ARI 6/2019
15 de enero de 2019

Hacia la fusión entre la ciberseguridad industrial y los sistemas de información corporativos

Javier Alonso Lecuit | Miembro del Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

Tema

La convergencia entre los sistemas de información y redes de operaciones (OT) que interconectan los distintos elementos de producción en planta y los sistemas de información corporativos (IT) de una industria plantea nuevos retos de ciberseguridad en el contexto de transformación de la industria 4.0.

Resumen

La digitalización de la práctica totalidad de los sectores industriales y la globalización de los modelos de producción son dos catalizadores que hacen inevitable la convergencia en las políticas de seguridad entre los sistemas de información del ámbito OT y los sistemas corporativos IT de las empresas de producción.

En este contexto, la ciberseguridad de los sistemas OT, en particular, se ve comprometida por vulnerabilidades sobrevenidas en un entorno con exigencias de seguridad específicas orientadas a la producción y considerablemente diferenciadas de las exigencias estándares de los sistemas de información corporativos. A ello hay que añadir un escenario de crecientes amenazas de distinta naturaleza, bien intencional o accidental (errores, fraudes, espionaje, sabotaje, causas naturales, etc.), canalizadas en su mayor parte a través del ciberespacio y en no pocas ocasiones dirigidas a perturbar desde terceros países el funcionamiento de las infraestructuras críticas por razones geopolíticas o económicas.

Se evidencia, por tanto, la necesidad de abordar la gestión integral de la ciberseguridad industrial desde los distintos ángulos operativos, legales e institucionales.

Análisis

Industria 4.0, la cuarta revolución industrial

La digitalización ha pasado de ser un elemento relevante en la evolución de los sistemas de automatización industrial a convertirse en el epicentro de una nueva etapa, conocida como industria 4.0 o *smart manufacturing*. Esta cuarta revolución industrial surge de la convergencia entre la globalización de los modelos de negocio productivos y la confluencia de varios habilitadores tecnológicos explicados más adelante. Es una transformación de tintes disruptivos que viene caracterizada por la unión entre el mundo físico y el digital, un escenario global donde se diluyen conceptos tradicionales como fronteras geográficas, cadenas de valor, sectores, empresas o la propia distinción entre producto y servicio.

La digitalización industrial, además de constituir un reto para los actuales modelos productivos, proporcionará nuevas oportunidades de crecimiento económico, así como mejoras sustanciales a la competitividad, flexibilidad y eficiencia de los procesos de producción industrial. La integración de la tecnología de la información se traducirá en la optimización e interacción de los procesos de investigación y desarrollo, diseño, producción, logística y prestación de servicios asociados.

En el actual marco de competencia económica de ámbito mundial, las organizaciones habrán de participar en las cadenas de valor de sus respectivos sectores respaldadas por su aportación singular, especialización, diferenciación tecnológica y excelencia, con casi total independencia de su tamaño y emplazamiento geográfico. Tendrán que evolucionar hacia una oferta de productos personalizados y contar con una oferta de servicios y soluciones industriales para la obtención de un ingreso recurrente por uso –transformación conocida por *servitización*– que sustituirá al actual modelo transaccional basado en la venta de mercancías.

La Revolución Industrial 4.0 es posible gracias a la concurrencia de varias tecnologías habilitadoras. Entre ellas cabe señalar la conectividad entre los centros de producción industrial de una misma cadena de valor y los servicios en la nube a través de redes de alta velocidad y capacidad (fibra y 5G); el Internet de las Cosas de uso Industrial (IIoT), que comunica mediante redes inalámbricas e Internet los sensores y actuadores industriales instalados en emplazamientos remotos con la red OT y que proporciona inteligencia autónoma a los procesos; los servicios en la nube que ofrecen recursos de computación, aplicaciones y capacidad de almacenamiento bajo demanda a través de Internet con gran flexibilidad y escalabilidad a coste variable a toda empresa con independencia de su tamaño o emplazamiento, y la generalización de técnicas de fabricación aditiva, que flexibilizan e individualizan la producción de elementos.

