DE INTECO A INCIBE: UN PROCESO DE TRANSFORMACIÓN PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD DE LOS CIUDADANOS Y EMPRESAS EN ESPAÑA

ALBERTO HERNÁNDEZ MORENO
Director General de INCIBE

La crisis de WannaCry y Petya pusieron el pasado año de manifiesto la necesidad imperiosa de reforzar en nuestro país las capacidades de protección, tanto públicas como privadas, frente a las amenazas en el ciberespacio. El reciente mandato del Gobierno de revisar y actualizar la Estrategia de Ciberseguridad Nacional(1), así como el refuerzo de las capacidades del Instituto Nacional de Ciberseguridad (INCIBE), son un claro ejemplo de acciones en este sentido. Prevención, concienciación, detección y respuesta ante ciberataques, son pilares básicos sobre los que construir los servicios públicos que garanticen a medio y largo plazo un nivel de ciberseguridad adecuado en nuestro país.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (INTECO). ENERO 2006

Por acuerdo de Consejo de Ministros del 27 de enero de 2006, se constituyó, con sede en la ciudad de León, el Instituto Nacional de Tecnologías de la Comunicación (INTECO), Sociedad Mercantil Estatal adscrita al entonces Ministerio de Industria, Turismo y Comercio a través de la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), con un claro objetivo: contribuir de manera decisiva a la convergencia de España con Europa en el ámbito de la sociedad de la información.

Durante sus primeros años de andadura, INTECO apoyó el desarrollo en nuestro país, entre otros, de la administración digital, la accesibilidad y la movilidad. Es en el año 2012, con el aumento de la preocupación a nivel nacional e internacional por el incremento de los ciberataques y su impacto, que INTECO inicia un cambio en su orientación hacia la implementación de proyectos en el ámbito de la ciberseguridad. La firma ese mismo año de un Convenio de Colaboración entre la Secretaria de Estado de Seguridad (SES) y la SETSI en el ámbito de la ciberseguridad, refuerza esa necesidad de orientación de la entidad en el campo de la ciberseguridad, especialmente en el apoyo a la protección de las infraestructuras críticas, en colaboración con el ahora denominado Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

LA ESTRATEGIA DE CIBERSEGURIDAD NACIONAL. DICIEMBRE 2013

La importancia de la ciberseguridad a nivel europeo ha ido creciendo año tras año. En el año 2013 la Unión Europea pone el foco en ella desarrollando la Estrate-

FIGURA 1
ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

Fuente: http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional

gia Europea de Ciberseguridad (EUCS), (2). Presentada por la Comisión y la Alta Representación de la Unión Europea para Asuntos Exteriores y Política de Seguridad, dicha Estrategia expone la visión de la UE en este campo, aclara funciones y responsabilidades y establece las medidas necesarias, basadas en una promoción amplia y efectiva de los derechos de los ciudadanos y con el objetivo final de que el entorno en línea de la UE llegue a ser el más seguro del mundo.

Además, la EUCS incorpora e impulsa los valores europeos de libertad y democracia, velando por un crecimiento seguro de la economía digital. De esta forma, la visión de la UE para esta estrategia queda articulada en cinco prioridades estratégicas:

- lograr la ciberresiliencia, mediante la mejora de la concienciación en materia de seguridad,
- reducir drásticamente el crimen organizado,
- desarrollar una política en ciberdefensa y capacidades en materia de seguridad,
- desarrollar recursos industriales y tecnológicos para ciberseguridad y
- establecer una política de ciberespacio coherente a nivel internacional promoviendo los valores de la UE.

En sincronía con la Unión Europea, España aprueba el 5 de diciembre de 2013 su Estrategia de Ciberseguridad Nacional (ECSN). Esta estrategia constituye a día de hoy el eje vertebral del marco español de ciberseguridad.

La aprobación de dicho documento de carácter estratégico, tal y como se recoge en el preámbulo, pone de manifiesto el compromiso de una nación que apuesta en firme por garantizar su seguridad en el ciberespacio. Para España los avances en el ámbito de la ciberseguridad contribuyen, además, un incremento de nuestro potencial económico, ya que promueven un entorno más seguro para la inversión, la generación de empleo y la competitividad.

Esta Estrategia delimita el entorno del ciberespacio y su protección a través del despliegue de acciones de prevención, defensa, detección y respuesta frente a la ciberamenazas. Fija unos propósitos y principios rectores como son el liderazgo nacional y la coordinación de las capacidades, recursos y competencias involucradas, la responsabilidad compartida de todos los agentes públicos y privados con responsabilidad en esta materia, la proporcionalidad, racionalidad y eficacia en las medidas de protección adoptadas y la cooperación internacional.

Para ello, establece como objetivo global el lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques. Lo cual se conseguiría trabajando en el desarrollo de los siguientes objetivos específicos:

- Garantizar que los sistemas de información y telecomunicaciones que utilizan las Administraciones Públicas posean el adecuado nivel de ciberseguridad y resiliencia.
- Impulsar la seguridad y resiliencia de los sistemas de información y telecomunicaciones usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular.
- Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.
- Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.
- Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad.
- Contribuir a la mejora de la ciberseguridad en el ámbito internacional.

