Luis **JIMÉNEZ MUÑOZ**

Subdirector General del Centro Criptológico Nacional. Centro Nacional de Inteligencia (CNI)

Luis Jiménez es teniente coronel en situación de Servicios Especiales.

Es especialista criptológico, máster en Dirección de Sistemas de Tecnologías de la Información y las Comunicaciones por el Instituto Nacional de Administración Pública y la Universidad Politécnica de Madrid.

Es vocal del Consejo Nacional de Ciberseguridad de España, representante nacional en los Comités de seguridad de la información y ciberseguridad del Consejo de la Unión Europea y de la OTAN, y miembro del Comité Ejecutivo de la Comisión de Estrategia TIC de la Administración General del Estado.

Entre los principales cometidos de su actual puesto de trabajo se encuentran el impulso y desarrollo de la Estrategia Nacional de Ciberseguridad, el apoyo a la implementación del Esquema Nacional de Seguridad en las administraciones públicas, la mejora de las capacidades de Respuesta ante Incidentes de Seguridad y la mejora de las capacidades de Evaluación y Certificación de la Seguridad de las TIC.

El CNI fue pionero en garantizar la seguridad de las TIC en el ámbito de las administraciones públicas

La seguridad en las comunicaciones es uno de los aspectos clave en la actualidad. De ello se ocupa el Centro Criptológico Nacional, perteneciente al Centro Nacional de Inteligencia (CNI).

Su subdirector general, el Teniente Coronel Luis Jiménez, es un profesional de amplia experiencia. De hecho, su primer trabajo, en 1992, fue evaluar el algoritmo que se utilizaba en un cifrador de fax que se iba a colocar en la Casa Real. Con él conocemos el trabajo de estos organismos públicos.

UN EJEMPLO ESPAÑOL PARA EL MUNDO

El CNI se creó en el año 2002, adscrito al Ministerio de la Presidencia, y deriva del antiguo Centro Superior de Información de la Defensa, fundado en 1977.

Aunque es poco conocido, todo lo relacionado con el CNI está escrito. Así lo indica Luis Jiménez al afirmar que "si nos comparamos con los servicios de inteligencia que hay en el mundo, somos uno de los mejor regulados, y ejemplo para muchos países. Contamos con una Ley que define perfectamente a qué nos dedicamos, ampara a la sociedad a través de un magistrado del Tribunal Supremo en caso de tener que afectar a alguno de los Derechos Fundamentales de los españoles, y establece que tenemos que dar cuentas de nuestra actividad al Tribunal de Cuentas y al Congreso de los Diputados a través de la Comisión de Secretos Oficiales. De este modo, el Centro está sometido a controles económicos, políticos y de funcionamiento".

> Cuando se agota la vía diplomática entre dos países, todavía queda el servicio de inteligencia

El Centro trabaja de acuerdo con la Directiva de Inteligencia, un documento que emite anualmente el Gobierno, en el que se indican los objetivos que debe cumplir, y en base al cual se definen el presupuesto y las operaciones a llevar a cabo.

EFICACIA EN LA UNIDAD

La forma de funcionamiento del CNI es diferente a la mayoría de servicios equivalentes en el mundo, porque integra inteligencia interior, exterior, económica, contrainteligencia y ciberseguridad, lo que supone importantes ahorros y una gran eficacia.

Luis Jiménez junto a nuestro compañero Eugenio Gil, en la puerta del CNI momentos antes de la entrevista.

Francia, por ejemplo, tiene un servicio de inteligencia que trabaja en el interior y otro que trabaja con los intereses franceses en el exterior. En el caso de los Estados Unidos, la CIA trabaja de cara al exterior mientras que el FBI lo hace en el ámbito nacional, y además tienen otras 17 agencias.

La eficacia del esquema de funcionamiento español es claro. Así lo demuestra el gran trabajo realizado durante años en la lucha antiterrorista en España, ya que muchos de los éxitos logrados en este campo lo han sido gracias al trabajo del Centro, completados después con las acciones de los Cuerpos y Fuerzas de Seguridad del Estado, que ejecutan lo que se conoce como la *última milla*. "En este apartado ahora estamos trabajando en la lucha contra el yihadismo", concluye Jiménez.

UNA LEY PIONERA

El CNI es un órgano del trabajo del Gobierno, "fundamentalmente de presidente del Gobierno, y también de los distintos ministerios", tal y como indica Luis Jiménez.

Las funciones del Centro, según la Ley que lo define, son: elaborar inteligencia, hacer contrainteligencia –oponerse a la amenaza de otras acciones que puedan desestabilizar o ir en contra de los intereses nacionales–, inteligencia de señales –captación de las señales que puedan contribuir a misiones de inteligencia y contrainteligencia–, proteger la información clasificada, proteger sus propios medios, relacionarse con organizaciones nacionales e internacionales en el ámbito de la inteligencia, y garantizar la seguridad de las Tecnologías de la Información y de la Comunicación (TIC) en el ámbito de las Administraciones Públicas.

