UN PANORAMA [CASI] GLOBAL DE LAS POLÍTICAS PÚBLICAS Y LA AUTORREGULACIÓN PARA COMBATIR LA FRAGILIDAD DIGITAL EN LA INDUSTRIA

MIGUEL GARCÍA-MENÉNDEZ
iTTi The [Digital] Accountability Think Tank

Independientemente de lo que en cada momento reflejen los medios -en noviembre de 2017 hablaban del declive de la industria manufacturera estadounidense [1], mientras que en enero de 2018 reconocían crecimientos, para el sector, superiores a lo esperado [2]- lo cierto es que para quienquiera que, hoy, se acerque a una disciplina como la Ciberseguridad Industrial y, además, pretenda hacerlo adoptando una perspectiva elevada, distante, amplia, que favorezca la obtención de una visión de conjunto de las necesidades del sector, se hace sensato plantear la siguiente cuestión: ¿habrá [en el futuro cercano] *industria a la que proteger?* Y es que las alarmas saltan en cuanto se analiza la evolución que ha sufrido el ecosistema industrial en las últimas décadas.

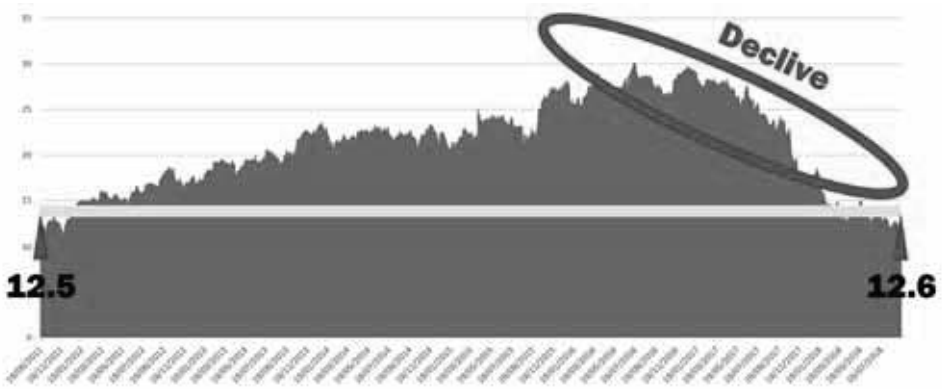
INTRODUCCIÓN: DUDAS Y PRIORIDADES

Un reciente informe de la firma McKinsey [3] deja poco margen para la duda: a) en 1980, en EEUU, la antigüedad promedio del equipamiento de una fábrica era de 7 años, cuando hoy es de 9 años; b) la propia antigüedad de una fábrica estadounidense era, de media, de 16 años en 1980, siendo hoy de 25 años; c) el número de fábricas en EEUU ha caído un 25% en los últimos 20 años; y d) el número de empleos en el sector manufacturero estadounidense se ha visto mermado, en el transcurso de dos décadas, en un 33%. Datos, todos ellos, que describen una situación nada prometedora para la industria actual; pero que, la propia McKinsey estima, podría revertirse con un programa anual de inversiones que la firma valora en torno a los 115.000 millones de dólares/año.

Sería más que razonable pensar que parte de tales inversiones, hoy, podrían tener como destino la transformación digital de la Industria. El vigente paradigma de la «IV Revolución Industrial» en cualquiera de sus acepciones -«industria 4.0», «Internet industrial de las cosas», «industria conectada», «industria o fábrica inteligente», etc.- ocupa, cada día, portadas en la prensa especializada (e, incluso, en la generalista). Las promesas de la transformación digital del sector industrial parecen superar ampliamente sus desafíos y, consecuentemente, quienes han abanderado la corriente digitalizadora en primer lugar -y con aparente éxito- acaban convertidos, habitualmente, en referente para el resto del sector. Tal ha sido el caso de General Electric, cuyos esfuerzos en este terreno han venido siendo ampliamente reconocidos, desde 2011.

El vuelco de General Electric hacia lo digital, su propia consideración como «'LA' (mayúsculas) empresa industrial digital», se ha asentado sobre la creación de una

FIGURA 1
COTIZACIÓN DE LA ACCIÓN DE GENERAL ELECTRIC EN EL PERÍODO 2011-2018 (EN DÓLARES)



Fuente: iTTi (elaboración propia a partir de datos de Yahoo Finance)

serie de nuevas capacidades (adopción masiva de sensores en sus productos, desarrollo de la plataforma software Predix para la Internet industrial de las cosas, modernización de sus procesos internos, etc.) y en la evolución de su modelo de negocio en consonancia con una renovada oferta industrial, conformada por los nuevos productos y servicios digitalizados.

Sin embargo, a pesar de que en el caso de General Electric ciertos beneficios de la transformación comenzaron pronto a hacerse patentes -incluida una mejora en los márgenes-, cabe, en este punto, volver a preguntarse: ¿habrá [en el futuro cercano] *industria, transformada digitalmente, a la que proteger?*

Dicho de otro modo, ¿constituye, el esfuerzo requerido por el proceso digitalizador, garantía suficiente para ver cumplidas las promesas de la transformación? En suma, ¿piensa Ud. que compensa, que las empresas industriales estarán por la labor de hacer esta travesía? ¡Piénselo dos veces!

Las reflexiones que los profesores Thomas H. Davenport (Babson College) y George Westerman (Instituto Tecnológico de Massachussets) recogen en su reciente artículo «Why so many high-profile digital transformations fail?» (¿Por qué fracasan tantas transformaciones digitales de alto perfil?) [4] desvelan la realidad que esconde el caso de General Electric. Como muestra, considere el dato de que la cotización alcanzada por el conglomerado industrial en el momento de escribir estas líneas- septiembre de 2018- está en los mismos niveles de hace siete años -septiembre de 2011-, cuando General Electric comenzaba su viaje transformador. Y ello, véase la figura 1, tras una caída continuada durante, al menos, el último par de años.

Como recuerdan Davenport y Westerman, no todo fueron luces en la transformación digital de General Electric, hasta el punto de que la impaciencia de ciertos accionistas activistas forzó, primero, la renuncia de Jeff Immelt -gran impulsor de la digitalización- como consejero-delegado de la compañía -lo ha sido hasta hace un año-; y, después, la reorientación de su sustituto, John Flannery, hacia la reducción del gasto como eje central de una nueva estrategia corporativa.

Los anteriores párrafos muestran un panorama en el que se hace difícil ubicar la [ciber] seguridad como principal preocupación del sector industrial. Por el contrario, factores como la competencia (por ejemplo, el mayor o menor tirón de los productos propios, frente a los de terceros), las restricciones financieras (derivadas de la coyuntura económica) o el cortoplacismo (materializado, por ejemplo, en la impaciencia de los inversores, como se ha señalado) sí parecen merecer un lugar preferencial, tanto en la lista de prioridades del sector, cuanto en las agendas de los individuos que están al frente del mismo. ¡Unos mimbres, por tanto, con los también habrá de contar quien, como ya se ha dicho, se aproxime a la Ciberseguridad Industrial!

Fragilidad digital

Más allá de las transformaciones fallidas o no satisfactorias, condicionadas por factores como los arriba expuestos, los esfuerzos de digitalización tienen una derivada adicional, relacionada con el señalado nivel de impaciencia de los inversores y podría decirse que, en general, con las «prisas» de los diferentes grupos con intereses en la organización. Una derivada que se traduce en la capacidad de la organización, habilitada por el uso de lo digital, de ofrecer sus productos o servicios, y/o de dar respuestas, de manera ágil.

Cabe presumir, de hecho, que la conversión de la organización en una entidad ágil pasa por ser una de las metas clave del proceso de transformación digital. No obstante, asumir tal afirmación- «¡La digitalización me hace más ágil!»- resultaría en exceso inocente, si uno no fuese, además, consciente de que lo que puede hacerle, en realidad, es más «frágil».

En 2013, los profesores Káganer, Zamora y Sieber de la IESE Business School introdujeron [5] el concepto de «densidad digital» como una consecuencia directa de

FIGURA 2
LISTA, NO EXHAUSTIVA, DE PAÍSES DOTADOS DE UNA ESTRATEGIA (AGENDA) DE CIBERSEGURIDAD

Fuente: ENISA

la corriente digitalizadora: «*Por densidad digital entendemos* -decían- *el número total de personas, cosas y procesos con conexión persistente a Internet en una unidad de actividad social, como una organización, un mercado, un país o el planeta. Con el adjetivo persistente queremos transmitir la idea de que estas conexiones siempre están activadas y facilitan una interacción y transferencia de información sin limitaciones*».

