ENTREVISTA A BEATRIZ MÉNDEZ DE VIGO
Secretaria General del Centro Nacional de Inteligencia

"El 30% del equipo del CNI son militares frente a un 70% de civiles"

En el Centro Nacional de Inteligencia trabaja un nutrido grupo de civiles afanado en velar por nuestra seguridad y distribuido entre una amplia variedad de destinos. Uno de ellos es su actual Secretaria General, Beatriz Méndez de Vigo, la cuarta mujer que ocupa este cargo en un Organismo que, hace más de veinticinco años, apostó por su carisma para reclutar talento femenino. En la presente entrevista nos confiesa algunos "secretos", revelándose como nuestra más cercana y sencilla confidente.

POR MAOLE CEREZO
Redactora Jefe de Boletic

¿Cuál ha sido la evolución del CCN en los últimos años y qué competencias han ido desarrollándose más con el paso de los años?

Cuando hace diez años se aprobó el decreto de creación del CCN (Real Decreto 421/2004, del 12 de marzo), se culminaba un proceso iniciado a principios de los años 80, en el seno del propio Centro, que ya había alcanzado un profundo conocimiento en amenazas, vulnerabilidades y riesgos de los sistemas de información y comunicaciones.

Ya entonces se iba perfilando un nuevo espacio, el ciberespacio, con numerosas posibilidades de progreso para la población, pero también con nuevas amenazas. La labor del CCN, a lo largo de los diez últimos años, ha sido precisamente intentar reducir los riesgos y las amenazas provenientes del ciberespacio, coordinando la acción de los diferentes organismos en la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las TIC en ese ámbito, informar sobre la adquisición coordinada del material Criptológico, velar por el cumplimiento de la normativa relativa a la protección de la información clasificada y formar al personal de las distintas administraciones públicas en este campo.

El CCN ha ido adecuándose a los nuevos desafíos potenciando las acciones, no sólo defensivas, sino primordialmente preventivas, correctivas y de contención. Así, en el año 2006 se creó el CCN?CERT o Capacidad de Respuesta a Incidentes de Seguridad, con responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y organizaciones de interés estratégico, es decir, aquellas empresas esenciales para la seguridad nacional y el conjunto de la economía española.

¿Cuál es su balance cuando se ha cumplido el décimo aniversario desde su creación?

El balance no puede ser más positivo, ya que el CCN?CERT, como CERT Gubernamental Nacional, se ha convertido en la primera línea de defensa frente a los ciberataques de este país. De hecho, por ejemplo, en 2014 gestionó un total de 13.000 ciberincidentes, de los cuales, el 11,6% fueron catalogados por sus expertos

con un nivel de riesgo entre muy alto y crítico; es decir, se tuvo constancia de que el ataque afectó a los sistemas de la organización y a su información sensible.

Por otro lado, el CCN ha jugado también un papel primordial en el desarrollo, implantación y seguimiento del Esquema Nacional de Seguridad (ENS), en la formación de su personal a través de los Cursos STIC en coordinación con el Instituto Nacional de Administración Pública (INAP), en el desarrollo de herramientas que facilitan la mejor gestión de la ciberseguridad y en la difusión de normas, instrucciones, guías y recomendaciones sobre múltiples aspectos de seguridad. Así, en su portal cuenta con más 250 documentos de ese tipo, lgunos de los cuales han sido descargados de su portal más de doscientas mil veces.

De igual modo, conviene destacar la aprobación en 2013 de la Estrategia de Ciberseguridad Nacional, en la que el CCN colaboró profusamente, así como la celebración anual de las Jornadas STIC CCN-CERT, que se han encumbrado al primer puesto de los eventos celebrados en España en materia de ciberseguridad. Otro de los logros a destacar es la mejora de la capacidad nacional de evaluación y certificación de productos de cifra y seguridad, reconocidos tanto nacional como internacionalmente.

