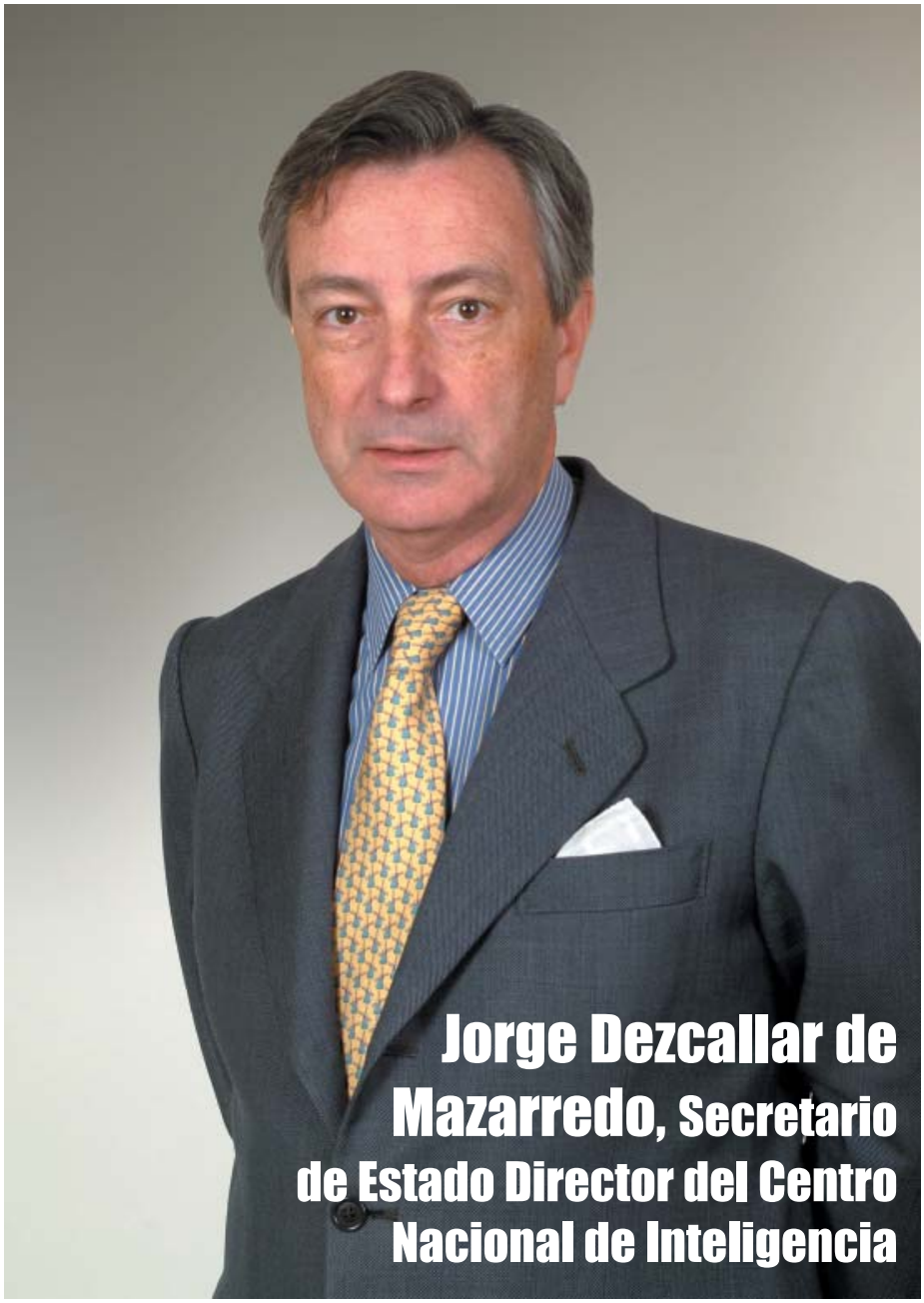
«El Centro Nacional de Inteligencia tiene previsto definir y desarrollar reglamentariamente los cometidos del Centro Criptológico Nacional»



Jorge Dezcallar de Mazarredo, Secretario de Estado Director del Centro Nacional de Inteligencia

El Centro Nacional de Inteligencia (CNI), tras su ampliación de competencias en materia de seguridad de la información, se encuentra actualmente en un proceso de definición y desarrollo de los cometidos del Centro Criptológico Nacional (CCN) con base en la denominada Política Infosec. De estas acciones, que van a tener una extraordinaria repercusión en todas las estructuras del Estado español, habla en la presente entrevista Jorge Dezcallar de Mazarredo, Director del CNI con categoría de Secretario de Estado.

