Area: Seguridad y Defensa
ARI 101/2010
Date: 18/06/2010

Ciberseguridad en España: una propuesta para su gestión

Enrique Fojón Chamorro y Ángel F. Sanz Villalba [*]

Tema: Las relaciones sociales, económicas y culturales dependen, cada vez más, de las tecnologías e infraestructuras de la información y comunicación (ciberespacio), haciendo necesario articular un sistema nacional de seguridad (ciberseguridad) que gestione los riesgos que amenazan su funcionamiento.

Resumen: Las Tecnologías de la Información y la Comunicación (TIC) han coadyuvado al bienestar y progreso de las sociedades de forma que gran parte de las relaciones públicas y privadas dependen de estas tecnologías. Con el tiempo y la evolución de las TIC, han aparecido riesgos que hacen necesario gestionar su seguridad. Inicialmente, la ciberseguridad se ocupó de proteger la información (*Information Security*) de una manera reactiva, pero posteriormente ha evolucionado hacia una posición proactiva que identifica y gestiona los riesgos que amenazan el ciberespacio (*Information Assurance*). Este ARI realiza una aproximación a los conceptos de ciberespacio y ciberseguridad, a los riesgos y amenazas conocidos, a la gestión existente en España y a la necesidad de desarrollar un sistema nacional de ciberseguridad que fomente la integración de todos los actores e instrumentos, públicos o privados, para aprovechar las oportunidades de las nuevas tecnologías y hacer frente a los retos que presentan.

Análisis:

Introducción a los conceptos de ciberespacio y ciberseguridad

Los términos ciberespacio y ciberseguridad gozan ya de un uso generalizado por amplios sectores de nuestra sociedad. Sin embargo, antes de abordar un análisis del estado de la ciberseguridad en España y de proponer una aproximación a su gestión, es imprescindible alcanzar una definición del concepto de ciberespacio de manera que todos los individuos afectados por el mismo sean conscientes de sus implicaciones sociales, económicas y culturales. Una vez descrito el concepto de Ciberespacio, será inmediato comprender el concepto, y la necesidad, de Ciberseguridad.

Ciberespacio en un concepto que se emplea dentro de la comunidad de las TIC y se refiere al conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos. Para alcanzar una definición de ciberespacio que permita comprender las implicaciones referidas más arriba, será útil recurrir al

[*] *Enrique Fojón Chamorro, ingeniero superior en informática; y Ángel F. Sanz Villalba, ingeniero de telecomunicación*

concepto de servicio, entendido como la prestación que recibe un usuario o consumidor por parte de un proveedor.

Podemos identificar relaciones proveedor-consumidor no sólo entre empresas y usuarios domésticos, sino también entre empresas, administraciones públicas y ciudadanos y, por supuesto, entre individuos. Estas relaciones han existido desde mucho antes de la aparición de las TIC, a mediados del siglo XIX, con la invención del telégrafo y, por supuesto, antes de su revolución a partir del descubrimiento y aplicación de las propiedades de los materiales semiconductores que permitieron el nacimiento de la "era digital". Pero es a partir de ese momento, precisamente, cuando las TIC se convierten en el catalizador de los servicios tradicionales que prestaban las empresas a sus clientes, tanto de su extensión o capilaridad como de su eficiencia económica, al mismo tiempo que permitían la aparición de nuevos servicios.

Por tanto, podemos definir el *ciberespacio* como el conjunto de medios y procedimientos basados en las TIC y configurados para la prestación de servicios. La definición permite comprender de inmediato que el ciberespacio es ya parte esencial de nuestras sociedades, economías e, incluso, puede llegar a ser factor determinante de la evolución de las culturas, o quizás de su convergencia. De ahí la importancia de proteger el ciberespacio. Anteriormente, la ciberseguridad obedecía a un enfoque de protección de la información (*Information Security*) donde solamente se trataba de proteger la información a accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones no permitidas. En la actualidad, este enfoque está evolucionando hacia la gestión de riesgos del ciberespacio (*Information Assurance*) donde la ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados.

Una de las razones para este nuevo enfoque es la caracterización del ciberespacio de una determinada entidad como un sistema TIC que proporciona servicios, de manera que la seguridad del sistema se consigue cuando éste se encuentra en un estado de riesgo conocido y controlado. Realmente, ambos enfoques, *information security* e *information assurance*, son diferentes pero complementarios, y con mucha frecuencia son utilizados indistintamente de manera errónea. Resumiendo, la ciberseguridad debe formularse proactivamente como un proceso continuo de análisis y gestión de los riesgos asociados al ciberespacio.