No obstante, quedarse sólo con la imagen de que la creciente densidad digital es fuente de valor para la organización y sus interesados -¡cuanto mayor sea el número de datos conectados [persistentemente], mejor!- conduce, cuando menos, a adquirir una visión muy parcial de la realidad que la transformación digital esconde: sus beneficios son claros, pero también lo son sus peligros. ¡Los riesgos de la aplicación y uso de lo digital son, lamentable y también crecientemente, incuestionables!

De ese modo, el concepto de «fragilidad digital» surge como contrapeso necesario al de la densidad de las conexiones. Sintetizando las palabras del consultor japonés William Saito [6] cabe recordar que la seguridad es un freno para las organizaciones; es el freno que limita la erosión del valor generado por las mismas (una erosión producida como efecto [negativo] del ineludible riesgo digital).

La fragilidad digital es función de la densidad digital; en definitiva, lo es de la creciente dependencia de lo digital que, hoy en día, padecen las «unidades de actividad social» (organizaciones, mercados, países, etc.). Además, la fragilidad digital es, también, función de la falta de conciencia sobre la referida dependencia y sus consecuencias.

Por tanto, cabría definir la fragilidad digital como aquella cualidad de una organización que determina su susceptibilidad a sufrir algún incidente, con origen en «lo digital», que perturbe su actividad (además de provocar otras consecuencias para las personas, el patrimonio o el medioambiente); y de cuya posible materialización no siempre existe conciencia. Una definición que describe con nitidez la coyuntura en la que se encuentran no pocas organizaciones -muchas de ellas, sin duda, del ámbito industrial- y que, consecuentemente, justifica la necesidad de protegerse.

La necesidad de protegerse

Parece evidente que el deseo de procurarse protección ha estado siempre presente -desde que el hombre pisa la faz del planeta- como necesidad primaria, y primitiva, de cualquier individuo, colectivo u organización.

Hasta no hace mucho tiempo, eran las fortalezas de piedra las que contribuían a ofrecer esa protección. El Castillo de San Marcos -en la actualidad, Castillo de San Marcos National Monument y, por tanto, parte del catálogo de infraestructuras críticas de los EEUU-, construido por los españoles en el último tercio del siglo XVII, cumplió ese cometido para los intereses de la corona de España al proteger la ciudad de San Agustín -la más antigua de los EEUU, ubicada en la costa nororiental del actual estado de Florida- de las incursiones realizadas por los británicos. En la otra punta del mundo, también los rusos recurrieron, en el siglo XIX, a las ventajas de una pequeña fortaleza, Fuerte Alejandría, construida en la desembocadura del río Sochi y cuna de la ciudad-balneario homónima, para proteger esa zona de la costa del Mar Negro ante posibles ataques de los circasianos(1).

Hoy en día las amenazas son otras y, de igual modo, son también otros los mecanismos de protección a los que se recurre. Como parte de estos, y ante el nuevo

FIGURA 3
ALCANCE DEL ESTUDIO REALIZADO: 15 PAÍSES

Fuente: iTTi

escenario digital, los países han abandonado la construcción de fortalezas de piedra y están optando por desarrollar políticas públicas que constituyan un primer paso, tanto para ellos, como para sus administrados -empresas y ciudadanos-, en el camino hacia la atenuación de su fragilidad digital.

Una de las materializaciones más habituales de tales políticas son las denominadas «estrategias nacionales de ciberseguridad». Hoy la proporción de estados que disponen de su propia estrategia de ciberseguridad supera ampliamente la relación 1 a 4: más de uno de cada cuatro estados, grandes y pequeños, ya han hecho públicas sus «ciber-agendas» (véase la figura 2); hay otros muchos trabajando en ellas. (Por cierto, para estos últimos vaya la siguiente recomendación: ¡Aprovechen la ocasión y no cometan el error de quienes ya les han precedido, de adjetivarlas como «nacionales»! Las estrategias de ciberseguridad, ni son nacionales -si Ud. observa en detalle cualquiera de ellas, verá, casi con total seguridad, que encierra una aproximación basada en la cooperación internacional para abordar el problema-, ni deberían serlo en un espacio sin fronteras como es el ciberespacio. Reflexione por un momento: ¿estaría Ud. cómodo, teniendo intereses empresariales en un país como la India, en cuya estrategia de ciberseguridad sólo tuviese cabida un enfoque estrictamente nacional/local).

Una perspectiva (casi) global

Durante el ejercicio 2017-2018, desde iTTi se participó activamente en la realización de un estudio [7] cuya motivación ha sido explorar la forma en que un determinado conjunto de países ha abordado -si es que lo han hecho (incógnita cuya resolución se encontraba en el germen mismo del trabajo planteado)- la fragilidad digital de su Industria. Más específicamente, la de los sistemas de control que sustentan los procesos productivos en sus fábricas y demás instalaciones industriales.

Los países elegidos (véase la figura 3) -a priori casi todos europeos, lo que ha determinado el título del informe final (2)- han sido, originalmente: Alemania, Bélgica, España, Francia, Holanda, Italia, Portugal, Reino Unido, Rumanía y Turquía. De igual modo, se consideró oportuno incorporar a Sudáfrica por lo relevante de algunos aspectos de su realidad corporativa. Posteriormente, la lista quedaría ampliada con la inclusión de China, EEUU y Singapur.

Finalmente, Rusia, cuyo análisis no se contempló en un principio, ha recibido, por tal motivo, un tratamiento específico. Ello, y pese a no haber sido incluida en el informe final en el momento de su publicación, no ha impedido identificar algunos hallazgos de interés que han querido recogerse en esta síntesis del informe original.

Esta amplia y variada selección de países ha permitido obtener una visión casi global de las políticas que actualmente imperan, en unas y otras geografías, para combatir la fragilidad digital del macrosector Industria.

¡El reto no ha sido menor! Al elevado número de países que se ha pretendido analizar, ha habido que sumar la gran disparidad idiomática de los mismos y el notable número de documentos revisados. Han llegado a manejarse más de un centenar de fuentes bibliográficas distintas, escritas en más de diez lenguas diferentes.

Aun así, la principal dificultad ha venido de la mano del dinámico comportamiento que se ha observado en la propia legislación. Una legislación tan cambiante -casi en permanente actualización- dificulta, sin duda, un análisis sosegado -las conclusiones obtenidas hoy, pierden su validez mañana, a la luz de un nuevo texto legal-; y dificulta, más si cabe, su adopción y aplicación a quienes son sus destinatarios últimos: los administrados/legislados. Una legislación tan cambiante denota, en definitiva, inmadurez, bien de la legislación misma, bien de la materia que aquella trata de regular.

Bajo estas premisas y dificultades, el análisis realizado ha tratado de abarcar, amén de otros aspectos normativos generales, la doble vertiente de la regulación y la autorregulación; esto es, estrategias nacionales de ciberseguridad, por un lado, y códigos de gobierno corporativo, por otro. De todo ello se hablará en las páginas que siguen.

TABLA 1
ESTRATEGIAS DE CIBERSEGURIDAD IDENTIFICADAS Y ANALIZADAS

País	Estrategia de Ciberseguridad
Alemania	«Estrategia de Ciberseguridad para Alemania 2016» (2016) URL:: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (alemán)
Bélgica	«Estrategia de Ciberseguridad .be: Proteger el Ciberespacio» (2012) URL:: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (francés) «Estrategia de Cibeseguridad para la Defensa» (2014). URL:: https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf (inglés)
China	«Estrategia de Ciberseguridad Nacional» (2016) URL:: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm (chino)
EEUU	«Ciberestrategia Nacional de los Estados Unidos de América» (2018) URL:: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (inglés) «Estrategia de Ciberseguridad del Departamento de Interior de los EEUU» (2018) URL:: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (inglés)
España	«Estrategia de Ciberseguridad Nacional 2013» (2013) URL:: http://www.dsn.gob.es/es/file/146/download?token=KI839vHG (español) «Estrategia de Seguridad Nacional 2017» (2017) URL:: http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf (español)
Francia	«Estrategia Nacional Francesa para la Seguridad del Ámbito Digital» (2015) URL:: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_es.pdf (español)
Holanda	«Agenda de Ciberseguridad Nacional» (2018) URL:: https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/national-cyber-security-agenda/1/National%2BCyber%2BSecurity%2BAgenda.pdf (inglés)
Italia	«Marco Estratégico Nacional para la Seguridad del Ciberespacio» (2013) URL:: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf (inglés) «Plan Nacional para la Protección Cibernética y la Seguridad Informática» (2017) URL:: http://www.governo.it/sites/governo.it/files/piano-nazionale-cyber-2017.pdf (italiano)
Portugal	«Estrategia Nacional de Seguridad del Ciberespacio» (2015) URL:: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Portuguese_National_Cyberspace_Security_Strategy_EN.pdf (inglés)
Reino Unido	«Estrategia de Ciberseguridad Nacional 2016-2021» (2016) URL:: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (inglés)
Rumanía	«Estrategia de Ciberseguridad de Rumanía» (2013) URL:: https://cert.ro/vezi/document/NCSS-Ro (inglés)
Rusia	«Concepto de Estrategia de Ciberseguridad de la Federación Rusa» (2014) URL:: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (ruso) «Doctrina de Seguridad de la Información de la Federación Rusa» (2016) URL:: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 (inglés)
Singapur	«Estrategia de Ciberseguridad de Singapur» (2016) URL:: https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf (inglés)
Sudáfrica	«Marco Normativo de Ciberseguridad Nacional para Sudáfrica» (2015) URL:: https://www.gov.za/sites/default/files/39475_gon609.pdf (inglés)
Turquía	«Estrategia de Ciberseguridad Nacional 2016-2019» (2016) URL:: http://www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf (inglés)

