de las herramientas del método CRAMM británico.

Es preciso indicar que el uso de las técnicas y herramientas de análisis y gestión de riesgo no se encuentra limitado a las tecnologías de la información, sino que también se empieza a utilizar en áreas como las de los desastres naturales o el sector de las telecomunicaciones y, de manera más genérica, para la protección de las infraestructuras críticas.

Asimismo, en algunos Estados, como Austria, el análisis de riesgo forma parte de los procesos de supervisión y control de los prestadores de servicios de certificación de firma electrónica, mientras que en Finlandia se ha utilizado como herramienta para los proyectos de cooperación financiera liderados por el Gobierno.

1.4. Evaluación de la seguridad de la información en productos y servicios

Con una orientación más particular hacia los productos, se encuentra ya consolidada la política de los Estados de fomentar la calidad y la seguridad de aquéllos mediante su certificación conforme a metodologías formales. Cada vez son más los Estados que exigen certificaciones de seguridad en los productos que han de adquirir para la realización de sus tareas.

El modo de implementar esta evaluación y certificación de la seguridad de la información consiste en la creación de un esquema nacional de evaluación, que permite la organización sistemática de las funciones de evaluación y certificación de la seguridad dentro de un país concreto, bajo la autoridad de un consejo de dirección o de una entidad de certificación de la seguridad, y tenga como objeto confirmar que se mantienen unos altos niveles de competencia y de imparcialidad, así como la consecución de la coherencia global del sistema.

Los esquemas nacionales se crean al amparo del Acuerdo de reconocimiento mutuo sobre los certificados de evaluación de la seguridad de las tecnologías de la información, de 26 de noviembre de 1997, aprobado por el grupo de altos funcionarios en seguridad de los sistemas de información de la Comisión Europea, de acuerdo con el mandato contenido en el punto tercero de la Recomendación del Consejo 95/144/CE, de 7 de abril de 1995.

Centrados inicialmente en la certificación de producto, de acuerdo con los criterios de evaluación de la seguridad de las tecnologías de la información (ITSEC) de 1991, en la actualidad, los Estados signatarios del Acuerdo también han asumido los llamados criterios comunes para la evaluación de la seguridad de las tecnologías de la información (*Common Criteria* o CC, ISO 15408), mediante la modificación del Acuerdo de 1997, así como la firma del Acuerdo sobre el reconocimiento de los certificados de criterios comunes en el campo de la seguridad de la tecnología de la información, de 23 de mayo del 2000.

Un esquema nacional de evaluación y certificación de la seguridad de las tecnologías de la información funciona de la manera siguiente:

- El esquema nacional es dirigido por un único organismo de certificación, de acuerdo con una política establecida por el propio organismo de certificación o por un consejo de dirección del esquema nacional, que deben crear y hacer cumplir los reglamentos operativos de aquél.
- El organismo de certificación ha de ser un organismo independiente, declarado competente por una norma legal o administrativa, o bien acreditado por una entidad de acreditación nacional. En cualquier caso, debe cumplir los requisitos EN 45011 o Guía ISO 65, o los requisitos descritos en el anexo C del Acuerdo ITSEC.
- El organismo autoriza la participación de los servicios de evaluación del esquema, controla el funcionamiento y la actividad de evaluación, examina todos los informes de ésta, elabora un informe de certificación con respecto a cada una de ellas y publica los certificados y los informes de certificación, así como una lista de productos certificados.

- El servicio o laboratorio de evaluación, además de ser autorizado por el organismo de certificación, debe ser previamente certificado por una entidad de acreditación nacional, excepto si ha sido creado y declarado competente por una norma legal o administrativa. En cualquier caso, ha de cumplir los requisitos EN 45001 o Guía ISO 25.

El Centro Criptológico Nacional, creado por el Real Decreto 421/2004, ha sido denominado órgano competente de certificación del esquema nacional de evaluación y certificación de la seguridad de las tecnologías de la información, mientras que el Instituto Nacional de Técnica Aeroespacial (INTA) actúa como laboratorio de evaluación autorizado para productos que traten información clasificada y no clasificada, y la empresa APPLUS actúa como laboratorio de evaluación autorizado para productos que traten información no clasificada, y ENAC como entidad de acreditación.

