novática
Revista de la Asociación de Técnicos de Informática
Nº 238, noviembre 2016 - febrero 2017 año XLII

Seguridad digital

Centro de
Ciberseguridad Industrial

UN ECOSISTEMA INTERNACIONAL

para compartir experiencias

CCI es una organización internacional, independiente y sin ánimo de lucro, con más de un millar de miembros en 35 países. Su misión es impulsar y contribuir a la mejora de la ciberseguridad industrial, en un contexto en el que la seguridad de sectores como el de fabricación o el energético juegan un papel crítico para los estados y el bienestar de sus ciudadanos.

info@CCI-es.org www.CCI-es.org B blog.CCI-es.org @info_CCI

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"

La seguridad digital

La vida está llena de retos. Habrá, incluso, quien la defina como un desafío continuo, permanente. Nuestra propia profesión lo es; no en vano, también está irremediablemente ligada al lance de la evolución continua y permanente. Es más, el hecho mismo de expresarlo de ese modo, *la profesión informática*, constituye una bravata. ¿Acaso hay sólo una? (La respuesta no está lejos. Piense en el variado colectivo de profesionales, y de profesiones, que conformamos ATI). Tal vez sería más oportuno hablar de *las profesiones informáticas* o de *las profesiones que habilita (*esto es, que hace posible) *la Informática* (aunque bajo este prisma, hoy serían casi todas). Desde la del tradicional, y ampliamente reconocido por el gran público, *programador informático*, hasta la de los más actuales *científicos de datos*, entre otras, la casuística de profesiones *informáticas* se antoja tan amplia que disculpará Ud. que no las enumeremos todas aquí. ¡Sería una difícil tarea!

La propia *informática*, la palabra, también parece encontrarse hoy en un brete. Quizás haya estudiado Ud. *informática* para acabar trabajando en el sector de las *tecnologías de la i*nformación, TI (o *de la operación*, TO), en lugar de hacerlo en su sector, el informático. O, mejor aún, es posible que haya pasado Ud. de ser un *responsable de informática* a convertirse en un *líder digital*.

¡Cambios, todos ellos, que no traen, sino nuevos retos!

Unos cambios, y sus retos, como los que afronta ahora ***Novática***, nuestra (y, naturalmente, suya) publicación corporativa. Cambios que se inician con la nueva etapa que abre este número 238 que Ud. ya disfruta en la pantalla de su tableta.

Como sabe (se anunció con generosidad), ***Encarna Quesada*** ha relevado, recientemente, a nuestro veterano compañero y amigo ***Llorenç Pagès***, al frente de la revista. Con este cambio llega, también, el momento de dar un nuevo impulso a la cuarentona ***Novática***, como ya hiciera el propio Llorenç una década atrás (aunque, entonces, no pasaba de treintañera). Tal es el compromiso que Encarna ha adquirido con esta JDG y del que preferimos no revelarle a Ud., en este momento, ningún secreto. Nadie mejor que ella misma para que vaya desvelándonos sus iniciativas y novedades a lo largo de las próximas entregas.

No obstante, hay que señalar que a Encarna también le toca recoger la herencia del pasado; una herencia que, a nuestro juicio, es rica y fructífera, y de la que la monografía que da cuerpo al presente número forma parte. Impulsada inicialmente por Llorenç y respaldada, a posteriori, por Encarna, agradecemos que ambos hayan sabido identificar como primer hito de la nueva etapa la relevancia de una temática que hoy concentra los mayores retos a los que se enfrente la disciplina informática: la protección de la actividad de organizaciones e individuos en el ciberespacio. Una temática tampoco exenta de cambios, como prueba el hecho de que la seguridad ya no es informática, sino digital; y en la que los malos han dejado de ser delincuentes informáticos para pasar a ser meros ciberdelincuentes.

Mencionamos, en este punto, al miembro de esta JDG, vocal para la revista y actual vicepresidente, nuestro compañero Miguel García-Menéndez, quien también aceptara el reto de editar un monográfico bajo las anteriores premisas.

A todo ellos y a cuantos autores (de la monografía y de las secciones técnicas) han contribuido a este número, de especial significación por cuanto hemos dicho, nuestro más sincero agradecimiento.

Y recuerde: la de hoy no es más que una primera piedra. Los cambios que Ud. disfrutará en próximas entregas serán resultado de los desafíos que irá superando Encarna. Le deseamos a ella la mayor de las fortunas y le ofrecemos nuestro mayor apoyo, como no puede ser de otro modo.

Entre tanto, permanezca Ud. atento y disfrute de la lectura.

La Junta Directiva General de ATI

en resumen Nuevos tiempos, nuevos aires

Encarna Quesada Ruiz
Coordinación Editorial de ***Novática***

Un día a finales del año 2008 ***Llorenç Pagès Casas*** me llamó y me propuso ser la editora invitada de una monografía de ***Novática*** que saldría a principios de 2009 y que titularíamos *"Web universal, ubicua e inteligente"*. Este fue un punto de partida sin retorno, a partir del cual surgieron más monografías, más colaboraciones, más conversaciones y poco a poco me fui enredando y encandilando con ***Novática*** y su labor. Una labor que considero ha sido extraordinaria, por donde han pasado grandes profesionales que han compartido su experiencia y puntos de vista sobre diversos temas, generando una gran *base de conocimiento,* lista para ser consumida, procesada, analizada y compartida.

A finales del año pasado, Llorenç decide dejar el testigo de la dirección de la revista, después de algo más de diez años de una labor excelente. Surge por lo tanto, la posibilidad de presentar un proyecto editorial para asumir la dirección de ***Novática***. Lo primero que pensé fue *"!Llorenç ha puesto el listón muy alto! Va a ser una labor difícil"*. Y la verdad es que ha sido una larga y estupenda labor la de Llorenç. ¡No se ya cuántos de nosotros se lo hemos dicho! Y es que cuando alguien trabaja como lo ha hecho Llorenç con esta revista hay que reconocerlo, y no puedo más que tragar saliva al pensar que pueda yo tomar las riendas de ***Novática***. Finalmente presenté mi candidatura, centrándome más

en lo que estaba por venir, en los cambios que podría llevar a cabo, que pudieran complementar esta gran labor y hacer más visible la revista por la que tantos profesionales han pasado y van a pasar.

Ahora llego yo, con ganas de, por un lado preservar la labor de un gran profesional y de todos aquellos que han pasado por estas páginas, y por otro lado, traer aires nuevos, con cambios que hagan de esta revista *el lugar* de referencia y que permitan realizar una labor de divulgación.

Hablar de nuevos tiempos significa adaptarnos a una nueva manera de consumir la información pero, desde mi punto de vista, sin perder la calidad e independencia de una revista como ***Novática***. Quiero representar *el cambio*, pero un cambio que empodere la labor que lleva haciendo la revista desde hace tantos años e ir moldeando lo que ofrecemos desde ella a las modificaciones que hay en nuestra sociedad.

En este mi primer número como directora, en el que de forma paralela se ha procedido a realizar el trasvase de quehaceres de la revista, nos centramos en algo de vital importancia y que olvidamos con mucha facilidad, *la seguridad*. Además, teniendo como editor invitado a ***Miguel García-Menéndez***, experto en esta área, que ha conseguido reunir en la monografía opiniones diversas de profesionales a nivel nacional e internacional. ¡No se me ocurre mejor manera de empezar como directora! El objetivo es hacernos reflexionar, cuestionarnos e incluso generar inquietud sobre la idea de que quizá los beneficios que nos otorga un mundo digitalizado nos hagan olvidar lo más esencial de nuestra interacción con ese entorno. A través de esta monografía y de los expertos que han participado en ella podremos ver la importancia de conocer qué sucede con nuestros datos y de que la prevención del ciberdelito es algo en lo que los que están al frente de las organizaciones deben ser parte activa, porque esto es *asunto de todos*.

Y con un tema que es asunto de todos, dejamos al lector con esta primera monografía de una nueva etapa que comienza para ***Novática*** y que abre la puerta a lo que está por venir…nuevos tiempos, nuevos aires.

Noticias de CEPIS

Red sobre temas legales y seguridad CEPIS LSI SIN

Maite Villalba de Benito

Representante de ATI en CEPIS LSI SIN;
Profesora titular y Directora del Máster Universitario en Seguridad TIC de la Universidad Europea de Madrid

<maite.villalba@universidadeuropea.es>

CEPIS (Council of European Professional Informatics Societies) [3] dispone de una red de especial interés en temas legales y de seguridad llamada "CEPIS Legal & Security Issues Special Interest Network" (CEPIS LSI SIN). Dicha red está formada por expertos en legislación relacionada con las Tecnologías de la Información (TI) y temas de seguridad pertenecientes a los miembros de las asociaciones socias de CEPIS, en el caso de España, ATI está representada por nuestra socia Maite Villalba de Benito, profesora titular y directora del Máster Universitario en Seguridad TIC de la Universidad Europea de Madrid. La misión de este grupo de interés es recoger, sincronizar y proporcionar experiencia profesional independiente a las diferentes instituciones y grupos europeos. Entre las actividades que lleva a cabo se incluyen el desarrollo, discusión y promoción de normativa y leyes en el área de las TI y la seguridad TI; proporcionar experiencia y conocimiento a las instituciones europeas o sus participantes, por ejemplo, el Parlamento o la Comisión Europea; y proporcionar experiencia y conocimiento en seguridad en el área de la formación en los proyectos de CEPIS.

La última declaración completa publicada se trata de una recomendación de revisión de las políticas de privacidad de los proveedores de servicio de Internet [1]. Dichas políticas se consideran claramente invasivas de la privacidad de los ciudadanos. Un ejemplo de ello es el de la dependencia de Google como proveedor de servicios de Internet, y en particular de su navegador Chrome. Las posibles consecuencias derivadas del ejercicio por parte de los ciudadanos en la defensa de su privacidad, pueden verse en los hechos recientemente ocurridos con la extensión para bloquear anuncios maliciosos o publicidad no solicitada de AdNauseam que fue eliminada del Google Store en enero de este año aunque sigue disponible aún para Firefox y Ópera [6]. Cada vez más vemos casos similares en los que el ciudadano se ve obligado a aceptar condiciones de privacidad como una especie de devolución de favor a cambio del uso de dichos servicios. Si no quieres quedarte fuera de las últimas tecnologías, por ejemplo, vídeo o televisión online, no parece que haya otro remedio que aceptar los términos que los proveedores de dichos servicios obligan a aceptar antes de poder usarlos. Los usuarios también se ven obligados a aceptar las últimas actualizaciones de los sistemas, apps y servicios,

aunque previamente seamos consultados, finalmente estamos más o menos obligados a aceptarlas, aunque puedan causar graves daños en nuestros sistemas o datos. Después de la actualización, el usuario debe revisar la política de privacidad porque puede haber cambiado aunque no haya sido notificado de ello. Además, cada vez más nos vemos obligados a utilizar estas tecnologías para interactuar con las administraciones públicas. Todo ello, demuestra la dependencia de ciudadanos, empresas y gobiernos de dichos servicios y la necesidad de concienciación general acerca de la obligación de aceptar las políticas de privacidad para usarlos, lo que conlleva a que los ciudadanos no las lean puesto que saben que no les queda otro remedio que aceptarlas para usar el servicio. Tampoco los ciudadanos son informados claramente sobre dónde deben dirigirse en caso de vulneración de sus derechos de privacidad. Esto contradice la Regulación de Protección de Datos Generales (GDRP) [4] en especial con respecto a la recogida de datos personales a gran escala. Varios trabajos han resaltado ya la excesiva recogida de datos por parte de los proveedores de servicios [5], y la Unión Europea ha tomado ya cartas en el asunto. El Grupo de Trabajo 29 sobre protección de datos (conocido como G29 o Art.29 WP) con estatus consultivo en la Unión Europea, envió en julio de 2016, como parte de sus investigaciones sobre Microsoft Windows 10, una nota formal a Microsoft por no cumplir las leyes de protección de datos francesas como aviso previo a posibles acciones legales [2].

Como conclusión del trabajo llevado a cabo por CEPIS LSI SIN, varias recomendaciones fueron enumeradas para poder avanzar hacia una protección de datos robusta y a la vez eficiente, a través de nuevos mecanismos que prevengan la dependencia y hegemonía de las condiciones que los proveedores de servicio incluyen en sus políticas de privacidad. Reforzar la confianza del ciudadano en la protección de sus datos es primordial para el avance tecnológico en la Unión Europea. Para ello, deberían introducirse alcances de protección alternativos a los ya existentes. Dichos mecanismos no deben garantizar sólo la privacidad por diseño, si no también promover la introducción de medidas que impidan la dependencia tecnológica de los ciudadanos, empresas y gobiernos por parte de los proveedores. Para alcanza esto, se requerirá de algún tipo de regulación para los proveedores. Además, la confianza del ciudadano debe reforzarse a través de la transparencia sobre cómo sus datos son tratados por terceros, en concreto por los proveedores de servicios *cloud computing* y de seguridad. Las compañías deberían colaborar para definir un nivel de seguridad razonable frente al ahorro de costes. Entre las alternativas propuestas se encuentran el requerir de un certificado de conformidad como prueba de conformidad con la regulación de protección de datos vigente en la UE; que los grandes proveedores de servicio estén obligados a disponer de una estrategia preventiva con respecto a la protección de privacidad de sus usuarios mucho más elaborada y detallada, y que el usuario pueda seleccionar qué datos está de acuerdo con enviar y cuáles no (cambio al modelo *opt-in* en lugar del *opt-out* actual); o la creación de un grupo independiente de expertos en privacidad TIC que lleve a cabo una inspección independiente obligatoria previa a la publicación de nuevos sistemas operativos, aplicaciones y servicios.

Referencias

[1] CEPIS Legal& Security Issues. "Critical technological dependency requires a revised privacy policy of major service providers". <https://www.cepis.org/media/LSI.Statement.57Council.20161.pdf>.

[2] Commission Nationale de l'Informatique et des Libertés. "Décision n°2016-058 du 30 juin 2016. Décision n° 2016-058 du 30 juin 2016 mettant en demeure la société MICROSOFT CORPORATION". *Julio 2016.* <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000033680640&fastReqId=1173431031&fastPos=4>.

[3] Council of European Professional Informatics Societies (CEPIS). <http://www.cepis.org/>.

[4] European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 27 de Abril 2016.

[5] M. T. Villalba de Benito, M. de Buenaga Rodríguez, D. Gachet Páez, F. Aparicio Galisteo. *Security* **analysis of** *an IoT* **architecture for healthcare**. Lecture Notes of the Institute for Computer Sciences, in Proceedings of the 2nd EAI International Conference on IoT Technologies for HealthCare. Springer International Publishing. Octubre 2015.

[6] ObserverMedia. "Freedom from privacy. Tracking Tricker AdNauseam Removed From the Chrome Store". *Enero 2017.* <http://observer.com/2017/01/adnauseam-google-chrome/>.

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.

El ciberpuzle. Cómo el sentido común puede resolverlo

John McCarthy
Director General de Oxford Systems (Reino Unido)

<john.mccarthy@oxfordsystems.co.uk>

Traducción: Miguel García-Menéndez (Vicepresidente de ATI, editor invitado de la monografía).

Resumen: *A lo largo de este artículo, el autor intenta poner de relieve los problemas a los que, hoy, se enfrenta quien trata de entender las incógnitas que se ciernen en torno a la seguridad digital. Sugiere 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 que le permitan mitigar muchas de las ciberamenazas actuales. Finalmente, 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, que permita atajar las amenazas de hoy y de mañana.*

Palabras clave: *cíber, ciberhigiene, ciudad inteligente, cultura, Internet de las Cosas, IoT, SCADA, seguridad digital,* smart city.

Autor

John McCarthy es una autoridad en estrategia, desarrollo y puesta en marcha de programas de seguridad digital. Obtuvo su doctorado en Ciberseguridad y Desarrollo de Negocios Electrónicos y es un autor reconocido internacionalmente. Entre sus escritos se cuenta una serie de informes académicos que recogen todos los aspectos de la seguridad digital en el mundo moderno. Asimismo, comparte regularmente sus reflexiones, en forma de pequeñas píldoras, que publica como entradas en la bitácora electrónica de Oxford Systems <http://www.oxfordsystems.eu/index.php/blogs>. Es un destacado instructor y experto en buenas prácticas y concienciación en materia de ingeniería social, disciplina sobre la que versará su próximo libro. McCarthy participa frecuentemente como experto invitado en grupos de trabajo y como ponente en reputadas conferencias internacionales de seguridad digital. Colabora en un notable número de destacados comités estadounidenses que prestan asesoramiento y orientación sobre políticas en materia de seguridad digital a la Administración de los EE.UU. Forma parte del grupo de expertos del Comité Estadounidense de Investigación para el Transporte, que está trabajando sobre las mejores prácticas de seguridad digital para los aeropuertos ubicados a lo largo y ancho de los EE.UU. Es un activo miembro del Comité de Seguridad en la Aviación de ACI Europe, la vertiente europea del Consejo Internacional de Aeropuertos; de la Sociedad Informática Británica (BCS, por sus siglas en inglés) y de su foro de liderazgo en Tecnologías de la Información, ELITE; del Comité Internacional de Guerra de la Información y Seguridad; y de la organización no gubernamental londinense "The Worshipful Company of Information Technologists". Además, John ostenta el honor de ser un "Freeman" (Hombre Libre) de la Ciudad de Londres. En la actualidad, el Dr. McCarthy es el Director General de Oxford Systems.

1. El Salvaje Oeste

Se dice a menudo que Internet es una nueva frontera, preparada para ser descubierta y explorada. A veces se aprecia un paralelismo entre el ciberespacio y el Salvaje Oeste. En cierto modo, dicho paralelismo es cierto. Tanto el Salvaje Oeste, como el ciberespacio son dos territorios sin ley, en los que los delincuentes pueden actuar y actúan con impunidad. Muchos colectivos marginados presintieron la libertad del Salvaje Oeste y emigraron a los EE.UU. donde pudieron actuar y comportarse a su antojo. Esos mismos grupos, hoy, pueden estar utilizando Internet como plataforma para sus intereses; unos intereses que podrían no ser bien vistos en cualquier otro lugar.

Tanto Internet como el Salvaje Oeste son dominios carentes, o que carecieron, de censura. Para algunos este espíritu pionero es lo que resulta atractivo; sin embargo, para otros es motivo de preocupación. Una diferencia fundamental es que el Salvaje Oeste era un lugar concreto. Uno viajaba a él o lo evitaba, según su voluntad. Internet no cuenta con una ubicación física específica y, aunque también se la puede probar o evitar, en las economías desarrolladas resulta ubicua. Toca cada aspecto de la vida de la gente [2]. Incluso aunque alguien no la *use*, todo el mundo a su alrededor lo hará, así que no hay escapatoria.

Dicha diferencia no puede obviarse. En el pasado uno podía sentarse en su civilizado hogar y hablar sobre los peligros y depravaciones del Salvaje Oeste, plenamente consciente de que a menos que lo visitase, permanecía seguro. No puede decirse lo mismo de Internet. Sus peligros rodean a todo el mundo, a sus hijos y a sus negocios. A la gente le gusta pensar que Internet es *segura*. Puede ser muy segura y un completo descontrol al mismo tiempo. Es necesario entender esta dicotomía, algo que los gobiernos también se esfuerzan por comprender.

En el Salvaje Oeste, en última instancia, el problema se resolvió ligando la ubicación física y la seguridad. Se llevaron alguaciles y eso permitió tener una idea, más o menos clara, de lo que estaba seguro y protegido. No se puede aplicar esta solución a Internet, dado que no tiene ubicación. Pueden hacerse algunas cosas, por ejemplo, uno puede mantener su propia casa en orden; pero se trata de una solución muy limitada. Se ha creado un mundo donde todo está conectado a todo lo demás: *Internet de las Cosas* (IoT, por sus siglas en inglés) y *Ciudades Inteligentes* (del inglés *smart cities*) son dos expresiones que están de moda, aunque lo cierto es que los conceptos subyacentes son, ya, una realidad. Un débil enlace interconectado se convertirá en el enlace débil de todo el mundo. Mucha gente, simplemente, no está preparada para asumir que la seguridad digital va más allá de las fronteras internacionales o de las legislaciones. Es natural que cada uno reaccione en función de dónde está. Tristemente, esto resulta de poca ayuda en el dominio de *lo cíber*.