Las tecnologías *Big Data* permiten analizar un amplio abanico de información, desde las preferencias de los clientes a los ajustes de la producción, según las predicciones analizadas o el mantenimiento predictivo de equipos. El “gobierno del dato” es, por lo tanto, la base sobre la que se sustenta la nueva economía digital. La globalización de mercados, la proliferación exponencial de equipos y sensores interconectados que generan datos constantemente, la intensa actividad *online* de los usuarios y, en general, el conjunto de las actividades económicas englobadas bajo la economía digital genera volúmenes de datos que los sistemas tradicionales de análisis, tratamiento y gestión de bases de datos no son capaces de manejar. El uso de la inteligencia artificial en el análisis de la información, en la actuación de los sistemas robotizados de producción o en las aplicaciones de realidad aumentada permite redefinir los procesos industriales y mejorar la competitividad de la producción.

De esta manera, adquiere una particular relevancia la adopción de especificaciones, estándares y buenas prácticas, así como una regulación que facilite la transferencia y uso de la información entre los distintos agentes privados, instituciones públicas y Estados con las adecuadas garantías legales en materia de privacidad, confidencialidad o protección de propiedad intelectual e industrial. En el mismo sentido, la seguridad de los datos y de los sistemas de información en la esfera de las industrias y de las redes públicas de comunicaciones electrónicas e Internet es una prioridad estratégica en los

ámbitos privado y público, en particular en lo relativo a la protección de las infraestructuras críticas de los Estados. Las vulnerabilidades de los agentes productivos y las amenazas en materia de ciberseguridad industrial pueden tener importantes efectos tanto en la seguridad como en la economía, sean públicas o privadas.

En el campo de la normalización, cabe señalar dos iniciativas de particular relevancia. La primera es la Especificación UNE 0060:2018: "Industria 4.0. Sistema de gestión para la digitalización. Requisitos", de septiembre de 2018, resultado de la colaboración público-privada para favorecer la digitalización de las organizaciones industriales mediante un sistema adecuado de gestión (abordar de partida una digitalización total puede ser excesivamente ambicioso y, posiblemente, contraproducente para la industria, tanto por motivos presupuestarios como organizativos)[1]. Así, la especificación se centra en aquellos procesos de negocio que tienen un impacto significativo en los ingresos, costes o experiencia de los clientes y de los que es esperable un mayor retorno proveniente de su transformación digital. Establece cuatro procesos básicos obligatorios que incluir en la planificación del proceso de digitalización de toda empresa: el diseño de productos/servicios, la fabricación, la logística y distribución y las relaciones con el cliente. La especificación señala 91 requisitos para que una industria de cualquier tamaño y actividad pueda ser considerada industria digital, agrupados en los siguientes campos: liderazgo, planificación, infraestructuras, competencia, talento, capital humano, innovación y seguridad de la información. La especificación incluye en particular requisitos sobre ciberseguridad destinados a garantizar la existencia de los controles, infraestructura y formación del personal adecuados para interactuar en el mundo digital de forma segura.

La segunda iniciativa es la contribución liderada por los organismos internacionales de normalización (International Standardisation Organisation, ISO e International Electrotechnical Commission, IEC) y sus miembros nacionales (Asociación Española de Normalización, UNE) en torno a la normalización en las áreas clave para la implantación de la industria 4.0, principalmente los habilitadores tecnológicos y su imprescindible interoperatividad. En paralelo, UNE ha establecido el Foro UNE "Estándares para la Industria Conectada 4.0".

A nivel internacional, actualmente existen 68 comités técnicos de normalización que abordan los distintos aspectos de la industria 4.0, con más de 100 normas aprobadas o en curso. Entre las áreas clave figura la ciberseguridad, para la cual el comité técnico ISO/TC 292/WG 2 elabora los estándares sobre continuidad y resiliencia; el comité ISO/IEC JTC 1/SC 27, sobre técnicas de seguridad para tecnologías de la información, y el comité IEC/SC 65C/WG13, sobre redes industriales (series IEC 61158 e IEC 61784). El grupo de trabajo ISO/IEC JTC 1/WG 10 elabora modelos de referencia para aplicaciones del IoT y el ISO/IEC JTC 1/WG 7 se centra en la interoperatividad de redes de sensores IoT. Otras áreas clave son la estandarización y arquitectura de referencia del *Big Data* (ISO/IEC JTC 1/WG 9); la impresión 3D y la fabricación aditiva (ISO TC

[1] José Antonio Jiménez, "Digitalización industrial, un reto inaplazable", *UNE. La revista de la normalización española*, n.º 8, septiembre de 2018, https://revista.une.org/8/digitalizacion-industrial-un-reto-inaplazable.html.