Para alcanzar estos objetivos, la ECSN se articula a través una serie de líneas de acción:

- Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas, haciendo énfasis en la cooperación de los organismos en ciberseguridad, en especial el CERT de la Administración Pública del Centro Criptológico Nacional (CCN-CERT), el Mando Conjunto de Ciberdefensa

de las Fuerzas Armadas (MCCD) y el entonces denominado CERT de Seguridad e Industria o CERTSI (operado técnicamente por INCIBE bajo coordinación del propio INCIBE y el CNPIC).

- Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas, garantizando la implantación del Esquema Nacional de Seguridad, reforzando las capacidades de detección y mejorando la defensa de los sistemas clasificados.

- Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas mediante la adopción, entre otras medidas, de la ampliación y mejora de las capacidades del CERTSI.

- Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia, potenciando las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.

- Seguridad y resiliencia de las TIC en el sector privado, impulsando la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privado.

- Conocimiento, competencias e I+D+i, promoviendo la capacitación de profesionales, impulsando el desarrollo industrial y reforzando el sistema de I+D+i en materia de ciberseguridad.

- Cultura de la ciberseguridad a través de la concienciación a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.

INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (INCIBE). OCTUBRE 2014

Con la aprobación de la ECSN a finales del 2013, INTECO inicia un completo y profundo proceso de transformación con el objetivo de poder dar respuesta lo más rápidamente posible a las necesidades y retos que nuestro país tenía y tiene por delante ante las nuevas ciberamenazas.

Estos retos se refieren a la construcción y puesta en marcha de aquellas capacidades que permitan hacer frente al rápido incremento del número de ciberataques y el aumento de su sofisticación, así como el desarrollo de iniciativas de carácter preventivo que fomenten el uso seguro y confiable de las tecnologías entre los ciudadanos y las empresas.

Además, la ciberseguridad, como un nuevo sector industrial en constante crecimiento, presenta una verdadera oportunidad para el desarrollo de nuestra economía, la creación de empresas y, por lo tanto, la creación de puestos de trabajo, por lo que INCIBE requería adaptarse para generar iniciativas que fomentasen y aprovechasen esta oportunidad.

Para dar cumplimiento a estos retos fue necesario iniciar un proceso de transformación de la entidad, interno y externo, que permitiese:

- La identificación de INTECO por parte de nuestros ciudadanos y empresas como la entidad de referencia nacional en el ámbito de la ciberseguridad y, por lo tanto, el organismo público al que poder acudir en caso de sufrir un incidente de ciberseguridad o un ciberataque o como canal para acceder a recursos de formación o concienciación.

- La aprobación por el Consejo de Administración de INTECO en octubre de 2014 del cambio de denominación de la entidad a Instituto Nacional de Ciberseguridad de España (INCIBE), constituyó el primer paso para reforzar el posicionamiento de la entidad como organismo de referencia en ciberseguridad en el ámbito del ciudadano y el sector privado.

- La prestación de nuevos y mejores servicios públicos de ciberseguridad orientados a la prevención, detección, análisis y repuesta ante incidentes de ciberseguridad.

- Disponer de la capacidad necesaria para apoyar a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) en la lucha contra el cibercrimen, especialmente en lo que se refiere a su formación y capacitación pero también en el desarrollo de tecnologías innovadoras.

- La promoción del talento en ciberseguridad en nuestro país, el fomento de la I+D+i en este campo así como el apoyo al emprendimiento.

- El impulso de la acción internacional de INCIBE con los objetivos de:

    - Por un lado, apoyar en la construcción de capacidades de ciberseguridad en otros países, de tal forma que éstos dispongan de capacidades adecuadas para la contención de ciberataques y que, en definitiva, contribuyan a la protección frente a éstos de nuestro país.

    - Mejorar el posicionamiento de la marca España en el ámbito de la ciberseguridad y por lo tanto de nuestras empresas, contribuyendo a la internacionalización de éstas.

Este proceso requería no sólo de la definición de una nueva estrategia externa de la compañía en la que primase una clara vocación de servicio público, sino también de una estrategia de transformación interna que hiciese posible el diseño e implementación de dichos servicios.

Así, en estos últimos cuatro años toda la organización ha estado inmersa en un profundo proceso de transformación apoyado en los siguientes pilares:

- La necesidad de un cambio cultural, que permitiese el cambio de orientación de toda la organización hacia la ciberseguridad, siendo el trabajo en equipo una herramienta indispensable para la mejora de la eficiencia y el fomento de la innovación. En el año 2017 y por primera vez desde la creación de la entidad, se definieron y aprobaron los valores corporativos de la entidad, como son: Lealtad, Compañerismo, Respecto y Honradez. Estos nuevos valores vienen además acompañados con una nueva metodología de evaluación del desempeño que valora no sólo el resultado conseguido de manera individual y colectiva sino cómo se han alcanzado.