Fuente: iTTi

Análisis de las políticas públicas materializadas en las estrategias de ciberseguridad

Sintetizar aquí el estudio llevado a cabo se antoja una tarea nada sencilla, dadas las comprensibles limitaciones espaciales de esta monografía, y de este artículo en particular. No obstante, a ese fin y con el ánimo de acercar al lector la información más relevante, se ha creído oportuno adoptar una presentación tabular de la información recabada, clasificada y analizada. Ello habrá de servir para facilitar la comparativa entre países y, al mismo tiempo, para extraer las conclusiones más destacadas del análisis ejecutado. Las estrategias de ciberseguridad identificadas y revisadas quedan resumidas en la tabla 1.

Como ya se ha señalado en otro punto de este artículo, hay una clara tendencia -no en todos los países- a utilizar el adjetivo «nacional» para calificar las diferentes estrategias. Y ello, a pesar de la, también clara, vocación internacional de todas ellas, como se explicitará, y del unánime reconocimiento de que la colaboración resulta un elemento clave en el esfuerzo de atajar la fragilidad digital de naciones y organizaciones.

TABLA 2-1
ANÁLISIS DETALLADO DE LAS ESTRATEGIAS DE CIBERSEGURIDAD (1/3)

País	Alemania	Bélgica	China	EEUU	España
Documento	«Estrategia de Ciberseguridad para Alemania 2016»	«Estrategia de Ciberseguridad .be: Proteger el Ciberespacio»	«Estrategia de Ciberseguridad Nacional»	«Ciberestrategia Nacional de los Estados Unidos de América»	«Estrategia de Ciberseguridad Nacional 2013»
Año	2016	2012	2016	2018	2013
Generación	2ª (prev. 2011)	1ª	1ª	5ª (pr. 2003, 2009, 2013, 2017)	1ª
Justificación	enormes oportunidades y potencial	potencial científico y económico	grandes oportunidades económicas, sociales y culturales	prosperidad económica	potencial económico y competitividad
Protección de valores fundamentales, derechos y deberes	Sí	Sí	Sí	Sí	Sí
Responsabilidad / sensibilización de consejeros y directivos	No	No	No	No	Sí (objetivo)
Espíritu internacional	específica (liderazgo)	genérica (cooperación)	específica (cooperación y asistencia)	específica (cooperación)	específica (cooperación)
Promoción del sector ciber local	Sí (fortalecimiento)	Sí (estimulación)	Sí (estimulación [del crecimiento])	Sí (innovación, eliminación de barreras, internacionalización)	Sí (internacionalización)
Normativa de protección de infraestructuras críticas	específica (Ley de Seguridad de las TI de 2015)	especifica (Ley de 1 de julio de 2011 sobre la seguridad y protección de infraestructuras críticas)	específica (Ley de Ciberseguridad)	genérica (se mencionan algunos sectores estratégicos)	genérica (normativas sobre protección de infraestructuras críticas)
Ciberseguridad industrial	genérica (Industrie 4.0)	específica (SCADA / sistemas de control industrial)	específica (sistemas de control automatizados)	-	genérica (sector industrial)
Indicadores	-	-	-	-	-
Presupuesto	-	-	-	-	-

Fuente: iTTi

De igual modo, se hace patente la disparidad idiomática de los documentos analizados. Si bien se ha tratado de acudir prioritariamente a fuentes en inglés -el informe original a que se refiere este artículo fue publicado en dicho idioma-, no siempre ha sido posible. La relativa novedad de algunos de los documentos ha podido contribuir a ello, haciendo que no estén disponibles las traducciones al inglés en el momento en el que se redactan estas líneas; aunque dicha justificación, naturalmente, no aplica en todos los casos. En particular, España es uno de los países no angloparlantes que ofrece una edición de su estrategia en inglés; no obstante, para este artículo ha preferido referenciarse la edición en español. En este mismo sentido, cabe destacar el caso de Francia que ofrece su estrategia en francés, inglés y español, edición que también ha sido de preferencia en esta ocasión.

Tanto en este frente, el de las estrategias de ciberseguridad, como en el de los códigos de gobierno corporativo, de los que se hablará más adelante, se ha tratado de poner la atención en un documento concreto y específico que centralizara la regulación en la materia, en cada país. Sin embargo, en los casos de Bélgica, EEUU, España, Italia y Rusia se identifican, aquí, documentos adicionales por su estrecha relación con el «principal» o porque, de algún modo, lo complementan. Así:

a. en el caso belga se hace referencia de su ciber-estrategia para la Defensa;

TABLA 2-2
ANÁLISIS DETALLADO DE LAS ESTRATEGIAS DE CIBERSEGURIDAD (2/3)

País	Francia	Holanda	Italia	Portugal	Reino Unido
Documento	«Estrategia Nacional Francesa para la Seguridad del Ámbito Digital»	«Agenda de Ciberseguridad Nacional»	«Marco Estratégico Nacional para la Seguridad del Ciberespacio»	«Estrategia Nacional de Seguridad del Ciberespacio»	«Estrategia de Ciberseguridad Nacional 2016-2021»
Año	2015	2018	2013	2015	2016
Generación	1ª	3ª (prev. 2011, 2013)	1ª	1ª	2ª (prev. 2011)
Justificación	prosperidad económica	oportunidad económica	prosperidad	beneficios económicos y sociales	economía e intimidad
Protección de valores fundamentales, derechos y deberes	Sí	Sí	Sí	Sí	Sí
Responsabilidad / sensibilización de consejeros y directivos	No	No	No	No	Sí (plan de puesta en marcha)
Espíritu internacional	específica (cooperación)	específica (cooperación y liderazgo)	específica (cooperación)	específica (cooperación)	específica (asociación y liderazgo)
Promoción del sector cíber local	Sí (promoción e internacionalización)	Sí (certificación, I+D, innovación)	Sí (desarrollo)	Sí (innovación)	Sí (estimulación [del crecimiento, la innovación y la internacionalización])
Normativa de protección de infraestructuras críticas	específica (Ley Nº 2013-1168, de 18 de diciembre de 2013, relativa a la programación militar para los años 2014 a 2019 y que contiene diversas provisiones referidas a la defensa y la seguridad nacional)	específica (Ley de Telecomunicaciones; Ley de Tratamiento de Datos y Obligación de Notificaciones de Ciberseguridad; Ley de Ciberseguridad)	genérica (se menciona, simplemente, la Directiva del Consejo 2008/114/EC, de 8 de diciembre, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección)	genérica (la ciberestrategia no menciona el Decreto-Ley 62/2011)	genérica (adecuado marco normativo; no existía una legislación concreta, específica, sobre protección de infraestructuras críticas en el Reino Unido; en su lugar había diversas políticas públicas)
Ciberseguridad industrial	genérica (accidente industrial / actividad industrial)	-	específica (SCADA / procesos industriales)	genérica (industria)	específica (sistemas de control industrial)
Indicadores	-	-	-	-	Sí
Presupuesto	-	-	-	-	1,9 millardos de libras esterlinas

Fuente: iTTi

b. también se menciona la recientemente publicada -mayo de 2018- ciber-estrategia del Departamento de Interior de los EEUU;

c. en España, se cita la estrategia de seguridad, de 2017, que adelanta algunos aspectos que deberán tener mayor desarrollo en una futura ciber-estrategia (sustituta de la actual, de 2013);

d. en el caso italiano, se ha incluido la reseña al plan de trabajo diseñado para la puesta en marcha de la ciber-estrategia; y,

e. finalmente, en el caso ruso, se ha incluido la última actualización (2016) de su «doctrina» de la seguridad de la información, en tanto que ayuda a enmarcar la propia ciber-estrategia, de 2014.