261 y CEN/TC 438); la robótica avanzada (ISO/10218 e ISO/TS 15066), o la computación en la nube y las plataformas distribuidas (ISO/IEC JTC 1/SC 38).

El tercer elemento impulsor de la industria 4.0, no menos importante, es el apoyo coordinado de las instituciones académicas y gubernamentales y autoridades regulatorias. En particular, son de obligada referencia las iniciativas emprendidas por la Comisión Europea y por el Ministerio de Industria con los programas Industria Conectada 4.0, Activa Industria 4.0 o 12 retos de la industria 4.0. En el ámbito autonómico hay que citar, entre otros, el programa de internacionalización emprendido por el gobierno vasco con el Grupo SPRI en torno a la iniciativa Basque Industry 4.0 Innovation Hub o el International Advanced Manufacturing 3D HUB (IAM 3D Hub) de Cataluña.

Convergencia de la ciberseguridad OT e IT

Simultáneamente al proceso de transformación de la industria 4.0, el mundo de la ciberseguridad OT presenta notables vulnerabilidades que afectan a las redes de información y a los sistemas de las plantas de producción al no estar estas diseñadas para interconectarse con redes externas a la empresa a través de Internet o con múltiples dispositivos inalámbricos. La remotización en la supervisión de la maquinaria llevada a cabo por sus suministradores (mantenimiento proactivo por diseño), la variedad y número de dispositivos inalámbricos IIoT o la obsolescencia de sistemas operativos son tan solo algunos ejemplos que revelan el alcance de estas vulnerabilidades, con el añadido de un escenario internacional caracterizado por crecientes amenazas de ciberseguridad en el ámbito industrial, particularmente en las infraestructuras críticas.

En consecuencia, y con independencia del grado de participación que las compañías decidan asumir en la cuarta revolución industrial para la transformación de sus modelos de negocio, han de resolver previamente las vulnerabilidades en materia de ciberseguridad OT (en la actualidad, gran número de instalaciones industriales carecen de mecanismos para realizar una gestión eficaz de la ciberseguridad OT) y, por ende, enfrentarse a la tesitura de iniciar una convergencia organizativa y técnica con el ámbito del IT corporativo. Esta convergencia viene dada por la necesidad de afrontar la ciberseguridad de la empresa en un marco de negocio global desde la perspectiva integrada a través de la aplicación de una única política de ciberseguridad acompañada de un plan de inversión y acción.

Como punto de partida en el análisis de la ciberseguridad industrial, es muy importante señalar las notables diferencias que existen entre los entornos OT e IT, diferencias que comprenden desde aspectos organizativos y culturales a características técnicas que a continuación se indican y que son muestra del importante reto que implica conjugar la ciberseguridad OT e IT en la empresa. En efecto, desde el punto de vista cultural y organizativo, el responsable de la planta de producción es habitualmente un ingeniero industrial especializado, garante de los procesos y sistemas instalados en la planta industrial de la empresa, a diferencia del responsable de la infraestructura de información corporativa IT, persona de perfil informático a cargo de los sistemas, redes e información corporativa. La carencia de una cultura de ciberseguridad en los entornos

industriales dificulta que las personas implicadas en el entorno OT puedan gestionar proactivamente la ciberseguridad de la planta de producción. Por consiguiente, es cada vez más relevante potenciar la colaboración entre los responsables de las áreas de OT e IT en materia de ciberseguridad a pesar de las distintas responsabilidades que estos cargos conllevan.

En lo relativo a los aspectos tecnológicos, la red IP de una empresa de producción se haya habitualmente segmentada en tres subredes de distintas características y diseño. La subred IT es una red corporativa de datos diseñada para entornos transaccionales. La subred OT está destinada para la supervisión de los procesos y la operación de la maquinaria de producción. Una tercera subred conocida como DMZ industrial o 'zona industrial desmilitarizada', intermedia entre la subred IT y la subred OT, evita el tráfico directo entre ambas por motivos de seguridad y facilita el intercambio de información y el uso de aplicaciones comunes a las dos redes para llevar a cabo la gestión y administración integrada de la producción.