- La mejora de la conciliación laboral, mediante la flexibilización del horario, la introducción de metodologías de trabajo Agile y el establecimiento de salas colaborativas, entre otras, como medidas para el fomento de la compartición de la información y la mejora de la colaboración con el objetivo final de poder alcanzar nuevos y más ambiciosos resultados.

- La reorganización de los procesos productivos y de la propia organización, lo que ha permitido:

    - Implantar una nueva forma de comunicar acorde a las necesidades de los receptores de la misma: ciudadanos y empresas que no tienen, en general, un conocimiento avanzado en ciberseguridad. La comunicación representa en este momento una actividad de carácter estratégico para la entidad y también para la propia Seguridad Nacional. Es necesario comunicar en tiempo y forma a los ciudadanos y empresas todo aquello que les pueda afectar en este nuevo ámbito que es la ciberseguridad. Dos claros ejemplos de ello supusieron las crisis de Wannacry y NotPetya del pasado año. Ambas, motivadas por la infección por malware tipo ransomware (3) a sistemas de grandes empresas, produjeron sendas crisis internacionales en las que la comunicación a los ciudadanos y empresas fue fundamental. Dicha comunicación requirió trasladar de forma continua a la ciudadanía, todo lo que estaba ocurriendo y, lo más importante, de qué forma podían protegerse. Para ello, además, era necesario utilizar un lenguaje que fuese entendible por toda la sociedad y no sólo por los expertos que trabajan en este campo.

    - La eliminación de duplicidades internas y la mejora de la especialización, maximizando la eficiencia de la organización y por lo tanto la gestión de los fondos públicos.

    - El rediseño de un nuevo modelo organizativo que permita por un lado generar mayor número de servicios públicos y, por otro, hacerlo dinamizando el sector de la ciberseguridad sin entrar en conflicto con los legítimos intereses comerciales de los proveedores de ciberseguridad. Para ello se ha establecido un canal permanente de dialogo con la industria y una permanente evaluación de los servicios prestados por INCIBE.

    - La implementación de una nueva capacidad interna que permita la gestión efectiva de crisis nacionales en el ámbito de la ciberseguridad. La pasada crisis de WannaCry puso de manifiesto, no sólo en España sino a nivel mundial, la necesidad de que INCIBE, al igual que el resto de organismos públicos de ciberseguridad, dispongan de capacidades adecuadas en formato 24x7 que permitan hacer frente a verdaderas crisis nacionales e internacionales propiciadas por ciberataques que muy probablemente debamos abordar en el futuro.

MODELO DE GOBERNANZA Y COLABORACIÓN DE LA CIBERSEGURIDAD EN ESPAÑA. 2014-2018

INCIBE es a día de hoy la entidad de referencia en ciberseguridad en el ámbito de ciudadanos y sector privado, pero la ciberseguridad de nuestro país se construye, al igual que en la gran mayoría de los estados occidentales, conjuntamente con multitud de actores:

- Los reguladores sectoriales, dependientes de cada ministerio, que tienen capacidad normativa y supervisora para obligar a que en las organizaciones de su sector de actividad se implementen medidas de seguridad.

- Los reguladores transversales, como la Agencia Española de Protección de Datos (AEPD) o el CNPIC, que afectan a todos los sectores de actividad.

- Los distintos centros de respuesta ante incidentes de ciberseguridad o CSIRTs (Computer Emergency Response Teams), públicos y privados, estatales y regionales, con capacidades de respuesta, pero que en muchos casos también trabajan en la prevención y detección.

- Las policías y la fiscalía, que son quienes pueden investigar y perseguir a los cibercriminales.

- Las fuerzas armadas y los servicios de inteligencia, que tienen la responsabilidad de defendernos ante ataques procedentes de otros estados y organismos de inteligencia.

- El Ministerio de Asuntos Exteriores, responsable de las relaciones internacionales, más necesarias que nunca porque el ciberespacio permite moverse entre diferentes jurisdicciones nacionales instantáneamente y sin necesidad de pasar controles fronterizos.

- El Ministerio de Educación y todas las universidades y centros educativos, que deben formar a menores, ciudadanos y profesionales en el uso seguro de las tecnologías.
- Los prestadores de servicios de Internet y prestadores de servicios digitales en general, que son a la vez objeto y medio de los cibercriminales.
- Las empresas privadas que prestan servicios de ciberseguridad y sin cuyo trabajo no se podría garantizar la ciberseguridad del país.
- Las propias organizaciones, del ámbito público o privado, que deben velar por su propia ciberseguridad, y que en el caso de ser operadores de infraestructuras críticas tienen una responsabilidad añadida que afecta a la seguridad de todos los ciudadanos.

Aunque con todas las piezas anteriores es posible construir una barrera de defensa ante la ciberamenaza, los criminales buscan las grietas que puedan quedar entre ellas. Por tanto, es necesario conseguir la coordinación entre todos los actores, que permita cerrar los huecos y asegurar un sistema de ciberseguridad coherente y completo.

