CERT de seguridad e industria

Por una sociedad digital más segura

Hablar de ciberseguridad sólo es posible si hablamos de cooperación y coordinación entre todos los agentes involucrados. En España se ha impulsado esta coordinación entre las agencias públicas que trabajan para lograr un ciberespacio más seguro. La Agenda Digital para España, la Estrategia de Ciberseguridad Nacional, o el Consejo de Ciberseguridad Nacional son ejemplos de que la coordinación en materia de ciberseguridad es una realidad. Fruto de alianzas entre dos ministerios, surge el CERT de Seguridad e Industria, que presta servicios de respuesta a incidentes tanto reactivos como proactivos para ciudadanos, empresas, operadores del sector estratégico e infraestructuras críticas y red académica.

MIGUEL REGO
Director General
de INCIBE

A la hora de hablar de lo que estamos haciendo en España en materia de ciberseguridad, es necesario destacar el importante esfuerzo realizado en los últimos años por parte de todos los actores involucrados. Nuestro gobierno ha impulsado la máxima coordinación de las agencias públicas que trabajan de manera conjunta desde diferentes aproximaciones con el objetivo de lograr un ciberespacio más seguro y establecer puentes de colaboración con el sector privado.

De este modo, en 2013 se aprobaban consecutivamente la Agenda Digital para España y, a finales de ese mismo año, la Estrategia de Ciberseguridad Nacional, con la que se alcanzaba una visión integradora basada en la coordinación entre los diferentes actores implicados, a la vez que nuestro país alineaba su posición en el contexto mundial. Corresponde al Consejo de Ciberseguridad Nacional, del cual INCIBE forma parte bajo esa consigna de coordinación pública, la definición de planes específicos que permitan implementar las líneas de acción señaladas por la Estrategia de Ciberseguridad Nacional.

La Agenda Digital para España incluye, dentro de sus objetivos estratégicos, reforzar la confianza en el ámbito digital a través de tres ámbitos de actuación: impulsar el mercado de los servicios de confianza, reforzar las capacidades actuales para promover la confianza digital e impulsar la excelencia de las organizaciones en materia de confianza digital. Para su desarrollo se estableció el Plan de Confianza en el ámbito Digital (PCD), que supone la combinación de estrategia, cultura, capacidades, excelencia y talento para el avance de la sociedad y la economía digital de España.

Dicho plan, aporta instrumentos para la construcción de un clima de confianza que contribuya de manera efectiva a un desarrollo sostenible de este modelo de crecimiento, empleo y bienestar que supone la economía digital.

Consciente de la importancia que ello tiene para la sociedad, el MINETUR ha apostado por realizar un esfuerzo presupuestario sin precedentes, dotando al Plan con un total de 59 millones de euros para las 25 medidas a desplegar durante el período 2013-2015, correspondiendo a INCIBE el rol principal en su ejecución.

Junto con la Estrategia, la iniciativa de MINETUR se complementa con la construcción y el afianzamiento de alianzas de colaboración y cooperación que permiten optimizar capacidades y sumar esfuerzos y recursos en campos diversos de la ciberseguridad.

