novática
Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*), representa a España en **IFIP** (*International Federation for Information Processing*) y es miembro de **CLEI** (*Centro Latinoamericano de Estudios de Informática*) y de **CECUA** (*Confederation of European Computer User Associations*). Asimismo tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*) y colabora con diversas asociaciones informáticas españolas.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Gutierre de Cetina 24, 28017 Madrid •Tlfn.914029391 <novatica@ati.es>
Administración y Redacción ATI Cataluña
Calle Ávila 50, 3a planta, local 9, 08005 Barcelona
Tlfn.934125235 <secregen@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <novatica.subscripciones@atinet.es>
Publicidad Gutierre de Cetina 24, 28017 Madrid
Tlnf.914029391 <novatica@ati.es>
Imprenta: Impresión Offset Derra S.L., Llull 41, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: "El guardián" - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

sumario

Nº 238, noviembre 2016 - febrero 2017, año XLII

Monografía del próximo número: "Salud y tecnología"

Miguel García-Menéndez
Socio y Vicepresidente de ATI; Co-fundador y Presidente del Instituto de Tendencias en Tecnología e Innovación (iTTi); Vicepresidente del Centro de Ciberseguridad Industrial (CCI).

<{mgarciamenendez, miguel.garciamenendez}@{ittrendsinstitute, CCI-es}.org>

Presentación. La hora de la seguridad digital

1. La seguridad digital

Permítame iniciar esta monografía de ***Novática*** empleando la primera persona. Con ello pretendo acercarle, en el tono más familiar posible, la que ha sido mi vinculación, desde hace ya un buen número de años, con nuestra revista. Al mismo tiempo, y con igual familiaridad, pretendo recordar a quienes, a lo largo de este tiempo, facilitaron dicha vinculación. En uno u otro sentido todo ello guarda relación con (y está en el germen de) la temática elegida para este nuevo número: la *Seguridad digital*.

Corría el año 2003 cuando, junto a mi buen amigo ***José Fernando Carvajal Vión***, tuve (tuvimos) la oportunidad de participar en la que para nosotros sería la primera monografía de ***Novática***. ¡Seguirían otras! La invitación llegó de la mano del veterano ***Roberto Moya Quiles***, coeditor invitado en aquella ocasión, mientras que las directrices y la supervisión procederían del entonces director de la revista, el maestro ***Rafael Fernández Calvo***. Fernando y yo redactamos conjuntamente un par de artículos, "*Controles para la continuidad de negocio en ISO 17799 y COBIT*" [4] e "*Iniciativas públicas norteamericanas y europeas frente a contingencias en las infraestructuras de información*" [7], que irían destinados al número 166 de la revista, correspondiente a la entrega de noviembre-diciembre de aquel año, bajo el paraguas que ofrecía la monografía "*Planes de Contingencia TIC y continuidad del negocio*" [13], un tema al que (con un lenguaje actualizado) se presta una atención puntual en el especial que aquí les presento.

Hubieron de transcurrir otros diez años hasta que mi mentor, más que amigo, y socio, ***Manolo Palao***, viejo conocido de esta casa y de esta publicación, corresponsable durante largo tiempo de la sección técnica "*Auditoría de los Sistemas de Información y de las Tecnologías de la Información y las Comunicaciones (SITIC)*", convenciese a la dirección de ***Novática***, entonces ya en manos de mi apreciado ***Llorenç Pagès***, de la conveniencia de habilitar un nuevo espacio dedicado al "*Gobierno Corporativo de las Tecnologías de la Información (TI)*", dentro de la sección "*Referencias Autorizadas*" que acompaña habitualmente a cada número de la revista. Yo me convertiría, entonces, en corredactor, junto a Manolo, de la nueva sección técnica. Una tribuna desde la que llevamos casi cuatro años intentando hacer confluir a los *consejos de administración* con *lo digital*. Conceptos ambos que, como a continuación verá, están nuevamente presentes en la base del discurso de varios de los autores invitados al presente monográfico.

¡Y siguieron otras (como les había adelantado)!