Con este objetivo, la ECSN establece el marco de coordinación de la política de ciberseguridad creando una estructura orgánica que se integra en el marco del Sistema de Seguridad Nacional a través del Consejo de Seguridad Nacional (CSN).

Este Consejo dispone de cinco Comités Especializados, entre los que está el Consejo Nacional de Ciberseguridad (CNCS), el cual es un órgano colegiado de apoyo al CSN que se creó por Acuerdo del mismo el 5 de diciembre de 2013 con el objetivo de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, facilitando la toma de decisiones del propio CSN mediante el análisis, estudios y propuestas de iniciativas, tanto en el ámbito nacional como internacional.

En el seno de este Consejo se acordó proceder a marcar las directrices de desarrollo de la Estrategia para los siguientes dos años, mediante la elaboración de un Plan Nacional de Ciberseguridad (PNCS), que desarrollase a través de actuaciones concretas las líneas de acción previstas en la ECSN, utilizando los mecanismos que fueran necesarios para ello. Dicho plan se llevó a la aprobación del CSN el 31 de octubre de 2014 y constituyó así el primer nivel en la planificación de la ECSN.

El PNCS, partiendo de la definición de las amenazas a las que se enfrentaba España, asumía las líneas de actuación de la ECSN y se proponía como misión lograr que en España hiciésemos un uso seguro de los sistemas de información y telecomunicación fortaleciendo las capacidades de prevención, defensa, detección, recuperación y repuesta a los ciberataques, mediante el cumplimiento de los objetivos establecidos en la estrategia.

Las líneas de acción establecidas fueron:

- Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de defensa y otros sistemas de interés nacional.
- Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección en las Administraciones Públicas y mejorar la defensa de los sistemas clasificados.
- Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
- Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
- Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.
- Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.
- Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
- Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

Desde el desarrollo de este PNCS y sus planes específicos, los diferentes organismos públicos con cometidos o funciones en ciberseguridad en España, han venido trabajado intensamente en el desarrollo de las líneas de acción establecidas en los mismos.

DIRECTIVA NIS Y NUEVO PAQUETE LEGISLATIVO EUROPEO EN MATERIA DE CIBERSEGURIDAD. SEPTIEMBRE 2017

El 6 de julio de 2016, se aprueba la Directiva (UE) 2016/1148 del Parlamento y Consejo Europeo, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la UE. Dicha Directiva, conocida como Directiva NIS (Network and Information Security) viene a complementar la Estrategia de Ciberseguridad Europea aprobada en el año 2013 y se centra en la mejora de la protección de los servicios esenciales de los países miembros en el ámbito ciber.

Para ello, la Directiva NIS establece unos requisitos mínimos comunes de seguridad para los operadores de

servicios esenciales y los proveedores de servicios digitales, a los que insta a adoptar las medidas oportunas para gestionar los riesgos de seguridad y notificar los incidentes que puedan tener un impacto significativo en éstos. Dicha notificación se debe realizar a las Autoridades Competentes nacionales, proponiendo el establecimiento de centros de respuesta ante incidentes en el ámbito nacional que apoyen en la gestión de los incidentes de ciberseguridad así como la creación de una red de cooperación entre todos los Estados Miembros.

Dicha Directiva ha sido traspuesta al ordenamiento jurídico español 7 de septiembre de 2018 mediante el Real Decreto-Ley (RDL) 12/2018.

En paralelo a la aprobación de la Directiva NIS, en septiembre de 2017 la Comisión Europea presentó un ambicioso conjunto de medidas de reforma en materia de ciberseguridad, con el objetivo de hacer frente a la creciente amenaza en Europa que plantean los ataques cibernéticos, así como aprovechar las oportunidades que presenta la nueva era digital.

Un mes más tarde, en concreto los días 19 y 20 de octubre de 2017, y como consecuencia de la propuesta de dichas medidas por la Comisión Europea, el Consejo Europeo solicitó la adopción de un planteamiento común de la ciberseguridad en la UE. Son precisamente los retos de ciberseguridad asociados al Internet de las Cosas o y la importancia del uso seguro de las redes y de los sistemas de información y telecomunicaciones en el marco de la UE, lo que hace además prioritario la adopción de este planteamiento común.

Con este compromiso, el Consejo de Transporte, Telecomunicaciones y Energía (4) de la UE celebrado el 24 de octubre, acordó elaborar un plan de actuación para la reforma de la ciberseguridad de la UE. Los ministros europeos destacaron que la ciberseguridad era esencial para las empresas y los ciudadanos europeos, apoyando a nivel de Consejo Europeo el impulso a una reforma legal.