– ¿Qué se entiende en el Centro Nacional de Inteligencia (CNI) por seguridad de la información y por gestión de la seguridad en los sistemas de información tecnológicos utilizados para su tratamiento?

– El objetivo de la seguridad es proteger los recursos (personal, información, material, instalaciones) y las actividades. Según sea el recurso a proteger, el CNI utiliza los términos de seguridad del personal, seguridad de la información, seguridad del material, seguridad de las instalaciones, o seguridad de operaciones. Cuando se trata de proteger el recurso información, el CNI tiene en cuenta que la información puede existir en la mente humana, en un documento, o en forma electrónica en un sistema de información y comunicaciones, y por tanto, aborda el problema de la seguridad de la información bajo estos tres aspectos.

Con respecto a la gestión de la seguridad de la información en los sistemas de información tecnológicos, el Centro utiliza el acrónimo Infosec para referirse al conjunto de medidas de seguridad que tienen por objeto proteger la información procesada, almacenada o transmitida, por sistemas de comunicaciones, sistemas de información u otros tipos de sistemas electrónicos, contra la pérdida de confidencialidad, integridad o disponibilidad, ya sea accidental o intencionada, e impedir la pérdida de la integridad y de la disponibilidad de los propios sistemas.

– ¿Le parece adecuada la actual gradación de la información clasificada, o sería necesario modificarla?

– Clasificar la información es uno de los principios básicos de cualquier política de seguridad de la información, sea cual fuere el ámbito de la misma. Las de Secreto y Reservado son las actuales clasificaciones que la antigua pero vigente Ley sobre Secretos Oficiales (LSO) ha establecido para proteger las materias objeto de reserva. En el ámbito del Ministerio de Defensa, y en virtud de la posibilidad de desarrollo reglamentario que otorga la propia LSO, se han establecido dos categorías más de clasificación, que son Confidencial y Difusión Limitada. Esta gradación de la información clasificada está en línea con la utilizada por la mayoría de los países de la UE y de otras organizaciones internacionales a las que España pertenece, principalmente la OTAN, y en este sentido me parece adecuada. No hay que olvidar que se trata de la gradación establecida en la política de seguridad que se aplica a las materias objeto de reserva interna que la LSO establece.

– Al igual que existe una clasificación oficial de la información en atención al epígrafe de la confidencialidad, podría haberla también en atención a los de integridad y disponibilidad. ¿Se está contemplando esta posibilidad?

– Efectivamente. El propio concepto de Infosec que he mencionado antes aborda la protección de la información no sólo en su aspecto de

confidencialidad, sino también en el de su integridad y disponibilidad, e incluso va mas allá, pues tiene en cuenta la integridad y disponibilidad de los sistemas que sustentan o soportan la información. Actualmente, para la clasificación de la información en atención a su integridad y disponibilidad, se asigna el nivel de clasificación en función del daño que causaría la pérdida de integridad o disponibilidad de una determinada información, por equivalencia al daño que causaría la pérdida de confidencialidad de otra información, aunque hay que señalar que este criterio todavía no tiene respaldo normativo.

Además, se está promoviendo que en las especificaciones y pliegos de los sistemas de información y comunicaciones se establezcan las especificaciones de integridad y disponibilidad, y que en el apartado de requisitos de seguridad se expresen las medidas que garanticen que se puede acceder a la información manejada por el sistema conforme a las especificaciones del mismo.