1.5. Investigación y desarrollo en seguridad de la información

La investigación y el desarrollo en materia de seguridad de la información es una de las políticas más habituales de los Estados avanzados en la cultura de la seguridad, especialmente por el impacto posterior en la competitividad de las empresas productoras de tecnologías de seguridad, que comercializan sus productos en el mercado global.

En este sentido, desde una perspectiva de política de la Unión Europea, la Resolución del Consejo, de 22 de marzo del 2007, sobre una estrategia para una sociedad de la información segura en Europa, considera que los recursos destinados a investigación y desarrollo (I+D) e innovación, tanto a nivel nacional como comunitario, constituyen uno de los elementos fundamentales para reforzar el nivel de seguridad de las redes y de la información de los nuevos sistemas, aplicaciones y servicios.

En consecuencia, se considera importante intensificar el esfuerzo a escala europea en los ámbitos de la investigación y la innovación en relación con la seguridad, en particular mediante el Séptimo programa marco y el Programa marco para la competitividad y la innovación.

Adicionalmente, es preciso realizar esfuerzos para implantar medidas destinadas a la difusión y promoción de la explotación comercial de los resultados, incluida la evaluación de su utilidad para la comunidad en su conjunto, lo que contribuirá a mejorar la capacidad de los proveedores europeos para suministrar soluciones de seguridad que respondan a las necesidades específicas del mercado europeo.

La mayoría de los Estados reconocen la importancia de las actividades de investigación y desarrollo para la seguridad de la información, ya que son la clave para producir soluciones innovadoras que puedan hacer frente a los requisitos presentes y futuros de la seguridad de la información. Como se ha avanzado, la inversión en investigación y desarrollo en seguridad de la información se percibe como un elemento que contribuye al incremento global de innovación y competitividad de los Estados.

Sin embargo, los estudios muestran que pocos Estados han establecido programas específicos de investigación en seguridad de la información con fondos públicos; la mayoría financia la investigación en seguridad mediante programas más amplios de investigación, habitualmente relativos a los aspectos computacionales (por ejemplo, criptografía) y tecnológicos, sin que se consideren de modo general los aspectos sociales, legales y económicos de la seguridad de la información.

De manera general, estas tareas de investigación y desarrollo son realizadas por las universidades, habitualmente por institutos específicamente creados para tratar la cuestión de la seguridad de la información y, con menos frecuencia, en cooperación con la industria. También resulta notable que la cooperación internacional en materia de investigación y desarrollo de la seguridad de la información sea limitada.

Como ejemplos de las actividades en esta área, se pueden mencionar los siguientes:

- El proyecto de los Países Bajos SENTINEL, con el objetivo de desarrollar aplicaciones seguras para sistemas de usuario, administración electrónica y comercio electrónico, que presenta una interesante aproximación multidisciplinar.
- El proyecto Oppidum (Francia) y el IKT SoS (Noruega).
- Los proyectos Seguridad 2020 (España) y los proyectos españoles de investigación específica, dentro de líneas de alcance tecnológico más amplio (caso similar

a Austria, Dinamarca, Alemania, Corea, Reino Unido o EE. UU.).

En algunos casos, las tareas de investigación son apoyadas o realizadas por organizaciones gubernamentales con responsabilidades de seguridad de la información, como la Oficina federal alemana de seguridad de la información, la Agencia coreana de seguridad de la información, el Establecimiento público canadiense de seguridad de las comunicaciones o la División de ciberseguridad del Departamento de Interior de Estados Unidos. Estas tareas de investigación persiguen el desarrollo de nuevas soluciones, como RFID, biometría o tecnología sin hilos, o solucionar necesidades o problemas inmediatos.