Así, por ejemplo, se ha logrado obtener el primer cifrador IP español certificado NATO-SECRET y disponer de equipos nacionales para comunicaciones seguras por satélite desplegados en Afganistán, tras ganar a nivel internacional dentro de OTAN los concursos de OMLT y POMLT. En la parte de productos de seguridad, se dispone de dispositivos para el intercambio seguro de información y separación de dominios de seguridad para distintas pasarelas, desplegadas nacionalmente en el entorno de Defensa y Seguridad y en organismos como el Centro de Satélites de la Unión Europea.

¿La ciberseguridad es un asunto de Estado?

Por supuesto. La dependencia cibernética de las sociedades avanzadas es absoluta. La intensidad y sofisticación de los ciberataques ha puesto en evidencia la capacidad de los atacantes para causar enormes daños, ya sean económicos, políticos o sociales, y afectar al desarrollo futuro de cualquier país. El ciberespionaje se ha erigido en una de las mayores amenazas para gobiernos, empresas y ciudadanos y así lo han entendido buena parte de los dirigentes de todo el mundo, incluido el nuestro, que está realizando un importante

La principal amenaza a la que nos enfrentamos es el ciberespionaje, centrada sobre todo en las técnicas denominadas APTs; es decir, ciberataques a medida contra un objetivo concreto, bien de la Administración, la industria o un sistema en particular

esfuerzo en este campo, impulsando la colaboración internacional y la necesaria implicación de organismos y empresas en la defensa del ciberespacio.

Hay que tener en cuenta que tras las redes y los sistemas de información, ya sean públicos o privados, hay importantes intereses que no se limitan a la mera información, sino que se extienden a todo tipo de servicios, vitales para el normal desarrollo de nuestras sociedades y que deben por tanto ser defendidos.

Por otro lado, tal y como quedó plasmado en la Estrategia Española de Ciberseguridad, desde el CCN se trabaja igualmente para prevenir cualquier forma de ataque, lo que implica tanto actividades de formación y concienciación del personal de la Administración, con los ya mencionados cursos STIC, como actividades encaminadas a fomentar el desarrollo industrial de productos y servicios nacionales en materia de ciberseguridad. Por último, cabe mencionar las actividades encaminadas a la certificación y el reconocimiento de productos de cifra y seguridad, que permiten incrementar el grado de protección de los sistemas de la Administración.

¿Cuál es el papel del CCN en la ciberseguridad nacional?

El CCN, y según la distinta normativa existente, tiene el deber de garantizar la seguridad TIC de las Administraciones Públicas, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada. Del mismo modo, tiene responsabilidad en prevenir ciberataques sobre estos mismos sistemas clasificados y sobre sistemas de la Administración, empresas y organizaciones de interés estratégico para el país.

También tiene asignadas las funciones de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas; formar al personal de la Administración; constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad; valorar y acreditar los productos de cifra; coordinar la promoción, el desarrollo y la obtención de la tecnología de seguridad y establecer las necesarias relaciones, así como firmar los acuerdos pertinentes con organizaciones similares de otros países.

Además, entre los planes futuros, se encuentra la definición y elaboración de un catálogo de productos de cifra certificados y de productos de seguridad recomendados, que permita ofrecer una cierta confianza en los equipos a emplear y que se adapte a las exigencias de agilidad temporal del mercado de las TIC. Por último, cabe destacar que los responsables TIC de las diferentes administraciones pueden ponerse en contacto con el CCN si necesitan algún tipo de asesoría en este sentido, teniendo siempre como primer punto de contacto la web www.ccn.cni.es.

España acaba de estrenar una Estrategia de Ciberseguridad. ¿Cumple con las demandas del sector público y privado?