La buena experiencia disfrutada con la sección técnica "*Gobierno Corporativo de las TI*", creada en 2013, dio como para plantear de nuevo a Llorenç la elaboración de una monografía homónima, de la que el propio Manolo y yo mismo, junto a nuestra compañera ***Mª José de la Calle***, seríamos editores invitados, y que vería la luz con motivo de la publicación del número 229 de ***Novática*** [8], en noviembre de 2014. Casualmente en esos días se cumplía el primer aniversario del ataque cibernético sufrido por la cadena estadounidense de hipermercados Target [14]; un caso que, a la vista de sus consecuencias, resultaría paradigmático y serviría para que el mensaje de *lo cíber* (y, por extensión el de *lo digital)* comenzase a llegar a los consejos de administración, al menos en la América corporativa.

¡Y siguieron más!

La celebración del XL aniversario de la revista, que tuvo lugar en 2015, constituyó, para mí, la excusa perfecta para darle, por vez primera, un tratamiento específico al tema que hoy ocupa la portada del vigente número. Dadas las particularidades de la ocasión, sería el propio Llorenç, en tanto que Director de ***Novática***, quien, en la primavera del citado año, se encargaría personalmente (de nuevo con el apoyo de Manolo Palao, coeditor invitado) de impulsar una monografía con la que celebrar ese especial cumpleaños de nuestra veterana publicación. La temática y título elegidos para el monográfico, "*Año 2025: El futuro de la Informática*" [6], heredaban el espíritu (y casi el nombre) de una monografía anterior, "*Horizonte 2025*" [12], publicada en 2000 con motivo del XXV aniversario de la revista. Como había ocurrido en el caso de ese aniversario previo, el especial de 2015 era lo suficientemente abierto como para aglutinar un amplio abanico de temas entre los que la seguridad digital parecía encontrar su merecido hueco. Justo es decir, sin embargo, que problemas de agenda me impidieron cubrir, en ese momento, dicho hueco, quedando la publicación final del artículo "*Seguridad digital 2025*" [9], postergada para el número siguiente de la revista, el 235, correspondiente al período enero-marzo de 2016.

Concluido este *periplo* de escritos y temas, y con la referencia reciente de ese último artículo, fue nuevamente Llorenç quien sugirió que, tal vez, había llegado **la hora de la seguridad digital**.

Editor invitado

Miguel García-Menéndez es socio y Vicepresidente de ATI, co-fundador y Presidente del "*think tank*" Instituto de Tendencias en Tecnología e Innovación (iTTi), y Vicepresidente del Centro de Ciberseguridad Industrial (CCI). Ha dedicado más de dos décadas a padecer (y en algún caso, seguramente, a provocar), a asesorar, a estudiar y a divulgar los diferentes problemas ligados al papel de *lo digital* en el seno de los negocios. Antiguo CIO él mismo, en ese tiempo ha tratado de ayudar a otros CIOs (y CISOs) a cumplir con sus obligaciones y a ganar visibilidad dentro de sus respectivas entidades. Hoy sus esfuerzos se centran en concienciar a los líderes corporativos sobre sus responsabilidades en materia de rendición de cuentas en relación al uso que las organizaciones hacen de las tecnologías y a las consecuencias de dicho uso. Pionero del estudio y la divulgación del gobierno corporativo de las tecnologías de la información en España, en 2007 creó "Gobernanza de TI", la bitácora decana, en español, sobre la materia; y en 2011 alumbró la idea de dar vida a iTTi, el primer, y único, centro de análisis español (dotado de vocación internacional) interesado en el papel del directivo en la toma de decisiones sobre el uso de lo digital en las organizaciones. Ha promovido el desarrollo de estas disciplinas en diferentes foros académicos, profesionales y corporativos. Su incorporación a CCI a finales de 2014 ha supuesto, para él, una vuelta a un sector, el industrial, al que dedicó sus primeros años de vida profesional, y a una disciplina, la seguridad digital, que, en realidad, nunca le ha abandonado.

¡Y ahora sigue ésta!