El siguiente paso dado en el seno de la UE fue el acometido por el Consejo de Asuntos Generales (5), el cual instó el 20 de noviembre de ese mismo año a reforzar la ciberseguridad europea y mejorar la ciberresiliencia en toda la UE. Los ministros europeos destacaron la necesidad de que todos los países miembros de la UE proporcionasen las inversiones y los recursos necesarios para abordar la ciberseguridad y subrayaron la importante relación entre la confianza en la Europa digital y la consecución de la ciberresiliencia en toda la Unión. Con estos objetivos se tomaron medidas a dos niveles:

- A nivel estratégico, estableciendo un grupo que deberá estar compuesto por representantes de los Estados miembros, la Comisión y la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) y cuyo objetivo es el de evaluar las capacidades de los estados miembros.

- A nivel operacional, constituyendo una red de CSIRTs nacionales que contribuya al desarrollo de la confianza mutua entre los Estados miembros y para promover una cooperación rápida y eficaz. La red estará compuesta por representantes de los CSIRTs de los Estados miembros y el centro de respuesta ante incidentes de la UE o CERT-UE. La Comisión participará en la red en calidad de observador y ENISA se hará cargo de la secretaría y apoyará activamente la cooperación entre los CSIRTs. Entre las tareas de este grupo se encuentran: el intercambio de información sobre servicios, operaciones y capacidades de cooperación de los CSIRTs, el apoyo a los Estados Miembros a la hora de hacer frente a incidentes transfronterizos o, en determinadas condiciones, el intercambio y análisis de información relativa a incidentes y riesgos asociados.

CONSOLIDACIÓN DE INCIBE COMO AGENTE DEL SISTEMA NACIONAL PÚBLICO EN CIBERSEGURIDAD. SEPTIEMBRE 2018

El RDL de trasposición de la Directiva NIS de septiembre de 2018, asigna a INCIBE competencias públicas en ciberseguridad. Así, el centro de respuesta ante incidentes de ciberseguridad de INCIBE, INCIBE-CERT, es designado en dicho RDL como el centro de referencia para ciudadanos, entidades de derecho privado y, en colaboración con el CNPIC, en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos del sector privado.

No obstante, desde el inicio de su proceso de transformación en 2014 hasta la fecha INCIBE, como instrumento del Estado en materia de ciberseguridad al amparo de la ECSN, ha venido reforzando sus capacidades técnicas y los servicios públicos que presta a ciudadanos y empresas.

- Servicios a ciudadanos y empresas

  El impulso a los servicios de seguridad para ciudadanos y empresas y la innovación en los recursos disponibles ha incluido el refuerzo de la Oficina de Seguridad del Internauta (OSI), el Centro de Seguridad del Menor de Internet o Internet Segura for Kids (IS4K), las herramientas gratuitas de concienciación y formación enfocadas a las empresas «Protege tu empresa», el evento CyberCamp y el centro de respuesta a incidentes de INCIBE (INCIBE-CERT).

  La OSI, como portal dirigido a aquellos ciudadanos que utilizan Internet de forma habitual o diaria, sin tener unos conocimientos avanzados en informática, telecomunicaciones o seguridad TIC, ha ampliado considerablemente el número de contenidos y mejorado su orientación y facilidad de aprendizaje. El objetivo fundamental de la OSI es ayudar a los ciudadanos a:

  - Entender, asimilar y adoptar un conjunto mínimo de buenas prácticas en seguridad al navegar y usar Internet.

  - Tomar conciencia de su responsabilidad en materia de seguridad, pasando a ser un ele-

mento activo y proactivo en la seguridad de su información y sus dispositivos.

- Reducir la cantidad y criticidad de riesgos o incidentes a los que se exponen cuando utilizan Internet.

La OSI dispone de numerosos mecanismos para acercar la ciberseguridad a los ciudadanos, como son: el centro de atención telefónica al internauta enfocado a que los ciudadanos puedan llamar y resolver las dudas y los problemas que puedan tener con la seguridad en Internet, la aplicación Conan Mobile para dispositivos móviles basados en Android que mejora el estado de seguridad de los terminales en los apartados de configuración, análisis de aplicaciones y permisos de usuarios y, el servicio antibotnet que pone a disposición de los usuarios mecanismos para poder identificar si desde su conexión a Internet se ha detectado algún incidente de seguridad relacionado con botnets, además de ofrecer información y enlaces a herramientas que les ayudarán en la desinfección de los dispositivos.

En relación con IS4K o Internet Segura for Kids, creado en 2017 y que tiene por objeto la promoción del uso seguro y responsable de Internet y las nuevas tecnologías entre los niños y adolescentes, se garantiza que España esté alineada con la estrategia Europea (BIK), que busca sensibilizar y formar no sólo a menores de edad sino también a su entorno directo: familia, docentes, educadores y profesionales del sector, sobre un uso seguro y responsable de Internet y de las nuevas tecnologías.