Las tablas 2-1 a 2-3 resumen el análisis detallado realizado y permiten la comparación de las políticas públicas en materia de ciberseguridad en los quince países estudiados.

Tener identificado, para cada país, el documento que recoge el detalle de su ciber-estrategia, ha permitido

TABLA 2-3
ANÁLISIS DETALLADO DE LAS ESTRATEGIAS DE CIBERSEGURIDAD (3/3)

País	Rumanía	Rusia	Singapur	Sudáfrica	Turquía
Documento	«Estrategia de Ciberseguridad de Rumanía»	«Concepto de Estrategia de Ciberseguridad de la Federación Rusa»	«Estrategia de Ciberseguridad de Singapur»	«Marco Normativo de Ciberseguridad Nacional para Sudáfrica»	«Estrategia de Ciberseguridad Nacional 2016-2019»
Año	2013	2014	2016	2015	2016
Generación	1ª	1ª	1ª	1ª (borrador 2010)	2ª (prev. 2013)
Justificación	innegables beneficios sociales	desarrollo económico y modernización	desarrollo económico y social	crecimiento económico, integración, educación y participación	crecimiento económico y eficiencia
Protección de valores fundamentales, derechos y deberes	Sí	Sí	genérica (crear un ciberespacio seguro para empresas y comunidades)	Sí	Sí
Responsabilidad / sensibilización de consejeros y directivos	No	parcialmente Si (involucrar a las organizaciones empresariales)	parcialmente Sí (hacer de «lo cíber» una prioridad para la empresa, mediante las patronales y las cámaras de comercio)	parcialmente Sí (el papel y la responsabilidad del sector privado)	Sí (acción específica)
Espíritu internacional	específica (cooperación)	específica (cooperación)	específica (asociación)	específica (cooperación)	genérica (capacidad competitiva y cooperación)
Promoción del sector cíber local	No	Sí (apoyo a los productores nacionales, incentivos fiscales, internacionalización)	Sí (impulso al crecimiento, la internacionalización y la innovación)	Sí (promoción del crecimiento, I+D)	No (ecosistema cooperativo, todo lo más)
Normativa de protección de infraestructuras críticas	genérica (estrategia nacional para la protección de infraestructuras críticas; formalmente, Decisión Gubernamental nº 718 de 13 de julio de 2011, que no se menciona)	específica (Información del Consejo de Seguridad del 8 de agosto de 2013)	específica (nueva Ley de Ciberseguridad)	genérica (promoción del desarrollo de una estrategia de infraestructuras de información, críticas, nacionales)	específica (Resolución Nº 2, de 20 de junio de 2013, del Consejo de Ciberseguridad)
Ciberseguridad industrial	-	específica (sistemas automatizados)	-	-	-
Indicadores	-	-	-	-	-
Presupuesto	-	se menciona; pero no se detalla	8% del presupuesto TIC del Gobierno (en SG$): 2,4 millardos -> 192 millones	-	-

Fuente: iTTi

desarrollar un análisis basado en los parámetros que se detallan a continuación.

En primer lugar, se ha tenido en cuenta el año de publicación de cada estrategia. Una rápida mirada a las tablas-resumen indica que sólo la estrategia belga (2012) es anterior a 2013, año en que tuvo lugar el paradigmático ciber-incidente de la empresa estadounidense Target [8], que supuso un antes y un después para el mundo corporativo, al menos en algunas geografías. Sorprende, igualmente, que EEUU haya estado sin ciber-estrategia hasta hace tan solo unos días (casi hasta el momento de cerrar la edición de este artículo). Y sorprende por cuanto EEUU fue pionero al publicar su primera estrategia de ciberseguridad en 2003 [9] (revisada en 2009 [10]), adelantándose casi una década al resto de países analizados, cuyas estrategias más antiguas datan de 2011. En su lugar -esto es, en lugar

de disponer de un documento «central» que recogiese su estrategia-, los EEUU han contado hasta este mes de septiembre de 2018 con una serie de fuentes diversas -entre ellas, dos Órdenes Ejecutivas firmadas por los presidentes Obama (2013) [11] y Trump (2017) [12], respectivamente-, que, en conjunto, han conformado las directrices básicas del país en la materia.

Un segundo aspecto analizado ha sido el denominado generación, que hace referencia a la existencia, o no, de versiones anteriores de la estrategia, lo que permite señalar que la ciber-estrategia de un país es de primera generación (no ha habido ninguna anterior), de segunda generación (hay un antecedente), de tercera generación (ha habido dos antecedentes), y así sucesivamente. El interés de este parámetro estriba en que puede interpretarse, en positivo, como una medida de la madurez del país en sus esfuerzos por hacer frente a la fragilidad digital: a priori, no debería merecer la misma consideración el país que únicamente ha redactado (y ejecutado) una estrategia (Bélgica, China, España, Francia, Italia, Portugal, Rumanía, Singapur o Sudáfrica), que el que ya ha pasado por el esfuerzo de elaborar una segunda, incluso, una tercera, etc., habiendo sacado provecho, en el proceso, de las lecciones aprendidas (Alemania, EEUU, Holanda, Reino Unido o Turquía). Un caso particular puede ser el de Rusia, que, si bien no ha publicado más que una edición (2014) de su «concepto» de estrategia de ciberseguridad, tiene una tradición más amplia en relación a su «doctrina» de seguridad de la información, de la que lleva dos ediciones (2000 y 2016).

En el apartado justificación -el porqué de la necesidad de dotarse de una ciberestrategia- hay una coincidencia generalizada en los mensajes, todos los cuales parecen confluir en aspectos como el potencial, la prosperidad o el beneficio económico de «lo digital», como valor a salvaguardar (amén de otros beneficios sociales, culturales, etc.).

La protección de valores fundamentales, derechos y deberes es otro aspecto en el que la coincidencia es prácticamente unánime. Todas las ciber-estrategias analizadas lo citan explícitamente. La excepción, aquí, puede ser Singapur, donde la referencia a este punto se hace de una manera más genérica -no tan explícita-, abogando por un ciberespacio seguro para empresas y comunidades.

La responsabilidad, en materia de rendición de cuentas por el uso de «lo digital» y sus consecuencias, y la sensibilización de consejeros y directivos hacia ese asunto constituye el quinto aspecto al que se le ha prestado atención en la revisión de las ciber-estrategias de los países seleccionados. De ellos, sólo tres contemplan en sus textos, de forma expresa, la figura del consejero y/o del directivo, dedicándoles un espacio en sus objetivos (España), plan de acción (Reino Unido) y acciones específicas (Turquía). Adicionalmente, podría decirse que Rusia, Singapur y Sudáfrica incluyen estas figuras parcial o indirectamente, cuando hablan de involucrar a las organizaciones empresariales, de hacer de «lo cíber» una prioridad para la empresa y de subrayar el papel y responsabilidad del sector privado, respectivamente. [El apartado «Códigos de gobierno corporativo», más adelante, ofrecerá un mayor detalle sobre el papel de los órganos de gobierno de las empresas ante el desafío que supone la fragilidad digital].

El sexto parámetro analizado ha sido el espíritu internacional de las estrategias. A pesar de que mayoritariamente han sido calificadas de «nacionales» -ya se ha comentado-, todas ellas presentan, de forma específica o genérica, una orientación internacional asentada principalmente en el reconocimiento de la necesidad de atajar la fragilidad digital desde una óptica cooperativa.

La promoción del sector «cíber» local/nacional también se ha constituido en punto de interés dentro del análisis realizado. Nuevamente, casi de manera unánime, los países -sus estrategias- recogen la intención de promocionar el sector doméstico de la ciberseguridad mediante su estimulación, desarrollo, crecimiento, fortalecimiento, innovación, internacionalización, etc. Como excepciones, Rumanía no menciona este aspecto en su ciber-estrategia y Turquía apenas hace una referencia al desarrollo de un ecosistema cooperativo.