La propuesta de Llorenç pasaba, una vez más, por la elaboración de una nueva monografía (hoy la lee Ud. en la pantalla de su tableta). Sin duda, un atractivo reto al que difícilmente podía negarme. Máxime, cuando por el camino, Llorenç había cedido el testigo a ***Encarna Quesada***, actual Directora de ***Novática***, lo que elevaba el interés del desafío por cuanto suponía abordar el primer monográfico de una nueva etapa para la revista.

2. Pero, ¿por qué *seguridad digital*?

Ya sabe que, a pesar de mis intentos, a lo largo de mi carrera nunca me ha abandonado la seguridad. Circunstancia que me permite afirmar que más de un colega, purista, defendería con uñas y dientes los matices que diferencian las diversas denominaciones que, a lo largo del tiempo, han ido recibiendo las actividades, las técnicas, etc., relacionadas con la mitigación de los peligros asociados al uso (incluido, especialmente, el mal uso) de ordenadores/computadoras y de cuantas otras *cosas* computadorizadas formen parte, ahora o en el futuro, de la actividad diaria de organizaciones e individuos. Me refiero a denominaciones como seguridad informática, seguridad de la información, ciberseguridad, etc.

Por tanto, aunque a algunos se nos antoje innecesario, tal vez se haga oportuno, tras estos primeros minutos hablando de *seguridad digital*, detenerse un momento a reflexionar sobre el título elegido para esta monografía. Permítame, en ese sentido, recuperar algunos de los razonamientos que, al efecto, recogí en el artículo "*Seguridad digital 2025*".

La firma de análisis de mercado Gartner ha aportado, recientemente, su granito de arena al debate y, bajo su programa "*Smarter with Gartner*" (*Más Inteligente con Gartner*), ha abogado por un universo de múltiples *seguridades*: la física; la de las Tecnologías de Operación (TO), propias de los entornos industriales; la de las Tecnologías de la Información (TI), propias de los entornos corporativos; la de la información (a secas); la de la Internet de las Cosas (IoT, del inglés "*Internet of Things*"); o, simplemente, la de naturaleza cibernética. Según la consultora estadounidense, todas ellas quedan, hoy, amparadas bajo el paraguas general que conforma la seguridad digital [2].

Esa creciente toponimia de la seguridad que describe Gartner hace difícil llegar a un consenso; si bien es cierto que pocos se opondrán a identificar *cyber* (ciber) como el prefijo del momento. Sin embargo, va camino de *quemarse*, si no está chamuscado ya en este instante, como también comienzan a señalar otras voces [3]. Piense que propuestas anteriores (el caso de "*InfoSec*" (InfoSeg), por ejemplo, puede servir de paradigma) han tenido también su período de gloria que, sin embargo, parece haber concluido. No obstante, recuerden los nostálgicos (mal de muchos, …) que ese peligro acecha, por igual, a otros términos: *governance* (gobernanza/gobierno) o el propio *digital*, elegido aquí, están amenazados del mismo uso y abuso. (El caso del vocablo *ordenador*, que está cediendo su espacio a cualquier *cosa* conectada, ha quedado, también, explicado).

En cuanto al adjetivo *digital*, si bien ocupa, como acaba de señalarse, las portadas de todo cuanto se publica en estos días en materia tecnológica, parece que aplicado a la seguridad ha disfrutado hasta ahora sólo de un corto recorrido, lo que podría darle, aún, posibilidades de desarrollo futuro. Por eso ha sido el término elegido en esta ocasión.

Incluso la Organización para la Cooperación y el Desarrollo Económico (OCDE) ha optado por hablar de riesgos para la *seguridad digital* en su reciente revisión [11] del texto "*Recomendación del Consejo relativa a las Directrices de la OCDE para la seguridad de los sistemas y las redes de información: Hacia una cultura de la seguridad*", publicado originalmente en 2002. Reconforta saberlo, por cuanto ello parece avalar la apuesta renovadora que se pretende hacer con nuestra revista en esta nueva etapa, de la que, como se ha dicho, la presente monografía constituye su primer hito.

3. Vuelta a lo básico

La apuesta a que hacía referencia el último párrafo está siendo impulsada por ***Encarna Quesada***, a quien ya he presentado más arriba. Su intención de hacer de ***Novática*** una revista más abierta, que respete, pero amplíe con nuevos enfoques, el tradicional perfil academicista de la publicación, ha determinado, en esta ocasión, el carácter impreso a la monografía.