La Estrategia de Ciberseguridad Nacional fue aprobada en diciembre de 2013 y respondía a la creciente necesidad de preservar la seguridad del iberespacio por su enorme repercusión en cuestiones que afectan a la seguridad nacional, así como a la competitividad de nuestra economía y, en general, al progreso y prosperidad de nuestra sociedad. Dicha Estrategia estaba alineada con la Estrategia de Seguridad Nacional de 2013 , que contemplaba la ciberseguridad dentro de sus doce ámbitos de actuación, y que delimitaba el entorno del ciberespacio, fijaba principios, objetivos

y líneas de acción para el logro de la ciberseguridad nacional, y definía el marco de coordinación de la política de ciberseguridad.

Así, en su Línea de Acción 1 fijaba la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre el CCN-CERT, el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) y el CERT de Seguridad e Industria. Los CERT de las Comunidades Autónomas, los de las entidades privadas y otros servicios de ciberseguridad relevantes debían estar coordinados con los anteriores en función de las competencias de cada uno de ellos, articulando los instrumentos adecuados a tal efecto.

Estas tareas sí se han realizado, y en concreto el CCN-CERT mantiene estrecha relación con todos los organismos citados y participa en numerosos grupos de trabajo con los Ministerios de Defensa, del Interior, de Industria, Turismo y Comercio y, por supuesto, con el Ministerio de la Presidencia, en el que estamos integrados. En cuanto a las demandas del sector privado, en lo que al CCN-CERT se refiere, ha hecho una apuesta decidida por la colaboración público-privada, propiciando el intercambio de información y poniendo a disposición de las empresas y organizaciones de interés estratégico para España una serie de servicios que con los que afrontar, de forma activa, las nuevas ciberamenazas que permitan proteger el patrimonio tecnológico español, y por ende, los intereses de nuestro país.

De hecho se colabora con unas 100 compañías en la defensa ante ataques complejos. Asimismo, se han hecho públicos un buen número de cursos online de Seguridad, informes, Guías CCNSTIC a los que se puede acceder libremente y también se les brinda la oportunidad de registrarse en sus Jornadas STIC CCN-CERT.

¿Cuáles son los principales riesgos y amenazas en materia de ciberseguridad?

La principal amenaza a la que nos enfrentamos es el ciberespionaje, centrada sobre todo en las técnicas denominadas APTs; es decir, ciberataques a medida contra un objetivo concreto, bien de la Administración, la industria o un sistema en particular, llevado a cabo por un atacante con la intención y la capacitación técnica que le permitan ganar acceso a la información sensible almacenada electrónicamente en el mismo, durante un largo período de tiempo, debido a su habilidad para evitar la detección, su adaptabilidad al objetivo y su alta disponibilidad de recursos, tecnológicos, económicos o humanos.

Por otro lado se registra un incremento continuado del ciberdelito, realizado por profesionales y destinado a todo tipo de dispositivos, con especial incremento en los dispositivos móviles, y utilizando en numerosas ocasiones técnicas de ingeniería social a través de las Redes Sociales; así como ataques contra servicios web o los denominados Ransomware. Estos últimos son aquellos en los que se cifran datos o se bloquea el acceso a un sistema exigiendo dinero a cambio de recuperar la información y/o el sistema. Estas son algunas de las amenazas más presentes hoy en día, abonadas todas ellas por la falta de concienciación del usuario.

Estas amenazas, originariamente dirigidas a empresas e instituciones públicas, actúan también sobre personas individuales, incluyendo altos directivos de compañías y de organismos públicos, personajes notorios y responsables políticos. Se observa, además, una tendencia a atacar a los elementos más débiles de la cadena de intercambio de datos, como podrían ser los proveedores o ontratistas. Por este motivo, las organizaciones públicas y privadas que manejan información con alto valor estratégico, económico o político, esenciales para la seguridad nacional o para el conjunto de la economía, deben incrementar sus medidas de seguridad.

¿Cómo está evolucionando la ciberamenaza? ¿Va en paralelo el desarrollo de la ciberseguridad de las organizaciones?