En octavo lugar, el análisis repara en la mención, o no, que las estrategias de ciberseguridad hacen de la normativa local en materia de protección de infraestructuras críticas. En este punto se hace preciso señalar que el estudio se planteó con una perspectiva europea (no exclusivamente de la Unión Europea) que evolucionó, posteriormente, hacia una perspectiva más internacional. Por tal motivo, el análisis llevado a cabo no ha pretendido hallar, ni llegar a, conclusiones concretas que tuvieran que ver con la Directiva de protección de las redes y los sistemas de información (Directiva NIS) [13]. Cabe insistir, asimismo, en el hecho de que el hilo conductor de esta primera etapa del estudio han sido las estrategias de ciberseguridad (su contenido), la mayoría de las cuales son anteriores a la entrada en vigor de la propia Directiva, motivo por el cual no la citan. Bajo esas premisas, pudo verse que países como Alemania, Bélgica, China, Francia, Holanda, Rusia, Singapur y Turquía sí hacen mención específica, en sus ciber-estrategias, a la normativa legal que en ellos rige -regía a fecha de publicación de las citadas estrategias-, mientras que el resto de los países analizados adopta un lenguaje más genérico. Así, se tiene que:

a. EEUU simplemente enumera algunos sectores estratégicos;

b. España hace referencia a «normativas de protección de infraestructuras críticas», sin citarlas explícitamente;

c. Italia nombra la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008 [14], pero no menciona la normativa local (trasposición);

d. Portugal tampoco menciona su Decreto-Ley 62/2011 [15];

e. Reino Unido habla, simplemente, de un «adecuado marco normativo» (no existía, en el marco legal británico una regulación concreta, específica, en la materia, en el momento en que se publica su ciber-estrategia -2016-);

f. Rumanía cita la estrategia nacional para la protección de infraestructuras críticas, sin mencionar la Decisión Gubernamental nº 718 de 13 de julio de 2011 [16] que recoge formalmente dicha estrategia; y,

g. finalmente, Sudáfrica, en su ciber-estrategia recoge, precisamente, la conveniencia de promover el desarrollo de una estrategia de infraestructuras de información críticas, nacionales.

[NOTA: El marco normativo, en el ámbito de la protección de infraestructuras críticas, para España, Italia, Portugal, Reino Unido y Rumanía (además de para Alemania, Bélgica, Francia y Holanda, citados más arriba) se verá actualizado con la entrada en vigor de las disposiciones recogidas en la Directiva NIS.

Específicamente, a fecha de 9 de mayo de 2018, solamente Alemania, Italia y el Reino Unido habían cumplido con la obligación de trasponer a sus legislaciones locales la Directiva.

En el momento en que se cierra este artículo -septiembre de 2018-, también España y Portugal habían cumplido, ya en tiempo de prórroga, con el requisito de la trasposición.

Según datos de la propia Unión Europea, a la fecha, las trasposiciones de la Directiva NIS en Bélgica, Holanda, Francia y Rumanía reciben la calificación de «en progreso»].

Dado el interés último del estudio, su punto culminante llega, en cierto modo, con el análisis del tratamiento que las distintas ciber-estrategias evaluadas hacen de la ciberseguridad industrial. En este sentido, cabe señalar que ni EEUU, ni Holanda, ni Rumanía, ni Singapur, ni Sudáfrica, ni Turquía la mencionan. (Sorprende el caso de la ciber-estrategia nacional de EEUU, máxime, cuando en la ciber-estrategia de su Dpto. de Interior, publicada sólo cuatro meses antes, en mayo de este mismo año, sí lo hacía). Por su parte, Alemania, España, Francia y Portugal hacen una alusión genérica al mencionar elementos como la *Industrie 4.0*, el sector industrial, los accidentes y/o actividades industriales o la industria en su conjunto. En suma, sólo Bélgica, China, Italia, Reino Unido y Rusia recogen, en sus estrategias de ciberseguridad, referencias directas a los SCADA, a los sistemas de control industrial, a los sistemas automatizados de control o a los procesos industriales.

Sólo la estrategia de ciberseguridad del Reino Unido incluye indicadores para el seguimiento de sus políticas públicas en esta materia; esto es, para el seguimiento del grado de cumplimiento de la propia ciber-estrategia.

Finalmente, con relación al último aspecto analizado, los presupuestos, hay que indicar que, de nuevo, el Reino Unido resulta el país más transparente al recoger en el propio documento la cifra destinada a cubrir la ejecución de su estrategia de ciberseguridad (1,9 millardos de libras esterlinas). Junto a él, Singapur también señala que destinará a este capítulo un 8% de su presupuesto tecnológico, lo que supone un montante de algo menos de 200 millones de dólares singapurenses (de un total de 2,4 millardos). Rusia menciona el término presupuesto; pero no lo detalla.

Análisis de los códigos de gobierno corporativo de las empresas industriales cotizadas

Se ha visto más arriba cómo, hoy en día, el número de países que disponen de una estrategia de ciberseguridad supera la proporción «uno a cuatro» (uno de cada cuatro), a nivel mundial; una proporción que sigue creciendo. Cuesta creer, sin embargo, que esa misma proporción se esté dando en el ámbito corporativo; esto es, cuesta creer que haya un 25% de empresas con algún tipo de estrategia de esta naturaleza. La anterior reflexión invita a plantearse la siguiente pregunta: ¿cuán seriamente se están tomando las empresas la *ciberseguridad*? Las palabras de Dido Hardy, antigua consejera-delegada de la operadora de telefonía móvil Talk Talk, pueden arrojar alguna luz sobre la respuesta.

La operadora británica de telefonía celular Talk Talk fue víctima de su fragilidad digital -sufrió una brecha de seguridad- en el otoño de 2015 [17] (¡no sería la última vez!). Ante la gravedad del asunto y a la vista de la alarma social causada -por los miles de clientes afectados- las autoridades británicas encargaron un informe [18] que fue redactado en el seno de la Comisión de Cultura, Medios y Deportes del parlamento británico. Entre otros interesantes mensajes, el informe del «caso Talk Talk» guardaba el siguiente: «*Aunque la responsabilidad última sobre la ciberseguridad de una empresa recae en su consejero-delegado, resulta altamente inusual que esta persona tenga que dimitir como consecuencia de un ataque*».

Hay que lamentar que los diputados británicos no conociesen el trabajo de investigación que, sobre este particular, ha venido realizando iTTi en los últimos años [19]. Lo cierto es que la realidad -siempre tozuda- desmonta la premisa del informe británico ofreciendo numerosísimos casos (véase la figura 4) de líderes corporativos, de los más variados sectores, cuyas carreras se han visto truncadas, a consecuencia de la fragilidad digital de sus organizaciones (y de la suya propia, en tanto que todos ellos cometieron el error de pensar que «lo digital» no iba con ellos; que no era cosa suya).

Antes de su salida de Talk Talk, anunciada el 1 de febrero de 2017, la Sra. Hardy había dejado unas interesantísimas declaraciones [20]. En primer lugar, señaló: «*… a veces es bueno admitir que uno se equivoca*». A continuación, también declaró lo siguiente: «*Creíamos que estábamos tomándonosla [la ciberseguridad] en serio. Nuestros consultores externos nos decían que nos la estábamos tomando en serio. Ha quedado patente que no era así. Una cosa de la que estoy más convenci-*

FIGURA 4
LIDERAZGOS FRUSTRADOS COMO CONSECUENCIA DE LA FRAGILIDAD DIGITAL

Fuente: De la composición, iTTi. De los retratos originales, sus respectivos autores

da que cualquier otro consejero-delegado británico es que todos y cada uno de nosotros está subestimando la importancia de la ciberseguridad».

Tras la etapa de revisión de las estrategias de ciberseguridad, y a la vista de las palabras de la Sra. Hardy, ha parecido oportuno completar el estudio plurinacional con el análisis de los códigos de gobierno corporativo de las sociedades cotizadas, en los quince países seleccionados. La tabla 3 muestra una relación completa de todos los textos que, finalmente, se han revisado.

Los códigos de gobierno corporativo, amén de otros elementos del marco regulatorio (legislación mercantil, penal, etc.), determinan las directrices por las que han de regirse los órganos de gobierno de las sociedades y, específicamente, sus miembros: consejeros y directivos. Es sobre estos individuos sobre quienes recae, cada día de forma más ineludible, la responsabilidad última, en materia de rendición de cuentas, sobre la adopción y uso de «lo digital»; así como sobre las consecuencias de dicho uso (consecuencias que pueden ser positivas, como las promesas de la transformación digital, hechas realidad; y, no pocas veces, negativas, ligadas a la fragilidad digital de las organizaciones). Explorar el contenido de los citados códigos habrá de ofrecer, necesariamente, alguna pista sobre los porqués de la situación y el tratamiento que hoy recibe la ciberseguridad, desde una perspectiva empresarial.