– Entre las funciones del CNI se encuentran las descritas en el Artículo 4 punto e de la Ley 11/2002, que suponen una ampliación del ámbito de actuación del Centro a toda la Administración en las materias criptográficas, de seguridad en tecnologías de la información y de coordinación de adquisiciones. ¿Cómo están abordando el desarrollo de esta responsabilidad en estos tiempos en los que prácticamente todos los órganos de la Administración están inmersos en numerosos proyectos de protección de sistemas y aplicaciones mediante herramientas tecnológicas, algunas de ellas criptográficas?

– Partiendo de la idea de que la seguridad de las tecnologías de la información es tan importante para la seguridad y el bienestar de los ciudadanos y la economía como lo es la protección física de los propios ciudadanos y de las instalaciones, el CNI va a abordar el desarrollo de las funciones asignadas en la Ley 11/2002 Reguladora del Centro Nacional de Inteligencia que, en síntesis, hacen al CNI responsable de garantizar la seguridad de las Tecnologías de la Información de la Administración. Esa responsabilidad está especialmente remarcada en la adquisición o en el uso de medios o procedimientos de cifra que, por otra parte, hoy son muy habituales en la mayoría de las TI.

Para hacer frente a las responsabilidades asignadas, el CNI tiene previsto definir y desarrollar reglamentariamente los cometidos del Centro Criptológico Nacional (CCN), organismo que forma parte del CNI, y con el que comparte doctrina, actividades, presupuestos, personal y medios materiales. Las actividades del CCN seguirán la línea trazada en materia Infosec por los países avanzados y por algunas organizaciones internacionales, y abarcarán la concienciación y formación en Infosec, la certificación y acreditación de sistemas de las tecnologías de la información, y la publicación de instrucciones y guías técnicas para este ámbito. Todas las actividades estarán respaldadas por unos conocimientos que se obtendrán, entre otras vías, del estudio de las vulnerabilidades y amenazas a las que están sometidas las tecnologías de la información.

– España, a diferencia por ejemplo de Francia o Reino Unido, adolece de un Esquema Nacional de evaluación y certificación de la seguridad de productos de TI. A efectos no civiles, existe la certificación CNI y la evaluación Cesti (INTA) ¿Se muestra partidario de la existencia, publicación y entrada en vigor a todos los efectos en la Administración española de un Esquema Nacional de evaluación y certificación acorde con las líneas ITSEC de la UE y con los Criterios Comunes?

– En el CNI estamos convencidos de la absoluta necesidad de un Esquema de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información de ámbito nacional y no sólo exclusivamente para material de guerra, como el ahora existente al amparo del Reglamento de Homologación de la Defensa. El progreso habido en los últimos años en los foros nacionales e internacionales, en relación con los criterios y metodologías de evaluación de la seguridad de las tecnologías de la información, ha movido a los diferentes países y organizaciones internacionales a adoptar unos Criterios Comunes (*Common Criteria*) para la realización de las pruebas y evaluaciones de la seguridad.

Los Criterios Comunes constituyen un punto de encuentro y de consenso científico, técnico, comercial y gubernamental, para la evaluación y certificación de la seguridad de las tecnologías de la información. Más de 20 países del mundo han adoptado los Criterios Comunes, y 13 de ellos -incluido España, a través del Consejo Superior de Informática- firmaron en mayo de 2000 un Acuerdo de Reconocimiento Mutuo (ARM) de los certificados expedidos por aquellos países que disponen de Esquema de Evaluación y Certificación reconocido en dicho Acuerdo. El Centro ha constatado en los diferentes programas y foros de seguridad en los que participa, que el establecimiento de un Esquema de Evaluación reconocido por los diferentes países en el marco del ARM, y la adopción de los Criterios Comunes por parte de dicho Esquema, se convertirá en un futuro próximo en una condición "*sine qua non*" para que la industria nacional pueda participar en programas internacionales en condiciones de competitividad.

– ¿Podría explicar brevemente en qué consiste la Política Infosec nacional?