Desgraciadamente no. Las ciberamenazas van por delante de las medidas que adoptan las organizaciones para hacerles frente. En numerosas ocasiones, son los máximos responsables de las organizaciones los que menos concienciados están del pro-

LA ESCUELA DEL CNI

El CNI cuenta con una escuela que ofrece a los recién incorporados un Plan de Acogida para ayudarles a integrarse y adaptarse al Centro. Se les ofrece información sobre éste, (su cultura, su misión, sus compromisos...) y sobre las herramientas, procesos, procedimientos que aplicarán en sus respectivos puestos de trabajo. A su vez, la escuela cuenta con un Programa de Formación Continua y reciclaje profesional al que pueden acceder sus trabajadores. En la actualidad se está trabajando en el desarrollo e implantación de un modelo de carrera profesional aprobado recientemente.

El Centro ha suscrito convenios de colaboración con distintas instituciones académicas de probado prestigio con el compromiso de la difusión de la Cultura de Inteligencia, a través de una oferta formativa amplia y multidisciplinar.

blema y, por tanto, los que menos precauciones adoptan, siendo los altos cargos, tanto de la Administración Pública, como de la privada, los que manejan la información más valiosa para sus organizaciones.

Por otro lado, mientras que las capacidades de ataques van lideradas por el cumplimiento de objetivos, lo que les hace ser mucho más agresivos e imaginativos, las capacidades defensivas van lideradas por el cumplimiento normativo y por las limitaciones de personal y recursos, lo que hace que sus capacidades de respuesta sean inferiores. Haciendo una comparativa, mientras la infección y colonización de nuestras Administraciones Públicas por parte del atacante se pueda producir incluso en días, la detección y limpieza de este ataque puede llevar meses o incluso años.

¿Cuáles son los principales retos de seguridad que tendrán que hacer frente las Administraciones Públicas y empresas españolas?

El principal reto al que tiene que enfrentarse cualquier organización, ya sea pública o privada, es la protección de sus activos, siendo la información uno de los más destacados. Esto resulta difícil en una realidad cambiante en la que los ataques se incrementan día a día favorecidos por la rentabilidad que se obtiene, ya sea económica, política o de otro tipo; la facilidad y el bajo coste en el empleo de las herramientas utilizadas; así como el reducido riesgo para el atacante, que lo puede hacer de forma anónima y desde cualquier lugar del mundo.

Los esfuerzos, por tanto, se deben centrar en incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación, unido a una política de investigación y de cambio en la mentalidad. Trabajar como si se estuviera comprometido y por lo tanto proteger los activos fundamentales en un medio comprometido.

Se habla mucho de coordinación y cooperación, ¿existe suficiente entre los distintos organismos y entidades involucrados en la protección de las TIC?

Como ya he referido anteriormente, el CCN cree firmemente en la necesidad de cooperar y de coordinar las actividades de todos los agentes involucrados en la ciberseguridad: gobiernos, empresas y ciudadanos.

Además, en un mundo sin fronteras como es el del ciberespacio, esta coordinación debe ser entendida en términos transfronterizos. Así, si bien esta cooperación siempre es mejorable en cualquier ámbito, se puede decir que en el público existe de una forma bastante acertada, y es por tanto en el sector privado dónde se debería mejorar la colaboración e incrementar el intercambio de información.

¿Podría identificar las principales conclusiones extraídas por el Consejo de Seguridad Nacional en su primer año de existencia?

La principal conclusión es la necesidad de invertir en recursos humanos y económicos para llevar a buen término las más de 30 actividades derivadas de las ocho líneas de acción emprendidas, siendo la acción fundamental a abordar la mejora de las capacidades de detección y análisis de la amenaza. Además, es necesario que se mejore la colaboración y coordinación entre las diferentes Administraciones Públicas,así como entre ellas y el sector privado.