2. Proteger la propia casa

Si se es **víctima de un ciberdelito, las opciones de** que atrapen a los delincuentes son muy escasas. Probablemente habrán actuado desde otro país y, por tanto, el sistema legal de protección tendrá que vérselas con las dificultades derivadas de las diferentes jurisdicciones y del propio ciberdelito. Internet no respeta los estados soberanos. Por ejemplo, si enviamos un mensaje de correo electrónico, éste podría recorrer todo el mundo antes de alcanzar su destino; un destino, tal vez, muy cercano. Los protocolos que se utilizan en Internet están diseñados para eso.

A medida que la seguridad digital se va introduciendo en el ideario colectivo, con

> “ Existe la creencia general de que todos los sistemas pueden ser atacados y de que no hay nada a salvo de los atacantes ”

frecuencia, también se contamina por historias glamurosas de atacantes despiadados e inteligentes que han explotado sistemas por valor de millones de dólares. Existe la creencia general de que todos los sistemas pueden ser atacados y de que no hay nada a salvo de los atacantes. En el mundo de lo absoluto, en el que uno tiene en cuenta cada posibilidad, nada está libre de ser atacado. Sin embargo, si aplicase esta forma de pensar a otras áreas de su vida cotidiana, vería que el pensamiento absoluto no siempre ayuda. Consideremos el ejemplo de la puerta de entrada de una casa. Contestemos a la siguiente pregunta, “*¿puede derribarse esa puerta y que la casa sea allanada?*”. La respuesta es un evidente “*sí*”. En las casas se colocan puertas que se consideran suficientemente seguras para el papel que se les encomienda. De ese modo, lo que se hace es adoptar un enfoque de análisis del riesgo para la seguridad del propio domicilio.

Una lógica pragmática como ésta constituye la base sobre la que están construidos muchos sistemas de seguridad digital. Sin embargo, el gran público piensa en términos absolutos cuando trata con los problemas de seguridad digital. Suelen hacerme muchas preguntas. Entre las más habituales está “*¿quién debería responsabilizarse por la seguridad digital de la organización?*”. Una pregunta perfectamente razonable y sensible.

La respuesta fácil no pasará de aquí y es ésta: “*El consejo de administración. Es un asunto que ha de tratarse a nivel de consejo*”. Una gran verdad y, en mi opinión, vital para una evaluación, despliegue y gestión exitosas de la seguridad digital. Las organizaciones necesitan colocar la seguridad digital en sus registros de riesgos y adoptar un marco regulatorio de referencia para administrarla.

Una vez que el consejo de administración haya *comprado* la idea, ¿bastará, simplemente, con entregar la seguridad digital al departamento de Informática? Bien, si eso es todo lo que se va a hacer, será más que factible que surjan problemas. El Departamento de Informática tiene un importante papel que jugar; pero, ¿qué hay del director de las instalaciones? A menudo, se trata de una figura que está a cargo de un montón de sistemas de control, conocidos como SCADA[1], que suelen ser vulnerables a ciberataques. Con certeza, hoy la seguridad digital también forma parte de las atribuciones de este otro perfil.

En muchas organizaciones la gestión de las instalaciones y el Departamento de Informática son entidades distintas y separadas. Unir ambos silos es uno de los desafíos existentes a la hora de desplegar una seguridad digital eficaz. Cómo se logre variará de una organización a otra; pero, en todo caso, requerirá el apoyo del Consejo de Administración.

3. Manipular a la persona

Es un dato conocido que más del 80% de los ciberataques están relacionados con algún tipo de error u omisión por parte de alguna persona [1].

Hagámonos esta pregunta: “*¿Dispone mi departamento de Informática de las destrezas y de la capacidad necesaria para formar a todos los empleados en cómo mitigar los ataques de ingeniería social?*”.

Todo el mundo ha visto en televisión programas sobre timadores y cómo roban dinero a víctimas inocentes. Sin embargo, si hablamos con algún artista del timo (y yo he conocido a unos pocos), siempre dirán que es la misma víctima quien termina siendo presa de su propia codicia. Eso puede ser verdad en ciertos casos en los que trucos así, pensados para vulnerar la confianza de la gente, muestran su eficacia; pero no en la vasta mayoría. En la mayor parte de las ocasiones estos embaucadores se aprovechan del hecho de que uno pueda estar ocupado, distraído o cansado; momento que eligen para actuar.

Esto hace que cualquiera sea susceptible de caer en un engaño de ingeniería social. A la fría luz del día todo el mundo es capaz de reconocer los trucos que emplean los timadores; pero ¿qué hay de un viernes por la tarde, cuando uno ya lleva todo el peso de la semana sobre sus hombros?

Si tenemos prisa tendemos a no concentrarnos tan bien y podemos resultar más vulnerables ante trucos inesperados. Por otro lado, si estás leyendo esto y tienes hijos, seguro que sabes todo lo que hay que saber sobre expertos ingenieros sociales. En resumen, cualquiera puede resultar engañado o persuadido.

Todo el mundo puede estar alerta cuando se le dice que alguien va a engañarlo. Pero, por desgracia, estas cosas no se avisan.

La respuesta a esto parece estar en la creación de una cultura de la seguridad digital que promueva una buena *ciberhigiene*. En ese supuesto, ¿no debería estar incluyéndose una formación básica en seguridad digital en el paquete de bienvenida para cada nuevo empleado? De ese modo, ahora, la seguridad digital amplía su alcance y cae bajo la potestad de RR.HH.

Hablar de Seguridad Digital es similar a hacerlo de Seguridad y Salud Laboral. Es una responsabilidad de todos, aunque algunas áreas juegan un papel y tienen unas obligaciones más complejas que el resto, como el Departamento de Informática. Otro ejemplo es el Departamento Contable, que requiere formación especializada en ingeniería social y un alto nivel de ciberhigiene para mantenerse verdaderamente vigilante. De hecho, todo empleado necesita estar al corriente de la seguridad digital y exhibir una buena ciberhigiene. El que esto comience a ser así, supone que se están empezando a dar pasos hacia una mayor protección de la organización frente a ciberataques. Si se adoptan buenas prácticas de seguridad digital, mediante la formación y la protección de los sistemas, se tendrá la oportunidad de promover esa buena seguridad digital como un activo de la organización. No cabe duda de que la seguridad digital comienza en lo más alto, pero es parte de las obligaciones de cada uno garantizar una buena seguridad. Para decirlo con claridad hay que insistir en que *la responsabilidad es de todos*.

En la era digital el problema de la ingeniería social tiene consecuencias mucho más graves. Ahora uno puede convertirse en una puerta de entrada hacia sistemas informáticos que los ingenieros sociales pueden emplear para desplegar software nocivo, robar información o destruir datos. ¿Por qué harían algo así?

Bien, la ingeniería social es un *oficio* que se mantiene por sí mismo y que ha estado ahí durante siglos; sin embargo, es ahora cuando está siendo usado como un vector de ataque para entrar en los sistemas más seguros. Esto ha provocado que muchos ha-

> “ Hablar de Seguridad Digital es similar a hacerlo de Seguridad y Salud Laboral ”

yan adoptado, junto a otras habituales artes del engaño, técnicas de ingeniería social.

Los delincuentes han sabido reconocer rápidamente que los sistemas informáticos, a pesar de estar protegidos mediante caros y sofisticados sistemas de cortafuegos y de detección de intrusiones, resultan muy fáciles de acceder a través de los humanos que los operan.

4. Crear una cultura de la seguridad digital y promover la ciberhigiene

Las respuestas no están en los sistemas informáticos, sino en la formación del personal para que sea consciente de la existencia de los ingenieros sociales y de los ataques que llevan a cabo. Un entrenamiento de carácter informativo, junto a la creación de una cultura de la seguridad digital y al desarrollo de unas buenas prácticas de ciberhigiene pueden hacer muchísimo en favor de la mitigación de este tipo de amenazas. Una buena cultura y una buena higiene son importantes, dado que refuerzan la formación impartida para mitigar las técnicas de ingeniería social.

Una sencilla ciberhigiene podría evitar muchos de los actuales ataques y problemas. No obstante, la comprensión de cómo se opera en este nuevo entorno es, aún, muy precaria para la mayoría. En otros ámbitos de la vida cotidiana se practica una buena higiene. La gente se lava las manos cuando sale del baño y se cubre cuando estornuda. Es necesario desarrollar prácticas de ciberhigiene similares, dentro y fuera de los lugares de trabajo. Comencemos por ellas. Impliquemos a toda la empresa, comenzando por lo más alto, y hagamos que quienes estén al frente den ejemplo. Se requieren mensajes sencillos sobre buenas prácticas de seguridad digital que todo el mundo, en cualquier nivel de la organización, pueda entender y adoptar.

Una vez se cuente con una buena cultura, todos los departamentos de la compañía entenderán las necesidades de los demás en materia de seguridad digital. Muchos de los obstáculos que se observan hoy en relación con acercar a las partes para resolver problemas de seguridad digital serán más fáciles de superar. Crear una meta común, utilizando un lenguaje familiar, será un gran avance a la hora de ayudar a promover una saludable cultura de la seguridad digital y, por tanto, a la hora de abordar muchos de los problemas que se padecen en la actualidad.

5. El problema en perspectiva

La seguridad digital toca todos los aspectos de la vida de una empresa, de forma que no cae fácilmente en un silo específico. Esto es así debido a que en los últimos años se ha experimentado un nuevo nivel de interconectividad entre dispositivos y sistemas; y, por tanto, para entenderlo completamente y para comprender su impacto sobre la seguridad digital se necesita examinar el problema desde más allá de las fronteras tradiciones de la lógica departamental.

Esto es desafiante para cualquiera, dado que todos están dispuestos a hacer lo necesario; pero, a menudo, nadie comprende plenamente el papel que le toca jugar. La cuestión pendiente, por tanto, sigue siendo ¿cómo crear una meta y alcanzar un resultado común para todos los afectados? Los implicados técnicos y del departamento de Informática querrán aplicar soluciones tecnológicas al problema de la seguridad digital y, en cierta medida, estarán acertados al pretenderlo. Los directivos pueden estar valorando una estrategia y una solución contraria al riesgo, mientras que la Administración querrá asegurarse de que se está haciendo todo lo necesario para proteger las infraestructuras críticas nacionales.

Entonces, ¿cuál es la respuesta? Recuerde este sencillo hecho: todos los negocios interactúan. En el ecosistema de los sistemas informáticos empresariales, estos están entrelazados a muchos niveles. Por tanto, centrarse en una gran empresa únicamente, es como poner una puerta acorazada a la entrada de su domicilio, mientras deja una ventana abierta en la parte de atrás. Cualquier solución de seguridad digital necesita abarcar cualquier tipo de empresa, grande y pequeña, para tener alguna opción real de triunfar. Se trata de una tarea desafiante y requiere un cambio de paso en las prácticas operativas de aquellas empresas que tienen diferentes propietarios, pero que tendrán que trabajar en equipo. Esto no se producirá de forma fácil, ni natural. Necesitará identificarse un objetivo común y especificarse un lenguaje que sea global en su alcance y comprensión. Todo el mundo debería situarse en la misma página. Es necesario crear una cultura de la seguridad digital donde todos interioricen la ciberhigiene y las buenas prácticas como parte de su forma natural de actuar.

Una reflexión final: si alguien cree que no es una víctima potencial de la ingeniería social, que sus puntos de vista y sus ideas no pueden ser manipulados, entonces deberá responder a esta cuestión, ¿cuándo fue la última vez que compraste, o quisiste comprar algo pensando sólo en la marca?[2]

Referencias

[1] CeBIT Australia. “The human factor in cyber security”. *17 de enero de 2016*. <http://blog.cebit.com.au/the-human-factor-in-cyber-security>.

[2] Instituto de Tendencias en Tecnología e Innovación (iTTi). El Manifiesto iTTi sobre el Gobierno Corporativo de las Tecnologías de la Información”. *1 de septiembre de 2014* http://es.slideshare.net/iTTi_news/el-manifiesto-itti>.

[3] John McCarthy. A word about cyber security (with Dr. John McCarthy)”. *Bitácora electrónica de Oxford Systems*. <http://www.oxfordsystems.eu/index.php/blogs>. Último acceso: 13 de febrero de 2017.

Notas

[1] Nombre genérico empleado, habitualmente, en referencia a los sistemas de automatización y control industrial (IACS, por sus siglas en inglés). Se trata de los sistemas de información que soportan las operaciones en plantas de producción (fábricas, centrales energéticas, etc.). Recientemente, este tipo de sistemas han adoptado la denominación “Tecnologías de Operación”, TO, por analogía a las “Tecnologías de Información”, TI, propias de entornos corporativos. Estrictamente hablando, los sistemas SCADA (*Supervisory Control And Data Acquisition* / Supervisión, Control y Adquisición de Datos) son un subgrupo dentro de los IACS o Tecnologías de Operación.

[2] Nota del editor: Si el lector está interesado en conocer más en profundidad los puntos de vista del autor, le recomendamos que consulte periódicamente el blog de su empresa, Oxford Systems [3].

In medio stat virtus

Manolo Palao
Socio fundador y Director de Formación del "think tank" iTTi, Instituto de Tendencias en Tecnología e Innovación (España); Socio Sénior de ATI

<mpalao@ittrendsinstitute.org>

Resumen: *La Informática, probablemente por su juventud y dinámica de evolución vertiginosa, tiene muchos rasgos de inmadurez, que con certeza afectan a la seguridad digital. El autor explora algunos de esos comportamientos extremos: 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 y cargas; la globalización, el gigantismo de las redes y los macroproyectos; la supremacía de la gestión operativa frente al buen gobierno; la propia necesidad de evolucionar ante la evolución del entorno. Todo se resume en una llamada de atención sobre los "extremismos" y la recomendación de huir de los extremos y de los máximos, persiguiendo una áurea mediócritas y objetivos "satisfacientes".*

Palabras clave: *áurea mediócritas, extremismos, filosofía, inseguridad digital,* know-what*, saber qué, objetivos satisfacientes, seguridad digital.*

Autor

Manolo Palao es socio sénior de ATI. Escribió su primer programa informático en FORTRAN en 1963 y el último, hasta el momento, en Python estos últimos días. Entre ambas fechas ha sido desarrollador, CIO, CEO, auditor, consultor y formador, con experiencia internacional. Es socio director de Personas & Técnicas: Soluciones, SLU, una pequeña firma de consultoría 'boutique', que opera desde 1983. Es socio fundador y Director de Formación del 'think tank' español Instituto de Tendencias en Tecnología e Innovación (iTTi). Mantiene vivas las certificaciones CISA, CISM, CGEIT de ISACA; y COBIT 5 Accredited Trainer (F+I+A) de APMG. Ha trabajado en seguridad (¿inseguridad?) de la información desde que en la década de 1980 tradujo y adaptó para España 'ESPED', una metodología de auditoría de seguridad de la información, desarrollada en EE.UU. por Peat, Marwick & Co. (ahora KPMG). Desde entonces ha realizado decenas de auditorías de seguridad de la información (sobre todo en el sector financiero y en la administración pública). Actualmente, su empresa está prestando asistencia técnica a una entidad certificadora que tiene el objetivo de obtener la acreditación de ENAC para poder incorporar a su oferta servicios de certificación de sistemas de gestión de la seguridad de la información (SGSI), basados en la norma ISO 27001.

1. Introducción

"*In medio stat virtus*" es una vieja máxima latina[1] que significa que la virtud está en el punto medio, ni tanto ni tan calvo.

He elegido ese título no tanto por pensar que podría llamar así la atención de algún lector (legítimo truco de cualquier autor; y que me perdone el lector si lo que sigue le decepciona), cuanto porque creo que describe bastante bien el propósito y contenido de este artículo.

Mi propósito en estas líneas es esbozar unas cuantas reflexiones sobre temas relacionados con la seguridad digital, que creo merecen consideración sobre su uso extremado, en lugar de uno más centrado o equilibrado; una *áurea mediócritas*[2].

Me propongo tratar varios temas, aun bajo la fundada sospecha de que al lector se le ocurrirán otros que bien hubieran merecido figurar aquí. Y quiero tratarlos de forma suficiente para dejarlos planteados, pero sin elaborarlos rigurosamente, pues esto exigiría un tiempo y un espacio no previstos en esta ocasión.

No puedo ocultar que no soy un *nativo digital*, lo que me apena, por el déficit experiencial que mi tardía incorporación a ese nuevo mundo pudiera suponer, pero sobre todo por la cantidad de años que me quitaría.

Ya que no puedo invocar, como aval de mis reflexiones, el haber sido destetado con un *smartphone*, sí diré al menos que me aproximé a la Informática, por primera vez, usando el tercer o cuarto de los ordenadores (*mainframes*) instalados en Madrid; y, desde entonces, no he abandonado el tema, siendo por tanto un modesto *participante observador*[3] durante toda la historia de la Informática.

2. La seguridad corporativa

La seguridad digital (denominación que aún no supera en éxito a la, todavía de moda, *ciberseguridad)* [11] es un subconjunto de la seguridad corporativa. Esta última, en las grandes empresas, ha estado tradicionalmente encomendada a ex-altos mandos militares o policiales, incluso muchas veces aún tras la aparición de los CISOs tecnólogos.

La seguridad corporativa es multidimensional. Su gestión exige conocimientos de estructura político-económica mundial; del sector industrial concreto; de los actores y grupos de interés (buenos y malos); de estrategia; de psicosociología de las organizaciones; de fuentes de información de amenazas, vulnerabilidades y seguros; de gestión de riesgos; de vectores de ataque; de tácticas de prevención y disuasión; de tecnología y de otros muchos temas.

Concentrar la seguridad digital en un extremo alta o meramente tecnológico (véanse muchos temarios de cursos o perfiles de demanda de CISOs) es un error. Como lo fue, hasta no hace tanto, encomendarla solo a militares. Enfoques más en el *centro de masas* de los temas del párrafo anterior serían más equilibrados y coste-eficaces a medio y largo plazo.

3. Know-how y know-what

Hace tres cuartos de siglo, Norbert Wiener, Premio Nobel, "*Padre de la Cibernética*", dejó escrito:

> *"He dicho que el hombre moderno, y especialmente el estadounidense moderno, por mucho 'saber cómo' (know-how) que tenga, tiene muy poco 'saber qué' (know-what)"* [4].

Opino que, mientras no acompañemos al *saber cómo* de la seguridad digital con dosis importantes de *saber qué*, aquella tiene un futuro tenebroso que se volverá más sombrío con la generalización de la IoT (Informática de las Cosas) y la IA (Inteligencia Artificial).

¿Concierne a la seguridad digital el algoritmo de decisión de un coche autónomo ante dilemas de efectos no deseados? ("*¿Atropello a la viejecita o al joven CISO que están en mi camino inevitable?*"). Recientemente, cuestiones como la anterior, generalmente conocidas como el *dilema del tranvía*[5], han

> “ Del *know-how* se ocupa la Tecnología; del *know-what* la Filosofía. Tecnología sí, claro; pero Filosofía también ”

empezado a aparecer no solo en publicaciones de nuestro sector sino ya en los grandes medios[6].

Del *know-how* se ocupa la Tecnología; del *know-what* la Filosofía (y en particular la socrática)[7]. Tecnología sí, claro; pero Filosofía también[8] [13].

En mi generación, en el bachillerato, se estudiaba Filosofía que, aunque teñida por la circunstancia política, dejaba en el alumno algunas buenas semillas. La montaña rusa histórica en España de las leyes de educación, y la dispersión autonómica de su aplicación (ahora parece que vuelve la Filosofía) hace cuestionar los elementos de juicio de más de un diseñador de robótica, IA, etc., que no haya tenido al menos esos brochazos.

4. La seducción de la red

En nuestras sociedades (en nuestra *vida digital*, cada vez más amplia) hemos preferido hacer caso omiso del sentido común, cristalizado en el eslogan *no hay almuerzo gratis*[9]. E ignorar, o aceptar resignadamente, que *si no pagas, no eres el cliente, sino la mercancía*[10] [11].

Y es sabido que los ataques APT (amenazas persistentes avanzadas, por sus siglas en inglés), si bien recurren a múltiples vectores de ataque (a todos los que el agresor tenga disponibles), generalmente se inician con ingeniería[12] social, manipulando a empleados de buena voluntad para lograr su contribución (por la revelación de contraseñas, por ejemplo) a la ejecución de la agresión, sin que los empleados sean siquiera conscientes de ello.

Por ello, pasma el espectáculo de todos los usuarios compitiendo por difundir en las redes más y más información personal (y a menudo más íntima), que se añade a la muy numerosa que los sistemas ya captan automáticamente. Se actúa ignorando que “el mundo no es un nidito confortable hecho para la propia protección, sino un entorno amplio y mayormente hostil”[13] [13].

La gente dice estar seriamente preocupada por la protección de la intimidad, de los datos personales, y al tiempo se practica el estriptís en la red.