En otros casos, los Estados facilitan la participación de la industria y de otras instituciones independientes de investigación en sus iniciativas de búsqueda de seguridad de la información, como es el caso de España, Alemania, los Países Bajos o Austria.

2. El Plan nacional de seguridad de la información de Cataluña

El 17 de marzo del 2009, por Acuerdo de Gobierno 50/2009, publicado en el DOGC 5351, de 1 de abril, se aprobó el Plan nacional de seguridad de la información de Cataluña, según las competencias de la Generalitat de Cataluña en sociedad de la información y, en concreto, en el acceso a las tecnologías de la información y la comunicación (TIC), en comercio electrónico y consumo, y en administración electrónica, por el que se cree, en su caso, un centro de seguridad de la información de Cataluña (CESICAT), a fin de que desarrolle los objetivos estratégicos del Plan.

2.1. La seguridad TIC en el Estatuto de autonomía de Cataluña del 2006 (EAC)

Uno de los fundamentos importantes para afirmar la competencia de la Generalitat de Cataluña, y del resto de administraciones públicas catalanas en seguridad de la información, procede del importante artículo 40 del EAC («protección de las personas y de las familias»).

En este sentido, debemos partir del artículo 40.1, que exige a los poderes públicos «tener como objetivo la mejora de la calidad de vida de todas las personas» que, evidentemente, es necesario considerar aplicable en el más amplio sentido y, por supuesto, a la sociedad de la información, en la que las personas desarrollan una parte cada vez más importante de su vida.

Con respecto a los colectivos que se deben proteger especialmente, el artículo 40.3 del EAC determina que «los poderes públicos deben garantizar la protección de los niños, especialmente contra toda forma de explotación», incluyendo las formas de explotación que se pueden producir utilizando medios electrónicos, como en casos de acoso a través de la Red (*ciberbullying*) o de acoso sexual; una previsión estatutaria que se debe poner en relación con el artículo 142, que establece las competencias de la Generalitat en materia de juventud.

Asimismo, el artículo 40.6 del EAC establece que «los poderes públicos deben garantizar la protección de las personas mayores para que puedan llevar una vida digna e independiente y participar en la vida social y cultural», mandamiento estatutario que exige dirigir de manera específica los riesgos que la gente mayor puede sufrir en las redes telemáticas, para favorecer su integración y participación efectiva en la sociedad de la información, que dependerá, en parte, del grado de confianza que aquélla posea.

Finalmente, el artículo 40.8 del EAC indica que «los poderes públicos deben promover la igualdad de todas las personas con independencia del origen, la nacionalidad, el sexo, la raza, la religión, la condición social o la orientación sexual, y también deben promover la erradicación del racismo, del antisemitismo, de la xenofobia, de la homofobia y de cualquier otra expresión que atente contra la igualdad y la dignidad de las personas», obligación estatutaria que también hay que cumplir en relación con las nuevas formas de discriminación y todas las formas de atentados a los derechos y libertad que se puedan producir utilizando medios electrónicos, entre los que se incluyen los ciberdelitos.

Por su parte, el artículo 42.3 del EAC («cohesión y bienestar sociales») insiste en la obligación de los poderes públicos de «velar por la dignidad, la seguridad y la protección integral de las personas, especialmente de las más vulnerables», mención expresa de la seguridad que se debe considerar aplicable de manera plena a la seguridad de la sociedad de la información catalana.

Otro fundamento importante en relación con la competencia para actuar en esta materia lo encontramos en el artículo 49.1 del EAC («Protección de los consumidores y usuarios»), cuando determina que «los poderes públicos deben garantizar la protección de la salud, la seguridad y la defensa de los derechos y los intereses legítimos de los consumidores y usuarios».

Contiene esta norma otra referencia expresa a la seguridad, que también debe entenderse plenamente aplicable a la seguridad en la Red, en este caso con una especial atención a los consumidores y los usuarios (una parte muy importante de la ciudadanía, en el modelo económico actual), y que se identifica con un colectivo que debe ser protegido de modo específico.