Tras la finalización del plazo de aplicación del Esquema Nacional de Seguridad, ¿Cómo valora el nivel de seguridad de las Administraciones Públicas y cuál es el Plan trazado para impulsar la seguridad en los próximos años?

Efectivamente, el plazo de aplicación ha concluido. De hecho, el 9 de febrero fue la fecha tope para remitir comentarios al proyecto de modificación del Decreto por el que se regula el Esquema Nacional de Seguridad (ENS). Esta modificación se realizará una vez que el ENS se haya sometido a una minuciosa revisión, a la luz de la experiencia adquirida en su implantación, de la evolución de la tecnología y de las ciberamenazas, así como del contexto regulatorio europeo.

De tal forma, el proyecto de modificación del Esquema Nacional de Seguridad es el resultado de un trabajo coordinado por el Ministerio de Hacienda y Administraciones Públicas, en estrecha colaboración con el Centro Criptológico Nacional (CCN), con la participación de todas las Administraciones Públicas (Administración General del Estado, Comunidades Autónomas y los Entes Locales) incluyendo las universidades públicas (CRUE), a través de los órganos colegiados con competencias en materia de administración electrónica y TIC y sus grupos de trabajo.

Por lo que respecta a la valoración del nivel de seguridad de las Administraciones Públicas, el CCN ha desarrollado diversas herramientas como INES o CLARA y también Guías CCN-STIC, para permitir conocer en profundidad el estado de la implantación del ENS en las administraciones y, en concreto, para realizar una estimación preventiva de la seguridad, vía análisis del cumplimiento de determinados aspectos que se han estimado críticos para cualquier organismo, una estimación de la eficacia y eficiencia de las actividades en materia de seguridad y una estimación del esfuerzo humano y económico dedicado a seguridad TI.

En los próximos años, el Plan debería incluir una mejora de los productos, junto con una ampliación del catálogo de los mismos y de los servicios de Ciberdefensa, tanto para la Administración como para la Industria. A nivel particular vendría de la mano de una potenciación de las capacidades de evaluación y certificación, permitiendo una mayor confianza en la seguridad de los productos. De igual forma, se deben fortalecer las capacidades de prevención y respuesta ante incidentes.

¿Podría cuantificarnos y detallarnos los resultados del CCN-CERT a día de hoy?

Además de todo lo que hemos abordado ya en esta entrevista, me gustaría destacar los 13.000 incidentes gestionados, incluyendo apoyos directos a organismos que han sufrido incidentes muy altos y críticos; las más de 50 publicaciones de vulnerabilidades y los informes de amenazas y código dañino; así como la ostensible mejora de la oferta de formación, que a día de hoy, incluye siete cursos online disponibles en el portal, además de los 16 cursos presenciales anuales en los que se da formación a más de 500 alumnos.

En su opinión ¿Cuál es el papel de la Dirección TIC como impulsor de medidas de seguridad? ¿Qué necesidades tienen para alcanzar los objetivos?

Su principal papel en la seguridad es optimizar el modelo de interconexión de las Administraciones Públicas, reforzar la implantación y la seguridad de las infraestructuras comunes para mejorar las capacidades de detección del CCN-CERT, así como desarrollar nuevos servicios horizontales seguros basados en una arquitectura de red adecuada y en el correcto uso de productos certificados, como se marcan en la Línea de acción 2 de la Estrategia de Ciberseguridad.

Por supuesto, el CCN colaborará con la Dirección TIC en la consecución de todos estos objetivos. En relación con las necesidades existentes, es importante contar con arquitecturas de referencia de seguridad que permitan disponer de una aproximación global a los aspectos de seguridad de las redes de la Administración.

También es necesario que existan productos confiables para proteger dichas redes y la información que procesan, lo que únicamente se puede conseguir con productos de seguridad que hayan sido debidamente evaluados y certificados en sus aspectos de seguridad dentro del Esquema Nacional para la Evaluación y Certificación de las Tecnologías de la Información. ✱