Estado de riesgo del ciberespacio

El temor a las catastróficas consecuencias de un hipotético "ciber-Katrina" o a un "ciber-11S" ha provocado que países como EEUU, Francia, el Reino Unido, Israel y Corea del Sur, así como la ONU y la OTAN entre otras organizaciones internacionales, hayan tomado conciencia de la importancia y necesidad de un ciberespacio seguro y, por ello, han desarrollado o están desarrollando marcos normativos, planes y estrategias específicos para la defensa del ciberespacio. En definitiva, han tomado la decisión de gestionar la seguridad del ciberespacio bajo su responsabilidad de manera sistemática.

Por otro lado, China, Irán, Corea del Norte, Rusia y Pakistán han reconocido su interés estratégico en el ciberespacio como vehículo para alcanzar posiciones de liderazgo económico y político en sus áreas geográficas de influencia, y lo están concretando en la definición de políticas y en la ejecución de grandes inversiones económicas destinadas a recursos TIC y la formación de recursos humanos, con el objetivo de establecer "una

defensa beligerante" de su ciberespacio. Estos países, o al menos sus territorios, han sido identificados como el origen de la mayoría de las acciones agresivas acontecidas en el ciberespacio durante los últimos años. La continua y acelerada evolución de las TIC ha propiciado que los ataques sean cada vez más sofisticados, dando lugar a un ciberespacio cada vez más hostil, obligando a los gestores de la ciberseguridad a disponer de medios técnicos y humanos vanguardistas para poder hacer frente a las amenazas y sus posibles impactos.

Después de identificar y valorar los activos que han de protegerse, deben detectarse las posibles amenazas, las cuales tienen una naturaleza heterogénea y un alto grado de innovación. Las amenazas sobre el ciberespacio se concretan en ciberataques que pueden ser clasificados, en función de su autoría e impacto, según las siguientes categorías:

- Ataques patrocinados por Estados. Los conflictos del mundo físico o real tienen su continuación en el mundo virtual del ciberespacio. En los últimos años se han detectado ciber-ataques contra las infraestructuras críticas de países o contra objetivos muy concretos, pero igualmente estratégicos. Algunos ejemplos, ya conocidos para gran parte de la opinión pública, son el ataque a parte del ciberespacio de Estonia en 2007, que supuso la inutilización temporal de muchas de las infraestructuras críticas del país báltico o los ciber-ataques sufridos por las redes clasificadas del gobierno estadounidense a manos de atacantes con base en territorio chino.
- Terrorismo, extremismo político e ideológico. Los terroristas y grupos extremistas utilizan el ciberespacio para planificar sus acciones, publicitarlas y reclutar adeptos para ejecutarlas. Estos grupos ya han reconocido la importancia estratégica y táctica del ciberespacio para sus intereses.
- Ataques del crimen organizado. Las bandas del crimen organizado (*ciber-gangs*) han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que éste ofrece. Este tipo de bandas tienen como objetivo la obtención de información sensible para su posterior uso fraudulento y conseguir grandes beneficios económicos. Según datos del FBI,[1] en 2009 el impacto del cibercrimen por la acción de bandas organizadas ocasionó una perdidas, tanto a empresas como a particulares estadounidenses, por un valor superior a 560 millones de dólares.
- Ataques de perfil bajo. Este tipo de ataques son ejecutados, normalmente, por personas con conocimientos TIC que les permiten llevar a cabo ciber-ataques de naturaleza muy heterogénea y por motivación, fundamentalmente, personal.

Una reflexión rápida de los tipos de amenazas e impactos sobre los activos del ciberespacio y de los servicios que dependen de él evidencia que las TIC, al mismo tiempo que permiten disfrutar de más y mejores servicios en muchos ámbitos de nuestras sociedades, también aumentan el riesgo de sufrir ataques sobre tales servicios, con el agravante de que la extensión y popularización de las TIC difuminan las líneas de defensa del bien a proteger. Con la misma facilidad que un ciudadano accede al ciberespacio para gestionar desde su hogar sus cuentas bancarias, otro individuo puede acceder a información "en red" sobre cómo romper la seguridad de ese servicio y sustraer las claves privadas de aquél y suplantar su identidad.