Lejos de plantear el texto técnico, pseudo-científico, al que el tema elegido podría *dar pie y que más de un lector veterano p*udiera esperar, se ha pretendido volver a lo básico, abordando una monografía de naturaleza divulgativa que contribuya a abrir los ojos de diferentes audiencias, ante las consecuencias (negativas) de *lo digital*.

No obstante, aun acotando de esa manera el perímetro, el desafío lanzado no ha resultado menor, por cuanto en él cabe. Por fortuna, no ha sido una aventura en solitario. Una serie de expertos, todos amigos y profesionales reconocidos en materia de seguridad digital, han tenido a bien participar aportando su particular visión, lo que, a buen seguro, encerrará el verdadero valor de este monográfico.

Sin duda, dado el objetivo final de tratar de abrirle a Ud. los ojos, nada mejor que haber tenido la fortuna de contar con la compañía de un experto en ingeniería social, un permanente defensor de la naturaleza socio-técnica de *lo digital*, una periodista galardonada con un premio Emmy, una veterana analista metida a divulgadora tecnológica, un profesor universitario que, además, es Director de Seguridad Digital, y un par de especialistas en Ciberseguridad Industrial. Vaya mi agradecimiento a todos ellos.

Y, ahora, permítame que se los presente; a ellos y a sus escritos.

4. Estructura y contenido de la monografía

El británico ***John McCarthy*** es el primero en romper el hielo con *"El ciberpuzle. Cómo el sentido común puede resolverlo"*, un sugerente título para un artículo en el que comienza describiendo una asilvestrada situación, qué él compara con el *Salvaje Oeste*, para plantear, posteriormente, que los puntos de vista que se han tomado tradicionalmente al hablar de seguridad no siempre resultan de ayuda cuando se trata de este nuevo ámbito, el digital. Como consecuencia, opta por mirar más allá de la tecnología, examinar los problemas desde una perspectiva humana y ofrecerle, como lector, una batería de soluciones sencillas (de sentido común) que le permitan mitigar muchas de las ciberamenazas actuales a las que Ud. se enfrenta. John defiende que no se trata de un problema que uno pueda abordar en solitario, sino que requiere de un nuevo nivel de interacción entre organizaciones; una interacción que habrá de permitir atajar las amenazas de hoy y de mañana. Finalmente, apunta al consejo de administración como responsable último de la seguridad digital, dentro de la organización; pero concluye reconociendo que, en realidad, se trata de una carga compartida, en la que han de participar otros actores destacados como los departamentos de Informática, los de mantenimiento de instalaciones y producción, los de RR.HH., los de contabilidad, la dirección o las autoridades.

Manolo Palao explora, en su *"In medio stat virtus"* (La virtud se encuentra en el punto medio), algunos comportamientos extremos que desvirtúan el referido punto medio (esto es, el equilibrio): la tendencia a reducir la seguridad corporativa a ciberseguridad; el priorizar el *know-how* (saber hacer) ante el *know-what* (saber qué); el

desequilibrio entre Tecnología y Filosofía; la consideración del mundo digital como un paraíso gratuito y sin restricciones ni cargas; la globalización, el gigantismo de las redes y los macroproyectos; la supremacía de la gestión de la organización frente a su buen gobierno corporativo; y la propia necesidad humana de evolucionar ante la evolución del entorno. En suma, a criterio de Manolo, todo se reduce a una llamada de atención sobre los *extremismos* y a la recomendación de huir de los extremos y de los máximos, persiguiendo una áurea mediócritas y unos objetivos *satisfacientes*.

La estadounidense, ganadora de un Emmy, ***Kerry Tomlinson***, plantea la cuestión *"¿Confía Ud. en los cuidados que su médico les dispensa a sus datos personales?"*. Su maestría y veteranía periodísticas quedan reflejadas en este texto que, con formato y ritmo de crónica, va combinando elementos como la entrevista, la narración y los datos. Kerry repasa, con realismo, la historia de un personaje (bautizado como Eric) que acude a una clínica privada y a quien se le presentan una serie de situaciones que le hacen ir perdiendo la confianza que tenía depositada en aquella. A lo largo del relato, la cronista cuenta, además, con las opiniones de una interesante batería de especialistas. El sector elegido por Kerry para situar su acción, el sanitario, no puede resultar más oportuno, dado que la sanidad (pública y privada), en los últimos años, ha sido blanco permanente de los envites de los ciberdelincuentes.