– Consiste en promover que todos los niveles de la Administración tomen conciencia de los riesgos asociados al uso de las TI, que el personal de cada nivel reciba la formación necesaria para tomar las medidas oportunas para gestionar el riesgo, que se establezcan y ejecuten procedimientos de seguridad y que existan productos de TI de confianza certificada para satisfacer las necesidades de seguridad.

– Existe una relación no pública de productos con diversas finalidades de seguridad TI certificados por el Centro Criptológico Nacional-CNI. ¿Podría indicar hasta la fecha qué campos de la seguridad TI cubren y cuáles todavía no? Dicho de otro modo, ¿se dispone de IDS, cortafuegos o tarjetas criptográficas y lectores certificados para dar curso a las ingentes y diversas necesidades de la Administración española?

– El análisis y evaluación de la seguridad que el equipamiento criptográfico aporta para proteger la información clasificada es uno de los cometidos que el Centro viene realizando desde hace varios años, para su propio uso y en apoyo de otros organismos de la Administración, principalmente Presidencia del Gobierno, Ministerio de Asuntos Exteriores y Ministerio de Defensa. En la idea de promocionar el uso de productos de cifra nacionales evaluados y certificados para proteger la información clasificada y para rentabilizar el gran esfuerzo que supone la evaluación y certificación de productos de cifra, el Centro edita y difunde, anualmente, la Relación de Productos Certificados (RPC). La RPC que el CNI distribuye a diversas autoridades de la administración contiene actualmente sólo productos de cifra agrupados bajo las categorías de Cifradores Hardware (Telegrafía, VHF, Fax, Voz, Datos, IP), Centros de Gestión de Claves, Generadores Aleatorios, Proveedores de Servicios Criptográficos, Unidades de Transporte de Claves, y Cifradores Software (Soportes de Almacenamiento).

"En general los sistemas de información de la Administración se planifican, se desarrollan y se implementan con grandes carencias en la definición de las amenazas a las que estarán sometidos"

Actualmente está en proceso de certificación una tecnología software de PKI y en desarrollo una tarjeta inteligente criptográfica. Asimismo, existen otros tipos de productos Infosec como son los que menciona en su pregunta, y está previsto que en el futuro se incorporen a la RPC.

– ¿Se contempla la posibilidad de ir desclasificando dicha relación de productos certificados CNI e incluirla en el catálogo de Patrimonio?

– Sí. Nos dimos cuenta de que la relación, al ser clasificada, no se difundía a los niveles que realmente más lo necesitaban. Por ello se ha decidido eliminar de cada producto la información objeto de clasificación y hacer una versión pública de amplia difusión, incluso se baraja la posibilidad de incluirla en la página web del Centro (www.cni.es).

– Además de superar las pruebas de evaluación de seguridad CNI, ¿qué requisitos han de cumplir las herramientas tecnológicas para formar parte de la RPC? ¿Deben de cumplir requisitos específicos también los fabricantes de dichas herramientas?

– Hasta ahora los requisitos exigibles a un producto para ser certificado, aparte de la superación de las pruebas que se mencionan, eran básicamente que existiese la necesidad de certificar el producto, avalada por un organismo de la Administración, que el fabricante entregara absolutamente toda la información sobre su producto, y que el fabricante y el organismo de la Administración estuvieran dispuestos a sufrir un largo y costoso proceso de evaluación.

A partir de ahora los productos que vayan a ser certificados tendrán que haber pasado previamente una evaluación con los Criterios Comunes en un laboratorio acreditado en el marco de un Esquema.

– Existe en España una industria poco numerosa pero de gran calidad que desarrolla productos de seguridad TI -algunos de naturaleza criptográfica- muy competitivos. ¿Tiene intención el CNI de potenciar dicha industria?

– Sí, sin lugar a dudas. Este Centro ya lo viene realizando en la medida de sus posibilidades y no sólo con la industria sino también con la investigación en las universidades. Es de esperar que con el desarrollo y puesta en práctica de sus nuevas funciones, el Centro Criptológico Nacional sea un elemento dinamizador de la investigación y la industria de seguridad de las tecnologías de la información en nuestro país.