Y parecen hacerlo voluntariamente, con agrado, hasta compulsivamente, lo que el Prof. Byung-Chun Han explica con el concepto de *seducción*:

> *“El poder estabilizador del sistema ya no es represor, sino seductor, es decir, cautivador. Ya no es tan visible como en el régimen disciplinario […] Es ineficiente el poder disciplinario que con gran esfuerzo encorseta a los hombres de forma violenta con sus preceptos y prohibiciones. Es esencialmente más eficiente la técnica de poder que se preocupa de que los hombres por sí mismos se sometan al entramado de dominación”* [1].

Pero

> *“El Big Data anuncia el fin de la persona y de la voluntad libre”* [2].

Todo lo anterior no niega, claro, los muchos beneficios derivados de las redes; beneficios que, sin embargo, parece obvio que (al menos en lo monetizable) están muy asimétricamente distribuidos[14] [8].

5. El error de los macroproyectos

Parece demostrado que las grandes redes sociales tienden a un equilibrio de monopolio, u oligopolio de unas muy pocas[15] [4] [9]; aparte de que activamente sus gestores refuercen esa tendencia[16] [7]. Sin embargo, el crecimiento elefantiásico, por integración, de otros sistemas de información, resulta muy generalizado y opino que injustificado y desaconsejable.

Sirva como botón de muestra el caso del proyecto *+TIL* que saltó a los titulares en 2015:

> *“Madrid gasta 18 millones en un sistema informático que lleva 10 años en pruebas”.*
>
> *El Ayuntamiento licita por tercera vez una aplicación que no han podido terminar cinco empresas diferentes. El gobierno local insiste en externalizar, pese a contar con una oficina informática con 500 trabajadores.*
>
> *El programa informático que gestiona los ingresos del Ayuntamiento de Madrid está “en proceso de construcción” desde 2005. Diez años y al menos 18 millones de euros después, el sistema que debe automatizar los impuestos y las multas apenas tiene operativos dos módulos menores: el de impuestos de vehículos de tracción mecánica y el de ejecuciones sustitutorias, dos áreas de escasa relevancia para las cuentas del Ayuntamiento”*[5].

Debe ser un proyecto de sistema bastante grande, un megasistema. Sin descartar que haya habido otras concausas del fiasco a que se refiere el ejemplo, parece mentira que no hayamos aprendido, en algunos casos, a diseñar sistemas pequeños o medianos y a relacionarlos (cuando sea legal y necesario) más simplemente. Con modularidad y aplicación prudente de los conceptos de cohesión y acoplamiento. Diseñando sistemas cuasi-separables[17], como parece ser el modelo evolutivo biológico.

Por si sirve de consuelo al contribuyente madrileño, presento brevemente (con permiso de Miguel García-Menéndez que lo documentó y ha usado en cursos) un caso de las antípodas: el de la Nómina de Profesores de Nueva Zelanda, conocido como *caso Novopay*.

La historia de *Novopay* se remonta a enero de 2003, cuando la administración neozelandesa decide abordar un importante (el tiempo lo tildaría, además, de ambicioso) proyecto: sustituir el sistema de información en el que se tramitaba la nómina de todo el funcionariado adscrito al Ministerio de Educación, por uno nuevo, más moderno y, a priori, rebosante de las funcionalidades que el nuevo siglo, apenas recién estrenado, demandaría de un país avanzado y moderno como ese.

El camino no fue fácil ni en los primeros momentos. Seleccionar al nuevo proveedor llevaría más de cinco años (abril de 2008), tiempo que supuestamente se dedicó a elaborar una exquisita justificación, especificación y planificación del proyecto.

La realidad, sin embargo, mostraba otra cosa: el 11 de agosto de 2008 se firmaría un contrato con una planificación incompleta. Con dicha firma, además, daría comienzo la etapa desarrollo del proyecto, propiamente dicha. Un desarrollo no exento de las más básicas irregularidades, desde el punto de vista de la dirección de un proyecto software: unas especificaciones que nunca concluyeron y en las que jamás se tuvo en cuenta

> “La gente dice estar seriamente preocupada por la protección de la intimidad, de los datos personales, y al tiempo se practica el estriptís en la red”

la voz de importantes interesados (los usuarios, el proveedor anterior, que aún operaba el viejo sistema, etc.); reiterados cambios de interlocutores por el lado del ministerio; finalización del contrato de mantenimiento con el antiguo proveedor, desbaratando cualquier planificación de ejecución de los dos sistemas (el viejo y el nuevo) en paralelo; solapamiento entre las actividades de diseño, construcción y pruebas; aprobación de una prematura puesta en explotación del nuevo sistema (finalmente, se habían suprimido las fases de pruebas); etc.

La puesta en funcionamiento de “Novopay”, a pesar de ser prematura dadas las circunstancias del proyecto en aquellos momentos, se produciría el 20 de agosto de 2012, con un retraso de dos años respecto de la fecha planificada inicialmente. Esa urgencia y provisionalidad haría que tres años después, en 2015, aún se estuviesen sufriendo las consecuencias del mal funcionamiento del sistema (irregularidades en las nóminas; funcionarios que no sabían si debían dinero o, por el contrario, se les debía; desconocimiento del importe de dichas cantidades; etc.) [6].

Un ejemplo más de claros *extremismos*, o excesos (o defectos), que recayeron sobre el contribuyente neozelandés.

Hace 15 o 20 años (no he sabido ahora encontrar la referencia) la Administración de EE.UU. prohibió los megaproyectos informáticos en su seno.

Sin conocer más que por publicaciones los casos de *+TIL* y *Novopay* es aventurado avanzar juicios, pero parecen ser dos perfectos ejemplos de proyectos en los que ha habido (o se ha pretendido) construcción de software con un déficit de gestión de proyectos (PMBOK, PRINCE2), de control interno (COSO 1), de gestión de riesgos (COSO 2), de gobierno (COBIT 5), y de debida diligencia (legislación en vigor). O sea, un déficit generalizado de buenas prácticas y un supuesto predominio del código (programación) sobre todo lo demás. Diríase que son claros ejemplos de incurrir en un extremo, en lugar de en una combinación armoniosa de los diferentes elementos necesarios.

Sin embargo, en el sector, junto a un déficit de gobierno y desgobierno, frecuentemente observables, hay una proliferación (una epidemia, basta un vistazo a la literatura) de supuestos *gobiernos de las TI*: gobierno del *big data*, gobierno de la seguridad, gobierno de la nube, gobierno de las licencias, gobierno del análisis forense, etc.

Los equipos de mercadotecnia/*marketing* de muchos fabricantes han echado su leña a la hoguera: “*la nueva versión de nuestro software de contabilidad le resuelve definitivamente su gobernanza financiera*”.

Gobierno, gobernanza, son términos que suenan bien en el mundo de los negocios; como *revitalizador* suena bien en el mundo de las cremas. Términos que se usan, tanto si se gobierna, cuanto si se desgobierna; tanto si la crema realmente revitaliza, cuanto si su mejor cualidad (menos mal) es que es hipoalergénica.

No entiendo que no se hagan oír voces cualificadas contra tanta inflación conceptual y publicidad engañosa [12].

Una vez más, posiciones y manifestaciones exageradas (y claramente mendaces en ocasiones) como las apuntadas, deberían ceder ante planteamientos más centrales, matizados y veraces.

6. El buen gobierno

La informática industrial funcionaba hace 30 años con menos riesgos y, ciertamente, menos comodidad (las guardias y los turnos tenían que ser principalmente presenciales, no virtuales, aunque ya hubiera y se usaran buscapersonas y mensáfonos[18]). Probablemente, aislada de Internet, tenía las funcionalidades básicas y no muchas comodidades, claro. Ahora tiene más funcionalidades, mucha más comodidad, … y continuos ataques, facilitados por su incorporación a la Red.

Naturalmente, no estoy predicando un retorno (no deseable, e imposible por otra parte) a sistemas y procedimientos de museo. Simplemente planteo la pregunta de ¿integración en la Red, cuánta, cómo?

Al tomar grandes decisiones corporativas hay que saber contemplar todos los costes (incluso los de optimización) y todos los beneficios (conocidos e imaginados en escenarios). Es esa visión total la que permite elegir un punto central.

Y saber perseguir no siempre lo máximo, sino lo *satisfaciente* (del inglés, *satisficing*, palabro que acuñó hace 70 años el premio Nobel de Economía Herbert Simon, mezclando las palabras *satisfactorio* y *suficiente*)[19]: búsqueda práctica de soluciones alcanzables, suficientemente satisfactorias, aunque no sean óptimas.

Las consideraciones sobre informática industrial se pueden extender a sus parientes la domótica y las ciudades inteligentes, entre otros.

7. Déficit de madurez

He señalado unos cuantos aspectos en los que posiciones relativamente extremas suponen un detrimento de la seguridad digital. Ese *extremismo* es probablemente resultado del vertiginoso avance de las tecnologías y el asociado inevitable déficit de madurez (déficit de madurez de las tecnologías y déficit de madurez nuestro en el uso y diseño de las tecnologías).

> *“Hemos modificado tan radicalmente nuestro entorno que ahora tenemos que modificarnos nosotros para existir en este nuevo entorno”*[20].

Para concluir me permito recordar tres *extremismos* asociados con la inmadurez de las tecnologías (y la de la sociedad para convivir eficaz y placenteramente con ellas): la revolución de los luditas, las leyes de bandera roja y las clínicas de desintoxicación de las redes[21].

Los luditas (a principios del siglo XIX—temiendo que los inventos de la revolución industrial les dejarían sin puestos de trabajo) se dedicaron a destruir violentamente los nuevos elares[22].

¿Qué va a pasar esta década o la próxima cuando los obreros que aún no han leído las previsiones de la OCDE o de CaixaBank[23] sobre generalización de los robots en el mundo productivo las lean o vean que se realizan? [3].

¿O qué van a pensar los estibadores cuando adviertan que tras el cambio de escenario

> “Al tomar grandes decisiones corporativas hay que saber contemplar todos los costes (incluso los de optimización) y todos los beneficios (conocidos e imaginados en escenarios)”

Figura 1. Escena urbana británica de aplicación de las leyes de bandera roja.

que, para ellos, va a suponer el cumplimiento de las recientes exigencias europeas sobre liberalización del sector (el empleo en ese sector dejará de ser un coto privado), el siguiente movimiento sea la sustitución de gruistas por grúas autónomas?

El hipotético escenario de ataques a los robots (o grúas-robot), ¿sería una cuestión de seguridad digital o de mero vandalismo en el mundo físico?

La **figura 1** representa una escena urbana británica de aplicación de las *leyes de bandera roja*[24], que en el Reino Unido y en EE.UU. obligaron, hasta la última década del siglo XIX, a que un individuo con bandera (o farol, de noche) precediese a todo vehículo en circulación. ¿Qué pasaría en el hipotético escenario en que varios coches autónomos mostraran comportamientos de atropellar al joven CISO en lugar de a la viejecita, o al revés?

> “La adicción a las redes sociales activa las mismas áreas del cerebro que la cocaína”.
>
> A nivel profesional, dice el doctor Zafra (psiquiatra y director de una clínica de desintoxicación de Valencia) esta realidad es una verdadera alarma sanitaria y social … Entre […] las alarmas ante una posible dependencia […], tener una vida social virtual más rica que en persona; pasar más horas navegando por redes sociales que hablando con familiares y amigos; o mirar las alertas nada más levantarse y ser lo último que hacer antes de acostarse” [10]. ¿Estamos todos locos?

Termino con la expresión de dos deseos: *áurea mediócritas,* que no *mediocre*; y objetivos *satisfacientes*, que no máximos ni estresantes.

Y con algunas recomendaciones más concretas:

- conviene evitar el reducir la seguridad corporativa a ciberseguridad: tiene otros componentes importantes;
- hay que intentar reforzar el *saber qué* ante el *saber hacer*;
- tecnología sí, pero filosofía también;
- el mundo digital no es solo maravilloso y gratuito, tiene restricciones y cargas, y debe usarse con prudencia;
- la globalización, el gigantismo de las redes y los macroproyectos pueden no ser todos necesarios y pueden ser desaconsejables; y,
- se debe presidir la gestión operativa con buen gobierno; y,
- debiéramos ocuparnos de nuestra propia necesidad de evolucionar ante la evolución del entorno, que estamos acelerando.

Referencias

[1] B-C. Han. “¿Por qué hoy no es posible la revolución?”. *El País. (2014)*.<http://elpais.com/elpais/2014/09/22/opinion/1411396771_691913.html>.Último acceso: 11 de febrero de 2017.

[2] B-C. Han. *Psicopolítica*. Herder Editorial. Barcelona. p26. 2014.

[3] C. Sánchez. “El uso de robots se acelera y amenaza con destruir decenas de miles de empleos”. *El Confidencial. 15 de agosto 2016*.

[4] D. Easley y J. Kleinberg. *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*. Cambridge University Press, capítulo 17 “Network Effects”, sección “Network Effects and Competition”, pp. 517 (versión borrador: 10 de junio de 2010).

[5] D. Placer. “Madrid gasta 18 millones en un sistema informático que lleva 10 años en pruebas”. *EDeconomíaDigital. 9 de junio de 2015*. <http://www.economiadigital.es/es/notices/2015/06/madrid-gasta-18-millones-en-un-sistema-informatico-que-lleva-10-anos-en-pruebas-el-ayuntamiento-lici-72627.php>. Último acceso: 11 de febrero de 2017.

[6] J. Henderson. “3 years later, is the Novopay fiasco over?”. *Computerworld, 23 de septiembre de 2015.*<http://www.computerworld.co.nz/article/585105/3-years-later-novopay-fiasco-over/>.

[7] J. Lanier. *Who Owns the Future?* Penguin Books, pp. 54. 2014.

[8] J. Lanier. *Who Owns the Future?* Simon & Schuster. 2013. ISBN1451654967 (ISBN13: 9781451654967).

[9] J. McGee *Strategy - Analysis & Practice*. Graw-Hill, capítulo 12 “Strategy in the new economy”, 2005.

[10] La Vanguardia. “La adicción a las redes sociales activa las mismas áreas del cerebro que la cocaína”. *4 de julio de* http://www.lavanguardia.com/local/valencia/20140704/54410744726/adiccion-redes-sociales-activa-mismas-areas-cerebro-cocaina.html. Último acceso: 12 de febrero de 2017.

[11] M. García-Menéndez *Seguridad digital 2025*. Novática Nº 235, enero-marzo de 2016. <http://www.ati.es/novatica>. Último acceso: 13 de marzo de 2017.

[12] M. Palao. “Mi ignorancia del Gobierno de TI”. *Asociación Colombiana de Ingenieros de Sistemas. Revista “Sistemas”, 14 de septiembre de 2015.* http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no-132/item/199-mi-ignorancia-del-gobierno-de-ti>. Último acceso: 13 de febrero de 2017.

[13] N. Wiener *The Human Use Of Human Beings: Cybernetics And Society.* (1950, 1954). Última consulta: 11 de febrero de 2017.

> “ Ese ‘extremismo’ es probablemente resultado del vertiginoso avance de las tecnologías y el asociado inevitable déficit de madurez —déficit de madurez de las tecnologías y déficit de madurez nuestro en el uso y diseño de las tecnologías ”

Notas

[1] “*En el medio está la virtud*”. Parece que el *copyright* sería de Aristóteles, si entonces hubiera habido copyright y se hubiera perseguido el plagio eficazmente.

[2] Fuente: <https://es.wikipedia.org/wiki/Aurea_mediocritas>. Último acceso: 11 de febrero de 2017.

[3] ”Participante observador” me parece un término más ajustado, en este caso, que el usual “observador participante”. “La observación participante es un tipo de método de recolección de datos utilizado típicamente en la investigación cualitativa. Es una metodología ampliamente utilizada en muchas disciplinas, particularmente la antropología y la etnología, aunque también en sociología…”.
Fuente: <https://es.wikipedia.org/wiki/Observaci%C3%B3n_participante>.
Último acceso: 11 de febrero de 2017.

[4] “*I have said that the modern man, and especially the modern American, however much ‘know-how’ he may have, has very little ‘know-what’*.” <http://www.azquotes.com/author/15625-Norbert_Wiener>. Último acceso: 10 de febrero de 2017.

[5] Fuente: <https://es.wikipedia.org/wiki/Dilema_del_tranv%C3%ADa>. Último acceso: 11 de febrero de 2017.

[6] Si el lector está interesado en obtener más información relacionada con el dilema del tranvía, puede realizar una búsqueda en Google con las siguientes palabras “dilema del tranvía” “vehículo autónomo”. Último acceso: 11 de febrero de 2017.

[7] Si el lector está interesado en obtener más información relacionada con la Filosofía y el *know-what*, puede realizar una búsqueda en Google con las siguientes palabras philosophy “asking the what”. Último acceso: 11 de febrero de 2017.

[8] Wiener, N. (1950, 1954). *The Human Use Of Human Beings: Cybernetics And Society*. “The world of the future will be an even more demanding struggle against the limitations of our intelligence, not a comfortable hammock in which we can lie down to be waited upon by our robot slaves”.
Fuente: <https://www.goodreads.com/author/quotes/88990.Norbert_Wiener>. Último acceso: 11 de febrero de 2017.

[9] “*There ain’t no such thing as a free lunch*”. Expresión cristalizada por el premio Nobel de Economía Milton Friedman, sobre una idea del novelista R. Heinlein. Fuente: <https://en.wikipedia.org/wiki/There_ain’t_no_such_thing_as_a_free_lunch>. Último acceso: 11 de febrero de 2017.
Andrew Lewis: *“If you are not paying for it, you’re not the customer; you’re the product being sold”*.
Fuente: <https://www.quora.com/Who-originally-suggested-that-if-youre-not-paying-for-the-product-you-are-the-product>.

[10] “*When it was sold to Facebook for a billion dollars in 2012, Instagram employed only thirteen people … its value comes from the millions of users who contribute to their network without being paid for it*”. Lanier, J. (2014). *Who Owns the Future?* Penguin Books. p XX.

[11] Este tema lo he desarrollado un poco más ampliamente en: Palao, M. (2016). “Confianza y Seguridad”. *Magazitum*. México.
Fuente: < http://www.ittrendsinstitute.org/perspectives/tag/perspectives/Manolo%20Palao>.

[12] ¡Curioso uso del término, cuando se trata de pura psicosociología! Otro ejemplo de un uso (o referencia) extremo de la tecnología, dejando fuera de juego otras disciplinas.

[13] Wiener, N. (1950, 1954). *The Human Use Of Human Beings: Cybernetics And Society*. “The sense of tragedy is that the world is not a pleasant little nest made for our protection, but a vast and largely hostile environment, in which we can achieve great things only by defying the gods; and that this defiance inevitably brings its own punishment”.
Fuente: <https://www.goodreads.com/work/quotes/148587-the-human-use-of-human-beings-cybernetics-and-society>

[14] Una importante (a veces difícil y en parte discutible) lectura sobre este tema es el clásico: Lanier, J. (2013). *Who Owns the Future?* Simon & Schuster. ISBN1451654967 (ISBN13: 9781451654967).

[15] Por el efecto de basculación o vuelco que hace que “un ganador se lo lleve todo”. Este tema está bien planteado en McGee, J.et al. (2005). *Strategy - Analysis & Practice*. Mc Graw-Hill, Chapter 12 “Strategy in the new economy”. Y también en Easley, D. y Kleinberg, J. (2010, draft version: June 10, 2010). *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*. Cambridge University Press, capítulo 17 “Network Effects”, sección “Network Effects and Competition”, pp. 517 ss.

[16] “*For instance, Peter Thiel, founder of PayPal and foundational investor in Facebook, taught students in his Stanford course on startups to find a way to create ‘monopolies’”*. Lanier, J. (2014). *Who Owns the Future?* Penguin Books, pp. 54.

[17] Si el lector está interesado en obtener más información relacionada con la definición de cuasi-separables, puede realizar una búsqueda en Google con las siguientes palabras “quasi-decomposable systems” definition. Último acceso: 11 de febrero de 2017.

[18] Fuente: <https://www.wayerless.com/2012/03/una-breve-historia-del-beeper/>. Último acceso: 12 de febrero de 2017.

[19] Fuente: <https://en.wikipedia.org/wiki/Satisficing#In_survey_methodology>. Último acceso: 12 de febrero de 2017.

[20] Wiener, N. (1950, 1954). “*We have modified our environment so radically that we must now modify ourselves to exist in this new environment”.* Fuente: <http://www.azquotes.com/quote/797950>. Último acceso: 12 de febrero de 2017.