Precisamente en relación con este colectivo se libra en la actualidad una de las batallas importantes contra el fraude, en concreto frente al robo de identidades financieras (mediante el *phishing*), el robo de informaciones comerciales sensibles, como los datos de las tarjetas de pago, o contra las comunicaciones comerciales no solicitadas (*spam*).

Es preciso señalar que el artículo 123 del EAC determina la competencia exclusiva de la Generalitat de Cataluña en materia de consumo, indicando los aspectos de formación y educación, que resultan particularmente importantes en materia de seguridad de las TIC.

Con respecto al comercio electrónico, también hay que señalar la competencia exclusiva de la Generalitat de Cataluña relativa a su ordenamiento administrativo, según el artículo 112.1.a) del EAC, lo que, de acuerdo con la nueva ley de impulso de la sociedad de la información, incluye la declaración de las medidas de seguridad aplicables al comercio electrónico.

Más concretamente, el artículo 53 del EAC («Acceso a las tecnologías de la información y de la comunicación») impone obligaciones de actuación positiva a los poderes públicos en relación con las TIC, y en concreto, su apartado 1 determina que «los poderes públicos deben facilitar el conocimiento de la sociedad de la información y deben impulsar el acceso a la comunicación y a las tecnologías de la información, en condiciones de igualdad, en todos los ámbitos de la vida social, incluido el laboral; deben fomentar que estas tecnologías se pongan al servicio de las personas y no afecten negativamente a sus derechos, y deben garantizar la prestación de servicios por medio de dichas tecnologías, de acuerdo con los principios de universalidad, continuidad y actualización».

Como resulta evidente en el texto, la actuación pública debe garantizar que las tecnologías no afecten negativamente a los derechos de las personas, lo que exige de un programa público de seguridad de la sociedad de la información que se responsabilice de ello.

Por otra parte, el principio de continuidad impuesto por el EAC obliga a la vigilancia y protección de los elementos que componen la infraestructura crítica de las TIC, tanto cuando ésta se encuentra bajo responsabilidad de las administraciones y, en general, del sector público como en manos del sector privado, con el que es necesario establecer políticas de colaboración y apoyo mutuo.

Otra dimensión de actuación en materia de seguridad de las TIC deriva, por conexión, del resto de competencias de la Generalitat de Cataluña y de los gobiernos locales de Cataluña. Este es el caso, en relación con las competencias de seguridad y protección civil (artículo 132 del EAC), de seguridad pública (artículo 164 del EAC) y privada (artículo 163) o energía y, en concreto, en materia de seguridad nuclear, ya que los efectos de un incidente de seguridad de la información pueden manifestarse civilmente, lo que produce un efecto en cascada, especialmente cuando los incidentes afectan a las infraestructuras críticas TIC, que dan soporte a los sectores gubernamental y productivo que dependen de éstas.

Esta competencia en materia de seguridad TIC sobre infraestructuras críticas se fundamenta, adicionalmente, en el artículo 140.7 del EAC, en relación con las redes de comunicaciones electrónicas, cuya seguridad es necesario proteger, ya que estas redes son el factor principal que permite la existencia y la continuidad de la sociedad de la información. Como hemos visto anteriormente, la política de la Unión Europea en materia de seguridad TIC se trata en la sede del marco reglamentario de las comunicaciones electrónicas, en que el EAC otorga competencias ejecutivas a la Generalitat de Cataluña.

Finalmente, corresponde a la administración pública la competencia de organización y regulación del funcionamiento administrativo propio, así como el régimen jurídico

y procedimiento administrativo (artículo 159 del EAC), en el contexto de la legislación estatal básica, y en materia TIC, dentro del marco de la ley de acceso electrónico de los ciudadanos a los servicios públicos, que trata extensamente las obligaciones de seguridad de la actuación administrativa, y que incluye aspectos de firma electrónica, pero también el resto de aspectos de seguridad de la información.