Como en el caso de las estrategias de ciberseguridad, revisadas más arriba, también aquí se ha partido, para cada país, del documento concreto en el que se recogen las recomendaciones de buen gobierno corporativo que resultan de aplicación a las sociedades que cotizan en los mercados de valores locales (de cada país). Esta presentación de la información, nuevamente de forma tabulada, facilita, una vez más, la extracción de conclusiones y la comparativa entre naciones.

En ese sentido, el primer parámetro que incluye la tabla es el nombre de la entidad emisora del código de gobierno. A pesar del carácter, a priori, meramente informativo de esta columna, puede decirse que ofrece alguna pista sobre la naturaleza -siguiente parámetro- del código.

A lo largo de este artículo se ha venido diferenciando entre regulación y autorregulación; entre medidas regulatorias, asociadas al concepto de políticas públicas, traducidas en forma de estrategias de ciberseguridad, y medidas autorregulatorias, ligando este concepto a los códigos de gobierno corporativo. Esas han sido las dos principales vertientes del análisis que aquí se ha tratado de resumir. No obstante -siempre existen tonos de gris-, lo cierto es que no en todos los casos los códigos de buen gobierno surgen del propio sector, como iniciativas privadas, independientes, etc. En países como China, EEUU, España, Rusia, Singapur y Turquía la naturaleza de los códigos tiene una raíz gubernamental. En las restantes geografías analizadas (Alemania, Bélgica, Francia, Holanda, Italia, Portugal, Reino Unido, Rumanía y Sudáfrica) esa raíz está más cercana al ámbito privado, independiente, corporativo.

El siguiente aspecto analizado guarda relación con la arquitectura del sistema de gobierno que proponen los diferentes códigos. Básicamente se contemplan dos modelos arquitectónicos: uno, en el que el sistema de gobierno gira en torno a un órgano único, el consejo de administración; y otro, en el que, además, se contempla la existencia de un segundo órgano, el comité

supervisor, una línea de defensa adicional que vigila el comportamiento del propio consejo de administración. El modelo de una capa es propio del mundo corporativo anglosajón. El modelo de dos capas tiene una clara influencia alemana, como se puso de manifiesto en el caso de las emisiones Diesel que golpeó al fabricante automovilístico Volkswagen, cuyo comité de supervisión gestionó la salida del consejo de administración de su entonces presidente y consejero-delegado, Martin Winterkorn, quien aparece entre los personajes de la figura 4, más arriba.

Un aspecto relevante es el que determina el siguiente de los parámetros analizados: el marco de cumplimento o marco de conformidad del código de gobierno corporativo. Toda sociedad cotizada ha de adherirse a uno de estos códigos, que será el que rija el funcionamiento de su(-s) órgano(-s) de gobierno. Dicho esto, el criterio para cumplir las directrices recogidas en el propio código suele seguir un principio de voluntariedad, «cumplir o explicar». Esto supone que, si una recomendación no se cumple, bastará con indicarlo y explicar el motivo. Así debe quedar recogido en los informes anuales de gobierno corporativo de dicha sociedad. La excepción en este punto es Sudáfrica, uno de los países más avanzados en materia de gobierno corporativo o, cuando menos, uno de los más pioneros/innovadores, que ha evolucionado su marco de cumplimiento hasta situarse en el principio de «aplicar y explicar». (Naturalmente, también en los EEUU las cosas son distintas, dado que allí la referencia es una ley, la Ley Sarbanes-Oxley de 2002, que, como tal, no cabe sino cumplir -o, si no …-).

Se ha insistido en que la supervisión del riesgo digital es una responsabilidad ineludible de los consejos de administración. En realidad, no sólo la supervisión de este tipo de riesgos, sino la del riesgo en general. Para dar cumplimento a una obligación así, los consejos recurren a ciertas estructuras de apoyo. Son las comisiones del consejo de administración. Como puede observarse, la comisión de auditoría es a la que más habitualmente suele recurrirse. Otras propuestas, según los países, son las comisiones de riesgo, de control interno, de gobierno corporativo o, como ocurre con Turquía, de detección temprana del riesgo.

Finalmente, el estudio culminó evaluando en qué medida se contemplaba «lo cíber» dentro de los códigos de buen gobierno. El resultado no ha podido ser más descorazonador: ¡sólo Holanda, y, de nuevo, Sudáfrica recogen alguna alusión al término «cíber» como parte del contenido de sus códigos de gobierno corporativo! Y ello, como también se subrayó en el apartado dedicado a las ciber-estrategias, a pesar de que casi todos los códigos analizados han sido publicados después del ciber-incidente «Target», que marcó un antes y un después, dadas las consecuencias que acarreó a quien estaba al frente de la compañía. Llegados a este punto, se antoja fácil dar una respuesta a la pregunta planteada inicialmente: ¿cuán seriamente se están tomando las empresas la *ciberseguridad*?. Y ello, incluso sin contar con la amable opinión de la Sra. Hardy.

CONCLUSIONES

En el mundo real, y pese a lo que pueda pensarse o escucharse -esto es, frente a lo que la gente declara públicamente-, la seguridad, incluida la de naturaleza digital, todavía dista mucho de estar entre las principales preocupaciones de quienes están al frente de las organizaciones industriales. Los parámetros que mueven a dichos individuos a la toma de unas u otras decisiones tienen más que ver con aspectos como la coyuntura económica o las presiones de inversores y/o competidores.

Hoy se busca el Santo Grial de la generación de valor en la transformación digital. Se observa una apuesta generalizada por la digitalización, por parte de las organizaciones industriales (y las otras). Una apuesta que puede llegar a tener un punto de irracionalidad, en tanto que: a) no se toma conciencia de que las promesas de la transformación no siempre se cumplen (hay sonoros fracasos que lo atestiguan); y b) tampoco se toma conciencia de que avanzar en el proceso digitalizador supone acrecentar la fragilidad digital, propia y de terceros.

Dado que la fragilidad digital es, cada vez más, una realidad incontestable, la necesidad -el deber- de atenuarla se vuelve ineludible. Las políticas públicas, por vía de la regulación, constituyen un primer paso en el intento de las administraciones de atajar su fragilidad digital y la de sus administrados (empresas y ciudadanos). Sorprende ver cómo a las estrategias de ciberseguridad sigue dándoseles la consideración de «nacionales» (¿acaso locales?), cuando, en realidad, se refieren a un espacio sin fronteras donde todos los países comparten vecindad: el ciberespacio.

Existe la creencia popular de que la legislación -por lenta- siempre va por detrás del desarrollo tecnológico. Contrariamente a esa idea, la realización del estudio a que se ha referido el presente artículo ha enseñado que, en ocasiones, los cambios legislativos se suceden a tal velocidad -presumiblemente, por inmadurez de la propia legislación o de la cosa legislada- que pueden generar, igualmente, problemas -se hacen difíciles de seguir-, tanto para quien pretende analizarlos (a fin de elaborar un informe, por ejemplo), cuanto -y esto es lo grave- para quien ha de conocerlos, entenderlos y aplicarlos (léase, en este caso, los operadores a cargo de instalaciones industriales e infraestructuras críticas).

En línea con lo recogido en el párrafo anterior, el análisis llevado a cabo también ha permitido detectar lo que podría calificarse de síndrome presidencial de «yo-quiero-mi-propia-estrategia». El caso de EEUU -y posiblemente no sea el único- ha resultado paradigmático en ese sentido con una estrategia Bush (2003), una estrategia Obama (2009) y, desde hace unos días, una estrategia Trump (2018). Es lo que podría considerarse «cara B» de lo que, hasta ahora, se había interpretado, en sentido positivo, como un rasgo de madurez de los países que ya han pasado por varias ciber-estrategias -una aparente ventaja frente a los más noveles-. Esta nueva interpretación, no tan positiva, podría contrarrestarse si se atiende al principio de «legislar menos, legislar mejor».