[21] “La adicción a las redes sociales activa las mismas áreas del cerebro que la cocaína”. Fuente: <www.lavanguardia.com/local/valencia/20140704/54410744726/adiccion-redes-sociales-activa-mismas-areas-cerebro-cocaina.html>. Último acceso: 12 de febrero de 2017.

[22] Fuente: <https://es.wikipedia.org/wiki/Ludismo>. Último acceso: 12 de febrero de 2017.

[23] Sánchez, C. (20160815). “El uso de robots se acelera y amenaza con destruir decenas de miles de empleos”. *El Confidencial.*
“*Un reciente informe de la Organización para la Cooperación y el Desarrollo Económico (OCDE) situaba España, Austria y Alemania como los países más afectados por la revolución robótica. En concreto, la cuarta revolución industrial obligará a sustituir hasta un 12% de los empleados en estos tres países, frente a una media del 9% en la OCDE*”. “*Según las estimaciones del servicio de estudios de CaixaBank, un 43% de los puestos de trabajo actualmente existentes en España tiene un riesgo elevado (con una probabilidad superior al 66%) de poder ser automatizado a medio plazo*”.
Fuente: <http://www.elconfidencial.com/economia/2016-08-15/robots-automatizacion-ccoo-empleo-maquinas-industria_1245720/>. Último acceso: 12 de febrero de 2017.

[24] Fuente: <https://en.wikipedia.org/wiki/Red_flag_traffic_laws>. Último acceso: 12 de febrero de 2017.

Kerry Tomlinson
Redactora Jefe de Archer News, una división de Archer Security Group (EE.UU.)

<kerry.tomlinson@archerenergysolutions.com>

¿Confía Ud. en los cuidados que su médico les dispensa a sus datos personales?

Traducción: Miguel García-Menéndez (Vicepresidente de ATI, editor invitado de la monografía).

Resumen: *La maestría y la veteranía periodística de la autora le hacen ofrecer un artículo con un aire distinto, para lo que ha sido costumbre hasta ahora en Novática. El texto relata una crónica en la que se van combinando elementos como la entrevista, junto a la narración y a los datos. Se repasa, con realismo, la historia de Eric, un paciente de una clínica privada, 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, también, con las opiniones de una interesante batería de especialistas. Asimismo, el sector elegido para situar la 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.*

Palabras clave: *brecha, confianza, datos personales, hospital,* phishing*,* ransomware*, sanidad, seguridad digital.*

Autora

Kerry Tomlinson es periodista y escritora. Es la actual Redactora Jefe de Archer News, una división de la firma de servicios profesionales estadounidense Archer Security Group, desde la que trata de acercar a la gente el casi invisible, aunque potente, mundo de Internet. Galardonada con un premio Emmy, Kerry cuenta con varias décadas de experiencia en televisión, habiendo trabajado en diferentes cadenas de la costa oeste de los EE.UU.; entre otras, KATU News y KPTV Fox 12, en Portland (Oregón), y KXLY News en Spokane (Washington), para las que ha cubierto noticias alrededor del mundo en países como México, Rusia o Filipinas. Como fundadora de Archer News, y dentro de su búsqueda constante del siguiente gran reto y la mejor forma de resolverlo, los intereses profesionales de Kerry se centran, actualmente, en la seguridad digital y su impacto en el día a día de las personas.

1. La historia

¿Por qué algunos pacientes están perdiendo la confianza en la seguridad digital de la sanidad? Y, ¿cómo puede eso influir en lo que están pagando por sus cuidados?

El paciente vaciló.

Eric (no es su verdadero nombre) había acudido a una cita en su clínica habitual, donde llevaban atendiéndole desde hacía años.

La persona al otro lado del mostrador quiso hacer una copia digital de su permiso de conducir. Ya lo habían hecho el año anterior.

"*La mujer que me pidió el carnet me dijo que era parte del procedimiento, y que no sabía qué había sido de la copia anterior*", declaró Eric.

Pero Eric estaba preocupado. ¿De verdad necesitaban guardar una copia de su documento de identidad (particularmente, cuando ni siquiera sabían dónde había ido a parar la copia del año pasado)?

"*Todo esto me pone nervioso porque no hago más que escuchar cosas sobre fraudes, sobre información a la que se da un uso indebido y sobre otra que, simplemente, se roba o se pierde; especialmente, en los centros sanitarios*", dijo.

Eric habló con el director de la clínica, quien le entregó un folleto con información sobre protección de datos (y le hizo algunas advertencias).

"*El director me dijo: 'Si Ud. rehúsa facilitarnos la documentación que le pedimos, entonces no podremos atenderle en esta clínica'*", contó Eric.

Pero con las continuas brechas de información que se producen en el sector sanitario, y con los hospitales siendo víctimas de *ransomware*[1], Eric no es el único paciente preocupado por el camino que llevan los datos personales que dan en sus clínicas.

"*Sí*", dijo Lee Tien, miembro del equipo jurídico de la Electronic Frontier Foundation[2], una organización no gubernamental que trata de proteger los derechos de los usuarios en el ámbito digital. "*Es un problema gordo*". Y resulta, que es un problema tan gordo que, en última instancia, podría alterar la forma en que se obtienen los cuidados sanitarios, y el precio que se paga por ellos.

2. Perder los datos

A los delincuentes les gustan las contraseñas y los números de las tarjetas de crédito. Pero los historiales médicos les gustan incluso más, según la opinión de Satyamoorthy Kabilan, del centro de análisis estratégico The Conference Board of Canada[3], una organización no lucrativa dedicada a la investigación aplicada.

"*El valor de un historial clínico completo, con toda la información detallada sobre una persona, es increíblemente alto*", declaró Kabilan.

Valioso para los ciberdelincuentes, valioso para nosotros. A pesar de lo cual, las compañías sanitarias han perdido datos personales, a veces de forma masiva.

Unos invasores cibernéticos robaron, en 2015, información relativa a las cuentas de noventa millones de clientes de las aseguradoras sanitarias Anthem [6] y Premera Blue Cross [15], según datos del Departamento de Sanidad y Servicios Sociales de los EE.UU.

En 2016, unos atacantes se hicieron con más de dos millones de historiales médicos de 21st Century Oncology [21], 3,6 millones de Banner Health [19] y 3,4 millones de Newkirk Products [16], un fabricante de tarjetas de identificación sanitaria, según informó nuevamente el Departamento de Sanidad y Servicios Sociales estadounidense. Y estas son sólo tres de las más de trescientas brechas de seguridad que afectaron ese año a un total de más de quinientos millones de personas en los EE.UU.

3. Datos expuestos

El año pasado, grupos ciberactivistas lanzaron una campaña, en varias etapas, en Italia, contra diversas organizaciones sanitarias. Como consecuencia en marzo se produjo una brecha de información en la Cruz Roja italiana, en junio en el Instituto Nacional de la Salud y en agosto en varias clínicas de Nápoles y Turín, según información de Softpedia [3].

> “A los delincuentes les gustan las contraseñas y los números de las tarjetas de crédito. Pero los historiales médicos les gustan incluso más…”

Aunque no se trató de un ciberataque, el Complejo Asistencial de Ávila, en España, perdió quince mil radiografías, resonancias y otras imágenes médicas, tal y como recogía el periódico local, “*La Estrella Digital*” [4] [5], a principios de 2016.

Asimismo, el Hospital “Antoni van Leeuwenhoek” de Ámsterdam (Holanda) [10] informaba, en marzo, de la desaparición de datos de pacientes tras el robo del ordenador portátil de un investigador.

De igual modo, en agosto, un centro asistencial norirlandés [2] era sancionado con quince mil libras esterlinas por la pérdida de otro portátil que contenía información de pacientes en texto claro (sin cifrar).

4. Rehenes sanitarios

Como ya se ha dicho, el *ransomware* también está golpeando los hospitales. Así ocurrió en el caso del Hollywood Presbyterian de Los Ángeles (EE.UU.) [22] que pagó 17.000 dólares para recuperar sus ordenadores en febrero de 2016; y en el del Kansas Heart Hospital de Wichita (EE.UU.) [9] que pagó un rescate en mayo, sólo para ver cómo los atacantes le demandaban más dinero antes de *devolverle* todos sus ficheros.

No obstante, Europa tampoco se libra. También en febrero de 2016, al menos dos hospitales alemanes informaron de ataques de *ransomware*. Los facultativos del Hospital Lukas en Neuss [24] tuvieron que usar lápiz y papel, y volver al fax para comunicarse, durante el ataque. El incidente en el Klinikum Arnsberg [17], días después, se originó a través de un mensaje de correo electrónico infectado, según un portavoz del propio hospital.

E igual suerte se ha corrido en el Reino Unido. Tres hospitales británicos fueron desconectados (de Internet), en octubre, cuando el *ransomware* se hizo con el control de los sistemas informáticos de la Mancomunidad de Hospitales Públicos de Lincolnshire and Goole [1], lo que provocó que los pacientes de traumatología fueran derivados a otros hospitales y que se cancelaran cerca de tres mil citas. Y, más recientemente, en enero de 2017, otros cuatro centros [8], también en el Reino Unido, notificaron ser víctimas de lo que inicialmente se pensó que era un nuevo ataque de *ransomware*; pero que, finalmente, se identificó como la infección de un software nocivo, de tipo troyano. Afortunadamente, en este caso, la Mancomunidad de Hospitales de Barts declaró que había tenido que pasar su operativa a modo manual para tramitar algunas solicitudes que normalmente se habrían hecho por vía informática; pero que no habían padecido la pérdida de datos de ningún paciente.

En España, no son los hospitales, sino las farmacias, las que parecen haber entrado en el punto de mira de los ciberdelincuentes. Así lo apuntaba, mientras se elaboraba este reportaje, el medio local, digital, “*El Confidencial*” [20].

5. Previsión

Las fugas de datos sanitarios, prácticamente, se han duplicado en los EE.UU. en 2016, informa SC Magazine [7].

Globalmente, el *ransomware* contra instituciones sanitarias está en auge. Desde la firma de ciberseguridad Solutionary [23] señalan que casi el 90% del software nocivo de ese tipo que detectaron de abril a junio de 2016 se encontró en organizaciones del sector salud.

Los analistas predicen que 2017 también será horrible: “*Las organizaciones sanitarias seguirán siendo el objetivo prioritario con la aparición de ataques nuevos y más sofisticados*”, ha anunciado la firma Experian en su informe “*Predicciones Sectoriales de Brechas de Datos para 2017*” [11].

El próximo año entrará en vigor el Reglamento General de Protección de Datos (RGPD[4], por sus siglas en inglés) de la Unión Europea, publicado en 2016; y, con él, la obligación, para las organizaciones que sufran brechas de datos, de notificar este tipo de incidentes, tanto a las autoridades de protección de datos, como a los clientes afectados, en un plazo máximo, e improrrogable, de 72 horas.

“*Muchos expertos en seguridad esperan que el RGPD altere dramáticamente los debates sobre protección de datos y brechas de seguridad en el ámbito europeo, toda vez que la verdadera magnitud y severidad de la brecha sea conocida*” [18], según el portal BankInfoSecurity.

6. ¿Quién es responsable?

“*No es culpa de su médico*”, señaló Tien.

“*Yo no me atrevería a afirmar que mi ordenador es seguro. Ud. probablemente tampoco puede. Su médico menos aún; y, además, confío en que se dedique a tratar pacientes, no a auditar ordenadores*”, dijo.

“*No suele ser lo primero que se enseña en las facultades de medicina o en las escuelas de enfermería*”, sentenció Kabilan.

7. Apuesta por la historia clínica electrónica

El problema subyacente en los EE.UU., a criterio de Tien, es que el gobierno ha impulsado los historiales médicos electrónicos y el análisis de datos en medicina; pero no ha hecho lo mismo con la seguridad.

Otros países, entre ellos España, también han realizado esa apuesta.

Aunque la digitalización de estos documentos puede suponer un gran beneficio para la gestión y el tratamiento sanitarios, también constituye una desventaja.

“*Eso ha hecho que todo el mundo coja algo que estaba en lápiz y papel y lo pase al ámbito electrónico*”, apuntó Denise Anderson, presidente del Centro para el Análisis y la Compartición de Información sobre el Sistema Sanitario[5] (NH-ISAC, por sus siglas en inglés). “*Pero nadie ha dicho una palabra sobre seguridad*”.

“*Eso, de hecho, ha provocado que los historiales médicos de todo el mundo estén al alcance de los delincuentes y que, ahora, vayamos por detrás y ‘como pollos sin cabeza’, por decirlo de alguna manera*”, añadió.

8. Complejo

Algunos proveedores del sector de la salud están utilizando equipamientos o sistemas anticuados. A eso hay que añadir la rápida innovación que se está dando en la tecnología sanitaria, como los tensiómetros que remiten las mediciones al teléfono móvil o esas otras píldoras que, ingeridas, pueden hablar con la enfermera.

“*Tales niveles de comunicación van a hacer a esos dispositivos incluso más vulnerables*”, señaló Anderson.

> “En España, no son los hospitales, sino las farmacias, las que parecen haber entrado en el punto de mira de los ciberdelincuentes”

Además, “*si Ud. necesita disponer rápidamente de determinada información sobre su salud, una seguridad a prueba de bombas podría ser un obstáculo*”, declaró Kabilan.

“*Si Ud. llega a urgencias, ¿querría que a su enfermera le llevara tres horas y diecisiete contraseñas identificar su grupo sanguíneo?*” preguntó Kabilan. “¿O preferiría que la *misma enfermera le pudiese tomar una huella dactilar y —¡pum!— lo supiese de inmediato* (su grupo sanguíneo)*?*”.

El problema es complejo. “*No hay una respuesta sencilla para esto*”, concluyó.

9. ¿Recursos?

El centro sin ánimo de lucro NH-ISAC trabaja para compartir información sobre seguridad digital entre los proveedores del sector sanitario de todos los EE.UU., de forma que puedan estar mejor preparados.

El grupo asesora a las organizaciones en materia de *phishing*[6], robo de datos, *hactivismo*[7], *ransomware*, espionaje, terrorismo y otras cosas.

Comparte buenas prácticas como, por ejemplo, mantener un equipo de resonancias magnéticas, dotado de un software viejo y vulnerable, aislado de Internet; de forma que los ciberdelincuentes no puedan crear confusión con los datos que ofrece el equipo o con el tratamiento.

“*Los principales operadores en este campo disponen de buenas prácticas en vigor*”, señaló Anderson. “*Son bastante sofisticados en sus enfoques. Pero, luego, hay otro buen puñado de actores menores en el sector sanitario que, o bien no son conscientes de la situación, o bien no disponen de los recursos oportunos o de la financiación adecuada para hacer muchas de las cosas que se consideran buenas prácticas*”.

“*Esa es una meta, ayudar a los actores menores del sector que tenemos por delante*,” dijo.

10. Errores básicos

La mayoría de los proveedores de servicios sanitarios quieren ser seguros, según Anderson.

Algunos, no obstante, comenten errores muy básicos.

En enero de este año, la filial en Puerto Rico, MAPFRE Life, de la aseguradora de origen español MAPFRE, accedió a pagar más de dos millones de dólares al gobierno de los EE.UU. [14], después sufrir una pérdida de datos que afectó a dos mil doscientos pacientes y tras fracasar en sus prácticas de evaluación de riesgos y a “*poner en marcha suficientes medidas de seguridad para reducir riesgos y vulnerabilidades a un nivel razonable y apropiado*”, ha declarado el Departamento de Sanidad y Servicios Sociales estadounidense. Según este mismo organismo, la empresa no comenzó a cifrar los datos de sus pacientes en ordenadores portátiles y dispositivos de almacenamiento extraíbles hasta septiembre de 2014, a pesar de conocer el problema mucho antes.

En julio, la Universidad de las Ciencias y de la Salud de Oregón, en Portland (EE.UU.), acordó pagar dos millones setecientos mil dólares [12] por sus supuestas violaciones de la Ley estadounidense de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA, por sus siglas en inglés), las cuales condujeron a un “*significativo riesgo de daño*” para los más de mil pacientes afectados, según un informe del Departamento de Salud y Servicios Sociales, que tildó los problemas de “*amplios y diversos*”.

La Universidad de Massachusetts (UMass) en Amherst (EE.UU.) accedió a pagar seiscientos cincuenta mil dólares [13] en noviembre pasado por violar supuestamente las reglas de protección de la intimidad y la seguridad de la HIPAA. El Departamento de Sanidad y Servicios Sociales estadounidense reveló que la UMass no disponía, en 2013, de un cortafuegos (una protección de seguridad básica), permitiendo el acceso de atacantes malintencionados para robar datos médicos personales.

11. Nerviosos

Todo esto deja a algunos pacientes nerviosos ante la idea de entregar información personal crucial.

“*Buscar asistencia médica puede, en sí mismo, constituir una situación tensa* (para algunas personas)*, por lo que no pretendemos que Uds.* (las clínicas) hagan cosas que nos atemoricen aún más” observó Eric. “*Esa no es una buena ‘praxis’ médica*”.

Se cotejaron las declaraciones de Eric relativas a sus preocupaciones (manteniendo, naturalmente, su anonimato, en tanto que él así lo había solicitado) con Legacy Health, la organización al frente de la clínica de Eric en Portland, Oregón (EE.UU.).

“*Yo aprecio de dónde viene la persona*“, dijo John Kenagy, Director de Sistemas de Información de Legacy, entre otras funciones. “*Sus lectores, no se volverán paranoicos*”.

Kenagy declaró que Legacy trabaja constantemente para defenderse frente a ciberdelincuentes, probar sus sistemas, formar a los empleados, desplegar tecnología especial, supervisar el tráfico de Internet entrante y saliente, conducir evaluaciones de riesgo y auditorías, y asegurarse de que la organización cumple con los requisitos de seguridad e intimidad de la HIPAA.

“*Yo no soy sólo el Director de Sistemas de Información de Legacy, sino que también soy un paciente de la casa, y un padre y esposo de otros pacientes. Me tomo la seguridad muy, muy en serio*”, añadió. “*Todos nosotros sentimos una obligación moral y muchos de nosotros, una obligación personal*”.

“*Legacy envía a sus empleados mensajes de correo electrónico de prueba, con ‘phishing’, para ver si pulsan en el enlace dañino; y si lo hacen, reciben formación e información extra*”, explica.

Además, a los empleados no se les permite utilizar la cuenta personal de correo electrónico en el trabajo.

“*Eso era extremadamente impopular, pero permite cerrar un hueco. Intentamos ir un paso por delante de los malos*”, aclaró. “*Estamos muy, muy pendientes de lograrlo*”.

12. ¿Una copia digital del permiso de conducir?

En cuanto al permiso de conducir de Eric, Shannon Kennedy, Directora de Conformidad y Protección de Datos de Legacy, dijo no saber nada de ninguna política que requiriese una copia del carnet.

No obstante, mostrar una identificación válida, resulta crucial.

> “ Aunque la digitalización de estos documentos puede suponer un gran beneficio para la gestión y el tratamiento sanitarios, también constituye una desventaja ”

“*Una de las mayores evidencias sobre la que apoyarse ante una situación de robo de identidad médica es ser capaces de echar mano de una copia de la identidad de la persona*”, explicó.

“*Diría que es una práctica habitual consistente en asegurar que se está validando la identidad de la persona cuando estamos proporcionándole un servicio*” continuó.

Y apuntó que con Medicare la situación podría ser diferente, dado que Medicare requiere un número de identificación del suscriptor, que utiliza parte del número de la Seguridad Social de un paciente, añadió Kennedy.

Además, ¿y si un paciente no quiere digitalizar su carnet?

“*No hay problema, no tenemos que hacer ninguna copia de su documento de identidad. Simplemente hay que asegurarse de que es quien dice ser*”, señaló.

“*Los pacientes deberían recibir el número de teléfono del responsable de protección de datos, de forma que puedan llamarlo si tuviesen alguna duda sobre requisitos y normativas*”, añadió.

“*Deseo que los consumidores y los pacientes sepan, particularmente, que tienen verdadero acceso a un experto que puede resolver sus dudas*”, dijo.

Legacy Health ofrece una línea telefónica para que los pacientes llamen con preguntas sobre sus datos personales.

13. Confianza

Eric recibió ese número de mano del director de la clínica y una sugerencia para que llamase si no se encontraba cómodo con las normas de la casa. Pero era demasiado tarde, su confianza ya estaba perdida.

“*Preferí no hacerlo porque era consciente de que ya no quería saber nada de esa clínica*”, sentenció.

La confianza es vital, según Kabilan.

