TÍTULO

****

**España no ha vivido ciberataques como Ucrania, pero es una posibilidad de la que no estamos a salvo**

ENTREVISTA CON FERNANDO J. SÁNCHEZ, DIRECTOR DEL CENTRO NACIONAL PARA LA PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

Fernando J. Sánchez Gómez dirige desde su creación (2007) el Centro Nacional para la Protección de Infraestructuras y Ciberseguridad (CNPIC), organismo dependiente de la Secretaría de Estado de Seguridad, del Ministerio del Interior. Este centro vela por la seguridad de los sectores considerados estratégicos, es decir, fundamentales para el funcionamiento de un país. Teniente Coronel de la Guardia Civil ­–donde desarrolló gran parte de su carrera– y Diplomado de Estado Mayor, Sánchez cuenta con más de 25 años de experiencia en seguridad nacional. Coautor de varios libros sobre la materia, ha dirigido y participado en la elaboración de las normativas españolas clave como la Ley sobre protección de Infraestructuras Críticas (2011) y la Estrategia Nacional de Ciberseguridad (2013). Hoy es también el punto de contacto de España con la Unión Europea en materia de protección de infraestructuras críticas, lo que le otorga una visión global y precisa de lo que está ocurriendo en materia de Ciberseguridad en la UE.

**Pregunta.- En mayo entra en vigor la Directiva NIS y ya se está trabajando en un Anteproyecto de Ley para su adaptación. ¿Qué va a cambiar con esta regulación sobre la práctica actual en la protección de los servicios sensibles?**

**Respuesta**. La Ley sobre la seguridad de las redes y sistemas de información, que transpone la Directiva (UE) 2016/1148, establece las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea. Obliga a crear una Estrategia de Seguridad de las Redes de Información con el objetivo preventivo de intercambiar información y cooperar estratégicamente. A los operadores de servicios esenciales y a los proveedores de servicios digitales les obliga a adoptar unas medidas precisas para mejorar su capacidad de resistencia ante los ataques cibernéticos con el objetivo de garantizar en todo momento la fiabilidad, seguridad y desarrollo normal de las infraestructuras esenciales para la sociedad.

En el borrador del anteproyecto de Ley se dice que se aplicará a las entidades que presten servicios esenciales para la comunidad y dependan de las redes y sistemas de información para el desarrollo de su actividad. Para darle un enfoque global, su ámbito de aplicación se extiende a servicios tanto excluidos como no expresamente incluidos en la Directiva, aunque se preserva su legislación específica. Identificando los sectores en los que es necesario garantizar la protección de las redes y sistemas de información, estableciendo procedimientos para identificar los servicios esenciales de cada sector, así como los operadores que presten dichos servicios. Para garantizar su coherencia con la aplicación de otras normativas en materia de seguridad de la información, se ha igualado su ámbito de aplicación con la Ley 8/2011 sobre Protección de Infraestructuras Críticas (PIC), de forma que a los sectores contemplados en la Directiva se han añadido los ya señalados en la citada ley española.

La Ley PIC iba mucho más allá de la Directiva anterior (114/2008), considerando prioritarios sectores que la regulación europea no consideraba, al tiempo que abordaba significativamente algunas de las previsiones que la Directiva NIS estableció posteriormente en relación a los operadores de servicios esenciales. Ello nos ha permitido encontrarnos en una posición ventajosa con respecto a otros países europeos, al tener identificados a través de la Ley PIC a la mayoría de los operadores esenciales exigidos por la Directiva NIS.

**DESTACADO:**

**España parte con ventaja al adelantarse con la Ley de Protección de Infraestructuras Críticas (2011) a algunos aspectos de la Directiva NIS**

España, desde el año 2013, cuenta con la Estrategia de Ciberseguridad Nacional donde se sientan las bases para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información, y que seguirá desarrollando el marco institucional de la ciberseguridad, compuesto por las autoridades públicas competentes y los CSIRT de referencia, y la cooperación público- privada, por otra. Las autoridades competentes ejercerán las funciones de vigilancia derivadas de esta materia y aplicarán el régimen sancionador, si procede.