Los ámbitos de actuación de este centro son:

- Sensibilizar y formar a menores, jóvenes, familias, educadores y profesionales del ámbito del menor, a través del desarrollo de campañas, iniciativas y programas de ámbito nacional.
- Disponer de una línea de ayuda con un número de atención telefónica.
- Facilitar un canal de denuncia de contenidos o hotline, diferenciando el tratamiento de los mismos en función de su tipología:
    - Aquellos que puedan ser considerados inapropiados o perjudiciales para los menores peligrosos, y/o.
    - Aquellos de abuso sexual infantil que se encuentren en Internet y que han de denunciarse ante las FCSE.
- Reducir la disponibilidad de contenido criminal en Internet, principalmente de abuso sexual infantil, dando soporte a las FCSE.
- Organizar el Día de la Internet Segura (Safer Internet Day) en España.

Por su parte, los instrumentos que utiliza INCIBE a través de IS4K son:

- El programa de cibercooperantes con el que se pretende promover la colaboración de personas interesadas en la divulgación de la ciberseguridad a través de charlas de sensibilización sobre el uso seguro y responsable de Internet, así como los riesgos a los que se puede estar expuesto a través de las nuevas tecnologías, además de informar sobre los mecanismos de ayuda existentes en caso de problemas.
- El stand «Tu espacio de ciberseguridad» con el que se extiende la cultura de seguridad a los ciudadanos a través del contacto directo, sirviendo de punto de encuentro para que las familias puedan aprender jugando y poniendo a prueba los conocimientos en ciberseguridad, a través de diversos desafíos que facilitan a los participantes afianzar y conocer aquellas cuestiones que se pueden encontrar en su día a día en Internet.
- Las jornadas escolares para un uso seguro y responsable de la red enfocadas a implicar a la comunidad educativa en su conjunto, familias y equipos docentes en la sensibilización y formación de los menores.

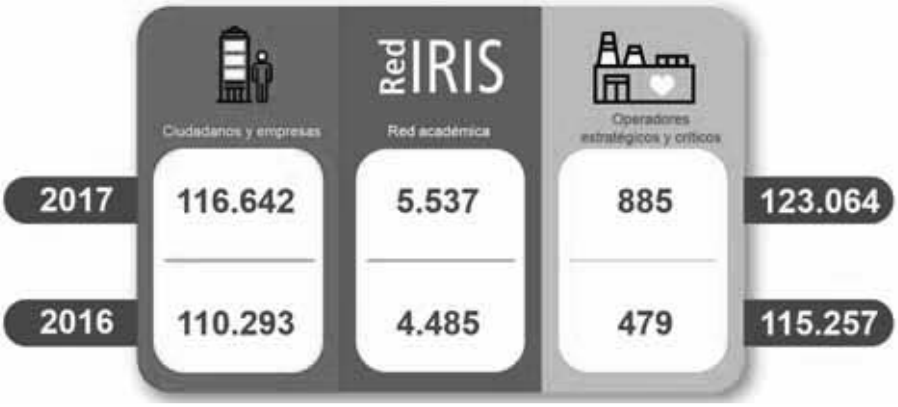
En cuanto a las herramientas de concienciación y formación enfocadas a las empresas, INCIBE las pone a su disposición para ayudarles a hacer de la ciberseguridad su valor diferencial, además de brindarles la posibilidad de protegerse, tomar conciencia del problema y, en su caso, prevenir los posibles incidentes que pudieran afectarles.

Entre dichos instrumentos figuran el blog (6), los avisos de seguridad (7) y el ya mencionado servicio antibotnet (8), que en el caso de las empresas les permite conocer si algún equipo informático de su red está siendo controlado de forma remota. Otra herramienta de utilidad para las empresas es el kit de autodiagnóstico (9), con el que éstas puedan evaluar en breves minutos y a través de unas sencillas preguntas, su nivel de ciberseguridad y así poder mejorar su protección frente a posibles riesgos y amenazas.

Además, INCIBE ofrece un servicio (10) (extorsión que surge tras el «secuestro» de la información del dispositivo por un virus), un catálogo de empresas y soluciones de ciberseguridad (11), y un juego de rol (12) que permite la simulación de cinco incidentes con sus posibles soluciones.

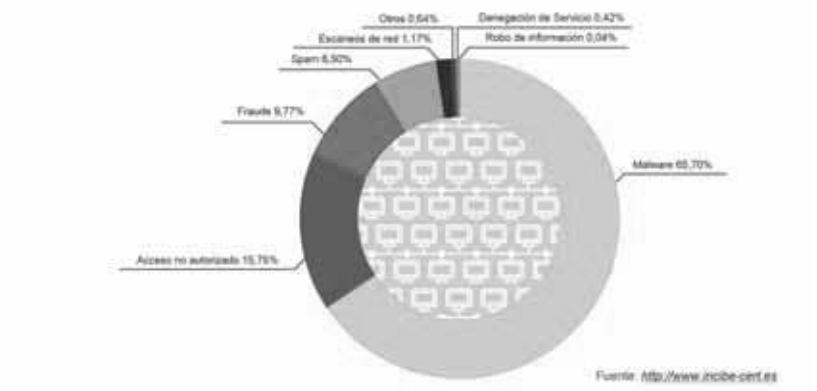
Entre los recursos de formación, se encuentran cursos online (13) bajo la metodología Massive Open Online Courses (MOOC), itinerarios interactivos sectoriales (14) y un «» sobre ciberseguridad, denominado «, se acabó el juego» (15), que ayuda a conocer los riesgos más importantes a los que se enfrentan los profesionales. Este juego gratuito re-

FIGURA 2
INCIDENTES DE CIBERSEGURIDAD GESTIONADOS POR INCIBE-CERT



Fuente: Elaboración propia

FIGURA 3
TIPOLOGÍA DE INCIDENTES DE CIBERSEGURIDAD GESTIONADOS POR INCIBE-CERT EN 2017



Fuente: Elaboración propia

cibió en 2016 el prestigioso premio al «Mejor » en el Festival.