La subred OT está segmenta en 5 niveles con arreglo a las funciones que se realizan en planta (modelo Purdue): la red de campo (nivel 0) conecta los sensores, instrumentación y actuadores de la planta; la red de control (nivel 1) está formada por controladores lógicos programables (*Programmable Logic Controllers*, PLC) y sistemas de control distribuido (*Distributed Control Systems*, DCS); la red de supervisión (nivel 2) está formada por los sistemas SCADA (Supervisión, Control y Adquisición de Datos) y las interconexiones hombre-máquina; la red o sistema de operación de planta (*Manufacturing Execution System*, MES) o nivel 3 se encarga de ejecutar las órdenes de trabajo e instrucciones al operador o de conocer el estado de los procesos; por último, la red de información de planta (*Enterprise Resource Planning*, ERP) está encaminada a la comunicación con el negocio sobre funciones de planificación, inventario, demanda y estado de la producción (nivel 4). Los cuatro niveles inferiores dan servicio a las tecnologías de operación, a diferencia del nivel superior, orientado a tecnologías de la información.

Cabe destacar los sistemas SCADA (nivel 1), elementos cuya seguridad es especialmente relevante en el ámbito de las infraestructuras críticas; comprenden todas aquellas soluciones y aplicaciones que recogen medidas y datos operativos de equipos de control locales y remotos. Los datos se procesan para determinar si los valores están dentro de los niveles de tolerancia y, de ser necesario, tomar medidas correctivas para mantener la estabilidad y el control. ENISA publicó en diciembre de 2013 un libro blanco titulado "Can we learn from SCADA security incidents?", en el que difunde buenas prácticas y actuaciones ante los incidentes de seguridad de los sistemas SCADA en el marco de la seguridad de infraestructuras críticas y las redes y sistemas de información que las soportan (Directiva NIS). Asimismo, ENISA proporciona directrices sobre este importante tema en la guía "Recommendations for Europe on SCADA patching".

Cada nivel de la subred OT se ve afectado por una casuística distinta en materia de ciberseguridad. Por ejemplo, el nivel 0 se dedicará al IoT industrial (IIoT). Este modelo facilita la aplicación de una política integral de defensa en profundidad (*Defence in Depth*, DiD) de la ciberseguridad por capas, en la que los sistemas de control industrial

se sitúan en el núcleo, protegidos por sucesivas capas encargadas de la seguridad de las aplicaciones, la integridad de sistema, la seguridad de la red y la seguridad física.
La comunicación entre sistemas de producción, supervisión y operación en planta tiene requisitos técnicos muy concretos y estrictos, entre ellos los protocolos de comunicaciones en tiempo real, de muy baja latencia y muy alta confiabilidad y resiliencia, y menos exigentes, por ejemplo, en términos de sesiones simultáneas o ancho de banda. Sin embargo, la red IT tiene exigencias casi complementarias; en particular, un elevado número de sesiones simultáneas y ancho de banda, así como menores exigencias en la latencia, calidad del servicio o confiabilidad.

Desde el punto de vista de la seguridad funcional de la planta de producción, centrado en asegurar la fiabilidad y rendimiento de los procesos industriales, priman con creces los objetivos de disponibilidad e integridad OT sobre la confidencialidad. Sin embargo, en la red corporativa IT es prioritaria la confidencialidad e integridad de la información a su disponibilidad.

El ciclo de vida medio de los componentes OT suele ser entre 10 y 20 años; además, cuentan con un reducido número de proveedores específicos de cada sector, lo cual propicia la obsolescencia de sistemas operativos y programas; en el ámbito IT, la vida media se sitúa en torno a los 3 años y cuentan con múltiples proveedores. La actualización de sistemas y parches y el uso de antivirus en entornos OT son poco habituales debido a la criticidad de los sistemas de producción, que pueden quedar afectados por reinicios o paradas e incurrir así en riesgos no asumibles para la producción, como la pérdida de garantía por parte de los proveedores. Esta criticidad y complejidad acelera la obsolescencia de los sistemas y, por lo tanto, la falta de apoyo técnico, a diferencia de las redes IT, donde las actualizaciones son una práctica habitual, fácil de ejecutar y automatizar.