Llama la atención que esta última función fue establecida por el legislador hace 15 años, "previendo –reconoce Luis Jiménez– la dependencia tan grande de nuestro Estado de Derecho de las TIC y que éste iba a ser un nuevo ámbito de riesgos emergentes, para el que este Centro iba a

> Nueve de cada diez máquinas están comprometidas

tener que prepararse. Fue algo muy novedoso, y por ello el Centro es pionero en ese aspecto".

INTELIGENCIA Y DIPLOMACIA

Cuando preguntamos a nuestro entrevistado por la coordinación con organismos similares en el mundo, afirma que "no nos coordinamos pero sí cooperamos con muchas organizaciones, esencialmente con el mundo occidental, y establecemos relaciones con otros centros de inteligencia de todo el mundo".

En este punto, Jiménez explica un aspecto de política internacional muy interesante. "Cuando se agota la vía diplomática entre dos países, todavía queda la vía del servicio de inteligencia; de hecho, podemos no tener embajada pero sí mantenemos contactos a través de estos servicios de inteligencia. Así ha ocurrido en algunas ocasiones de tensión diplomática, a lo largo de la historia".

La cooperación con los países occidentales se mantiene en materias como terrorismo, crimen organizado, comercio de material de doble uso, etc., a través de grupos de trabajo. En este ámbito internacional, si bien no hay establecidos foros comunes, sí existen los "clubes", bien europeos, o del norte de África y el mediterráneo, o latinoamericano, que comparten información de interés común, incluso entre países que aparentemente no mantienen buenas relaciones diplomáticas.

EL CENTRO CRIPTOLÓGICO NACIONAL

Los mensajes cifrados de Felipe II

La necesidad de proteger las comunicaciones escritas y de realizar el seguimiento de los mensajes cifrados de otros países se remonta a la época de Felipe II. Como indica Luis Jiménez, "en España siempre ha habido muy buenos matemáticos y científicos trabajando en el mundo de la criptología con el Gobierno de cada época".

El origen del Centro Criptológico Nacional, CCN, dependiente del CNI, se sitúa en la época del general Franco, "cuando el Alto Estado Mayor fundó un Gabinete de Cifras, que se encargaba de descifrar las comunicaciones externas y de utilizar los medios de cifra propios para proteger nuestras comunicaciones".

> Muy pocos países en el mundo disponen de criptografía propia. España es uno de ellos

"Esa pequeña y secreta unidad del Alto Estado Mayor pasó al CESID en el momento de su creación, y se dotó a esta actividad de un carácter científico y académico, incorporando matemáticos e informáticos, en paralelo a la revolución tecnológica que va surgiendo en los años 1976 y 1977".

DE LA DIPLOMACIA AL ÁLGEBRA

En sus inicios la criptología se utilizaba en los ámbitos diplomático y militar para proteger las comunicaciones propias e intentar interceptar las del adversario.

Cuando el CESID asumió esta actividad, "se empezó a abordar de una manera más profesional y totalmente académica, promoviendo investigaciones y colaborando con los departamentos de álgebra de las universidades, con dos objetivos fundamentales: mejorar la seguridad de nuestras comunicaciones y sacar ventaja de esa capacidad de criptoanálisis".

A finales de los años 90 y en los primeros años del milenio ocurre una convergencia entre las comunicaciones y la informática. "Ya no se habla –indica Jiménez– de informática y comunicaciones, se habla de las TIC, y el campo de actuación de la criptología aumenta, porque se pasa de proteger las comunicaciones a proteger todo lo relacionado con la información".

LOS PROTOCOLOS CRIPTOGRÁFICOS

Mucha gente –entre la que nos encontramos– no sabe que una de las piezas clave en las TIC son los protocolos criptográficos. "Cualquier *software* de comunicación tiene incorporado un protocolo criptográfico, que garantiza la autenticidad de origen y destino, la integridad o la confidencialidad".

Existen dos tipos de criptografías, la secreta y la pública. "La pública se divulga en los diferentes congresos de criptología a nivel mundial, y se publica en forma de estándares".

Por otro lado, hay algoritmos que sólo conocen los Estados. "En España –expone Jiménez– los cifradores de la Casa Real, el CNI, el Ministerio de la Presidencia o las Fuerzas Armadas, utilizan algoritmos públicos. Cuando la información es clasificada o de alto nivel, usan algoritmos secretos, diseñados en el CCN y la fabricación de los equipos se hace con empresas españolas".

CUESTIÓN DE SOBERANÍA NACIONAL

Una de las funciones del CCN es que se realicen algoritmos robustos, implementados con tecnología española y con un control absoluto en todo el proceso de fabricación y de generación, "de manera que no dependamos de terceros".

Como afirma Luis Jiménez, "disponer de criptografía propia es un ámbito de 'soberanía nacional'. Sólo aquellos países muy potentes pueden disponer de criptografía propia, y ése es nuestro caso". Muy pocos países pueden decir eso en el mundo; son Alemania, Australia, Canadá, España, Estados Unidos, Francia, Italia, Noruega, Reino Unido, Rusia, Suecia, Suiza y Turquía.