[1] *http://www.ic3.gov/media/annualreport/2009_ic3report.pdf.*

La gestión de la ciberseguridad en España

Una vez conocido el ámbito global del ciberespacio y de sus amenazas, será fácil comprender la dificultad de abordar su seguridad en una determinada parte del total del conjunto. Hablar de ciberseguridad en una determinada nación requiere plantear, al menos, dos dimensiones: la protección de bienes, activos, servicios, derechos y libertades dependientes de la jurisdicción estatal, y la responsabilidad compartida con otros Estados, bilateralmente o a través de organismos supranacionales, sobre la ciberseguridad.

En otras palabras, la dificultad estriba en lograr que la agregación de soluciones parciales aplicadas por los estados, aunque se haga de forma coordinada, resuelva los problemas globales creados por unas tecnologías que derriban fronteras. El ciberespacio está en continuo crecimiento y acelerada evolución, alcanzando una capilaridad tal que permite sostener las relaciones y dependencias sociales, económicas y culturales, que son fundamentales para el desarrollo y crecimiento de nuestro país.

Atendiendo a la primera dimensión del problema, es preciso identificar cuáles son los activos dependientes del ciberespacio en España, qué regulación existe, cuáles son los organismos con funciones y responsabilidades en la materia y quiénes son los participantes. La defensa de nuestro ciberespacio abarca a todos los activos y actores imaginables, pero debe centrarse, fundamentalmente, en la defensa de las infraestructuras críticas, el tejido empresarial y las libertades y derechos individuales.

Las infraestructuras críticas de nuestro país se encuentran agrupadas en los siguientes 12 sectores: administración, alimentación, energía, espacio, sistema financiero y tributario, agua, industria nuclear, industria química, instalaciones de investigación, salud, transporte y tecnologías de la información y las comunicaciones. En cualquiera de estos sectores, el grado de penetración del ciberespacio, tanto para la gestión interna como para la provisión de servicios, alcanzó su grado crítico ya hace tiempo. Cualquier contingencia que pudiese afectar a alguno de los activos pertenecientes a cualquiera de los 12 sectores estratégicos podría comprometer la seguridad nacional.

En cuanto al tejido empresarial español, la gran mayoría de las grandes empresas disponen de una organización interna suficientemente madura que les permite implementar las actividades y medidas que se enmarcan dentro de las prácticas de *information security* e *information assurance*. En el caso de las pequeñas y medianas empresas y autónomos (el 99% del total),[2] la falta de recursos económicos y humanos impiden la implementación de ciberseguridad aunque sus actividades se sustentan, fundamentalmente, en las TIC. El Gobierno está fomentando el acceso de las empresas y autónomos españoles a las TIC y a las buenas prácticas de la ciberseguridad mediante las líneas de financiación del Plan Avanza.[3]

En relación con los ciudadanos, el índice de penetración de los servicios de la sociedad de la información (correo electrónico, redes sociales, comercio electrónico) es ya suficientemente alto[4] como para que cualquiera de los tipos de amenazas enunciados pueda producir impactos graves en las libertades y derechos individuales.

[2] *http://estaticos.expansion.com/estaticas/documentos/2010/05/pymessocietarias.pdf.*
[3] *http://www.planavanza.es/Paginas/Inicio.aspx.*
[4] *http://www.mityc.es/dgdsi/esS/Servicios/Biblioteca%20Indicadores/METRICA_SI_06.pdf.*

Estado actual de la ciberseguridad en España

España, a diferencia de otros países de nuestro entorno, no ha definido todavía una legislación específica y completa en materia de ciberseguridad. Sí existe legislación distribuida en distintos ámbitos ministeriales, pero que no ha sido desarrollada a partir de una política común que refleje el ámbito nacional y estratégico de la ciberseguridad.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica,[5] constituye un buen punto de partida, pero, como su propio nombre indica, cubre únicamente el sector de las administraciones públicas, dejando fuera los otros sectores relevantes para la gestión de la ciberseguridad: otras infraestructuras criticas, las empresas y los ciudadanos. Además del citado Real Decreto existen leyes nacionales, europeas e internacionales que abordan la cuestión de la ciberseguridad. Entre estas, se encuentran la Ley Orgánica de Protección de Datos, la Ley General de Telecomunicaciones y la Ley de la Sociedad de la Información y Comercio Electrónico.