Su equipo llevó a cabo una investigación sobre el futuro de la tecnología y la sanidad. Sus escenarios mostraron que las principales brechas de seguridad podían erosionar la confianza hasta tal punto que la gente ya no creía que usar tecnología sanitaria supusiese beneficio alguno.

“*Lo que vimos fue un futuro donde el coste de los cuidados médicos se disparaba y la calidad se hundía*”, apuntó Kabilan.

“*Por el bien de nuestra propia salud futura, tenemos que asegurarnos de que esa confianza no se destruye*”, añadió.

Los investigadores dicen que la falta de confianza en la seguridad digital del sector sanitario conduce a un futuro donde el público no aceptará nuevos desarrollos en tecnología médica.

14. ¿Qué podemos hacer?

Formular preguntas, sugieren los expertos. Se podría empezar por el responsable de protección de datos de nuestro centro sanitario.

Las organizaciones sanitarias estadounidenses deben nombrar un responsable de protección de datos. Las europeas tendrán que tenerlo cuando entre en vigor el RGPD.

“*Hacer preguntas aumenta la concienciación*”, dijo Kabilan, quien también sugirió preguntar por las reglas relativas a la mejora de la seguridad digital, emitidas por las autoridades normativas para las instalaciones sanitarias.

“*Elevar la concienciación es estupendo*”, insistió Tien.

El propio Tien señaló que las acciones legales y las demandas colectivas ayudarán a las organizaciones sanitarias a cambiar sus prácticas de seguridad.

En cuanto a Eric, él mismo anima a hablar de las preocupaciones relativas a la seguridad en sanidad, en lugar de sumarse a cada demanda sin hacer ruido y de forma irreflexiva.

“*Creo que, en general, cumplimos ampliamente y que necesitamos cuestionar las cosas que no percibimos para obtener más información*”, dijo.

Referencias

[1] A. J. Martin. “Appointments on hold as (computer) virus wreaks havoc with NHS trust systems”. *The Register, 31 de octubre de 2016*. <http://www.estrelladigital.es/articulo/espanha/proteccion-datos-entra-oficio-perdida-15-000-radiografias-avila/20160127142130269637.html>. Último acceso: 16 de febrero de 2017.

[2] Belfast Telegraph. “Nursing home fined for data breach after laptop with patients’ details stolen”. *Belfast Telegraph, 25 de agosto de 2016*. <http://www.belfasttelegraph.co.uk/news/northern-ireland/nursing-home-fined-for-data-breach-after-laptop-with-patients-details-stolen-34994692.html>. Último acceso: 26 de febrero de 2017.

[3] C. Cimpanu. “Anonymous Hacks Four Italian Healthcare Organizations”. *Softpedia, 19 de septiembre de 2016.* http://news.softpedia.com/news/anonymous-hacks-four-italian-healthcare-organizations-against-adhd-508445.shtml>. Último acceso: 26 de febrero de 2017.

[4] C. Lospitao. “Un fallo informático provoca la pérdida de miles de radiografías y ecografías”. *Estrella Digital, 18 de enero de 2016.* http://www.estrelladigital.es/articulo/espanha/error-sistema-informatico-arcaico-pierde-miles-pruebas-radiologicas/20160118161732268402.html>. Último acceso: 16 de febrero de 2017.

[5] C. Lospitao. “Protección de Datos entra de oficio por la pérdida de 15.000 radiografías en Ávila”. *La Estrella Digital, 27 de enero de 2016.* <http://www.estrelladigital.es/articulo/espanha/proteccion-datos-entra-oficio-perdida-15-000-radiografias-avila/20160127142130269637.html>. Último acceso: 16 de febrero de 2017.

[6] C. Terhune. “Anthem hack exposes data on 80 million; experts warn of identity theft”. *Los Angeles Times, 5 de febrero de 2015.* http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html>. Último acceso: 16 de febrero de 2017.

[7] D. Olenik. “Number of U.S. healthcare data breaches almost doubles in 2016”. *SC Media, 13 de enero de 2017* https://www.scmagazine.com/number-of-us-healthcare-data-breaches-almost-doubles-in-2016/article/631606/ acceso: 16 de febrero de 2017.

[8] D. Palmer. “Trojan malware blamed for cyberattack at Barts Health NHS hospitals”. *16 de enero de 2017.* <http://www.zdnet.com/article/trojan-malware-blamed-for-cyberattack-at-barts-health-nhs-hospitals/>. Último acceso: 16 de febrero de 2017.

[9] Sun. “Hackers demand ransom payment from Kansas Heart Hospital for files”. *KWCH, 20 de mayo de 2016.* <http://www.kwch.com/content/news/Hackers-demand-ransom-payment-from-Kansas-Heart-Hospital-380342701.html>. Último acceso: 16 de febrero de 2017.

[10] E. van Steenbergen. “Gegevens kankerpatiën ten gestolen”. *NRC, 4 de marzo de 2016.* www.nrc.nl/nieuws/2016/03/04/gegevens-kankerpatienten-gestolen-1598045-a1087864>. Último acceso: 16 de febrero de 2017.

> “Los investigadores dicen que la falta de confianza en la seguridad digital del sector sanitario conduce a un futuro donde el público no aceptará nuevos desarrollos en tecnología médica..”

[11] Experian. “Fourth Annual 2017 Data Breach Industry Forecast”. *Experian Data Breach Resolution, 2017*. <http://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf>. Último acceso: 16 de febrero de 2017.

[12] HSS. “Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University”. *Departamento de Sanidad y Servicios Sociales de los EE.UU., 18 de julio de 2016*. <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ohsu/index.html>. Último acceso: 16 de febrero de 2017.

[13] HSS. “UMass settles potential HIPAA violations following malware infection”. *Departamento de Sanidad y Servicios Sociales de los EE.UU., 22 de noviembre de 2016.* <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/umass>. Último acceso: 16 de febrero de 2017.

[14] HSS. “Resolution agreement and corrective action plan“ (caso MAPFRE Life). *Departamento de Sanidad y Servicios Sociales de los EE.UU., 11 de enero de 2017.* <https://www.hhs.gov/sites/default/files/mapfre-ra-cap.pdf>. Último acceso: 16 de febrero de 2017.

[15] J. Finkle. “Premera Blue Cross Hacked, Medical Information Of 11 Million Customers Exposed”. *Reuters/The Hufftington Post, 17 de marzo de 2015.*<http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html>. Último acceso: 16 de febrero de 2017.

[16] J. Fink. “Cyber breach impacts BlueCross BlueShield members”. *Buffalo Business First, 5 de agosto de 2016.*<http://www.bizjournals.com/buffalo/news/2016/08/05/cyber-breach-impacts-bluecross-blueshield-members.html>. Último acceso: 16 de febrero de 2017.

[17] J. Leyden. “Medical superbugs: Two German hospitals hit with ransomware”. *The Register, 26 de febrero de 2016.* <https://www.theregister.co.uk/2016/02/26/german_hospitals_ransomware/>. Último acceso: 16 de febrero de 2017.

[18] M. J. Schwartz. “Report: US Data Breaches Reach Record Levels”. *InfoBankSecurity, 20 de enero de 2017.* <http://www.bankinfosecurity.com/blogs/reported-us-data-breaches-reach-record-levels-p-2374>. Último acceso: 16 de febrero de 2017.

[19] N. Versel. “Banner Health hacked, exposing data on 3.7M people”. *MedCityNews, 3 de agosto de 2016.* <http://medcitynews.com/2016/08/banner-health-hacked/>. Último acceso: 16 de febrero de 2017.

[20] R. Rodríguez. “Me ‹secuestraron› la farmacia y me pidieron un rescate en bitcoins”. *El Confidencial, 24 de febrero de 2017.* <http://www.elconfidencial.com/espana/2017-02-24/hacker-farmacia-robo-datos-bitcoins-ransonware_1338052/>. Último acceso: 16 de febrero de 2017.

[21] S. Greesin. “21st Century Oncology breach exposes patients’ info”. *Comisión Federal de Comercio de los EE.UU. Bitácora electrónica sobre información al consumidor, 4 de abril de 2016.* <https://www.consumer.ftc.gov/blog/21st-century-oncology-breach-exposes-patients-info>. Último acceso: 16 de febrero de 2017.

[22] S. Ragan. “Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers”. *CSO, 14 de febrero de 2016.* <http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html>. Último acceso: 16 de febrero de 2017.

[23] Solutionary. *“Solutionary SERT Q2 Report: 88 Percent of All Ransomware Is Detected in Healthcare Industry”.* Nota de prensa, 26 de julio 2016. <http://www.marketwired.com/press-release/solutionary-sert-q2-report-88-percent-all-ransomware-is-detected-healthcare-industry-nyse-ntt-2145268.htm>. Último acceso: 16 de febrero de 2017.

[24] S. Steffen. “Hackers hold German hospital data hostage”. *Deutsche Welle, 25 de febrero de 2016.* <http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030?maca=en-rss-en-all-1573-rdf>. Último acceso: 16 de febrero de 2017.

Notas

[1] Tipo de programa informático de naturaleza dañina, mediante el cual, un delincuente cibernético puede tratar de chantajear, impidiendo el acceso a la información que se guarda en el ordenador (la información suele quedar cifrada e inaccesible), hasta que no pague un rescate (*ransom*, en inglés) por ella. En principio, con el pago del rescate la información será descifrada, quedando nuevamente accesible. El *ransomware* es una de las principales amenazas a las que hoy se enfrentan los usuarios de redes informáticas como Internet.

[2] Fundada en 1990, la Fundación de la Frontera Electrónica (conocida como EFF por su denominación inglesa, *Eletronic Frontier Foundation*) es una organización no lucrativa que defiende las libertades civiles en el mundo digital (en la “*frontera digital*”). Trabaja para asegurar que derechos y libertades van a más y se respetan, a medida que aumenta la adopción de la tecnología. La EFF defiende el derecho a la intimidad, la libertad de expresión y la innovación mediante litigios de impacto, análisis de políticas, activismo de base y desarrollo tecnológico. <http://www.eff.org>.

[3] El Consejo de Conferencias de Canadá (del inglés, *The Conference Board of Canada*) es un centro de análisis estratégico independiente y sin ánimo de lucro, dedicado a construir un futuro mejor para los canadienses, mediante la búsqueda de una economía y una sociedad más dinámicas y competitivas. El Consejo está especializado en tendencias económicas, así como en aspectos relacionados con el rendimiento corporativo y las políticas públicas. El Consejo canadiense está afiliado a *The Conference Board, Inc. of New York*, aunque es independiente éste. <http://www.conferenceboard.ca>.

[4] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Texto legal: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>. Portal oficial: <http://www.eugdpr.org/>.

[5] El Centro para el Análisis y la Compartición de Información sobre el Sistema Sanitario (conocido como NH-ISAC por su denominación inglesa, *National Health Information Sharing and Analysis Center*) es una comunidad de confianza formada por propietarios y operadores de infraestructuras críticas, dentro del ámbito de la Sanidad y el Sistema Sanitario Público de los EE.UU. La comunidad se centra principalmente en la compartición de información oportuna, práctica y relevante entre sus miembros. Información que incluye elementos de inteligencia sobre amenazas, vulnerabilidades e incidentes, como indicadores de compromiso; tácticas, técnicas y procedimientos (TTP) de los delincuentes; consejos y buenas prácticas; estrategias de mitigación; y otro material valioso. El NH-ISAC promueve, asimismo, la construcción de relaciones mediante una serie de eventos formativos, con el fin último de favorecer ese clima de confianza. <https://nhisac.org/>.

[6] Técnica de ingeniería social que busca la *pesca* (*fishing*, en inglés) de usuarios (sus voluntades), engañándolos para que resulten en facilitadores a través de los cuales un determinado software dañino se introduzca en las redes informáticas de una organización. En el término *phishing* se produce un juego de palabras, propio de la lengua inglesa, en el que se combinan el sustantivo *phone* (teléfono) y el verbo *fish* (pescar). Se trataría, por tanto, de una *pesca por teléfono* que puede interpretarse, en un sentido más amplio, como una *pesca por medios telemáticos*.

[7] Activismo que emplea recursos digitales para llevar a cabo sus reivindicaciones. Como en el activismo tradicional de la realidad física, no virtual, en no pocas ocasiones los resultados de tales reivindicaciones pueden resultar en daños ocasionados a terceros o a su patrimonio. En el término original inglés, *hacktivism*, se da un juego de palabras, al combinarse el sustantivo *hacker* (experto informático [que emplea su destreza técnica para determinados fines -buenos o malos-]) con el también sustantivo *activism* (activismo). Se trataría, por tanto, de un *activismo de los expertos informáticos* o de un *activismo basado en, o que aprovecha, la pericia informática*.

La nueva "*3l1t3*"mediática

Mª José de la Calle
Cofundadora y Directora de Comunicación y Analista Senior del 'think tank' *español Instituto de Tendencias en Tecnología e Innovación (iTTi)*

<mjdelacalle@ittrendsinstitute.org>

Resumen: *A lo largo del artículo, la autora reconoce y traslada 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. Ello aporta una visibilidad, nunca imaginada, sobre una materia como ésta, tradicionalmente exclusiva de cierto ámbito profesional. La nueva 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 (3l1t3, en escritura "leet") mediática. Con la excusa de contribuir, también ella, a la divulgación de estos conceptos entre la referida audiencia, la autora hace un repaso de algunas de las amenazas para la seguridad digital más representativas del panorama actual, explicándolas a través de ejemplos y casos reales. Finalmente, se 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.*

Palabras clave: *calidad, datos personales, DDoS, fiabilidad, funcionalidad, gratuidad, inseguridad digital,* ransomware*, seguridad desde el diseño, seguridad digital.*

Autora

Mª José de la Calle es cofundadora, Directora de Comunicación y Analista Senior del '*think tank*' español Instituto de Tendencias en Tecnología e Innovación (iTTi). Con una experiencia de casi tres décadas en consultoría tecnológica, es una perfecta conocedora de las problemáticas ligadas al papel de la función informática en el seno de las organizaciones. Físico de formación y de corazón, muestra la misma pasión en su intención por hacer llegar el mensaje de la responsabilidad sobre *lo digital* a quienes componen los consejos de administración y otros órganos de gobierno de organizaciones públicas y privadas. En ello refleja, también, su experiencia como miembro de alguno de dichos órganos en entidades sin ánimo de lucro. Escribe regularmente sobre seguridad y tecnologías digitales en diferentes medios y revistas, como lo ha hecho para Novática anteriormente.

1. Contexto

Desde hace algunos años se ha empujado a la sociedad a un empleo masivo (acaso abusivo) de las tecnologías de la información, tanto para un uso personal como laboral. Objetivo que, a la vista está, se ha conseguido con creces[1].

Este uso masivo ha venido acompañado de una gran y creciente inseguridad en los datos y en la información que manejan los dispositivos digitales, que afecta no sólo a la marcha de los negocios y a la intimidad de las personas, sino a la propia integridad física de unos y otras, al haberse encomendado a los algoritmos parte del control de los procesos del mundo real y de las actividades de la vida diaria [2].

El problema de la inseguridad en el mundo virtual se conoce desde los inicios de la Informática. Ya en 1949, Von Neumann habló por primera vez de programas auto-replicantes y unos años después, en la década de los sesenta, verían la luz los primitivos predecesores de los actuales *virus* de naturaleza software [20]. Desde entonces, todo apunta a que no se ha sabido hacer las cosas mucho mejor. Reiteradamente ha primado la presión del *time-to-market* y, en lugar de producirse la evolución/revolución digital con una razonable seguridad, las prisas por situar nuevos productos en el mercado han llevado a ponderar, por encima de cualquier otro aspecto, su funcionalidad. Unos productos que, carentes de la debida calidad (y consiguiente seguridad; aunque sobrados de funciones), habitualmente han tenido que arreglarse (parchearse), a posteriori.

Peor aún, esa falta de seguridad innata ha venido acompañada de una *exigencia* que obliga al propio usuario a responsabilizase de mantener sus equipos seguros (para lo que se le ha venido dirigiendo una gran cantidad de advertencias y consejos sobre lo que debe hacer o lo que ha de evitar).

Tal enfoque, aun carente de toda lógica, parece haberse interiorizado. Y procedimentado: 1) vender productos defectuosos; 2) asignar al comprador la responsabilidad de utilizarlos correctamente para padecer los mínimos fallos; y, 3) al mismo tiempo, producir y comunicar (el fabricante) mejoras y parches.

No se trata de un tema tecnológico. Es una cuestión de moral y disciplina de mercado; de madurez del consumidor, quien debe despertar del ensueño inducido de productos buenos, seguros, gratis (o muy baratos), y sin otras contrapartidas.

Los ciberdelincuentes no son más listos que los desarrolladores de esos productos, no vienen de otro planeta. Y además, supuestamente, los desarrolladores pueden/deben conocer mejor que nadie dichos productos. ¡Son suyos! Por tanto, si, como parece evidente, disponen de la capacidad para arreglarlos después, ¡por favor, háganlo antes!

Como se ha dicho, lo que se está viendo es una carrera por sacar al mercado el producto antes que la competencia. Un gran plan para convertir a la ingente masa de usuarios/clientes (algunas empresas los cuentan, hoy, por miles de millones) en su departamento de calidad. ¡Y, encima, gratis! (O, siendo más precisos, con costes encubiertos para los propios usuarios/clientes, cual puede ser tener que hacer entrega de sus datos personales).

Hay en todo ello un trasfondo de regulación y voluntad política. Ambas escasas, dado que los propios gobiernos se benefician (cuando no las promueven), de las vulnerabilidades intrínsecas a las tecnologías digitales, para fines diversos, entre los que gozan de una posición de privilegio los de naturaleza militar y los de vigilancia/espionaje.

2. Nuevas celebridades: la jet set digital

Diariamente, la prensa generalista muestra, junto a noticias y comentarios sobre personajes políticos, futbolistas, artistas y otros protagonistas de la crónica informativa y social, términos que, hasta hace bien poco, nadie había visto (nadie habría imaginado ver) fuera de determinados ámbitos estrictamente profesionales. Hoy las menciones a anglicismos y/o neologismos relacionados con *lo digital* (algunos tan nuevos que aún no se tiene, apenas, referencia de ellos)

> “ El colectivo ciudadano es, precisamente, el que se muestra más expuesto ante las consecuencias de la inseguridad digital ”

como *ransomware*, *DDoS*, u otros, aparecen con regularidad en los titulares de noticias en televisión, en páginas web y en otros medios.

Muchos de dichos titulares juegan con la baza de contar con una audiencia entregada, por tratarse de noticias que se antojan propias de la crónica rosa y de la órbita de los paparazzi. Ejemplos de ello pueden ser casos como el del robo de fotografías comprometedoras de famosas, albergadas en la nube de Apple [5], o el de los ataques a páginas de contactos, como el portal AshleyMadison.com [15]. Otros están cargados de lecciones que deberían contribuir a que la opinión pública tomase conciencia de la ciberdebilidad (como efecto de la ciberdependencia) de la sociedad actual y de su estado del bienestar. Al menos, es el efecto pedagógico que debería tener el dar a conocer cómo más de doscientas mil personas se quedaron sin suministro eléctrico, hace poco más de un año, en Ucrania [21], tras un ciberataque. La revelación de los contenidos de mensajes de correo electrónico relacionados con la campaña de la candidata Clinton [24] y sus aparentes efectos sobre los resultados electorales en EE.UU., el pasado noviembre, deberían provocar, igualmente, más de una reflexión sobre lo *ciber-influenciable* que pueden llegar a ser las sociedades más conectadas.

En definitiva, se trata en todos los casos de sucesos que, independientemente del contexto en el que se producen, adquieren cada vez una mayor visibilidad y una mayor presencia mediática, por cuanto afectan, de forma creciente, al buen nombre, a la actividad y a la vida cotidiana de instituciones, empresas y ciudadanos en general.

Parece tratarse de una suerte de jet set digital que ensombrece al *establishment* y a la jet set tradicional. Es la nueva élite mediática.

El colectivo ciudadano es, precisamente, el que se muestra más expuesto ante las consecuencias de la inseguridad digital. La revelación de los datos médicos personales que cualquiera había confiado a su centro sanitario; la de la deuda contraída con determinada entidad, cuyas bases de datos se han podido ver comprometidas; o la aparentemente más inocente publicación, en la cuenta de Instagram de un antiguo compañero de universidad, de determinadas fotografías tomadas, entonces, tras una noche en la que compartieron algunas cervezas de más, son reflejo de la referida exposición.