TABLA 3
CÓDIGOS DE GOBIERNO CORPORATIVO IDENTIFICADOS Y ANALIZADOS

País	Código de Gobierno Corporativo
Alemania	«Código de Gobierno Corporativo Alemán» (2017) URL:: http://www.dcgk.de/files/dcgk/usercontent/en/download/code/170214_Code.pdf (inglés)
Bélgica	«El Código Belga de 2009 sobre Gobierno Corporativo» (2009) URL:: https://www.corporategovernancecommittee.be/sites/default/files/generated/files/page/corporategovukcode2009.pdf (inglés)
China	«Código de Gobierno Corporativo para las Empresas Cotizadas en China» (2001) URL:: http://www.ecgi.org/codes/documents/code_en.pdf (inglés)
EEUU	«Ley Sarbanes-Oxley de 2002» (2002) URL:: https://pcaobus.org/About/History/Documents/PDFs/Sarbanes_Oxley_Act_of_2002.pdf (inglés)
España	«Código de Buen Gobierno de las Sociedades Cotizadas» (2015) URL:: https://www.cnmv.es/docportal/publicaciones/codigogov/codigo_buen_gobierno.pdf (español)
Francia	«Código de Gobierno Corporativo de las Sociedades Cotizadas» (2016) URL:: http://www.afep.com/uploads/medias/documents/Corporate_Governance_Code_of_listed_corporations_November_2016.pdf (inglés)
Holanda	«El Código de Gobierno Corporativo Holandés» (2016) URL:: http://www.mccg.nl/download/?download=1&id=3367 (inglés)
Italia	«Código de Gobierno Corporativo» (2015) URL:: https://www.borsaitaliana.it/comitato-corporate-governance/codice/2015engclean.en.pdf (inglés)
Portugal	«Código de Gobierno de las Sociedades» (2017) URL:: https://www.cgov.pt/images/stories/ficheiros/codigo_pt_ebook.pdf
Reino Unido	«El Código de Gobierno Corporativo del Reino Unido» (2016) URL:: https://www.frc.org.uk/getattachment/ca7e94c4-b9a9-49e2-a824-ad76a322873c/UK-Corporate-Governance-Code-April-2016.pdf (inglés)
Rumanía	«Código de Gobierno Corporativo» (2015) URL:: https://www.bvb.ro/info/Rapoarte/Diverse/ENG_Corporate%20Governance%20Code_WEB_revised.pdf (inglés)
Rusia	«Código de Gobierno Corporativo» (2014) URL:: http://www.ecgi.org/codes/documents/final_code_english.pdf (inglés)
Singapur	«Código de Gobierno Corporativo» (2018) URL:: http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Corporate%20Governance%20of%20Listed%20Companies/Code%20of%20Corporate%20Governance%206%20Aug%202018.pdf (inglés)
Sudáfrica	«Informe King sobre Gobierno Corporativo para Sudáfrica 2016» (2016) URL:: https://c.ymcdn.com/sites/www.iodsa.co.za/resource/collection/684B68A7-B768-465C-8214-E3A007F15A5A/IoDSA_King_IV_Report_-_WebVersion.pdf (inglés)
Turquía	«Principios de Gobierno Corporativo» (2014) URL:: http://www.cmb.gov.tr/SiteApps/Teblig/File/479 (inglés)

Fuente: iTTi

A la vista de la atención que les han prestado la mayor parte de las ciber-estrategias analizadas, los consejeros de empresa y los directivos no parecen figurar en las agendas de los legisladores que se han ocupado hasta la fecha de elaborar políticas públicas relacionadas con la fragilidad digital. En ese mismo sentido, tampoco parece que la ciberseguridad industrial, específicamente, se encuentre en dichas agendas.

Podría finalizarse con un «… y viceversa»; esto es, tampoco parece que en las agendas de consejeros y directivos haya anotado nada relativo a la fragilidad digital y su responsabilidad en la materia. Unos consejeros que han de guiarse por unos códigos de buen gobierno corporativo, de obligatoria adhesión; pero cuyas recomendaciones siguen mayoritariamente el principio de «cumplir o explicar», lo que, en la práctica las hace voluntarias para las empresas. ¿Tiene sentido? Y unas empresas en las que la sorpresa viene dada por el sector privado turco, cuyos consejos de administración se apoyan en comisiones de detección temprana de los riesgos -incluidos los de naturaleza digital- a la hora de cumplir con su misión supervisora. ¿No sería deseable que todas las comisiones de riesgo actuasen de esa misma manera, tratando de detectar los riesgos de forma temprana (aunque fuese más allá de las fronteras turcas)?

Cabe, en definitiva, afirmar que no parece que haya nadie, ni en el sector público, ni en el privado, tomándose la ciberseguridad industrial suficientemente en serio.

Un mensaje de esperanza ...

No todo está perdido. En ocasiones la luz se muestra al final del túnel. El 27 de julio de este año los representantes del pueblo de los EEUU, James A. Himes, Thomas J. Rooney, Gregory W. Meeks y Denny Heck presentaron

TABLA 4
ANÁLISIS DETALLADO DE LOS CÓDIGOS DE GOBIERNO CORPORATIVO

País	Documento	Entidad emisora	Naturaleza	Arquitectura	Marco de Cumplimiento	Supervisión del Riesgo	Cíber
Alemania	«Código de Gobierno Corporativo Alemán» (2017)	Comisión Gubernamental del Código de Gobierno Corporativo Alemán.	auto-regulación	2- Capas	cumplir o explicar	Comisión de Auditoría	no-explícita
Bélgica	«El Código Belga de 2009 sobre Gobierno Corporativo» (2009)	Comité de Gobierno Corporativo	auto-regulación	1-Capa	cumplir o explicar	Comisión de Auditoría	no-explícita
China	«Código de Gobierno Corporativo para las Empresas Cotizadas en China» (2001)	Comisíon Reguladora de Valores de China (CSRC)	prom. por el Gobierno	2-Capas	cumplir o explicar	Comisión de Auditoría	no-explícita
EEUU	«Ley Sarbanes-Oxley de 2002» (2002)	Comisión de Valores y Cambio (SEC)	prom. por el Gobierno	1-Capa	cumplir o si no	Comisión de Auditoría	no-explícita
España	«Código de Buen Gobierno de las Sociedades Cotizadas» (2015)	Comisión Nacional del Mercado de Valores (CNMV)	prom. por el Gobierno	1-Capa	cumplir o explicar	Comisión de Auditoría	no-explícita
Francia	«Código de Gobierno Corporativo de las Sociedades Cotizadas» (2016)	AFEP/MEDEF	auto-regulación	1-Capa	cumplir o explicar	Comisión de Auditoría / Comisión de Riesgo	no-explícita
Holanda	«El Código de Gobierno Corporativo Holandés» (2016)	Comité de Supervisión del Código de Gobierno Corporativo (MCCG)	auto-regulación	2-Capas	cumplir o explicar	Comisión de Auditoría / Comisión de Riesgo	explícita
Italia	«Código de Gobierno Corporativo» (2015)	Comisión de Gobierno Corporativo	auto-regulación	ambas	cumplir o explicar	Comisión de Riesgo y Control	no-explícita
Portugal	«Código de Gobierno Corporativo» (2017)	Instituto Portugués de Gobierno Corporativo (IPCG)	auto-regulación	ambas	cumplir o explicar	Consejo Supervisor	no-explícita
Reino Unido	«El Código de Gobierno Corporativo del Reino Unido» (2016)	Consejo de Información Financiera (FRC)	auto-regulación	1-Capa	cumplir o explicar	Comisión de Auditoría / Comisión de Riesgo	no-explícita
Rumanía	«Código de Gobierno Corporativo» (2015)	Bolsa de Bucarés (BVB)	auto-regulación	ambas	cumplir o explicar	Comisión de Auditoría	no-explícita
Rusia	«Código de Gobierno Corporativo» (2014)	Banco de Rusia	prom. por el Gobierno	1-Capa	cumplir o explicar	Comisión de Auditoría / Comisión de Gobierno Corporativo / Comisión de Riesgo	no-explícita
Singapur	«Código de Gobierno Corporativo» (2018)	Autoridad Monetaria de Singapur (MAS)	prom. por el Gobierno	1-Capa	cumplir o explicar	Comisión de Riesgo	no-explícita
Sudáfrica	«Informe King sobre Gobierno Corporativo para Sudáfrica 2016» (2016)	Instituto de Consejeros en el Sur de África (IoDSA)	auto-regulación	1-Capa	aplicar y expliar	Comisión de Riesgo	explícita
Turquía	«Principios de Gobierno Corporativo» (2014)	Comision del Mercado de Capitales (CMB)	prom. por el Gobierno	1-Capa	cumplir o explicar	Comisión de Detección Temprana del Riesgo	no-explícita

Fuente: iTTi

ante la Comisión de Servicios Financieros de la Cámara de Representantes de los EEUU la propuesta de ley H.R.6638, «Cybersecurity Disclosure Act of 2018» (Ley de Información sobre Ciberseguridad de 2018) para promover la transparencia en la supervisión de los riesgos de ciberseguridad en las sociedades cotizadas [21].