A pesar de la existencia de este marco normativo, su grado de cumplimiento, en algunos casos, es preocupantemente bajo, lo cual supone un aumento del riesgo de nuestro ciberespacio. Las competencias relacionadas con la gestión de la ciberseguridad están repartidas entre un conjunto de organismos e instituciones, que dependen de diferentes ministerios del gobierno. Entre los más relevantes se encuentran:

- El Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI) que tiene, entre sus misiones, la gestión de la seguridad del ciberespacio dependiente de cualquiera de los tres niveles de las administraciones públicas: estatal, autonómico y local. El CCN-CERT (Capacidad de Respuesta ante Incidentes de Seguridad) es el centro de alerta nacional que coopera con todas las administraciones públicas para responder rápidamente a los incidentes de seguridad en su parte del ciberespacio y, además, es el responsable último de la seguridad de la información nacional clasificada.
- El Instituto Nacional de Tecnologías de la Comunicación (INTECO), dependiente del Ministerio de Industria, Turismo y Comercio, es responsable de gestionar a través de su CERT la defensa del ciberespacio relacionado con las PYMES españolas y los ciudadanos en su ámbito doméstico.
- El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), dependiente del Ministerio del Interior procura la ciberseguridad relacionada con estas infraestructuras.
- El Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional, dependientes ambos del Ministerio del Interior son responsables de combatir la delincuencia que se produce en el ciberespacio.
- La Agencia Española de Protección de Datos (AGPD), dependiente del Ministerio de Justicia, responsable de hacer cumplir la normativa en materia de protección de datos personales.

Además, en la administración autonómica existen centros homólogos a los referidos a nivel estatal como el CSIRT-CV de la Comunidad Valenciana y las Agencias de Protección de Datos de la Comunidad de Madrid y de la Generalitat de Cataluña, que igualmente tienen responsabilidades en la gestión de la ciberseguridad en su ámbito

[5] *http://www.csi.map.es/csi/pg5e42.htm.*

autonómico. En resumen, si bien existen organismos con responsabilidades claras en distintos ámbitos de las administraciones públicas, España no dispone de un órgano único, al más alto nivel, que asuma el valor estratégico que la ciberseguridad tiene para nuestro país y ejerza el liderazgo necesario para que todos esos organismos actúen según una única política nacional.

Industria

La industria española relacionada con la ciberseguridad está en pleno proceso de crecimiento y maduración, tal y como refleja el último "Catálogo de empresas y soluciones de seguridad" del INTECO,[6] cifrando en más de 1.000 las empresas españolas que se dedican a la ciberseguridad. En 2009, las principales empresas del sector se agruparon en el Consejo Nacional Consultor sobre Ciber-Seguridad (CNCCS) con el objetivo de fomentar la defensa del ciberespacio, poniéndose a disposición de entidades gubernamentales o privadas para asesorar en materias de ciberseguridad, y potenciar la innovación tecnológica y el crecimiento económico consiguientes.

Las empresas reconocieron pronto el valor estratégico del ciberespacio, tanto del propio como del concebido globalmente, y así aparecieron los departamentos de seguridad en sus organizaciones y las agrupaciones como el CNCCS. Sin embargo, apenas existen iniciativas desde el lado de la administración pública que fomenten la colaboración entre el Estado y la industria. Una relación que debería ser bidireccional: las empresas necesitan crear valor alrededor del negocio de la ciberseguridad y el Estado precisa de tecnología que le permita disponer de una capacidad solvente y vanguardista de ciberseguridad.

Participación ciudadana

España alcanzó en 2009 una tasa de penetración en Internet del 71,8%,[7] lo cual representa más de 30 millones de ciber-usuarios potenciales. Substrayendo la población pre-escolar y los mayores de 75 años, este porcentaje, superior al 70% de la población con acceso a los servicios del ciberespacio puede interpretarse como que, prácticamente, la totalidad de la población de España accede a tales servicios. La actual legislación española relacionada con la ciberseguridad hace especial énfasis en la necesidad de formación y concienciación de los ciudadanos en esta materia, así como en el uso responsable del ciberespacio. Sin embargo, la aplicación de estos principios hasta el momento es escasa debido, fundamentalmente, al desconocimiento generalizado de la legislación. El INTECO y el CCN, dentro del ámbito de sus competencias, desarrollan interesantes campañas de concienciación y formación en materia de seguridad TIC, pero aún sin la repercusión deseada. La industria española del sector de la ciberseguridad ha emprendido, igualmente, diversas campañas privadas para la concienciación y formación de determinados sectores de la sociedad como los escolares, jubilados y desempleados.