Otras diferencias relevantes en materia de ciberseguridad entre redes OT e IT son, por ejemplo, la ausencia de políticas de seguridad, la dificultad para realizar auditorías de seguridad en el entorno OT debido a la heterogeneidad de los sistemas, la complejidad de realizar pruebas de penetración sin afectar al funcionamiento de los sistemas, la inexistencia de metodologías estándares o la posibilidad de perturbar la producción de la fábrica, a diferencia de la aplicación de metodologías de pruebas estándares en redes IT.

La evaluación de riesgos del entorno OT ha sido hasta la fecha ocasional (salvo si es obligada por la regulación, como en el caso de la protección de infraestructuras críticas) frente al ámbito IT donde es habitual y, además, cuenta con un presupuesto de ciberseguridad. Ante incidentes, la aplicación de análisis forense es poco habitual en redes OT –salvo en las redes de las infraestructuras críticas–, mientras que es más fácil de desplegar en una red IT. La normativa de la seguridad IT se apoya en estándares genéricos sobre seguridad de la información (serie ISO/IEC 27000) –a diferencia de la seguridad de las redes OT (estándares ISA 99/IEC 62443) –, a los que hay que añadir la normativa de seguridad industrial específica de cada sector.

De este modo, las vulnerabilidades habituales del entorno OT son fruto de la obsolescencia casi generalizada y la desactualización de los sistemas operativos; el uso

de dispositivos auxiliares IoT inalámbricos en las plantas de producción al margen de la arquitectura y política de seguridad de la compañía (*Shadow OT*), que aumentan la superficie de exposición a los ciberataques y los accesos no autorizados; las prácticas de *bypass* a los sistemas de control del acceso; configuraciones y contraseñas programadas en ocasiones por defecto en el *hardware* o el *firmware* de la maquinaria o cortafuegos con claves preprogramadas, o aplicaciones, protocolos, comunicaciones y métodos de interconexión inseguros, entre otros. En este contexto, es importante señalar que la mayor parte de las vulnerabilidades no son fruto del descuido o la negligencia de los operadores de planta, sino de la ineludible necesidad de mantener en continuo funcionamiento la producción durante largos periodos de tiempo, así como el estratosférico coste de las paradas técnicas.

Algunos vectores de ataque específicos de los entornos OT son el acceso físico para la manipulación de los sensores remotos y controladores programables (PLC) y la interceptación, interferencia o manipulación de la información de los terminales remotos (RTU) a través de accesos inalámbricos *wifi* o GPRS (General Packet Radio Service) en ocasiones llevados a cabo desde drones.

En este sentido, resulta revelador el informe "Annual Assessment Report Industrial Control Systems Cyber Emergency Response Team FY2016", publicado por el ICS-CERT de EEUU, en el que alerta sobre el incremento en número y complejidad de los incidentes sufridos por sistemas de control industrial de infraestructuras críticas durante el año fiscal 2014-2015. Tras analizar 295 intrusiones, el informe recomienda utilizar 7 tácticas que han reducido el porcentaje de incidentes (indicado entre paréntesis): implantar una lista de aplicaciones autorizadas en cada sistema (38%), asegurar una adecuada configuración y gestión de parches (29%), reducir la superficie de exposición a ataques (17%), establecer un entorno defendible (9%), gestionar las autenticaciones de acceso (4%), monitorizar y responder a las intrusiones (2%) e implantar el acceso remoto seguro (1%)[2]. En cuanto a sectores, los más afectados son los sistemas de distribución y tratamiento de agua (43%), energía (17%), transporte (8%), instalaciones gubernamentales (8%), industria química (5%), comunicaciones (4%) e industria crítica (4%).

Las escasas referencias normativas consolidadas que traten, de manera particular, la gestión de la ciberseguridad en los sistemas de automatización y control industrial han motivado el desarrollo de nuevas directrices específicas para la gestión de los riesgos de ciberseguridad de las operaciones y de la información gestionadas por sistemas OT. Con el fin de favorecer la aplicación de las directrices, el Centro de Ciberseguridad Industrial del País Vasco (CCI) ha elaborado una "Guía para el responsable de construir un SGCI (Sistema de Gestión de la Ciberseguridad Industrial)", la cual señala la necesidad de considerar la independencia e integración de los sistemas OT con otros sistemas de gestión ya existentes en la organización, así como la agilidad y operatividad, y potenciar medidas que cubran requisitos de ciberprotección básicos sobre los

[2] Llama la atención que la ejecución de aplicaciones sea el caballo de Troya en las plantas de producción, lo que se explica debido al creciente uso de dispositivos personales (*Bring Your Own Device*, BYOD) y a la intrusión de aplicaciones maliciosas en los sistemas.

sistemas de automatización y control industrial, requisitos que podrán ir ampliándose posteriormente.