Ventajas de *lo digital* como la disponibilidad, a precios cada vez más asequibles, de los más variopintos dispositivos de almacenamiento o la facilidad de replicación, con impecable exactitud, de la información en formato electrónico, convierten la *huella digital* de cualquier individuo (el detallado rastro de sus acciones en Internet) en imborrable. Y ello, más allá del *derecho al olvido* con cuya invocación ese mismo individuo puede demandar de los buscadores la retirada de las pistas de su paso por Internet. ¡Una batalla perdida! En esta coyuntura, situaciones como las descritas en el párrafo anterior pueden jugar a la contra ante la solicitud de un préstamo, la posibilidad de un nuevo contrato de trabajo, etc., en tanto que aquellas circunstancias pasadas (quizás ya olvidadas por sus protagonistas), pueden cobrar una actualidad no deseada y tener unas consecuencias de pesadilla para los interesados.

Los fallos de seguridad, naturalmente, afectan también a las organizaciones (empresas e instituciones), que pueden ver deterioradas sus cuentas y su imagen pública como resultado de cualquier incidente que suponga revelación no autorizada de su información, interrupción de sus operaciones o servicios, etc.

Los actores que se encuentran tras ese tipo de incidentes tienen perfiles y nombres muy diversos. Hasta cierto punto, hoy la figura del ciberdelincuente solitario parece un rastro del pasado. Es cierto que la actual disponibilidad y facilidad de uso de multitud de herramientas ciberofensivas permiten hablar de *ejércitos de un solo hombre*; pero no lo es menos que la imagen (en ocasiones, idílica) del atacante autónomo, hoy, deja paso, por una cuestión de eficacia y rentabilidad, a grupos más numerosos, organizados y jerarquizados. Se trata de bandas delictivas en toda regla, cuando no estructuras al servicio directo de estados soberanos o pseudo-soberanos (piense en los esfuerzos que dedica Daesh a su promoción y a sus acciones en el ciberespacio [18]).

Y al igual que los actores, también sus motivaciones y objetivos son diversos, desde el clásico incentivo económico (hoy, por ejemplo, el espionaje industrial resulta inconcebible sin el apoyo de *lo digital*), pasando por el ideológico (el citado ciberterrorismo de Daesh puede ser un inmejorable ejemplo), hasta el político en el que son los estados soberanos, sus gobiernos, quienes explotan las posibilidades del ciberespacio para vigilar a sus propios ciudadanos, para materializar sus estrategias geo-políticas o, simplemente, para abortar las de sus adversarios (en 2010 las pretensiones nucleares iraníes se vieron seriamente afectadas por los efectos de una ofensiva cibernética).

La atención que se ha prestado a Stuxnet, nombre dado al código informático dañino empleado contra el programa nuclear iraní, no sólo ha servido para conocer la complejidad que pueden llegar a alcanzar los ciberataques, habitualmente, ejecutados por fases (recogida previa de información, acceso al sistema objetivo, introducción del código dañino que permitirá, posteriormente, obtener el control remoto del citado sistema, ataque propiamente dicho, etc.), sino que también ha permitido evidenciar el posicionamiento mediático que las amenazas cibernéticas son capaces de alcanzar. En el caso de Stuxnet, su supuesta condición de *primera ciberarma de la Historia* le ha permitido venir copando portadas y titulares desde entonces [11] [14].

Como ocurrió con Stuxnet, actualmente son otras las amenazas que han logrado colarse entre la ciberélite mediática: el *ransomware*, los ataques DDoS o las *botnet* son destacados ejemplos.

3. *Ransomware*, la estrella del momento

Esta forma de código informático dañino que *secuestra* los datos de los sistemas que infecta, los cifra, dejándolos inaccesibles, para liberarlos posteriormente sólo previo pago de un rescate (*ransom*, en inglés) no es nueva; no obstante, en los últimos años, está adquiriendo una enorme relevancia: entre septiembre de 2013 y junio de 2014 el virus CryptoLocker infectó alrededor de medio millón de ordenadores en todo el mundo, afectando, entre otras entidades a la NASA y al Departamento de Sanidad y Servicios

> “El *ransomware* se ha extendido a todo tipo de víctimas, desde el usuario residencial a las redes corporativas, desde la microempresa a las grandes corporaciones, sin olvidar las entidades del sector público”

Sociales de los EE.UU. (HSS, por sus siglas en inglés) [16].

El *ransomware* se ha extendido a todo tipo de víctimas, desde el usuario residencial a las redes corporativas, desde la microempresa a las grandes corporaciones, sin olvidar las entidades del sector público [8].

En el caso de los dispositivos personales y domésticos, un informe de TrendMicro publicado el pasado mes de enero [26] describía cómo un televisor inteligente LG había sido infectado por una variante del virus *Flocker* creado para el sistema operativo Android y descubierto en mayo de 2015.

El 29 de septiembre de ese mismo año [12], Google anunciaba que había mil cuatrocientos millones de dispositivos Android (de propósito, tanto personal, como profesional) activos en el mundo; mil cuatrocientos millones de dispositivos susceptibles de ser atacados.

De hecho, en el ámbito corporativo las noticias sobre este tipo de ciberataques también han ocupado permanentemente los titulares durante todo 2016. Así, en marzo, un artículo de la BBC daba a conocer que tres hospitales de EE.UU. habían sido extorsionados en los dos primeros meses del año [3].

En suma, el alcance y el crecimiento que está experimentando el *ransomware* hacen de él la ciberamenaza estrella del momento actual. El reciente *Informe Anual de Amenazas 2017* de SonicWall habla de *crecimiento explosivo* en la distribución de *ransomware* [4], lo que la convierte, posiblemente, en el segmento de mayor crecimiento de la ciberdelincuencia. Concretamente, las cifras indican que este tipo de ataques crecieron 167 veces en un año, desde los 3,8 millones en 2015 a los 638 millones en 2016. El informe apunta, como causa de ese crecimiento, a una confluencia de factores como la aparición del *ransomware-como-servicio* (RaaS) y la normalización/popularización del acceso al Bitcoin.

Es, nuevamente, TrendMicro quien señala que el modelo de negocio RaaS permite a los creadores de este tipo de código nocivo ganar dinero con él, apoyándose en redes de distribuidores, los cuales no requieren, apenas, conocimientos técnicos [25]. Por tanto, cualquiera que pretenda hacer dinero rápido a costa de terceros (individuos, empresas u otras entidades) no tendrá más que contratar este servicio.

4. DDoS y *botnet*, coprotagonistas

El ampliamente divulgado (aquel día abrió los telediarios) ataque de denegación distribuida de servicio (del inglés “*Distributed Denial of Service*”, DDoS) que tuvo lugar el pasado 21 de octubre de 2016 sobre la empresa estadounidense Dyn no buscó dañar un dominio o sitio web específicos [22].

Dyn administra un servicio de traducción de nombres de dominio (direcciones de Internet en formato alfanumérico, como las habituales *.com*, por ejemplo), convirtiéndolos a un nuevo formato cuasi-numérico denominado dirección IP (éstas actúan como identificadores de los ordenadores conectados a Internet), facilitando la comunicación, esto es, la transmisión de paquetes de datos, entre unos ordenadores y otros. Por tanto, cualquier acción de sabotaje sobre el sistema a cargo de esa traducción/casación de nombres-direcciones truncará, no sólo su operativa normal, sino el acceso a cuantos dominios cuyos nombres no hayan podido ser traducidos. Todo esto constituye, sin duda, un paso hacia un nuevo nivel en la productividad de los ataques.

En el caso del ataque a Dyn las páginas web de numerosas empresas, entre ellas algunas de las más relevantes empresas de Internet (Netflix, PayPal, Sony PlayStation, Twitter, …), quedaron inaccesibles durante horas, como si se hubiera ejecutado un ataque particular sobre cada una de ellas de forma independiente.

El éxito de los ataques DDoS se basa en la capacidad del atacante para colapsar los servidores atacados (afectando a su ancho de banda) de forma que éstos no puedan seguir dando respuesta a las solicitudes/peticiones que reciben desde otros nodos o dispositivos. Cuanto más ancho de banda haya disponible, más peticiones simultáneas se requerirán; o, lo que es lo mismo, más dispositivos lanzándolas.

Esto último no parece constituir, hoy, un reto infranqueable. La existencia de multitud (miles de millones) de dispositivos conectados a Internet y débilmente protegidos frente a posibles intrusiones, favorece un escenario en el que hacerse con el control de tales dispositivos, no será sino una primera fase antes de utilizarlos para el lanzamiento, sobre el sistema que se pretende colapsar, de un número de peticiones lo suficientemente elevado como para que se llegue con holgura a los niveles pretendidos de saturación.

Ese escenario es el que ofrece la llamada *Internet de las Cosas* (IoT, por sus siglas en inglés), paradigma bajo el cual todo tipo de *máquinas* conectadas a Internet (cámaras de tráfico o de vigilancia, dispositivos vigila-bebés, termostatos, encaminadores, televisores, frigoríficos, relojes y pulseras que miden pulsaciones, el ritmo cardíaco y/o la calidad del sueño, contadores de luz, agua o gas, etc.), son capaces de comunicarse entre sí, a menudo de forma autónoma.

Con el oportuno software de control, ese comportamiento autónomo, podría moldearse, reorientando la voluntad de las máquinas hasta convertirlas en una suerte de red de autómatas, o red de zombis (*botnet* en la bibliografía inglesa), que lanzase peticiones al servidor objetivo, con el fin de colapsarlo. En el *Caso Dyn*, con ayuda del software nocivo *Mirai*, se logró alcanzar una tasa de peticiones del orden de 1,2 terabits de información por segundo.

Mirai ya había saltado a las portadas el mes anterior, cuando fue utilizado para atacar la página del periodista y divulgador de la seguridad digital, Brian Krebs[2]. En el *Caso Krebs* unos 380.000 dispositivos, *a las órdenes de Mirai*, lograron colapsar el servidor enviándole peticiones, a razón de 665 Gbits/seg.

Poco después del ataque a Krebs, se publicaría el código fuente de *Mirai* [7], provocando que el número de *botnets* aumentara.

El 14 de octubre de 2016, a tan sólo una semana del ataque a Dyn, el Departamento de Seguridad Interior de los EE.UU. había publicado una alerta sobre *Mirai* [9] y sobre los peligros de los ataques DDoS ejecutados por *botnets* compuestas por dispositivos de la IoT. La alerta también preveía posibles ataques futuros.

> “Sí, hay remedio. ¡Debe haberlo! Con el importante matiz de que la seguridad total no existe”

Y así ocurrió. A mediados de noviembre pasado 900.000 clientes de la operadora alemana Deutsche Telecom vieron como su servicio quedaba interrumpido por una variante de *Mirai* introducida en los encaminadores que la compañía tiene distribuidos por los domicilios de sus clientes. Ello se había logrado gracias a una vulnerabilidad en el proceso que permitía a la operadora actualizar remotamente el *firmware* de sus equipos. También en el Reino Unido, la compañía de telefonía TalkTalk sufría la infección de *Mirai* en 2.400 de sus encaminadores. Además, en esos días, se daba a conocer la noticia de que más de ochenta modelos de cámaras Sony eran vulnerables a *Mirai*, pudiéndose tomar el control de ellas [17].

Se trata, por tanto, de un panorama en el que hasta los fabricantes legítimos de hardware/software/firmware quedan en entredicho, cuando sus propios mecanismos de actualización de equipos y dispositivos pierden toda fiabilidad, abriendo la puerta a riesgos de seguridad digital de cualquier tipo.

Por si todo esto no fuera suficiente, de nuevo se trata de servicios que, como se ha indicado para el caso del *ransomware*, se pueden comprar, alquilar o contratar [19] [23] [6].

5. El reto: ¿hay remedio a todo este desastre?

Sí, hay remedio. ¡Debe haberlo! Con el importante matiz de que la seguridad total no existe.

Sí, parece haber un primer remedio en la propia tecnología, en la aplicación de más tecnología. Lo parece porque es el tipo de remedio que más adeptos demuestra tener en el ámbito corporativo: los gastos en seguridad digital en las empresas no hacen más que aumentar. No obstante, no es un remedio que, hasta la fecha, se haya mostrado del todo eficaz (salvo para quienes viven de él, ofreciendo soluciones y servicios de seguridad digital): a pesar de que la inversión, año a año, va a más, los incidentes y sus consecuencias no van a menos. Es lo que el analista Garrett A. Bekker, III, denomina *La Gran Desconexión* [10].

Por tanto, añadir tecnología complementaria o *de subsanación* (se da por sentado que habrá vulnerabilidades y se opta, tanto preventiva, como reactivamente, según el tipo de soluciones que se apliquen, por *subsanarlas* mediante apósitos) no es suficiente.

Frente a esta frustración, una solución que se antoja más eficaz es la de considerar la seguridad como un requisito más de los productos y servicios de naturaleza digital. Todo dispositivo electrónico y cualquier software pueden ser razonablemente seguros. No obstante, por desgracia, no es éste un requisito que suela recogerse en las especificaciones de fabricación/desarrollo. No siempre se contempla la *seguridad desde el diseño*, como ocurre con otras especificaciones funcionales, de rendimiento, etc.

De hecho, la seguridad no sólo debería estar presente en las etapas más tempranas del diseño, debería formar parte de todos los procesos de la organización.

Finalmente, ponerle remedio a la actual situación pasa, necesariamente también, por una mayor exigencia del consumidor a la hora de adquirir productos seguros. Y por la obligación ciudadana de demandar de los representantes políticos legislaciones que obliguen a comercializar productos y servicios digitalmente seguros, dentro de lo razonable; como ocurre con otras seguridades, más tradicionales, en determinados sectores industriales.

Si no se le pone remedio, lo digital podría quedar relegado a su aplicación en actividades poco relevantes, poco críticas. Y a su sustitución en éstas, por mecanismos que, hoy, resultarían estrafalarios. Sirvan como aviso la vuelta a la máquina de escribir del Kremlin [13], ya anunciada en 2013; o el más reciente anuncio del hotel *Romantik Seehotel Jaegerwirt* de sustituir su moderno sistema informático de gestión de apertura y cierre de puertas, basado en el uso de tarjetas, por las más convencionales cerraduras con la llave de toda la vida [1].

Referencias

[1] A. Martí. “Cuando no puedes entrar a tu habitación de cuatro estrellas porque tu hotel ha sufrido un ciberataque”. *Xataka, 20 de enero de 2017.* <https://www.xataka.com/seguridad/cuando-no-puedes-entrar-a-tu-habitacion-de-cuatro-estrellas-porque-tu-hotel-ha-sufrido-un-ciberataque>. Último acceso: 19 de febrero de 2017.

[2] A. Reid. “Here’s how we can protect ourselves from the hidden algorithms that influence our lives”. *The Conversation, 20 de diciembre de 2016.* <https://theconversation.com/heres-how-we-can-protect-ourselves-from-the-hidden-algorithms-that-influence-our-lives-70674>. Último acceso: 16 de febrero de 2017.

[3] BBC. “Three US hospitals hit by ransomware”. *BBC News, 23 de marzo de 2016.* <http://www.bbc.com/news/technology-35880610>. Último acceso: 18 de febrero de 2017.

[4] B. Conner. “SonicWall Annual Threat Report reveals the state of the cybersecurity arms race”. *SonicWall, Blog, 6 de febrero de 2017.* <https://blog.sonicwall.com/2017/02/sonicwall-threat-report-reveals-cybersecurity-arms-race/>. Último acceso: 18 de febrero de 2017.

[5] C. Athur. “Naked celebrity hack: security experts focus on iCloud backup theory”. *The Guardian, 1 de septiembre de 2014.* <https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence>. Último acceso: 16 de febrero de 2017.

[6] C. Doctorow. “Two hackers are selling DDoS attacks from 400,000 IoT devices infected with the Mirai worm”. *BoingBoing, 28 de noviembre de 2016.* <http://boingboing.net/2016/11/28/two-hackers-are-selling-ddos-a.html>. Último acceso: 19 de febrero de 2017.

[7] C. Osborne. “Source code of Mirai botnet responsible for Krebs On Security DDoS released online”. *ZDnet/ZeroDay, 3 de octubre de 2016.* <http://www.zdnet.com/article/source-code-of-mirai-botnet-responsible-for-krebs-on-security-ddos-released-online/>. Último acceso: 19 de febrero de 2017.

[8] Departamento de Justicia de los EE.UU. “How to protect your networks from ransomware”. *Gobierno de los EE.UU., 2016.* <https://www.justice.gov/criminal-ccips/file/872771/download>. Último acceso: 18 de febrero de 2017.

[9] DHS/US-CERT. “Heightened DDoS Threat Posed by Mirai and Other Botnets”. *Department of Homeland Security/US Computer Emergency Readiness Team. Alert (TA16-288A), 14 de octubre de 2016.* <https://www.us-cert.gov/ncas/alerts/TA16-288A>. Último acceso: 19 de febrero de 2017.

[10] G. A. Bekker. “The 2017 Data Threat Landscape”. *451 Research, 14 de febrero de 2017.* <https://www.youtube.com/watch?v=N1uV9QYsxoI&feature=youtu.be>. Último acceso: 19 de febrero de 2017.

[11] G. Julián. “Stuxnet: historia del primer arma de la ciberguerra”. *Genbeta, 2 de diciembre de 2013.* <https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra>. Último acceso: 18 de febrero de 2017.

[12] J. Callaham. “Google says there are now 1.4 billion active Android devices worldwide”. *Android-Central, 29 de septiembre de 2015.* <http://www.bbc.com/news/technology-35880610>. Último acceso: 18 de febrero de 2017.

> “ Frente a esta frustración, una solución que se antoja más eficaz es la de considerar la seguridad como un requisito más de los productos y servicios de naturaleza digital ”

[13] J. Mendiola. “El Kremlin recupera la máquina de escribir como herramienta de inteligencia”. *El Confidencial, 16 de julio de 2013.* <http://www.elconfidencial.com/tecnologia/2013-07-16/el-kremlin-recupera-la-maquina-de-escribir-como-herramienta-de-inteligencia_766293/>. Último acceso: 19 de febrero de 2017.

[14] K. Zetter. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon”. *Wired, 3 de noviembre de 2014.* <https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/>. Último acceso: 16 de febrero de 2017.

[15] K. Zetter. “Hackers Finally Post Stolen Ashley Madison Data”. *Wired, 18 de agosto de 2015.* <https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/>. Último acceso: 16 de febrero de 2017.

[16] L. Franceschi-Bicchierai. “Even NASA got infected with ‹CryptoLocker› ransomware”. *Motherboard, 5 de junio de 2015.* <https://motherboard.vice.com/en_us/article/even-nasa-got-infected-with-cryptolocker-ransomware>. Último acceso: 18 de febrero de 2017.

[17] L. H. Newman. “The botnet that broke the Internet isn’t going away”. *Wired, 9 de diciembre de 2016.* <https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/>. Último acceso: 19 de febrero de 2017.

[18] M. Montgomery. “ISIS and the Internet. Turning a tool into a weapon”. *Radio Canada International, 20 de septiembre de 2016.* <http://www.rcinet.ca/en/2016/09/20/isis-and-the-internet-turning-a-tool-into-a-weapon/>. Último acceso: 17 de febrero de 2017.

[19] M. Wilson. “Want to launch your own DDoS attacks? Just buy them from Lizard Squad”. *BetaNews, 2015.* <https://betanews.com/2014/12/31/want-to-launch-your-own-ddos-attacks-just-buy-them-from-lizard-squad/>. Último acceso: 19 de febrero de 2017.

[20] Panda Security Internacional. “(I) Evolution of computer viruses: history of viruses”. *Communication USA. Nota de prensa, 12 de abril de 2004.* <http://www.pandasecurity.com/about/press/viewnews.htm?noticia=4944&entorno=&ver=&pagina=&producto=>. Último acceso: 16 de febrero de 2017.

[21] S. Khandelwal. “Hackers cause world’s first power outage with malware”. *The Hacker News, 5 de enero de 2016.* <http://thehackernews.com/2016/01/Ukraine-power-system-hacked.html>. Último acceso: 16 de febrero de 2017.

[22] S. Khandelwal. “Massive DDoS attack against Dyn DNS service knocks popular sites offline”. *The Hacker News, 21 de octubre de 2016.* <http://thehackernews.com/2016/10/dyn-dns-ddos.html>. Último acceso: 16 de febrero de 2017.

[23] T. Fox-Brewster. “Hackers Sell $7,500 IoT Cannon To Bring Down The Web Again”. *Forbes, 23 de octubre de 2016.* <http://www.forbes.com/sites/thomasbrewster/2016/10/23/massive-ddos-iot-botnet-for-hire-twitter-dyn-amazon/#dae9914c9156>. Último acceso: 19 de febrero de 2017.