En el ámbito de la ciberseguridad es necesario contar con mecanismos rápidos que faciliten la cooperación y el intercambio de información de todos los agentes implicados en la protección del ciberespacio. En este sentido, la Oficina de Coordinación Cibernética (OCC), integrada dentro del CNPIC, desde su creación en 2014 ejerce como canal específico de comunicación entre los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad, desempeñando la coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes.

**P. ¿Qué lecciones debemos aprender (y cuáles aprendió la administración española) de los ataques que vimos en 2017, WannaCry y NotPetya y, más en concreto, los ataques que sufrió Ucrania?**

**R.** En una primera instancia, debemos ser conscientes que los Sistemas de Información y Comunicación que empleamos a diario en nuestro entorno personal y empresarial son susceptibles de ser vulnerables a fallos de seguridad todavía no publicados por la comunidad de seguridad, y no solucionables por ende, por los desarrolladores de dichas tecnologías. Es lo que se denominan comúnmente como *0day* o fallos de seguridad de día cero que manejan ciertos actores como grupos criminales, *hacktivistas*, o servicios de inteligencia. El empleo de estas vulnerabilidades por parte de actores hostiles puede llegar a consolidarse como iniciadores de compañas masivas de distribución de *malware* y/o ataques más específicos mediante Amenazas Avanzadas Persistentes (APT).

En conclusión, se deben de extremar las medidas de seguridad lógica en lo relativo a actualizar y parchear cuantos fallos de seguridad sean publicados por los fabricantes y fuentes de confianza, en conjunción con unas buenas medidas de seguridad perimetral que permitan tomar consciencia situacional de amenazas desconocidas a través de análisis de actividades o tráfico anómalo. Todo con el objetivo de adoptar medidas efectivas de mitigación y contención de las amenazas.

Asimismo, en este tipo de ataques es de vital importancia mantener una buena relación con otros actores con competencias en el ámbito de la protección y coordinación de ciberincidentes, tales como el CNPIC, CSIRTs, o mercantiles y espacios virtuales especializados y compartir Indicadores de Compromiso (IOCs) u otra información relevante, algo que es clave en los primeros momentos de un ataque de esta magnitud.

**DESTACADO:**

**En ciberseguridad es clave contar con mecanismos rápidos que faciliten la cooperación e intercambio de información de todos los implicados**

**P. ¿Qué reflexiones le sugieren los datos cuantitativos y cualitativos del volumen de ciberincidentes registrados en España? ¿El nivel de detección es ahora mayor y más rápido? ¿Y la sensibilidad de las empresas, sean o no operadores críticos?**

R. El año pasado se registraron un total de 885 ciberincidentes relacionados con operadores críticos y estratégicos que fueron tratados por el CERT de Seguridad e Industria (CERTSI), el Instituto Nacional de Ciberseguridad (INCIBE) y el CNPIC.

Es importante precisar que este aumento exponencial del tratamiento de ciberincidentes no supone en ningún caso una mayor exposición a ataques o fallos de seguridad, sino que esto es debido, en algunos sectores al menos, a la incorporación de nuevos operadores y a la potenciación de las capacidades de detección de ciberamenazas de forma proactiva por parte del CERTSI.

Analizando las causas, cabe señalar que los ataques son cada vez más sofisticados, empleando vulnerabilidades del tipo día cero; en algunos casos extraídas de fugas de información perpetradas contra Servicios de Inteligencia (Ej.: *Shadow Brokers*), u obtenidas a través de *Black Markets* en la *Dark Web*.

Se ha venido apreciando cómo determinadas organizaciones criminales han perfeccionado sus metodologías de ataque a sectores estratégicos determinados, como el Financiero y Tributario, donde los ataques focalizados en emplear de forma fraudulenta el sistema SWIFT para transferir grandes sumas de dinero difieren muchos de burdos ataques de *Phishing* contra particulares. Actualmente en España no tenemos constancia de la perpetración de ataques de este primer tipo contra nuestros operadores.