2.2. Los objetivos estratégicos del Plan nacional de impulso de la seguridad de las TIC en Cataluña

El Plan se estructura alrededor de cuatro objetivos estratégicos principales:

1. Establecimiento de una estrategia nacional de seguridad TIC.

2. Apoyo a la protección de las infraestructuras críticas TIC nacionales.

3. Promoción de un tejido empresarial catalán sólido en seguridad TIC.

4. Incremento de la confianza y protección de la ciudadanía catalana en la sociedad de la información.

2.2.1. Establecimiento de una estrategia nacional de seguridad TIC

El primer objetivo trata sobre el desarrollo de una estrategia global de seguridad de la información a nivel nacional, política que se debe centrar en la necesidad de desarrollar herramientas de investigación y de concienciación del público en cuanto al número cada vez más importante de amenazas y vulnerabilidades de la seguridad en línea, definida por una aproximación multidisciplinar y con múltiples participantes, por un lado, y por una estructura de gobernanza de alto nivel, por otro.

Es preciso definir un modelo público catalán de seguridad de la sociedad de la información en Cataluña que dirija de manera global los retos que se planteen en cada momento, que actúe como interlocutor con todos los implicados y que tenga una capacidad de respuesta real a los problemas que se puedan producir, con un centro de seguridad y respuesta a incidentes como eje central vertebrador del Plan nacional de seguridad TIC, que efectúe un análisis de riesgo continuado y vele por la integridad y la continuidad de las redes y de los sistemas.

En todo caso, se debe indicar que una aproximación jerárquica, de arriba abajo, no resulta suficiente, también es necesaria la cooperación próxima de la industria y de todos los actores de la sociedad de la información, con el Gobierno como coordinador de los esfuerzos y las actividades requeridas. Al contrario, se considera que los gobiernos solos no pueden gestionar todos los retos y las cuestiones de seguridad, lo que implica una necesidad de involucrar al sector privado y a la sociedad civil, efecto que se puede conseguir con diferentes instrumentos, como las asociaciones público-privadas, el desarrollo de mejores prácticas, el suministro de consejo y la participación en órganos comunes.

Este sistema reforzará iniciativas y programas ya existentes, como el Sistema público catalán de certificación, bajo responsabilidad de la Agencia Catalana de Certificación, y la actuación de otros órganos supervisores (comercio, consumo, niños y jóvenes, policías públicas, etc.).

2.2.2. Apoyo a la protección de las infraestructuras críticas TIC nacionales

El segundo objetivo estratégico se orienta a la protección de los elementos que conforman las infraestructuras críticas TIC nacional, incluyendo las redes de comunicaciones electrónicas, pero también los principales elementos en los que éstas se basan, como los sistemas de energía y los principales centros de procesamiento de datos y de prestación de servicios críticos (como la energía, el suministro de agua, el transporte, el sector financiero, las telecomunicaciones y la salud), ya que en estas infraestructuras de información confían los gobiernos, la industria, los ciudadanos y el resto de la sociedad .

Las consecuencias de un ataque contra los sistemas industriales de control de las infraestructuras críticas podrían ser múltiples. Se considera que un ataque cibernético causaría pocas víctimas o ninguna, pero podría implicar la pérdida de servicios de infraestructura vitales, como el telefónico, en el que se confía por parte de los servicios de emergencia, mientras que ataques contra los sistemas de control de infraestructuras químicas pueden implicar escapes de materiales tóxicos, que en este caso podrían producir víctimas mortales.

Por otra parte, debemos indicar que los efectos en cascada pueden ser muy dañinos y provocar grandes caídas de los servicios públicos. Algunos supuestos que hay que tratar son los servicios TIC del Gobierno de la Generalitat de Cataluña y de los gobiernos locales de Cataluña, las redes de los servicios de emergencias y de protección civil (el número único 112, los mossos, el CECOPAL, los bomberos, los agentes rurales, etc.) y los servicios privados que ofrecen apoyo.

2.2.3. Promoción de un tejido empresarial catalán sólido en seguridad TIC

El tercer objetivo estratégico persigue la creación de un tejido empresarial en seguridad TIC en Cataluña que complemente la actuación pública en esta materia y potencie el sector TIC catalán en alguno de los mercados emergentes.