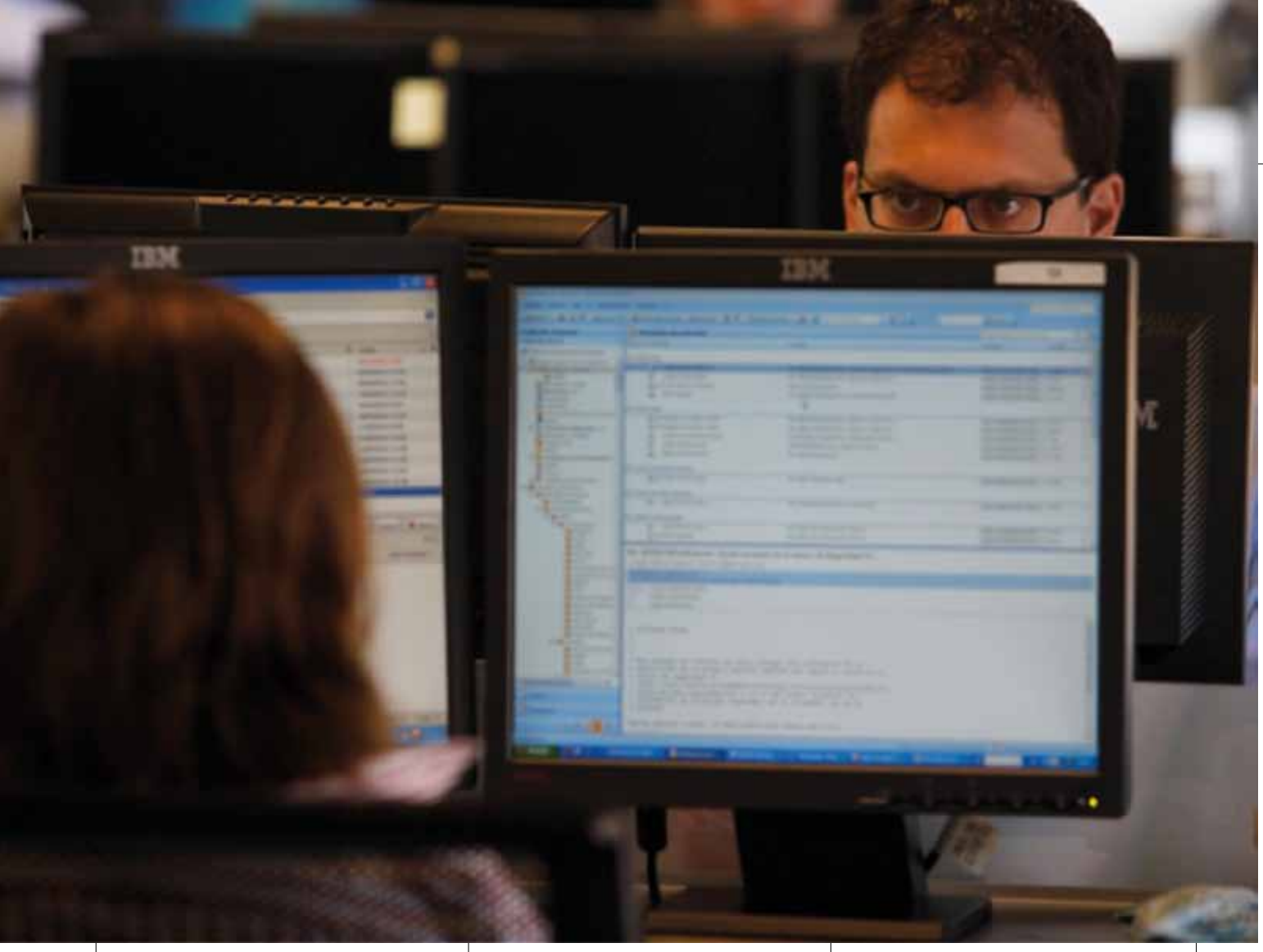
CERT de seguridad e Industria

A la hora de hablar de alianzas, es necesario destacar la establecida el pasado octubre de 2012, a través del convenio suscrito entre el Ministerio del Interior y el Ministerio de Industria, Energía y Turismo. Dicho acuerdo supuso un hito sin precedentes en la coordinación y optimización de las capacidades disponibles en materia de ciberseguridad, la lucha contra los ciberdelitos y la protección de las infraestructuras críticas, ejecutada por dos Secretarías de Estado y sus diversos organismos dependientes, y ha derivado en la puesta en marcha de nuestro CERT de Seguridad e Industria.

Se trata de un equipo especializado de respuesta a incidentes en ciberseguridad, que se administra conjuntamente desde INCIBE con el Centro Nacional, para la Protección de las Infraestructuras Críticas (CNPIC) y presta servicios a ciudadanos y empresas, operadores de infraestructuras críticas y Red Académica y de Investigación (RedIris).

Entre los servicios que nuestro CERT ofrece para sus diferentes públicos, destacan los servicios reactivos de respuesta a incidentes, así como los servicios de detección proactiva, alerta temprana o la labor de concienciación y sensibilización en materia de ciberseguridad a través de nuestros diferentes canales de comunicación.

Desde el punto de vista de la detección, nuestro CERT cuenta con un modelo de inteligencia en ciberseguridad (MICS), que aglutina información con el objetivo de identificar amenazas, vulnerabilidades y ataques en curso para lograr alertas de forma temprana a los administradores de los sistemas que sufren una agresión de cara a colaborar con ellos en su mitigación.



Una medida que permite valorar la capacidad de este modelo de inteligencia viene dada por los más de 1.500.000.000 de eventos de seguridad analizados durante el año 2014. Del mismo modo, es destacable la identificación diaria automatizada de más de 160.000 páginas web comprometidas o vulnerables a sufrir una explotación. El crecimiento de nuestro modelo de inteligencia es continuo, con la incorporación de fuentes de manera constante, como refleja la cifra de crecimiento de un 95% en la identificación de direcciones IP con actividad maliciosa entre enero y diciembre del pasado año.

Desde el punto de vista de la respuesta a incidentes, como indicadores acerca de la actividad de apoyo desarrollada por nuestro equipo ante las agresiones sufridas, destacan los 24.185 incidentes gestionados desde enero de 2014 a enero de 2015. Del mismo modo, hemos recibido en este período 46.594 solicitudes de apoyo ante una agresión. Por otro lado, una de las principales tareas de un CERT viene dada por la coordinación con otros agentes de cara a prestar apoyo a la entidad que haya podido sufrir un incidente. En este sentido, se han lanzado 174.393 investigaciones en el período indicado.