Las empresas privadas están altamente concienciadas con la ciberseguridad, especialmente con el creciente uso de las tecnologías en la nube. Prueba de ello, es el compromiso que manifiestan nuestros operadores año tras año para participar en eventos organizados por el CERTSI para medir la ciberesiliencia de sus organizaciones ante ataques informáticos o incidentes de ciberseguridad varios.

Las empresas son conscientes de que la inversión en ciberseguridad, a pesar de ser un presupuesto aparentemente poco agradecido, pues no reporta beneficios directos, es una inversión a medio-largo plazo para la continuidad de negocio en espectro de calidad óptimo y sin sobresaltos.

Es cierto que el número de incidentes es cada vez más elevado, no solo porque cada vez se producen más y más agresivos, sino, porque los operadores críticos están más mentalizados y denuncian más agresiones de este tipo. Es imprescindible contar con capacidades de prevención y evaluación de la amenaza, de cara a disponer, en caso de que se materialice un incidente o ataque, de la mayor información posible que permita actuar de forma eficiente y acorde con las circunstancias.

Por ello, es necesario fomentar una cultura de concienciación de la ciberseguridad entre los usuarios y responsables de los sistemas de información, tanto del sector privado y particulares como del sector público, dirigida a garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la prestación de servicios ampliamente utilizados, así como la gestión de las infraestructuras críticas.

**DESTACADO:**

**Los ciberataques son cada vez más sofisticados y numerosos, aunque parte del aumento es por la incorporación de nuevos operadores críticos y a la mayor capacidad de detección de ciberamenazas**

**P. ¿Qué conclusiones/reflexiones obtienen de los test que con cierta periodicidad se realizan para calibrar la ciberseguridad tanto en España como en Europa?**

**R.** En el marco de la colaboración existente entre el CNPIC y el INCIBE, anualmente se realiza una consulta para medir la capacidad de los operadores críticos para anticiparse, resistir, recuperar y evolucionar ante un ataque de ciberseguridad, lo que denominamos ciberresiliencia.

La tendencia constatada en los últimos años es el aumento en el número, tipología y gravedad de los ataques contra los sistemas de infraestructuras estratégicas y críticas españolas. Ante estos ataques, los resultados de la consulta ofrecen datos positivos, evidenciando que los operadores participantes en ediciones anteriores mejoran los niveles de madurez en ciberresiliencia. Sin embargo, algunos de los operadores evaluados tienen necesidades de mejorar su capacidad para recuperar sus servicios frente a un posible incidente de Ciberseguridad. Asimismo, un tercio de los operadores tiene grandes retos para mejorar la ciberseguridad y, con ello, la capacidad para resistir ante posibles ataques de ciberseguridad contra sus sistemas.

Las áreas en las que, de forma general, es necesario profundizar para mejorar en ciberseguridad son las relacionadas, por un lado, con el establecimiento de políticas de Gestión de Vulnerabilidades que permitan identificar, analizar y gestionar las vulnerabilidades en los activos que sustentan la prestación de los servicios esenciales. Y, por otro, el desarrollo de políticas de Gestión de Incidentes para establecer los procesos que permitan aplicar una adecuada respuesta organizativa.

Como resumen se podría concluir que la cultura de la ciberresiliencia se va instaurando en el seno de las organizaciones de nuestro país y, cada vez más, se va interiorizando el mensaje de la ciberprotección de los servicios esenciales.