– Un país dispone de numerosas infraestructuras criticas de información de cuyo buen funcionamiento depende su estabilidad. Muchas de estas infraestructuras son hoy de gestión privada; sin embargo, la protección de las TI que soportan dichas infraestructura es, por decirlo de algún modo, un «asunto de Estado». Para liar más las cosas, muchas de estas infraestructuras están íntimamente relacionadas con las de otros países. ¿Cómo creé que debería encararse la seguridad TI en este contexto tan complejo y multilateral?

– La seguridad TI de las infraestructuras críticas debe contemplarse como un aspecto más de la protección de dichas infraestructuras. La forma en como otros países abordan estos asuntos es variada. En algunos se han creado agencias

"Esperamos que, en la medida en que las limitaciones de la Administración lo permitan, el Centro pueda recibir más profesionales y más recursos, y llegar a configurar un equipo de trabajo en materia Infosec de la magnitud que España necesita".

exclusivas para la protección de las infraestructuras críticas de la nación, abarcando la protección en todos sus aspectos, en otros el problema ha sido encargado a algún organismo o agencia ya existente, y en otros, como puede ser el caso de España, la protección de dichas infraestructuras está repartida en diferentes ministerios y competencias de las administraciones, realizándose la necesaria coordinación mediante comisiones y comités sectoriales. En cualquier caso, la actividad que desarrolle el CCN sobre la seguridad TI será de utilidad también en la protección de las infraestructuras críticas del país, y así será tenido en cuenta por los responsables.

– La seguridad de la información y de las TI no es gratis. Hay que destinar personas y presupuesto. ¿Qué actitud se ha tomado al respecto en el CNI-Centro Criptológico Nacional?

– Desde la publicación de la Ley 11/2002, que asigna al CNI-CCN la responsabilidad de garantizar la seguridad de las TI en la Administración, el CNI no ha recibido personal adicional para realizar las tareas que conlleva el cumplimiento de esa misión. Sin embargo, sin esperar a que se produjera el incremento en su dotación, el CNI ya dedica una destacable cantidad de personas muy cualificadas, y otros recursos, para cumplir la misión. Esperamos que, en la medida en que las limitaciones de la Administración lo permitan, el CNI pueda recibir más profesionales y más recursos y llegar a configurar un equipo de trabajo en materia Infosec de la magnitud que España necesita.

– ¿En qué epígrafes de la seguridad cree que sería necesario reforzar los conocimientos de los profesionales de la Administración española especializados en la protección de la información y en seguridad TI?

– La formación es fundamental, es una de las primeras medidas de seguridad a tener en cuenta. El Centro ha constatado una gran necesidad de formación en todos los niveles de la Administración. Quizás una de las carencias más llamativas sea la dificultad que tienen los diferentes organismos para expresar sus necesidades de seguridad.

En general los sistemas de información de la administración se planifican, se desarrollan y se implementan con grandes carencias en la definición de las amenazas a las que estarán sometidos, de los requisitos de seguridad que deben satisfacer, y finalmente en la arquitectura de seguridad que debe implementarse. El desconocimiento de las tecnologías de seguridad no lo consideramos un problema pero el desconocimiento de las necesidades de seguridad sí que lo es.

Para mitigar este problema, el CCN ha establecido un plan de formación Infosec para la Administración. El Plan ha identificado tres niveles de formación, un primer nivel de carácter informativo y de concienciación que hemos denominado "seminarios Infosec"; un segundo nivel de conocimiento del problema de la seguridad y de las medidas de toda índole que deben adoptarse; este nivel en gran parte se satisface con el curso Infosec, que se convoca en el BOE todos los años y del cual ya se han celebrado tres ediciones; y un tercer nivel de especialización en los aspectos concretos de la seguridad.

Este tercer nivel consiste en la organización de cursos específicos de análisis de riesgos, de configuración segura de sistemas operativos, de seguridad de redes, de seguridad en bases de datos, de seguridad del fenómeno Tempest, etc. La idea es que estos cursos de especialización sean impartidos por las empresas del sector, si existe oferta comercial, y por el propio CCN si la materia es específica. ■

Texto. **José de la Peña Muñoz**
Fotografía: **CNI**