Esta guía tiene como referencia los estándares ISO/IEC 27001, ISO/IEC 62443 e ISO/IEC 27002 y establece un marco de actuación en la empresa en los seis dominios:

1. Elaborar una estrategia de ciberseguridad industrial coherente con la estrategia corporativa y en la que se incluyan los fundamentos del negocio, el sistema de gestión, la política y la organización de la ciberseguridad industrial.

2. Adoptar un sistema de gestión de riesgos para analizar los riesgos e identificar activos, vulnerabilidades y amenazas en el ámbito industrial.

3. Fomentar una cultura de la ciberseguridad industrial mediante la selección de medidas de protección, el establecimiento de una normativa de ciberseguridad del personal, la formación y la concienciación.

4. Adoptar medidas de ciberprotección de los datos y la información, seguridad física y del entorno, control de acceso lógico a los sistemas, redes de comunicaciones y relaciones con terceros en el contexto de la automatización industrial.

5. Asegurar la recuperación y continuidad de los sistemas de operación (resiliencia) mediante pruebas y evaluar el impacto sobre ellas de las tecnologías de operación.

6. La implantación, revisión, mejora y sostenibilidad del sistema de gestión de la ciberseguridad industrial (SGCI), es decir, el desarrollo y mantenimiento del SGCI, la gestión documental y el proceso de supervisión y revisión del sistema (auditoría interna, revisión por la dirección, supervisión y mejora).

Resulta obligado hacer referencia a las guías técnicas CCN-STIC SCADA, publicadas por el Centro Criptológico Nacional, y a las directrices emitidas por ENISA: "Communication network dependencies for ICS/SCADA Systems" sobre la dependencia de los sistemas industriales en planta con las redes externas y "Certification of Cyber Security skills of ICS/SCADA profesional" sobre la capacitación y certificación de perfiles profesionales orientados a la ciberseguridad industrial.

En el plano legislativo, son elementos centrales los desarrollos para la protección de las infraestructuras críticas y las medidas destinadas a garantizar la seguridad de las redes y sistemas de información (transposición de la Directiva NIS). También habría que señalar nuevos marcos regulatorios en debate vinculados a los habilitadores tecnológicos; por ejemplo, e-Privacy Regulation, que contempla controvertidos aspectos de implementación sobre la confidencialidad y privacidad de las comunicaciones con dispositivos IoT, o el código de conducta sobre la Inteligencia Artificial ("Draft Ethics guidelines for trustworthy AI").

Conclusiones

La necesidad de establecer una política de ciberseguridad que integre las operaciones industriales OT en planta con los sistemas de información corporativos IT de las empresas de producción viene dada por dos factores concurrentes: por una parte, las notables vulnerabilidades evidenciadas en las redes y sistemas de producción al no estar diseñados para la conexión a través de Internet a sistemas externos a la empresa, y, por otra, la digitalización de los procesos de producción como epicentro de la actual revolución de los modelos productivos (cuarta revolución industrial o industria 4.0).

Con independencia del tamaño de la empresa y su participación en este proceso de transformación, todas ellas han de hacer frente a amenazas globales de ciberseguridad cuyas motivaciones transcienden la seguridad económica a las que se hayan expuestas sus plantas de producción –en particular las infraestructuras críticas, con potenciales impactos en la seguridad nacional–. Para ello, las empresas habrán de adoptar un enfoque holístico e integral de la ciberseguridad OT e IT mediante una política de ciberseguridad acompañada de un plan de inversión e implantación.

Dada la magnitud y complejidad de esta tarea, es altamente aconsejable recurrir a las guías técnicas, estándares y metodologías ofrecidas por los organismos de normalización y autoridades en materia de ciberseguridad industrial para la implantación de un sistema integral de gestión de los riesgos. Por último y no menos importante, es preciso contemplar, en un plano distinto, la ciberseguridad OT en el marco de la revisión, actualmente en curso, de la Estrategia Nacional de Ciberseguridad de 2013.