A continuación, ***Mª José de la Calle*** le acerca el mensaje de que la seguridad digital ha alcanzado su mayoría de edad: las noticias sobre incidentes de naturaleza cibernética, y sus causas, abren hoy los telediarios. De ahí que ella hable de *"La nueva '3l1t3' mediática"* (léase, la nueva *élite* mediática), señalando que la seguridad digital alcanza, en la actualidad, una visibilidad, nunca imaginada para una materia tradicionalmente restringida al ámbito profesional. *La* audiencia ampliada, constituida por ciudadanos, empresas (y sus empleados) y administraciones (y sus funcionarios), consigue, de este modo, familiarizarse con una serie de elementos (vulnerabilidades y amenazas) y actores (individuos, bandas organizadas y estados) que, como consecuencia, conforman una suerte de nueva élite mediática. La autora hace, también, un repaso por algunas de las amenazas para la seguridad digital más representativas del panorama actual y, finalmente, plantea provocadoramente la cuestión de la viabilidad de atajar estos problemas; apuntándose, como una de las soluciones clave, a la necesidad de abordar la seguridad digital desde las etapas más tempranas del diseño de productos y servicios.

Permítame, ahora, respetando el orden de los artículos en la monografía, hablarles brevemente de *"Quién se hace cargo"*. Comparto la creencia generalizada de que la seguridad digital es un asunto de todos, como ya adelantaba John; pero me atrevo a pensar que lo es de unos más que de otros [10]. Quienes, tal vez, más intensamente han de asumir el citado asunto como propio son quienes están al frente de las organizaciones. Los consejos de administración y, de forma particular, sus miembros, los consejeros, tienen en su mano la potestad para decidir sobre el devenir de aquellas. También en lo que respecta a lo digital, y sus consecuencias. Esa misma potestad, les ata, al mismo tiempo, a la responsabilidad última en materia de rendición de cuentas sobre las decisiones tomadas (y sobre las que no se llegaron a tomar). Como *prueba empírica* de tal hipótesis, me permito ofrecerle un repaso por los nombres propios más relevantes (todos ellos líderes de primer orden en sus organizaciones) que por uno u otro motivo, siempre con la tecnología de fondo, se vieron obligados a renunciar a sus puestos, en cumplimiento de esa alta responsabilidad antes señalada.

En este punto, el gran divulgador colombiano ***Jeimy Cano***, quien ya compartiera conmigo, generosamente, sus reflexiones para "*Seguridad digital 2025*", habla de *"Alfabetización digital. Desconectando los saberes previos de la junta directiva en clave digital"*. Jeimy vuelve a incidir en el papel de los consejos de administración instándolos a actualizar sus enfoques, de modo que los nuevos les permitan enfrentarse a la vigente realidad digital de sus organizaciones y a la inestabilidad que producen los ataques informáticos sobre las mismas. Jeimy aborda el reto de una alfabetización digital de los veteranos directivos presentes en estos órganos de gobierno, indagando en los saberes previos que han acuñado en su experiencia y efectuando una lectura desde lo digital, donde la incertidumbre, la complejidad y la ambigüedad son parte fundamental para poner de relieve las nuevas capacidades que requieren para tomar decisiones ágiles, así como para afrontar los riesgos de forma inteligente.