**DESTACADO:**

**Los test anuales para medir la capacidad de los operadores de infraestructuras críticas muestran, en general, mayores niveles de ciberresiliencia aunque un tercio tiene todavía grandes retos**



Para ampliar la imagen, [pinche aquí.](https://home.kpmg.com/content/dam/kpmg/es/pdf/2018/04/compromiso-ciberseguridad-mundo.pdf)

**P. En el** [**Global Cybersecurity Index 2017**](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf) **elaborado por el International Telecommunication Union (ITU) de la ONU, España aparecía en el puesto 19 de un total de 193. ¿En qué destacamos?**

R. El informe destaca el elevado compromiso de España, sobre todo en cuatro pilares.

En primer lugar, la cooperación entre los diferentes organismos actuantes en materia de ciberseguridad. En el ámbito de actuación del Ministerio del Interior, la Oficina de Coordinación Cibernética (OCC) del CNPIC es el órgano técnico de coordinación en materia de ciberseguridad, ejerciendo como canal específico de comunicación entre los Centros de Respuesta a Incidentes de seguridad de la información (CSIRT). Además, a nivel internacional, es el punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros.

En segundo lugar, I+D+i. Los datos reflejan que España es un país puntero en I+D+i, con la implicación de 9 centros tecnológicos, 94 universidades y 1 centro de investigación que conjuntamente nos posicionan a la cabeza de los países de nuestro entorno en investigación en materia de ciberseguridad.

En tercer lugar, destaca nuestra avanzada regulación legal. La consolidada Estrategia de Ciberseguridad Nacional junto a la inminente trasposición de la directiva NIS y las reformas legislativas que sobre ciberseguridad se han llevado a cabo tanto en el Código Penal como en la Ley de Enjuiciamiento Criminal, posicionan a España a la vanguardia en cuanto a instrumentos normativos en materia de Ciberseguridad y cibercrimen.

En cuarto lugar, España destaca en buenas prácticas. La abundante cantidad de guías que los dos principales CERTS nacionales generan en relación con la ciberseguridad es un claro ejemplo del interés gubernamental por profundizar y consolidar las políticas estatales encaminadas a garantizar un uso seguro de las TIC a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques.

**P. ¿Y en qué podríamos mejorar?**

Citaría dos aspectos que requierenmayor desarrollo. Uno, la estandarización, entendida como la puesta en valor e implantación de estándares de Ciberseguridad, tanto en las organizaciones como en su personal, siendo imprescindible la involucración de los organismos y entidades de normalización tanto nacionales e internacionales. Este es un reto que, de forma general, compartimos con nuestros socios europeos. Y dos, se debe avanzar en la consecución de acuerdos multilaterales que favorezcan una mayor cooperación en el intercambio de información con otros estados europeos e impulsar las iniciativas que, tanto desde las esferas públicas como privadas, se puedan producir en el campo de la ciberseguridad. En este sentido, el Plan Nacional de Ciberseguridad, a través de uno de sus planes derivados, establece acciones concretas para el desarrollo de la actividad formativa en ciberseguridad.

**DESTACADO:**

**La cultura de la ciberresiliencia se va instaurando en las organizaciones y, cada vez más, se va interiorizando el mensaje de la ciberprotección de los servicios esenciales**

**P. De los sectores sensibles o servicios esenciales ¿hay quizá algunos que pudiéramos identificar como “más sensibles” por el mayor efecto que tendría en la sociedad su colapso o porque lleven cierto retraso respecto a otros en materia de ciberseguridad?**

R. Todos los sectores estratégicos son importantes debido a que comprenden a un grupo de operadores que brinda servicios esenciales a la sociedad, y el cese en la prestación de estos tendría un impacto sustancial en el normal desenvolvimiento de la convivencia ciudadana, y en casos extremos de la seguridad nacional.

Bien es cierto que, el cese en la prestación de determinados servicios supondría un impacto mayor o menor, sobre todo si se atiende a diversos criterios, tales como la facilidad de replicar el servicio, afectación en la seguridad de las personas, costes económicos, interdependencias con otros servicios prestados, etc.

En lo que se refiere al nivel de criticidad de determinados servicios esenciales, estos también atienden a otro tipo de razones al margen del ámbito de la ciberseguridad, si bien el sector de las TIC es transversal a todos ellos. Asimismo, determinados sectores estratégicos tienen implantado en menor medida el modelo de seguridad integral (Cibernética y Física) que se potencia desde el CNPIC debido a que, por razones que atienden a las características intrínsecas del sector, no mantienen un desarrollo de las capacidades ciber al completo.