[24] T. Hamburger, K. Tumulty. “WikiLeaks releases thousands of documents about Clinton and internal deliberations”. *The Washington Post, 22 de julio de 2016.* <https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.7863428b8545>. Último acceso: 16 de febrero de 2017.

[25] TrendMicro. “Ransomware-as-a-Service: Ransomware operators find ways to bring in business”. *TrendMicro, 2 de septiembre de 2016.* <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-ransomware-operators-find-ways-to-bring-in-business>. Último acceso: 18 de febrero de 2017.

[26] TrendMicro. “Ransomware Recap: Dec. 19 - Dec. 31, 2016”. *TrendMicro, 10 de enero de 2017.* <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-dec-19-dec-31-2016>. Último acceso: 18 de febrero de 2017.

Notas

[1] Seguramente, habrá llamado la atención del lector el uso de la palabra “3l1t3” en el título del artículo, la cual viene a significar “élite” en escritura “leet”. Este tipo de escritura alfanumérica es propia de algunas comunidades de Internet, y consiste en la sustitución de caracteres alfabéticos (letras, principalmente vocales) por dígitos numéricos. Considerada una forma de comunicación sólo para iniciados, debe su nombre, leet speak (1337 5p34K) precisamente a eso: la forma de hablar de la élite (elite speak, en inglés).

[2] “KrebsOnSecurity. In-depth security news and investigation” (KrebssobreSeguridad. Noticias e investigación en profundidad sobre seguridad). <https://krebsonsecurity.com/>. Último acceso: 19 de febrero de 2017.

¿Quién se hace cargo?

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>

Resumen: *La seguridad digital es un asunto de todos; pero, quizás, de unos más que de otros. El autor desarrolla esa idea, reparando en el papel de quienes, tal vez más intensamente, han de asumir el citado asunto como propio: 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 sus organizaciones. 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 afirmación, el autor, hace 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.*

Palabras clave: *ATI, CCI, cíber, consejo de administración, consejero delegado, imputabilidad, iTTi, monografía, Novática, rendición de cuentas, responsabilidad, seguridad digital.*

Autor

Miguel García-Menéndez, Socio y Vicepresidente de ATI, es 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.

1. Introducción

A estas alturas de la monografía voy a pediros que me permitáis compartir con vosotros alguna sana confidencia. Actuar como editor de cualquier obra literaria coral, incluidas las de carácter técnico como la presente, otorga una serie de ventajas que uno debe aprovechar y con las que ha de saber jugar.

Para empezar, ser el punto de confluencia de todos los textos con los que el resto de coautores contribuyen al documento final permite saciar la curiosidad propia semanas antes de que el lector pueda hacer lo mismo con la suya.

Por otra parte, conocer el contenido completo de los referidos textos ofrece una perspectiva general, sobre los mensajes que encierran, que habrá de ayudar a no repetirlos (máxime, si uno los lee antes de redactar los suyos) o, en su defecto, habrá de ayudar a justificar el motivo de una supuesta repetición (presumiblemente, siempre molesta para el lector).

Finalmente (enumero sólo estas ventajas, consciente de que hay muchas más), ser editor de una monografía facilita la ventaja de poder mencionar al resto de coautores y sus reflexiones, al objeto de complementar las que uno mismo desea plasmar. Serlo de la que tiene en pantalla en este momento me permite citar a John McCarthy, quien, como parte de sus razonamientos, recogidos en el artículo "*El ciberpuzle. Cómo el sentido común puede resolverlo*", de esta misma monografía, plantea la siguiente cuestión: "*¿quién debería responsabilizarse por la seguridad digital de una organización?*", "*una pregunta perfectamente razonable y sensible*", según él mismo declara.

2. Consejos de administración

La respuesta que ***John McCarthy*** da a su propia pregunta es ésta: "*El consejo de administración. Es un asunto que ha de tratarse a nivel de consejo*". Una respuesta que él mismo tilda de "*una gran verdad, vital para la evaluación, despliegue y gestión exitosas de la seguridad digital*". ¡No puedo estar más de acuerdo (tanto con su respuesta, cuanto con su valoración)!

En efecto, una respuesta fácil (califica el autor) que, no obstante, no invalida la idea de que la seguridad digital es un asunto de todos [13]; que todos los miembros de una empresa (incluido el personal subcontratado y otros interesados), dentro de su ámbito de actuación, han de velar, tratar de evitar y, en todo caso, estar alerta ante cualquier incidente de naturaleza cibernética que pueda producirse y detectarse; contribuyendo, de ese modo, al éxito de las referidas evaluación, despliegue y gestión de la seguridad digital.

Una respuesta *fácil,* y rápida, porque no tiene en cuenta, a priori, el papel prioritario de áreas (el propio autor las menciona) como las de tecnología, las de producción, las de RR.HH., las de asesoría jurídica, etc., en la gestión operativa de la seguridad digital.

Ciertamente, sin desmérito de los relevantes papeles que pueden corresponder a los diferentes grupos con interés en la protección de una organización ante los riesgos que la acechan, el que le toca interpretar a quienes están al frente de aquella (consejeros y directivos), en materia de rendición de cuentas por su responsabilidad sobre el uso que la propia organización hace de lo digital y sus consecuencias, merece una particular atención.

Una valoración muy optimista de la situación vivida hasta ahora permitiría afirmar que lo digital (y, particularmente, *lo cíber)* no ha sido un tema que interesara, en demasía, a los señores consejeros. En ello pueden haber influido los antecedentes, particularmente los académicos, de estos individuos; y su edad, la cual dibuja, a su vez, un perfil académico determinado: juristas y economistas componen, mayoritariamente, el censo de consejeros actual, lo que podría contribuir a alejarlos de la responsabilidad que hoy les toca asumir en plena era digital.

> “ Una valoración muy optimista de la situación vivida hasta ahora permitiría afirmar que lo digital (y, particularmente, lo cíber) no ha sido un tema que interesara, en demasía, a los señores consejeros ”

En unos años la Biología estará haciendo su trabajo y habrá comenzado a colocar en los consejos a unos nuevos sesentones (la firma Spencer Stuart sitúa la edad media del consejero español en los sesenta años [21]). La diferencia con sus actuales colegas será que, para entonces, aquellos habrán desarrollado toda o gran parte de su carrera tras el debut de la Internet comercial (1995), lo que supondrá, en poco tiempo, trayectorias de un mínimo de veinticinco o treinta años interactuando con el medio digital. Como consecuencia, la confianza en el efecto del salto generacional lleva a imaginar unas futuras agendas corporativas distintas a las que manejan hoy la mayoría de consejeros.

Mientras se produce ese salto, otros parecen ser los incentivos que contribuirán a acercar el mensaje *cíber* (y, con él, el digital) a los consejos de administración [4] [9]: haber sufrido en carne propia (o en las proximidades) algún incidente digital; el mandato de los organismos reguladores; la opinión de las agencias de calificación; las pólizas de seguros cibernéticas; y, en última instancia, la búsqueda de la resiliencia y la perdurabilidad de sus respectivas organizaciones [12].

Aun así, como señala desde el MIT el Profesor Peter Weill, esta entrada de *lo digital* en las agendas de los consejos de administración por la vía de *lo cíber*, no es más que “una aproximación excesivamente defensiva” [17]. A su juicio, los consejos deberían aprovechar la inercia que comienza a ofrecer su incipiente preocupación por la seguridad digital, y tomarla como un primer estadio en el camino hacia otro nivel más estratégico, desde el cual puedan percibir la verdadera contribución de lo digital y se ocupen, en consecuencia, de temas clave para el progreso de sus empresas, como los vinculados a la innovación y al resto de oportunidades que lo digital les brinda.

3. Nombres propios

Esa situación de consenso en relación al papel de los consejos de administración y los consejeros (hoy comienzan a ser, ya, múltiples las voces que comparten la idea de su imputabilidad digital) resulta gratificante para quienes, hace ya muchos años, comenzamos la solitaria tarea de predicar ese principio. Las discrepancias, no obstante, surgen en su interpretación.

Para los miembros del parlamento británico (elaboraron un informe al respecto tras el primero de los ciberincidentes en la operadora TalkTalk [7]) resulta evidente que la responsabilidad última en materia de seguridad digital recae en el consejo de administración o, más precisamente, en uno de sus miembros, el consejero delegado de la organización. A dicha figura dirigen, también, ciertas cautelas como la de fijar parte de su retribución bajo un criterio variable que responda al comportamiento de la empresa en relación a la seguridad digital (a menos incidentes y mejor gestionados, mayor garantía de retribución).

Sin embargo, el informe de los parlamentarios británicos señala algo más: a pesar de su responsabilidad desde el punto de vista del rendimiento de cuentas, un consejero delegado no tendrá por qué dimitir ante la declaración de una crisis de naturaleza cibernética. Así ha sido en el caso de ***Dido Harding***, consejera delegada de la operadora británica, y en el de otros muchos en la reciente historia de los incidentes relacionados con la seguridad digital. Sin embargo, y aquí está nuestra discrepancia, no es menos cierto que la nómina de directivos que en los últimos años han sufrido, en carne propia, las consecuencias de algún problema de naturaleza tecnológica, no ha parado de crecer.

El reciente informe “*Beneficios de la Ciberseguridad para las Empresas Industriales”,* publicado conjuntamente por los *“think tanks”* españoles CCI (Centro de Ciberseguridad Industrial) [CCI17] e iTTi (Instituto de Tendencias en Tecnología e Innovación) [9], recoge una numerosa relación de nombres propios, correspondientes a casos en los que los primeros directivos de una serie de organizaciones se vieron en la obligación de rendir cuentas a título personal, tras verse envueltos en diferentes escándalos o incidentes de consecuencias notables, con algún tipo de trasfondo tecnológico.

Dicha relación de nombres propios se reproduce, a continuación, de forma ampliada.

3.1. Frank Hopf. Olympic Pipe Line Company (EE.UU., 1999)

Las gravísimas consecuencias (fallecieron un adolescente y dos niños) del accidente que tuvo lugar en la tarde del 10 de junio de 1999 en la localidad de Bellingham (WA, EE.UU.), tras la fuga y posterior explosión de gasolina procedente del oleoducto de la compañía Olympic Pipe Line Company, truncaron la carrera de Frank Hopf, entonces Vicepresidente de la empresa [16]. Como demostraría la investigación posterior, el negligente uso que se hizo de los sistemas de supervisión y control (SCADA, por sus siglas en inglés) empleados en la operación de la instalación fue uno de los factores que contribuyeron a la gravedad del incidente (o, al menos, a no mitigarla). Hopf se vería obligado a dejar su puesto como ejecutivo al frente de las operaciones del oleoducto y sería imputado en el juicio posterior.

3.2. Randy Rademacher. Comair (EE. UU., 2004)

La Nochebuena de 2004 Papá Noel dejó a miles de niños estadounidenses sin sus regalos de Navidad. El motivo: los más de doscientos mil emisarios del viejo finlandés que se quedaron atrapados en decenas de aeropuertos del medio-oeste de los EE.UU. La compañía doméstica Comair canceló aquella jornada la mayor parte de sus vuelos, aparentemente debido al mal tiempo que desde hacía días llevaba sufriendo el centro del país. La verdadera razón, sin embargo, fue un fallo (por obsolescencia y saturación) de uno de los sistemas de información críticos de la aerolínea. El Consejero Delegado de la compañía, Randy D. Rademacher, dimitiría, a consecuencia de estos hechos, apenas tres semanas después, el 17 de enero de 2005 [20].

3.3 Peter Darbee. Pacific Gas and Electric Corporation (EE.UU., 2010)

El hombre es el único animal que tropieza dos veces en la misma piedra. Y, en ese sentido, el subsector energético del petróleo y el gas parece seguir disciplinadamente los pasos de la Humanidad. Algo más de una década después de los sucesos de Bellingham, relatados más arriba, otro incidente de similares características (esta vez con consecuencias aún más graves) tuvo lugar en la localidad de San Bruno (CA, EE.UU.).

En torno a las 06:11 horas de la tarde (hora del Pacífico), del 9 de septiembre de 2010, la inesperada explosión de un gasoducto que transportaba gas natural abría un cráter en plena calle en la citada ciudad californiana. El incendio generado tras la explosión arrasaría treinta y ocho viviendas, afectaría

> “ El grupo atacó la infraestructura informática de HBGary Federal, llevándose miles de mensajes de correo electrónico que, posteriormente, publicaría ”

a otras setenta y, lo que es más grave, se llevaría por delante la vida de ocho personas, hiriendo a muchas más. Como en el *caso Bellingham,* la investigación llevada a cabo posteriormente concluiría dando un papel relevante a los sistemas de supervisión y control del gasoducto (SCADA, por sus siglas en inglés). Las causas del accidente fueron múltiples, principalmente, las deficientes prácticas de control de calidad seguidas durante la construcción e instalación del tubo más de cincuenta años atrás. Sin embargo, las limitadas funcionalidades de los sistemas SCADA desde los que se operaba el gasoducto, como recogió el informe, junto a la falta de un claro protocolo de respuesta ante la emergencia que recogiera las instrucciones destinadas, entre otros, al personal que operaba el SCADA, contribuyeron a que las consecuencias del accidente no fueran mucho menores. Estos hechos, junto a otras recientes decisiones erróneas, atribuidas a Peter Darbee, como Presidente Ejecutivo de la corporación, forzaron su dimisión (en realidad una jubilación anticipada, pactada), que sería anunciada el 21 de abril de 2011. Un par de semanas antes, el día 6, también habían sido apartados de sus cargos John *(Jack)* Keenan, Director de Operaciones de la subsidiaria que operaba el gasoducto de San Bruno, PG&E Co., y su Vicepresidente Senior de Ingeniería y Tecnologías de Operación, Edward Salas [3].

3.4. Aaron Barr. HBGary Federal (EE. UU., 2011)

Pretender recomponer la maltrecha economía de una empresa valiéndose de un golpe de efecto mediático que le devuelva visibilidad y, con ello, mejores expectativas comerciales, tiene sus riesgos. Máxime si el efecto mediático pretende aprovechar la popularidad de un tercero. Y, más aún, si ese tercero es el grupo *hacktivista* Anonymous. Esa fue, precisamente, la apuesta que hizo Aaron Barr, entonces Consejero Delegado de la firma de servicios de ciberinteligencia HBGary Federal, cuando a principios de 2011 anunció que desvelaría las identidades de los cabecillas de Anonymous en la conferencia de ciberseguridad “B-sides” de San Francisco (EE.UU.). La reacción de Anonymous ante el anuncio no se hizo esperar. El grupo atacó la infraestructura informática de HBGary Federal, llevándose miles de mensajes de correo electrónico que, posteriormente, publicaría. El contenido revelado por los mensajes dejaba en muy mal lugar, tanto a Barr, como a la propia HBGary Federal, por el perfil poco ético de algunas de las propuestas de colaboración profesional (rozando lo ilegal) que había planteado a, o que había ejecutado para, alguno de sus clientes. De hecho, todo ello ponía en tela de juicio, también, la ética de los propios clientes. El mazazo a la reputación de HBGary Federal y a la del propio Barr derivó en la dimisión de éste, que se produjo el 28 de febrero de aquel mismo año [15].

3.5. Satoru Nishibori. Mizuho Bank (Japón, 2011)

¡Las desgracias nunca vienen solas! Los japoneses padecieron un destructivo terremoto y un, aún más devastador, tsunami el 11 de marzo de 2011. Algunos de ellos, además, tuvieron la desgracia de encontrarse con otro problema añadido: aquellos que acudieron a los cajeros automáticos del banco comercial Mizuho vieron frustradas sus intenciones de hacerse con efectivo. La red de cajeros de Mizuho Bank se había caído (hay que decir que por saturación, y ¿obsolescencia?; y no como consecuencia directa del terremoto). De hecho, no era la primera vez que la entidad se enfrentaba a un problema como ese. Ya había ocurrido en 2002 (¡las desgracias nunca vienen solas!). Dado el nuevo infortunio causado a sus clientes en esos inoportunos y desgraciados momentos, Satoru Nishibori, Consejero Delegado del banco, anunció su dimisión el 23 de abril. Una dimisión que se haría efectiva durante la junta de accionistas prevista para el mes de junio de aquel año [5].

3.6. Sue Lewis. NHS (Reino Unido, 2012)

¡Dormir con el enemigo! Todo comenzó en un restaurante indio de Guildford (Inglaterra, Reino Unido). Debía ser 2010. Aquel día los comensales eran Peter Raymond Barry Lewis, Director de Informática del Royal Surrey County Hospital NHS Foundation Trust, y uno de sus proveedores, Richard Norman Moxon. En el transcurso de la comida, Lewis (no era la primera vez que tenía este comportamiento) sugirió a Moxon que podría favorecer su propuesta …, siempre que él se viese, también, favorecido. Había en juego un suculento nuevo contrato de software, con destino al área de urgencias del hospital, por valor de más de 900.000 libras esterlinas sólo el primer año. El contrato sería, finalmente, adjudicado a la empresa de Moxon y los ingresos, a raíz de unas 7.000 libras esterlinas al mes, comenzarían a llegar a la misma cuenta en la que Lewis recibía su nómina, en enero de 2011. Para cuando el fraude pudo ser descubierto, en diciembre de aquel año, el dinero desviado ya superaba las 80.000 libras. Además, el software entregado por Moxon no cumplía las especificaciones, por lo que la pérdida económica para el hospital resultó ser mucho mayor. Peter Lewis sería despedido en aquel mismo momento (diciembre de 2011). Apenas unas semanas después, su esposa, Sue Lewis, quien, al parecer, no había tenido nada que ver con el comportamiento de su marido y quien, hasta entonces, ocupaba un puesto en la junta directiva del hospital, en tanto que Directora General Adjunta y Directora de Operaciones, se vio abocada a dimitir, tras el bochorno sufrido, hecho que se produjo el 8 de febrero de 2012, después de una trayectoria de más de diecisiete años en la institución. Cinco años después, el 6 de enero de 2017, tanto Lewis, como Moxon, escucharían su sentencia condenatoria en el palacio de justicia de Guildford [8].

3.7. Jim Etter. Departamento de Tributos de Carolina del Sur (EE.UU., 2012)

El 13 de agosto de 2012 un funcionario del Departamento Tributario de Carolina del Sur abrió un mensaje de correo electrónico que nunca debió haber abierto. La acción del funcionario permitió que el remitente introdujera en la red del Departamento un programa informático dañino del que se valdría un mes después para realizar el mayor robo de datos personales ocurrido, hasta entonces, en una administración estatal, dentro de los EE.UU. El botín fueron los datos (números de la Seguridad Social, números de cuentas bancarias, etc.) de más de tres millones de contribuyentes. El 20 de noviembre la Gobernadora del Estado aceptó la dimisión del veterano Jim Etter, quien había sido, hasta ese momento, Director del citado Departamento [14].

3.8. Gregg Steinhafel. Target (EE.UU., 2013)

En cierto sentido, el caso *Target* podría tildarse de paradigmático. Parece haber marcado un antes y un después en la historia

> “ Unos cuarenta millones de clientes vieron comprometidos los datos relativos a sus tarjetas de crédito ”

de los ciberataques corporativos. La atención mediática que ha recibido y algunas de sus consecuencias (la dimisión del Presidente de su Consejo de Administración) han hecho de él un caso de libro que ha despertado la atención y el interés por la ciberseguridad de no pocos directivos (al menos, en EE.UU.). La conocida cadena de tiendas (hipermercados) sufrió un importante robo de datos entre finales de noviembre y principios de diciembre de 2013. Unos cuarenta millones de clientes vieron comprometidos los datos relativos a sus tarjetas de crédito. El notable impacto sobre la reputación de la empresa, aceleró, primero, el cese de su Directora de Sistemas de Información, Beth Jacob (el 5 de marzo de 2014); y, después, la dimisión de su Presidente Ejecutivo y Consejero Delegado, Gregg Steinhafel (el 5 de mayo de 2014) [6].

3.9. Amy Pascal. Sony Pictures Entertainment (EE.UU., 2014)

Lamentablemente, el historial de ciberataques al grupo Sony distaba de estar limpio cuando el 24 de noviembre de 2014 le llegó el turno a su rama cinematográfica. La atribución (origen) de este tipo de ataques siempre resulta problemática; pero, en este caso, todo indicaba que Corea del Norte podía estar tras el trabajo firmado por los “*Guardians of Peace”* (#GOP). No en vano, en el centro de la tormenta estaba el inminente estreno de la comedia *“The Inteview”*, en la que se relataba una conspiración para asesinar al líder norcoreano Kim Jong-un. Argumento que no pareció resultar del agrado de las autoridades de Pionyang. Las consecuencias de la disputa sobre la distribución, o no, de la película no se hicieron esperar. #GOP cumpliría sus amenazas, publicando el botín de documentos y otro material obtenido en el ataque. Entre ellos, una serie de mensajes de correo electrónico, firmados por Amy Beth Pascal, en los que no dejaba en muy buen lugar a personajes como el entonces Presidente de los EE.UU., Barack Obama, ni a actores como Leonardo DiCaprio o Angelina Jolie. El 5 de febrero de 2015, Pascal sería despojada de sus cargos de Co-Presidente del Consejo de Administración de Sony Pictures Entertainment y Presidente del Consejo de Administración del Motion Pictures Group [23].