La sorpresa fue doble. La propuesta de ley no sólo trataba de elevar el discurso de la ciberseguridad llevándolo a cotas corporativas más altas; sino que, literalmente aludía, a la ciberseguridad industrial, al definir sistema de información (sección 2, apartado a, punto 3.B) como aquel que: «*incluye sistemas de control industrial, tales como los sistemas de control de supervisión y de adquisición de datos, los sistemas de control distribuido y los controladores lógicos programables;*»

Era la tercera vez que se intentaba. Un año antes, el 3 de julio de 2017, habían sido los senadores Jack Reed, Susan M. Collins, Mark R. Warner y John McCain quienes habían presentado, ante el Comité de Banca, Vivienda y Urbanismo del Senado de los EEUU un proyecto de ley, el S.536, «Cybersecurity Disclosure Act of 2017» [22], con idéntica finalidad y contenido. Y año y medio antes, el 17 de diciembre de 2015, los mismos Reed y Collins, la habían presentado como proyecto de ley S.2410, «Cybersecurity Disclosure Act of 2015» [23]. Una insistencia que parece indicar un alto grado de sensibilidad hacia la ciberseguridad [industrial] y la pertinencia de incorporarla a la agenda de los consejos de administración.

NOTAS

[1] El autor se ha tomado la licencia de hacer esta doble referencia al Castillo de San Marcos National Monument, localizado en la ciudad de Saint Augustine (FL, EEUU), y al Fuerte de Alejandría, cuyos restos pueden verse en la ciudad-balneario de Sochi (Rusia) como guiño a las conferencias «S4x18», de Digital Bond, y «KICS», de Kaspersky Lab, celebradas este año 2018 en las ciudades de Miami Beach y Sochi, respectivamente. En ambas tuvo ocasión de presentar los principales hallazgos del estudio a que se refiere el presente artículo.

[2] El informe «European Industrial Cybersecurity Regulatory Landscape. A multi-lateral perspective» (Panorama Regulatorio Europeo de la Ciberseguridad Industrial. Una perspectiva multilateral) fue publicado la pasada primavera por el Centro de Ciberseguridad Industrial, del que el autor ha sido vicepresidente y director de análisis hasta el presente ejercicio.

BIBLIOGRAFÍA

[1] Soergel, Andrew. «*Making Manufacturing Great Again Would Add $530 Billion to GDP*». USNews.com. 20 de noviembre de 2017.

URL (a 2018-06-04): https://www.usnews.com/news/economy/articles/2017-11-20/making-manufacturing-great-again-would-add-530-billion-to-gdp

[2] Yuk, Pan Kwan. «*US manufacturing grows more than expected in December*». Financial Times. 3 de enero de 2018.

URL (a 2018-06-04): https://www.ft.com/content/7ccf058c-afab-327e-abc9-96d5265fb0b8

[3] Ramaswamy, Sree; Manyika, James; Pinkus, Gary; George, Katy; Law, Jonathan; Gambell, Tony y Andrea Serafino. «*Making it in America: Revitalizing US manufacturing*». McKinsey Global Institute. Noviembre de 2017.

URL (a 2018-04-06): https://www.mckinsey.com/featured-insights/americas/making-it-in-america-revitalizing-us-manufacturing

[4] Davenport, Thomas H. y George Westerman. «*Why so many high-profile digital transformations fail?*». Harvard Busines Review. 9 de marzo de 2018.

URL (a 2018-04-06): https://hbr.org/2018/03/why-so-many-high-profile-digital-transformations-fail

Este mismo artículo apareció traducido al castellano, bajo el título «*¿Por qué fracasaron las transformaciones digitales de General Electric y Nike?*» en el número de la «Harvard Business Review en español» publicado el día 3 de septiembre de 2018.

URL (a 2018-09-13): https://hbr.es/modelos-de-negocio/1309/por-qu-fracasaron-las-transformaciones-digitales-de-general-electric-y-nike

[5] Káganer, Evgeny; Zamora, Javier y Sandra Sieber. «*Cinco habilidades del líder digital*». IESE Insight, nº 18. Tercer trimestre de 2013.

URL (a 2018-09-13): https://www.iese.edu/es/conoce-iese/prensa-noticias/noticias/2013/november/cinco-habilidades-lider-digital

[6] García-Menéndez, Miguel y Manolo Palao. «*La Seguridad Digital como freno*». Novática, número 238. Sección «Referencias autorizadas», pág. 62. Noviembre 2016-Febrero 2017.

URL (a 2018-09-13): http://www2.ati.es/novatica/2017/238/Nv238-Digital.pdf

[7] CCI y otros. «*European Industrial Cybersecurity Regulatory Landscape. A multi-lateral perspective*». Centro de Ciberseguridad Industrial. 13 de marzo de 2018.

URL (a 2018-09-13): https://www.cci-es.org/web/cci/detalle-actividad/-/journal_content/56/10694/527184

[8] O'Connor, Clare. «*Target CEO Gregg Steinhafel Resigns In Data Breach Fallout*». Forbes. 5 de mayo de 2014.

URL (a 2018-09-13): https://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/#74dd388d5dfd

[9] Gobierno de los EEUU. «*The National Strategy to Secure Cyberspace*». La Casa Blanca. Febrero de 2003.

URL (a 2018-09-13): https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[10] Gobierno de los EEUU. «*Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communication Infrastructure*». La Casa Blanca. 2009.

URL (a 2018-09-13): https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf

[11] Gobierno de los EEUU. «*Presidential Executive Order, No. 13636, on Improving Critical Infrastructure Cybersecurity*». La Casa Blanca. 12 de febrero de 2013.

URL (a 2018-09-13): https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[12] Gobierno de los EEUU. «*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*». La Casa Blanca. 11 de mayo de 2017.

URL (a 2018-09-13): https://www.whitehouse.gov/presiden-

tial-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[13] Unión Europea. «*Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*». Diario Oficial de la Unión Europea. 19 de julio de 2016.

URL (a 2018-09-13): https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

[14] Unión Europea. «*Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección*». Diario Oficial de la Unión Europea. 23 de diciembre de 2008.

URL (a 2018-09-13): https://publications.europa.eu/en/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10/language-es

[15] Gobierno de Portugal/Ministerio de la Defensa Nacional. «*Decreto-Lei n.º 62/2011, de 9 de Maio*». Diario de la República. 9 de mayo de 2011.

URL (a 2018-09-13): https://dre.pt/application/file/a/286659

[16] Gobierno de Rumanía. «*HOTĂRÂRE nr. 718 din 13 iulie 2011 pentru aprobarea Strategiei naţionale privind protecţia infrastructurilor critice*». Monitorul Oficial. 4 de agosto de 2011.

URL (a 2018-09-13): http://legislatie.just.ro/Public/DetaliiDocument/130566

[17] BBC. «*TalkTalk cyber-attack: Website hit by 'significant' breach*». BBC News. 23 de octubre de 2015.

URL (a 2018-09-13): https://www.bbc.co.uk/news/uk-34611857

[18] Comisión de Cultura, Medios y Deportes. «*Cyber security: Protection of personal data online*». Cámara de los comunes del parlamento británico. 20 de junio de 2016.

URL (a 2018-09-13): https://publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/148.pdf

[19] García-Menéndez, Miguel. «¿Quién se hace cargo?». Novática, número 238. Monografía «Seguridad Digital», pág. 27 y siguientes. Noviembre 2016-Febrero 2017.

URL (a 2018-09-13): http://www2.ati.es/novatica/2017/238/Nv238-27.pdf

[20] Saunders, Andrew. «*TalkTalk boss Dido Harding is stepping down*». Management Today. 1 de febrero de 2017.

URL (a 2018-09-13): https://www.managementtoday.co.uk/talktalk-boss-dido-harding-stepping-down/leadership-lessons/article/1406542

[21] Himes, James A. (patrocinador). «*H.R.6638 – Cybersecurity Disclosure Act of 2018*». Library of Congress. 27 de julio de 2018.

URL (a 2018-09-13): https://www.congress.gov/115/bills/hr6638/BILLS-115hr6638ih.pdf

[22] Reed, Jack (patrocinador). «*S.536 – Cybersecurity Disclosure Act of 2017*». Library of Congress. 3 de julio de 2017.

URL (a 2018-09-13): https://www.congress.gov/115/bills/s536/BILLS-115s536is.pdf

[23] Reed, Jack (patrocinador). «*S.2410 – Cybersecurity Disclosure Act of 2015*». Library of Congress. 17 de diciembre de 2015.

URL (a 2018-09-13): https://www.congress.gov/114/bills/s2410/BILLS-114s2410is.pdf