Colaboración internacional

España forma parte de organizaciones internacionales que promueven la defensa del ciberespacio. Destaca nuestra participación en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN y en organismos como ENISA (*European Network Information*

6 *http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_lopd_pymes.*

7 *http://www.inteco.es/icdemoest/Seguridad/C_Demostrador*.

Security Agency),[8] el AWG (*Antiphising Working Group*),[9] y el *Art.29 Data Protection Working Party*.[10] Nuestra presencia y colaboración en organismos internacionales no sólo permiten compartir experiencias y conocimientos sobre los riesgos y las soluciones, sino que corroboran que ningún ciberespacio nacional podrá ser gestionado eficazmente si el resto de porciones del ciberespacio global no se encuentran en un nivel de riesgo similar. Uno de los principios no escritos de la seguridad de las TIC afirma que la cadena siempre se rompe por el eslabón más débil. De poco o nada le sirve a una nación implementar una ciberseguridad muy avanzada, si el resto o alguno de los países que intervienen en el ciberespacio no se encuentran en un nivel parecido.

Conclusión

Propuestas para la gestión española de la ciberseguridad
España, a pesar de los esfuerzos realizados, no dispone aún de una capacidad sólida que permita realizar una dirección y gestión eficaces y eficientes de nuestra ciberseguridad. Para definir y obtener dicha capacidad, se deberían aplicar los siguientes principios:

(1) El gobierno de España debe identificar la seguridad de su ciberespacio como un objetivo estratégico de la Seguridad Nacional, puesto que la materialización de una amenaza sobre nuestro ciberespacio puede afectar muy negativamente al desarrollo social, económico y cultural de nuestro país.

(2) Se debe elaborar una Estrategia Nacional de Ciberseguridad de la que emane un marco normativo específico que regule el ciberespacio y su seguridad. La reciente publicación del Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, es un buen punto de partida, pero será necesario adecuar y hacer cumplir la legislación vigente.

(3) La dirección de la ciberseguridad debe realizarse de manera centralizada. Como corolario del principio anterior, el Estado debe crear un organismo con la misión de dirigir la ciberseguridad nacional, coordinando a las entidades públicas y privadas implicadas.

(4) El gobierno debe fomentar y reforzar la cooperación internacional en materia de ciberseguridad. Las alianzas multinacionales y bilaterales en materia de ciberseguridad son indispensables. En el caso español, tenemos una oportunidad de liderazgo responsable con países iberoamericanos y se deberán alcanzar acuerdos con aquellos países que, aunque no se encuentren dentro de nuestro entorno geopolítico más próximo, son relevantes para controlar las amenazas sobre nuestro ciberespacio.

(5) Las administraciones del Estado se deberán promover una cultura de la ciber-responsabilidad, basada en la concienciación y formación continua en ciberseguridad. Para ello, los planes de estudio de las enseñanzas primaria, secundaria y universitaria deberían incluir en sus currículos materias relacionadas con el uso responsable del ciberespacio.

[8] *http://www.enisa.europa.eu/.*
[9] *http://www.apwg.org/.*
[10] *http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.*

(6) El Estado debe promover e invertir en la investigación, el desarrollo y la innovación (I+D+i) del sector de la ciberseguridad, que proporcione soluciones TIC de primer nivel y empleo cualificado.

Por tanto, el gobierno debe asumir el liderazgo en materia de ciberseguridad para concienciar a los ciudadanos de la necesidad de proteger el ciberespacio del que dependen nuestros servicios básicos, infraestructuras críticas, economía y progreso como sociedad. Las TIC no son el problema, son parte de la solución y su protección y empleo seguro no son sólo responsabilidad del gobierno, sino de las demás administraciones autonómicas y locales junto con el sector privado, empresarial y doméstico. Todos son corresponsables, pero le corresponde al gobierno el liderazgo y la dirección de la gestión nacional de la ciberseguridad. Responsabilidades que no pueden delegarse y que deben traducirse en proporcionar el impulso, las ideas y la dirección que España necesita.

Enrique Fojón Chamorro
Ingeniero Superior en Informática

Ángel F. Sanz Villalba
Ingeniero de Telecomunicación