Esta necesidad se ha puesto de manifiesto en el estudio sobre el mercado de las TIC en Cataluña[1], realizado por la Fundación Observatorio de la Sociedad de la Información de Cataluña (FOBSIC), que indica como línea recomendada de actuación el impulso a la pyme del sector TIC, para lo que utiliza la promoción de las certificaciones de calidad y las tecnológicas de las empresas del sector mediante programas de comunicación de las empresas clientes de los beneficios de la certificación, normativas de obligado cumplimiento en la contratación con la administración, apoyo a programas de formación y certificación en metodologías y procesos de prestación de servicios.

En este sentido, se promoverá la creación de una red de pyme para la prestación de servicios de seguridad y respuesta a incidentes de seguridad, así como una comunidad en seguridad TIC especializada en todos los aspectos de la seguridad, con una especial atención a la formación y certificación de profesionales, empresas, productos y software, en este caso basándose en las potencialidades tanto de un mercado de software libre de seguridad como de la innovación y la investigación.

Esta comunidad se debe utilizar como herramienta para la generación de negocio TIC en el territorio; por este motivo, se considera necesario ubicarlo en algún espacio adecuado para esta finalidad; en concreto, el tecnoparque de Reus.

2.2.4. Incremento de la confianza y protección de la ciudadanía catalana en la sociedad de la información

El cuarto objetivo estratégico se dirige a velar por la confianza y la protección de los ciudadanos y ciudadanas en su uso de la sociedad de la información, con una atención especial a los colectivos con más riesgos, como los niños y los jóvenes, mediante el establecimiento de programas de concienciación y apoyo específicamente dirigidos a estos colectivos.

También se actuará en apoyo de la lucha contra todas las formas de delincuencia informática, de manera coordinada con los agentes competentes y reforzando las capacidades de detección y denuncia de ilegalidades de todo tipo, así como el filtraje de contenidos y el análisis forense de evidencias electrónicas.

1. FOBSIC y Penteo Research (marzo, 2008), «El Mercat de les Tecnologies de la Informació i la Comunicació a Catalunya: 2007-2010».

Cita recomendada

ALAMILLO, Ignacio (2009). «Las políticas públicas en materia de seguridad en la sociedad de la información». En: «V Congreso Internet, Derecho y Política (IDP). Cara y cruz de las redes sociales» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 9. UOC. [Fecha de consulta: dd/mm/aa].

‹http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_alamilo/n9_alamillo_esp›

ISSN 1699-8154

Sobre el autor

Ignacio Alamillo

Ignacio Alamillo es consultor sénior en seguridad de la información (Dirección General de la Sociedad de la Información. Secretaría de Telecomunicaciones y Sociedad de la Información. Generalitat de Cataluña)

Licenciado en Derecho. Abogado del ilustre Colegio de Madrid. Director del Área de Asesoramiento e Investigación de la Agencia Catalana de Certificación (diciembre 2002-febrero 2008). Director del Área de Consultoría y Servicios Legales de la Agencia de Certificación Electrónica-ACE (julio 1997-diciembre 2002). Miembro del grupo directivo europeo de Seguridad de Redes y de la Información y del grupo directivo de la Iniciativa Europea de Normalización de la Firma Electrónica, con asesoramiento a la Comisión Europea. Miembro del Consejo de Certificación de ASIMELEC. Ha sido miembro del grupo directivo europeo de la Iniciativa Europea de Normalización de la Firma Electrónica y del grupo de Infraestructura de Seguridad de Firma Electrónica del Instituto Europeo de Normas de Telecomunicaciones. Es autor del ABC de la firma electrónica y coautor de cuatro libros sobre aspectos jurídicos de la sociedad de la información, de numerosos artículos y ponencias en firma electrónica y su campo de aplicación.

ASTREA, La Infopista Jurídica, S. L.
Blondel, 21
25002 Lleida, España