Las actividades desempeñadas para la mitigación de los incidentes han requerido de una respuesta técnica avanzada y capacidades de coordinación, entre las que destacan las que desarrollamos con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) así como los proveedores de servicio a Internet (ISP). El CERT-SI presta sus servicios en una modalidad de 24x7x365, lo que permite apoyar de la forma más ágil posible cuando se produce un incidente.

Inversión en capacidades y nuevos servicios

Todos los que trabajamos en este importante sector somos conscientes de que cualquier esfuerzo es poco a la hora de dotar de capacidades a los agentes responsables de la ciberseguridad, por lo que es necesario invertir continuamente en evolucionar tanto los servicios, como la tecnología desplegada o las capacidades de detección. En este sentido, en INCIBE se prevé invertir en este año 2015 alrededor de 1.550.000 de euros en nuevos servicios para los públicos objetivo del CERT-SI, que abarcan el despliegue de sondas en 10 operadores del sector estratégico, la elaboración de

un Esquema Nacional de Ciberseguridad Industrial, que comprende la elaboración de guías, recomendaciones, benchmarking, así como la creación de un laboratorio de evaluación remoto ScadaLab y la contratación de Testbeds industriales, la evolución de mecanismos de alerta temprana a través del mejor servicio de vulnerabilidades 0-day que hay a día de hoy disponible en el mercado, y la mejora de nuestro motor de inteligencia.

En otras materias, como la I+D+i, contamos con un equipo de 25 expertos dedicados a investigación y desarrollo tecnología, e invertimos alrededor de 2.000.000 de euros. Todo esto sin olvidar que, siendo conscientes de que la ciberseguridad comprende un entramado complejo, es imperativo dedicar una importante labor a la concienciación y sensibilización de nuestros diferentes públicos, para lo que dedicamos un equipo de 10 técnicos especializados y cerca de 1.000.000 de euros.

Oficina de Seguridad del Internauta

Es importante señalar que un 80% de todos los incidentes gestionados desde el CERTSI, afecta a los ciudadanos. Sin duda este dato es significativo. De ahí que la apuesta de INCIBE por esta labor de concienciación sea crucial. A través de iniciativas como nuestro portal Oficina de Seguridad del Internauta, nos ocupamos de llegar a los ciudadanos con un lenguaje llano, simple, conciso, carente de tecnicismos, de cara a lograr que cualquier usuario pueda estar al día en materia de ciberseguridad, sin tener que disponer de conocimientos técnicos especializados.

Los servicios que se prestan desde la OSI incluyen un blog con contenido especializado para estos usuarios sin conocimiento técnico, así como avisos, alertas, historias reales, infografías, o herramientas útiles para protegerse en la red.

Una de las iniciativas que hemos lanzado desde la Oficina de Seguridad del Internauta como parte de los servicios preventivos que se prestan desde el CERTSI viene dada por la puesta en marcha del Servicio Antibotnet, que permite ayudar a los usuarios cuyos equipos puedan estar infectados y formar parte de una botnet, de cara a poder identificarla y ayudar así a eliminar dicha infección. Para ello contamos con la información que generamos desde nuestro modelo de inteligencia, así como la colaboración de operadores como Telefónica, que por su parte envía en una segunda fase a los usuarios infectados códigos de incidente de cara a notificarlos. Todo ello con el objetivo de que consulten desde nuestro servicio tanto la botnet de la que forman parte como los mecanismos necesarios para la desinfección.

Como reflejo de la labor que venimos realizando en materia de concienciación a través de la Oficina de Seguridad del Internauta, podemos destacar que el 40% de los accesos provienen del continente latinoamericano.

El servicio público es esencial

El aspecto más importante de todos los que aquí se comentan, es recordar que INCIBE tiene ante todo, vocación de servicio. Disponemos hoy de capacidades, posicionamiento y proyección sustentados en un equipo técnico de alta cualificación, todo ello para aportar el mayor valor posible a una sociedad interconectada, dependiente de los servicios basados en las TIC.

Hablar de ciberseguridad es imposible sin hablar de cooperación y coordinación entre los diferentes actores que forman parte del conglomerado a nivel mundial, pues todos sabemos que a día de hoy en el ciberespacio las amenazas se suceden de forma global, de manera simultánea desde diferentes puntos del globo.

Un 80% de todos los incidentes gestionados desde el CERTSI afecta a los ciudadanos. A través de iniciativas como el portal Oficina de Seguridad del Internauta se llega a los ciudadanos para que cualquier usuario pueda estar al día en materia de seguridad

Es crucial que desde todos los estamentos que trabajamos para garantizar un ciberespacio más seguro, recordemos siempre que sólo la evolución, innovación y potenciación de nuestras capacidades y servicios de manera continua nos permitirán alcanzar nuestro fin, que no es otro que velar por la ciberseguridad de este mundo digital en el que todos cohabitamos. ✱