Finalmente, mis compañeros al frente del Centro de Ciberseguridad Industrial (CCI), ***Susana Asensio*** y ***Jose Valiente*** abordan el debate ¿seguridad o resiliencia? En ese sentido, cabe, antes de nada, señalar que la seguridad, con todas sus tradicionales (milenarias) connotaciones, es un término demasiado asentado como para que uno pueda temer por su desaparición (a diferencia de lo que, presumiblemente, ocurrirá, más pronto que tarde, con los ejemplos mencionados más arriba). Pero, por encima del debate léxico, lo verdaderamente relevante es que, cada vez más, nos adentramos en una época de total desconfianza. Estamos ante un panorama desalentador en el que ya se oyen algunas voces que comienzan a plantear hasta qué punto merece la pena sumirse en la transformación digital, dadas las penalidades cibernéticas que las organizaciones sufren día tras día [5]. Abusando del tópico, lo cual no lo hace menos cierto, la conclusión pasa por reconocer, una vez más, que la seguridad plena resulta inalcanzable. Y por pensar que, dado que la seguridad nunca será resuelta, a cambio, habrá de ser administrada. Esto se traduce en un cambio de paradigma en el que se está abandonando un enfoque para la seguridad basado en *la prevención y la protección*, para abrazar otro nuevo, fruto de una cierta resignación, que se apoya en *la detección y la corrección* (incluidas la respuesta y la recuperación). ¡Un obligado cambio de modelo que se acentuará en los próximos años!

En ese contexto, toma sentido el objetivo básico por el que ha de moverse toda empresa: perdurar en el tiempo (priorizar cualquier otra meta resultaría absurdo a partir del incumplimiento de esa condición básica). Y, en el escenario descrito, la seguridad se antoja insuficiente como garantía de esa perdurabilidad. En su lugar, el nuevo fetiche se denomina resiliencia [1].

Es la misma tesis que defienden Susana y Jose en su *"En el camino hacia la resiliencia"*, colofón a la monografía. En él, ofrecen una visión del actual contexto digital, con la que ponen de relieve que la adopción de una actitud orientada a garantizar la seguridad digital puede ser un enfoque demasiado tímido. La coyuntura de nuevas tendencias digitales, muy particularmente la vinculada a la disposición de multitud, millones, de dispositivos interconectados de manera autónoma en el espacio de Internet, la *Internet de las Cosas*, hacen pensar que se requiere una aproximación más ambiciosa.

Reparando en el caso concreto del sector industrial, en el que los autores tienen actualmente puestos sus intereses profesionales, el nuevo paradigma de la *Industria 4.0*, como expresión particular de la citada *Internet de las Cosas*, se ha convertido, ya, en el punto de confluencia del mundo digital y del mundo real (el mundo *ciberfísico)*, donde las consecuencias de cualquier incidente de seguridad de naturaleza, en principio, digital, pueden impactar no sólo sobre los sistemas de control industrial, como pieza informática, virtual, sino sobre el patrimonio, el medioambiente y, en última instancia, las personas (el mundo físico).

Esa peculiaridad de las instalaciones industriales, unida a las interdependencias que existen entre ellas e, incluso, con algunas otras que, sin ser industriales, pueden resultar críticas para las sociedades, les lleva finalmente, a plantear la necesidad de un enfoque de resiliencia tecnológica como garantía de salvaguarda última de los actuales ciberecosistemas nacidos al albor de las mencionadas tecnificación e interconectividad. Un enfoque en el que la búsqueda de la resiliencia ha de interpretarse, además, necesariamente, como un esfuerzo común de las empresas y los Estados.

Disfrute de la lectura. Y, por cierto, naturalmente no quiero despedirme sin agradecerle a Ud., también, su interés y su tiempo.

Referencias

[1] A. P. Calder. "Cyber security is no longer sufficient to ensure business sustainability. Cyber resilience should become the new boardroom priority". *@info_CCI, 30 de marzo de 2015.* <https://twitter.com/info_CCI/status/582441048112304128>. Último acceso: 29 de marzo de 2017.

[2] Gartner Inc. "Understanding your new role in Digital Security". *@iTTiresearch, 9 de julio de 2015.* <https://twitter.com/iTTiresearch/status/608295938185170944>. Último acceso: 29 de marzo de 2017.

[3] J. B. Dickson. "We need a new word for cyber". *Dark Reading (DarkReading.com), 23 de noviembre de 2015.* <http://www.darkreading.com/attacks-breaches/we-need-a-new-word-for-cyber/a/d-id/1323278>. Último acceso: 29 de marzo de 2017.