**P. ¿España no ha vivido situaciones extremas/delicadas como las que ha vivido Ucrania estos años o sí los ha habido pero no nos hemos apercibido públicamente de ello?**

R. España, al igual que otras naciones del entorno de la UE, sufre a diario ataques sofisticados provenientes de actores desconocidos muy profesionales en el ámbito del cibercrimen, la inteligencia, el espionaje industrial, la denegación de servicios, o los ataques avanzados de diversa índole. Se trata de ataques puntuales y dirigidos, que son detectados y mitigados por los diversos actores intervinientes, entre los que se encuentran el CNPIC, el CERTSI, y el CCN-CERT del Centro Nacional de Inteligencia (CNI).

La recomendación siempre es operar como si se estuviera comprometido, o si estos ciberataque pudieran producirse hoy mismo, aplicando una serie de medidas perimetrales de detección y mitigación, redundado de servicios, implantación de sistemas de *backup*, planes de contención y continuidad de negocio, etc.

Hasta la fecha, en España no se ha producido un ciberincidente del calibre al sufrido por Ucrania, si bien es una posibilidad sobre la que no estamos a salvo por lo que el CNPIC la tiene en cuenta también como hipótesis a la hora de confeccionar sus Planes Estratégicos Sectoriales y protocolos de actuación internos y para con los Operadores Críticos y Estratégicos.

**DESTACADO:**

**España, al igual otros países de la UE, sufre a diario ataques sofisticados y puntuales provenientes de actores desconocidos muy profesionales en el ámbito del cibercrimen**

**P. Desde el punto de vista de ciber protección de los sectores sensibles, ¿qué cambia cuando un nivel de riesgo sube de 3 (nivel medio) a 4 (riesgo alto) o a 5 (riesgo muy alto)?**

R. En el nivel 4 (riesgo alto), se refuerzan las medidas de seguridad graduales consignadas por el Operador Crítico en el Plan de Protección específico de cada Infraestructura Crítica, así como los correspondientes dispositivos reactivos y preventivos que las Fuerzas y Cuerpos de Seguridad tengan previstos en los Planes de Apoyo Operativo~~.~~

En lo que se refiere al ámbito de la respuesta de ciberincidentes, la actividad del CERTSI se verá reflejada por un SLA de respuesta inicial del ciberincidente tras notificación de 45 minutos. En lo referente al Operador Crítico, se eleva el número de comunicaciones que debe realizar sobre las diversas taxonomías de ataque para así tomar conciencia situacional plena de los incidentes acaecidos en las infraestructuras. Todo ello reportará información de alto valor de diversos actores comprendidos en varios sectores estratégicos, con la cual se podrán emitir alertas de Ciberseguridad y directrices para la detección y mitigación de ciberamenazas.

Asimismo, desde el punto de vista operativo, el CERTSI a través de la Oficina de Coordinación Cibernética (OCC) del CNPIC, canalizará las informaciones hacia diversos actores competenciales en este ámbito: altas instancias de la Secretaría de Estados de Seguridad, Unidades de Investigación Tecnológica de la Policía Nacional y la Guardia Civil, CCN-CERT del CNI (en lo relacionado con las Administraciones Públicas), EUROPOL, así como otros CSIRT y organismos de carácter internacional.

Respecto al nivel 5 (riesgo muy alto), se trata de un nivel de alerta reservado para estados de situación excepcionales y puntuales en el tiempo, los cuales suponen el máximo grado de implicación de las Fuerzas y Cuerpos de Seguridad, así como de los órganos, centro o instituciones con competencias específicas de seguridad o protección, afectando de forma muy especial a los operadores críticos. En este caso, la respuesta del CERTSI tras la notificación del incidente es de 30 minutos y las comunicaciones que se esperan de los Operadores Críticos abarcan un amplio compendio de taxonomías al completo, las cuales nos dotan todavía de mayor cantidad de información, con la que detectar, valorar y mitigar determinadas amenazas.