EL CCN Y LAS EMPRESAS. EVALUACIÓN Y CERTIFICACIÓN PARA EMPRESAS

Si bien el ámbito de trabajo del CCN se circunscribe a garantizar la seguridad de las TIC en la Administración del Estado, sí aborda algo tan importante como evaluar y certificar la seguridad funcional de productos en base a estándares internacionales.

"Esto lo hacemos con una ventanilla de cara al público, donde cualquier empresa que quiera evaluar y certificar un producto puede acudir al CCN. Aquí, el producto es sometido a un proceso de evaluación, que concluye con una resolución del secretario de Estado, que se publica en el BOE certificando el producto en estudio".

Existe una segunda ventanilla abierta al público, que tiene que ver con empresas que reciben ataques informáticos o que gestionan la ciberseguridad. "En este punto, estamos abiertos a establecer canales de colaboración para compartir información sobre ciberataques, aunque no tenemos capacidad para dar servicio a empresas privadas, ya que hay otros organismos dentro de la Administración que sí tienen esas responsabilidades, como CNPIC".

EL CASO DE LAS INSTALACIONES NUCLEARES

En lo que se refiere al sector, la colaboración del CCN se establece con el CNPIC. "Aunque llevamos muchos años colaborando con ellos, este último año hemos empezado a trabajar más coordinadamente en relación con los análisis de riesgos y con un conjunto de medidas, recomendaciones o buenas prácticas a implementar en los sistemas de información y comunicaciones de las empresas que operen centrales nucleares o el de las propias centrales".

> La seguridad de las tecnologías es un problema de concienciación y de madurez como sociedad

Indica Luis Jiménez que "lo que antes eran redes aisladas en las diferentes centrales ahora se están interconectando a redes corporativas que, a su vez, están conectadas a Internet, y ahí es donde puede estar el riesgo. En este aspecto nuestro trabajo es de apoyo al CNPIC".

LOS TRES COMPONENTES DE LA SEGURIDAD

La seguridad actual de las TIC se basa en tres componentes: humano, políticas de seguridad y tecnología segura, según indica nuestro entrevistado.

"El componente humano se refiere a buenos hábitos, concienciación y formación para saber manejar la tecnología de una manera segura. Las políticas de seguridad se traducen en procedimientos de seguridad escritos, conocidos y puestos en práctica por las organizaciones, donde se establecen los principios, lo que hay que proteger o las responsabilidades. Por último, la tecnología segura se consigue desarrollándola sin vulnerabilidades. El CCN apoya al otros organismos, como el CNPIC, en la parte técnica dentro de los tres ámbitos citados".

LA VULNERABILIDAD DE LA TECNOLOGÍA

Reconoce Luis Jiménez que el apartado de la tecnología es muy deficiente en nuestra sociedad, "porque se lanza al mercado tecnología con muchas vulnerabilidades".

El ejemplo es claro: "cuando compramos un ordenador debemos ser conscientes de que, en unos pocos segundos después de su instalación, la máquina es escaneada por terceros para comprobar su grado de vulnerabilidad".

Las cifras son espectaculares: nueve de cada diez máquinas están comprometidas. "Cualquier ordenador –afirma Jiménez– tiene dos cosas que interesan a los *hackers*: capacidad de disco duro y capacidad de proceso. Con la capacidad de disco duro pueden almacenar en zonas ocultas toda la información que ellos consideren necesario, y que el propietario del ordenador desconoce. Hay una gran probabilidad de que un ordenador forme parte de una red de ordenadores manipulados por *hackers* para el trasiego información de todo tipo".

El hecho de que un usuario esté infectado no sólo es un problema para el propietario del ordenador, sino que puede tener "consecuencias de seguridad muy grandes en todos los órdenes de la sociedad", como afirma Luis Jiménez.

CONSEJOS PARA EL INTERNET DE LAS COSAS

Como usuarios de la tecnología, somos también responsables de la seguridad. Por eso, nos interesamos por conocer los consejos de los profesionales.

Una de las cosas que deberíamos aprender, tal y como indica nuestro entrevistado, es a "tener dos usuarios, uno de administrador para mantener la máquina y otro para navegar por Internet, que no tiene privilegios de instalar *software*".

Un paso más nos lleva a las máquinas virtuales, que pueden ser gratuitas, "donde se instala una capa virtual por encima del sistema operativo, que se utiliza para navegar por Internet, instalar *software* y hacer el trabajo diario. Esa capa es virtual y desaparece cuando se apaga el ordenador".

Otra de las opciones es configurar el navegador del móvil y el del ordenador con distintos parámetros de seguridad. La llegada del *Internet de las cosas*, que nos lleva a estar conectados a muchos dispositivos, es un riesgo indudable si no se tiene conciencia de seguridad. "Es un problema de concienciación y de madurez como sociedad, y debemos avanzar en su mejora", concluye Luis Jiménez.