CyberCamp (16), el gran evento de ciberseguridad que INCIBE organiza anualmente, tiene como objetivo de acercar la ciberseguridad a todos los ciudadanos, independientemente de su edad y de su nivel de conocimiento. Además, durante el evento hay numerosas actividades que permiten identificar, gestionar y promocionar el talento en ciberseguridad, así como identificar trayectorias profesionales para los jóvenes talentos. Desde 2014 se han celebrado cuatro ediciones, dos en Madrid, una en León, haciéndola coincidir con el décimo aniversario de la creación de INCIBE y otra en la ciudad de Santander, superando en esta última edición la cifra de 20.000 asistentes.

Es a través del INCIBE-CERT desde el que se trabaja para detectar, alertar y ayudar a ciudadanos y empresas frente a ciberataques. Este centro, de referencia para los ciudadanos y sector privado, despliega y ejecuta servicios de inteligencia en ciberseguridad, detecta de forma proactiva amenazas, realiza alerta temprana de nuevas amenazas, responde y analiza incidentes de seguridad de la información, aumenta la ciberresiliencia de las organizaciones, diseña medidas preventivas para atender a las necesidades de la sociedad, y ofrece su apoyo en la toma de decisiones estratégicas relativas a la ciberseguridad nacional.

A modo de balance estadístico, resulta destacable que en el ejercicio 2017 el INCIBE-CERT ha gestionado más de 123.000 incidentes de ciberseguridad en España, superando la cifra de 115.000 de 2016. De estos, más de 116.00 han correspondido a ciudadanos y empresas, más de 5.500 a la red académica RedIris y 885 a operadores estratégicos y críticos. Asimismo se han realizado más de 49.000 notificaciones a ISPs, empresas y operadores estratégicos y críticos informándoles de ciberataques y recomendándoles medidas de mitigación.

- Apoyo al ecosistema empresarial y de I+D+i de ciberseguridad

  La ciberseguridad supone una oportunidad para el desarrollo económico de todos los países y por lo tanto de España. En este sentido, INCIBE ha venido trabajando en los últimos años en el impulso al desarrollo de la industria nacional de ciberseguridad y su internacionalización, así como en el apoyo a la creación de nuevas empresas a través de diferentes programas de incubación y aceleración verticales.

  Para ello, se ha trabajado intensamente en la generación de un entorno propicio mediante la cooperación y la colaboración con agentes públicos y privados. Mediante el estudio sistemático de la situación española relativa al ecosistema industrial e investigador, hemos identificado y desplegado acciones dirigidas a responder a las necesidades detectadas, dedicando una especial atención a los programas de refuerzo de la oferta y demanda tecnológica.

  Un ejemplo es la realización en 2015 del «Estudio de viabilidad, oportunidad y diseño de una red de centros de excelencia I+D+I en ciberseguridad», en colaboración con agentes relevantes de este ecosistema, en el que se analizan las características del ecosistema investigador nacional, así como sus retos y oportunidades para el horizonte temporal 2015-2018, y que ha facilitado la puesta en marcha de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), actualmente integrada por 21 universidades y centros tecnológicos (17), el desarrollo de nuevas cátedras en ciberseguridad impulsadas por empresas del sector y la organización de un congreso anual que actúa como punto de encuentro para los 104 grupos de investigación formados por más de 1.300 investigadores del sector.

  La puesta en marcha del Polo Tecnológico Nacional de ciberseguridad, un foro que reúne a más de 270 empresas especializadas en esta industria, ha sido otra de las medidas desplegadas por INCIBE que facilita un espacio de diálogo con el sector empresarial a través del que identificar propuestas y comunicar las oportunidades de apoyo.

  El apoyo a la internacionalización de la industria ha permitido multiplicar las convocatorias de apoyo a misiones empresariales en el exterior, para lo cual INCIBE ha desarrollado varias acciones en colabo¬ración con socios de referencia como el ICEX España Exportación e Inversiones, lo que le ha permitido llevar a cabo misiones comerciales directas y acciones de networking en los principales eventos de ciberseguridad a nivel mundial (RSA, Infosecurity Londres, Cybertech Israel, Mobile World Congress, DES Madrid, etc.). Asimismo, en el marco del Encuentro Internacional de Seguridad de la Información (ENISE) que se realiza anualmente en la ciudad de León, se han organizado durante los dos últimos años un foro de emprendimiento y otro de negocio internacional, en el que se han analizado propuestas innovadoras de emprendedores nacionales e internacionales y se han mantenido sólo en el 2018 172 entrevistas B2B entre vendedores nacionales y compradores internacionales respectivamente.