[4] J. F. Carvajal Vión, M. García Menéndez. "Controles para la continuidad de negocio en ISO 17799 y COBIT". *ATI. "Novática", nº 166. Monografía "Planes de Contingencia TIC y continuidad del negocio", noviembre-diciembre de 2003.* <www2.ati.es/novatica/2003/166/nv166sum.html#art15>. Último acceso: 26 de marzo de 2017.

[5] J. Scott. "What are cyber disruptions costing businesses?". *Entrevista a Jason Healy, autor del éxito editorial de 2012 "A Fierce Domain, Cyber Conflict 1986 to 2012" y fundador y miembro "senior" de la Iniciativa de Políticas Cibernéticas del Centro "Brent Scowcroft" sobre Seguridad Internacional, del gabinete de análisis estratégico estadounidense The Atlantic Council. Aparecida en "Agenda" del Foro Económico Mundial. 26 de octubre de 2015.* <https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car>. Último acceso: 29 de marzo de 2017.

[6] L. Pagès, M. Palao. "Presentación. 2015-2025: En la encrucijada de los nuevos tiempos". *ATI. "Novática", nº 234. Monografía especial XL aniversario, "Año 2025: El futuro de la Informática", octubre-diciembre de 2015.* <http://www2.ati.es/novatica/2015/234/Nv234-BloqueEditorial.pdf> Último acceso: 27 de marzo de 2017.

[7] M. García Menéndez, J. F. Carvajal Vión. "Iniciativas públicas norteamericanas y europeas frente a contingencias en las infraestructuras de información". *ATI. "Novática", nº 166. Monografía "Planes de Contingencia TIC y continuidad del negocio", noviembre-diciembre de 2003.* <http://www2.ati.es/novatica/2003/166/nv166sum.html#art27>. Último acceso: 26 de marzo de 2017.

[8] M. García-Menéndez, M. Palao; M. J. de la Calle. "Presentación. Una aproximación multidimensional al gobierno corporativo de las tecnologías de la información". *ATI. "Novática", nº 229. Monografía "Gobierno corporativo de las TI", julio-septiembre de 2014.* <http://www2.ati.es/novatica/2014/229/Nv229-Presentacion.pdf>. Último acceso: 26 de marzo de 2017.

[9] M. García-Menéndez. "Seguridad digital 2025". *ATI. "Novática", nº 235. Secciones técnicas, Seguridad, enero-marzo de 2016.* <http://www2.ati.es/novatica/2016/235/nv235sum.html#art62>. Último acceso: 27 de marzo de 2017.

[10] M. García-Menéndez. "Hacer de la Ciberseguridad (Industrial) un asunto de todos". *Editorial Peldaño. "Cuadernos de Seguridad", nº 138, enero de 2017.* <https://issuu.com/peldano/docs/cuadernos-de-seguridad_318/50?mode=window>. Último acceso: 6 de marzo de 2017.

[11] OCDE. "Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document". *Organización para la Cooperación y el Desarrollo Económico (OCDE), 17 de septiembre de 2015.* <http://www.oecd-ilibrary.org/docserver/download/9315051e.pdf?expires=1449023749&id=id&accname=guest&checksum=C406E2455B393194FCC2F28B988B6A7F>. Último acceso: 29 de marzo de 2017.

[12] R. Fernández Calvo. "Presentación. 2025: Novática cumple 50 años". *ATI. "Novática", nº 145. Monografía especial XXV aniversario, "Horizonte 2025", mayo-junio de 2000.* <http://www2.ati.es/novatica/2000/145/pres145.html>. Último acceso: 27 de marzo de 2017.

[13] R. Moya Quiles, S. Zanero. "Planes de Contingencia TIC: más que tecnología". *ATI. "Novática", nº 166. Monografía "Planes de Contingencia TIC y continuidad del negocio", noviembre-diciembre de 2003.* <http://www2.ati.es/novatica/2003/166/166-3.pdf>. Último acceso: 26 de marzo de 2017.

[14] TARGET. "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores". *TARGET Corporation. Nota de prensa, 19 de diciembre de 2013.* <https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car>. Último acceso: 26 de marzo de 2017.