  Para favorecer la dinamización del sector de la ciberseguridad nacional a fin de estimular el desarrollo de la I+D+i, desde INCIBE se ha promovido la transferencia tecnológica a través de RENIC mediante procesos públicos de compra innovadora con empresas y organismos regionales. Estos programas han tenido una gran acogida por parte de las empresas demandantes de tecnología en España, las cuales reclaman nuevos canales de colaboración con los centros generadores de conocimiento en ciberseguridad. De este modo en 2018 se ha facilitado la identificación de quince retos tecnológicos no resueltos por el mercado y que persiguen el impulso a la innovación tecnológica en materia de ciberseguridad. En este ámbito, las empresas nacionales disponen de un amplio potencial de crecimiento permitiéndoles captar financiación y ofrecer respuestas globales a los riesgos de ataques cibernéticos.

  En cuanto a los programas de apoyo al emprendimiento en ciberseguridad iniciados en 2014, en el pasado año 2018 la convocatoria de apoyo al emprendimiento Cybersecurity Ventures, destinada a la aceleración de proyectos empresariales, se cerró con un total de 45 precandidaturas y 12 finalistas que han accedido a un paquete de ayudas múltiple. Estos programas garantizan el crecimiento empresarial y la renovación generacional en un momento de crecimiento mundial de la demanda y resultan esenciales para los intereses estratégicos nacionales.

  Cabe destacar también el papel que INCIBE desempeña como parte activa de la representación española en el consorcio público privado europeo (cPPP) European Cyber Security Organisation (ECSO) promovido por la Comisión Europea, foro que pretende desarrollar, promover y fomentar la ciberseguridad en Europa a través del impulso de proyectos de investigación e innovación en esta materia y generar buenos hábitos en la industria. En dicho foro europeo, INCIBE es punto oficial de contacto de España y entidad pública representante del Estado junto con la Secretaria de Estado para el Avance Digital (SEAD) y el Centro de Desarrollo Tecnológico Industrial -CDTI. La experiencia de INCIBE le permite aportar tanto la perspectiva pública y gubernamental como su experiencia como demandante avanzado en el mercado europeo de ciberseguridad, impulsando activamente la participación de la industria española. Con 32 socios España representa el colectivo más numeroso en este clúster europeo.

Este impulso a la visibilidad internacional de la industria y sector tecnológico en el ámbito de la I+D+i, se ha reforzado con la puesta en marcha, en septiembre de 2017,de la oficina de apoyo a proyectos europeos de I+D+i de INCIBE, que ha permitido en sus primeros 15 meses de actividad impulsar la presentación de 35 candidaturas españolas, contribuyendo a cerrar el año con una tasa de retorno de participación en la línea de I+D+i en ciberseguridad para el programa comunitario Horizonte 2020 del 16%, siendo España el primer país de la UE por este concepto.

Desde INCIBE somos conscientes que queda mucho trabajo por hacer y que además lo debemos hacer conjuntamente con el resto de actores públicos y privados. No obstante, siguiendo la estrategia marcada nuestro país podrá disponer de los niveles de ciberseguridad adecuados que protejan a nuestros ciudadanos, empresas y administraciones públicas.

NOTAS

[1] Orden PCI/870/2018, de 3 de agosto, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia de Ciberseguridad Nacional. Más información disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-11472

[2] Comisión Europea: Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. Más información disponible en: http://europa.eu/rapid/press-release_IP-13-94_es.htm

[3] Malware diseñado para cifrar información en sistemas y redes informáticas una vez que éstos han sido infectados, con el objetivo de pedir un «rescate» o pago económico para descifrarlo.

[4] Más información disponible en: http://www.consilium.europa.eu/es/meetings/tte/2017/10/24/

[5] Más información disponible en: http://www.consilium.europa.eu/es/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/

[6] Más información disponible en: https://www.incibe.es/protege-tu-empresa/blog

[7] Más información disponible en: https://www.incibe.es/protege-tu-empresa/avisos-seguridad

[8] Más información disponible en: https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antibotnet

[9] Más información disponible en: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[10] Más información disponible en: https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

[11] Más información disponible en: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

[12] Más información disponible en: https://www.incibe.es/protege-tu-empresa/juego-rol-pyme-seguridad

[13] Más información disponible en: https://www.incibe.es/formacion/ciberseguridad-para-micropymes-y-autonomos

[14] Más información disponible en: https://itinerarios.incibe.es/

[15] Más información disponible en: https://www.incibe.es/protege-tu-empresa/hackend

[16] Más información disponible en: https://cybercamp.es/empieza-aqui/cybercamp17

[17] Más información disponible en: https://www.renic.es/es