3.10. Katherine Archuleta. OPM (EE. UU., 2015)

Los problemas cibernéticos para la Oficina de Gestión de Personal de los EE.UU. (OPM, por sus siglas en inglés) habían comenzado en julio de 2014 (presumiblemente antes); pero en abril de 2015 se intensificaron, cuando se descubrió que los sistemas de la agencia estaban siendo comprometidos. El anuncio se hizo el 4 de junio: la brecha afectaba a unos cuatro millones de funcionarios y/o exfuncionarios (además, de candidatos, familiares, etc.). Sin embargo, esto no sería más que el principio. Una semana después se reveló la existencia de una segunda fuga de datos. Esta vez la cifra de afectados superaba los veinte millones. El 10 de julio, la Directora General de la agencia, Katherine Archuleta, presentaba su renuncia ante la Casa Blanca. La OPM requería un nuevo liderazgo más cercano a (conocedor de) la problemática digital, sugería el comunicado oficial [11].

3.11. Noel Biderman. Avid Life Media (EE.UU., 2015)

El rostro de una mujer pidiendo silencio en la imagen corporativa del portal de contactos Ashley Madison, propiedad de Avid Live Media, no libró al fundador de ésta, Noel Biderman, de la indiscreción de los ciberdelincuentes. Éstos publicaron, entre otros, unos comprometedores mensajes de los que se desprendía la presunta infidelidad del Noel Biderman (casado y padre de dos hijos). Todo empezó, en julio de 2015, con el ataque al portal y el compromiso de los datos personales de treinta y siete millones de clientes. Y terminó, el 28 de agosto, con la dimisión de Noel Biderman de su puesto como Consejero Delegado de ALM. No obstante, hubo quien corrió peor suerte: algunos de los clientes del portal acabaron suicidándose por temor a que se descubriesen sus propias infidelidades [22].

3.12. Keith McNeil. NHS (Reino Unido, 2015)

¡No todo son *“ciberataques”!* Casos como *Comair* o *Mizuho,* entre otros de los vistos más arriba, sirven para atestiguarlo. No obstante, los problemas pueden ir más allá de la obsolescencia tecnológica. Así lo atestigua el caso *Lewis*, ya descrito. De hecho, no sólo las acciones directas de fraude relacionadas con la Informática, sino una gestión cuestionable de las inversiones en esa materia también pueden acarrear problemas serios. Ese fue el caso del Complejo Hospitalario Universitario de Cambridge (tutelado por el Cambridge University Hospitals NHS Foundation Trust), cuya Gerencia estuvo en manos del reputado cirujano australiano Keith McNeil, entre noviembre de 2012 y septiembre de 2015. El hospital Addenbrooke, cabecera del complejo, era considerado, a la llegada de McNeil, uno de los mejores del sistema público británico (NHS, por sus siglas en inglés). En el momento de su marcha, el hospital padecía en sus cuentas una sangría semanal superior al millón de libras esterlinas. A ello había contribuido la puesta en marcha, no exenta de problemas, de un nuevo sistema de historia clínica electrónica, cuyo coste alcanzó los 200 millones de libras. El Dr. McNeil, acompañado de su Director Financiero, dejaría el cargo el 14 de septiembre de 2015, apenas una semana antes de que se conociera el contenido del informe que auditaba su gestión al frente del hospital [2].

3.13. Martin Winterkorn. Volkswagen (Alemania, 2015)

El debate sobre el gobierno de la tecnología (sobre quien tiene la potestad para ejercer el gobierno de la tecnología) es un viejo debate, al menos, entre los responsables de tecnología. Pero también es un debate perdido (para ellos). Los individuos al frente de las organizaciones son quienes tienen, en última instancia, dicha potestad. Son ellos quienes pueden gobernar, esto es, decidir sobre, la orientación y el uso que van a dar a la tecnología presente en sus organizaciones. Sobre ellos recae, también, la responsabilidad última de rendir cuentas por las consecuencias, buenas o malas, de tales decisiones. Los casos presentados en esta serie son, todos, muestra de ello; pero el caso *Volkwagen* lo es de manera paradigmática. El 18 de septiembre de 2015 saltaba a la opinión pública el que se conocería como *escándalo de las emisiones:* el grupo automovilístico alemán Volkswagen (VW) había decidido instalar en sus vehículos diésel un software que permitía falsear los resultados de las pruebas de emisiones realizadas en laboratorio. Corolario: los coches contaminaban más de lo que se creía. El impacto de la noticia, en forma de sospecha, alcanzó a todo el sector. En clave interna, dentro de VW, se llevó por delante al que, hasta ese momento, era el ejecutivo mejor pagado de Alemania, Martin Winterkorn, Consejero Delegado del grupo. Winterkorn dimitió el 23 de septiembre de 2015. Actualmente

> “ El debate sobre el gobierno de la tecnología (sobre quien tiene la potestad para ejercer el gobierno de la tecnología) es un viejo debate, al menos, entre los responsables de tecnología ”

Martin Winterkorn está siendo investigado, junto a otros treinta y seis imputados, por la fiscalía alemana [10].

3.14. Walter Stephan. FACC (Austria, 2016)

El 19 de enero de 2016 el fabricante industrial del sector aeronáutico FACC sufría un ciberataque. La modalidad elegida por los atacantes fue la conocida como el *timo del Consejero Delegado:* un empleado del departamento de contabilidad recibió un mensaje de correo electrónico, cuyo remitente, aparentemente, era el Consejero Delegado, Walter Stephan. Éste le solicitaba al empleado la realización de una transferencia por una importante suma. Naturalmente, el empleado no cuestionó la solicitud de su jefe. En la operación, los atacantes se llevaron un botín de cuarenta y dos millones de euros. El 25 de mayo el Consejo de Administración de FACC anunció el cese de Walter Stephan, apuntando a su negligencia en el cumplimiento de sus deberes al frente de la compañía (el Director Financiero, también había sido despedido, semanas antes; tras el incidente) [19].

3.15. Atiur Rahman. Banco Central de Bangladés (Bangladés, 2016)

Los días 4 y 5 de febrero de 2016 el Banco Central de Bangladés fue testigo, y víctima, del que pudo convertirse en el robo del siglo. Unos ciberdelincuentes, tras apropiarse de las credenciales de algún empleado de la entidad, trataron de extraer los 951 millones de dólares (855 millones de euros) que figuraban en la cuenta de la que el Banco era titular en la Reserva Federal de Nueva York. Finalmente, sólo lograrían llevarse algo menos de la décima parte, 81 millones de dólares (73 millones de euros), que irían a parar a cuentas particulares de Sri Lanka y Filipinas. El asunto saltó a la luz, a finales de febrero, precisamente en la prensa filipina. El 15 de marzo las autoridades de Bangladés forzaron la dimisión de Atiur Rahman, hasta entonces Gobernador del Banco Central bangladesí [24].

3.16. Debbie Wasserman Schultz. Comité Nacional Demócrata (EE.UU., 2016)

La primera víctima de los devaneos dentro del Comité Nacional Demócrata, aireados por Wikileaks en 2016, tras el robo masivo de mensajes de correo electrónico de miembros del citado Comité, supuestamente ejecutado por ciberatacantes rusos, no fue la mujer archiconocida que lleva el apellido del cuadragésimo segundo Presidente de los EE.UU. La primera víctima de ese ataque fue, también, una mujer, de apellidos alemanes, desconocida para el gran público, especialmente, el no estadounidense que no haya seguido muy de cerca la política del país norteamericano (la del Partido Demócrata, en particular) en los últimos años. Esa mujer fue Debbie Wasserman Schultz, Presidente del Comité Nacional Demócrata hasta la fecha de su dimisión, el 24 de julio de 2016.

Como en los casos Barr, Pascal o Biderman, y salvando prudentemente las distancias, la acción combinada de los ciberatacantes, primero, y de Wikileaks, después, dejaron al descubierto unas prácticas y unos usos, todos ellos cuestionables, seguidos por los miembros del Comité Nacional Demócrata que, lejos de arrojar una imagen de imparcialidad, reflejaban a las claras su inclinación por la candidata Clinton en perjuicio de su contrincante y compañero de partido, Bernie Sanders, en su carrera hacia la nominación como candidatos para las elecciones presidenciales de ese año. Probablemente, el malestar causado entre los seguidores de Sanders estuvo en el origen de una campaña electoral que, finalmente, no favorecería ni a unos, ni a otros, dentro del Partido Demócrata. Con toda seguridad, a quien no favoreció la situación creada fue a Wasserman Schultz, quien, dicho sea de paso, se resistió a renunciar, hasta el punto de que fue el propio Presidente Obama quien tuvo que persuadirla personalmente para que lo hiciera [1].

3.17. Hillary Diane Rodham Clinton. Elecciones Presidenciales (EE.UU., 2016)

Clinton es, de momento, el último de esta lista de nombres ilustres, que han tenido que vérselas con las consecuencias del uso de *lo digital* que se ha hecho en sus organizaciones. En este sentido, los primeros problemas de Hillary Clinton estuvieron relacionados con su etapa como Secretaria de Estado de los EE.UU. (2009-2013). El escándalo saltó cuando se conoció que, en aquella época, ella había decidido utilizar un servidor de correo electrónico personal, en lugar de hacer uso de la infraestructura oficial que ponía a su disposición el Departamento de Estado, con los riesgos (por falta de medidas adecuadas de seguridad) que ello podía conllevar. Sin embargo, el que fuese muy cuestionada por ello no parece un asunto tan relevante como su frustrada carrera hacia la Casa Blanca. Aquí, el compromiso de la infraestructura informática empleada por determinados miembros del Comité Nacional Demócrata y la posterior revelación de la información obtenida (seguramente, junto a otros factores) parecen haber tenido una influencia determinante en el resultado final de la convocatoria electoral estadounidense celebrada el 8 de noviembre de 2016. Todos estos hechos forzarían, además, a la Administración estadounidense a incluir el sistema electoral dentro del catálogo de infraestructuras críticas nacionales. Lo haría el 6 de enero de 2017, declarándolo como subsector del sector de infraestructuras críticas gubernamentales (Instalaciones del Gobierno).

Este exhaustivo repaso a semejante colección de nombres propios debería enseñar, al menos, un par de cosas. En primer lugar que, en torno a la seguridad digital, esto es, a la protección de las organizaciones de posibles riesgos digitales, o vinculados a lo digital, existen más amenazas que las meramente ligadas al ámbito de lo que habitualmente se conoce como estrictamente *cíber* (ciberataques, ciberdelincuentes, …). Las negligencias (incluidas las cometidas a la hora de tomar decisiones en materia de tecnología), los fallos y la obsolescencia de equipos y sistemas, la mala administración (por ejemplo, de presupuestos e inversiones de base digital), las malas artes de la condición humana, etc., están presentes en multitud de situaciones corporativas que terminan siendo perniciosas para las organizaciones y sus protagonistas.

Por otro lado, parece probado que hay quien ha entendido (incluso tarde) que la rendición de cuentas por su responsabilidad al frente de una organización, en ningún caso, excluye lo digital. ¡No quieras verte en la próxima reedición que hagamos de esta lista y ponerte al frente de la toma de decisiones que, en tu organización, requiera la tecnología! (O, al menos, mantente, y pide que lo mantengan, al día).

Finalmente, hay que entender que lo recogido en el texto hasta este punto no tiene la menor intención de asustar. Más al contrario, el único objetivo ha sido contribuir a abrir los ojos [18].

> “Finalmente, hay que entender que lo recogido en el texto hasta este punto no tiene la menor intención de asustar. Más al contrario, el único objetivo ha sido contribuir a abrir los ojos”

Referencias

[1] A. Gearan, P. Rucker, A. Phillip. “DNC chairwoman will resign in aftermath of committee email controversy”. *The Washington Post, 24 de julio de 2016.* <https://www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html?utm_term=.85dfa308824c>. Último acceso: 5 de marzo de 2017.

[2] BBC. *“Addenbrooke’s Hospital chief executive Keith McNeil resigns”. BBC News, 14 de septiembre de 2015.* <http://www.bbc.com/news/uk-england-cambridgeshire-34249646>. Último acceso: 28 de enero de 2017.

[3] CBS. “PG&E Chief Resigns In Wake Of San Bruno Blast, Gets $35M Retirement”. *CBS Broadcasting Inc. / CBSLocal San Francisco Bay Area, 21 de abril de 2011*. <http://sanfrancisco.cbslocal.com/2011/04/21/pge-executive-resigns-in-wake-of-san-bruno-blast/>. Último acceso: 5 de marzo de 2017.

[4] CCI, iTTi. “Beneficios de la Ciberseguridad para las Empresas Industriales”. *Centro de Ciberseguridad Industrial / Instituto de Tendencias en Tecnología e Innovación, 23 de febrero de 2017.* <https://www.cci-es.org/web/cci/detalle-actividad/-/journal_content/56/10694/327876>. Último acceso: 5 de marzo de 2017.

[5] C. Fujioka, R. Birsel. “Mizuho Bank head to resign over computer glitch: report”. *Reuters, 23 de abril de 2011.* <http://www.reuters.com/article/us-mizuho-idUSTRE73M06I20110423>. Último acceso: 27 de enero de 2017.

[6] C. O’Connor. “Target CEO Gregg Steinhafel Resigns In Data Breach Fallout”. *Forbes, 5 de mayo de 2014.* <http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/#5d5e0e9d6e61>. Último acceso: 28 de enero de 2017.

[7] Comisión de Cultura, Medios y Deporte. “Cyber Security: Protection of Personal Data Online”. *Cámara de los Comunes. Parlamento británico, 20 de junio de 2016.* <http://www.publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/148.pdf>. Último acceso: 12 de diciembre de 2016.

[8] getSurrey. “Royal Surrey boss quits after husband sacked”. *10 de febrero de 2012.* <http://www.getsurrey.co.uk/news/local-news/royal-surrey-boss-quits-after-4811742>. Último acceso: 5 de marzo de 25017.

[9] iTTi, CCI. “Beneficios de la Ciberseguridad para las Empresas Industriales”. *Instituto de Tendencias en Tecnología e Innovación / Centro de Ciberseguridad Industrial, 23 de febrero de 2017.* <http://www.ittrendsinstitute.org/news/item/itti-en-colaboracion-de-cci-publica-el-documento-beneficios-de-la-ciberseguridad-para-las-empresas-industriales>. Último acceso: 5 de marzo de 2017.

[10] J. Ewing. “Volkswagen C.E.O. Martin Winterkorn resigns amid emissions scandal”. *The New York Times, 23 de septiembre de 2015.* <https://www.nytimes.com/2015/09/24/business/international/volkswagen-chief-martin-winterkorn-resigns-amid-emissions-scandal.html>. Último acceso: 28 de enero de 2017.

[11] K. Vinton. “OPM Director Katherine Archuleta Resigns After Federal Data Breach Affects 25 Million Americans”. *Forbes, 10 de julio de 2015.* <http://www.forbes.com/sites/katevinton/2015/07/10/opm-director-katherine-archuleta-resigns-after-federal-data-breach-affects-25-million-americans/#23aad2d6418b>. Último acceso: 28 de enero de 2017.

[12] M. García-Menéndez. “Continuidad del Negocio y Auditoría de Sistemas (por Manolo Palao)”. *Blog “Gobernanza de TI”. Presentación del Texticulillo™ (nº 12) homónimo, de Manolo Palao, en su edición para “Gobernanza de TI”, 15 de octubre de 2010.* <https://gobernanza.wordpress.com/2010/10/15/continuidad-del-negocio-y-auditoria-de-sistemas-por-manolo-palao-2/>. Último acceso: 12 de diciembre de 2016.

[13] 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.

[14] M. Isikoff. “One email exposes millions of people to data theft in South Carolina cyberattack”. *NBC NEWS. Investigations, 20 de noviembre de 2012.* <http://investigations.nbcnews.com/_news/2012/11/20/15313720-one-email-exposes-millions-of-people-to-data-theft-in-south-carolina-cyberattack>. Último acceso: 28 de enero de 2017.

[15] P. Roberts. “HBGary Federal CEO Aaron Barr steps down”. *TheatPost, 28 de febrero de 2011*. <https://threatpost.com/hbgary-federal-ceo-aaron-barr-steps-down-022811/74971/>. Último acceso: 29 de enero de 2017.

[16] P. Shukovsky. “Criminal indictments in deadly pipeline explosion”. *Seattle Post-Intelligencer (SeattlePI), 13 de septiembre de 2001.* <http://m.seattlepi.com/local/article/Criminal-indictments-in-deadly-pipeline-explosion-1065760.php>. Último acceso: 27 de enero de 2017.

[17] P. Weill, J. Christensen. “Responsibilities of the Board in a Digital Economy”. *MIT CISR, 22 de octubre de 2015.* <http://cisr.mit.edu/publications-and-tools/publication-search/boards-digital-disruption/>. Último acceso: 12 de diciembre de 2016.

[18] R. Greene. “The Russian Hack Absolutely Affected The Outcome of The 2016 Election”. *The Huffington Post. The Blog, 16 de diciembre de 2016.* <http://www.huffingtonpost.com/richard-greene/the-russian-hack-absolute_b_13656802.html>. Último acceso: 29 de enero de 2017.

[19] S. Nasralla, A. Croft. “Austria’s FACC, hit by cyber fraud, fires CEO”. *Reuters, 25 de mayo de 2016.* <http://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF>. Último acceso: 28 de enero de 2017.

[20] S. Overby. “Comair’s Christmas disaster: Bound to fail”. *CIO, 1 de mayo de 2005.* <http://stephanieoverby.com/files/Comair.pdf>. Último acceso: 28 de enero de 2017.

[21] S. Spencer. “International comparison”. *SpencerStuart “Board Index 2015), 30 de octubre de 2015.* <https://www.spencerstuart.com/~/media/pdf%20files/research%20and%20insight%20pdfs/internationalcomparison_oct30_sp.pdf?la=en>. Último acceso: 5 de marzo de 2017.

[22] S. Thielman. “Ashley Madison CEO Noel Biderman resigns after third leak of emails”. *The Guardian, 28 de agosto de 2015.* <https://www.theguardian.com/technology/2015/aug/28/ashley-madison-neil-biderman-stepping-down>. Último acceso: 28 de enero de 2017.

[23] T. Kenneally. “Amy Pascal Sony Resignation: A Timeline of Cyberterror and Misfires”. *The Wrap, 5 de febrero de 2015.* <http://www.thewrap.com/amy-pascal-sony-resignation-timeline/>. Último acceso: 28 de enero de 2017.

[24] V. Sonawane. “Atiur Rahman, Bangladesh Central Bank’s Governor, Quits After Hackers Steal $101M From Foreign Reserves”. *International Business Times, 15 de marzo de 2016.* <http://www.ibtimes.com/atiur-rahman-bangladesh-central-banks-governor-quits-after-hackers-steal-101m-foreign-2336545>. Último acceso: 29 de enero de 2017.

Jeimy J. Cano M.
Director de la Revista "Sistemas" de la Asociación Colombiana de Ingenieros de Sistemas, ACIS.

<jcano@acis.org.co>

Alfabetización digital. Desconectando los saberes previos de la junta directiva en clave digital

Resumen: *La nueva realidad digital de las organizaciones y la inestabilidad que producen los ataques informáticos en las empresas actuales, demanda una renovación de los imaginarios propios de los miembros de las juntas directivas. En este sentido, este documento explora el reto de una alfabetización digital de los ejecutivos veteranos presentes en estos cuerpos de gobierno, indagando sobre los saberes previos que han acuñado en su experiencia y efectuar una lectura desde lo digital, donde la incertidumbre, la complejidad y la ambigüedad son parte fundamental para resignificar las nuevas capacidades que requieren para tomar decisiones ágiles, así como riesgos de forma inteligente.*

Palabras clave: *alfabetización digital, ciberataques, digital, juntas directivas, saberes previos.*

Autor

Jeimy Cano es miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho, y profesor distinguido de la misma Facultad, en la Universidad de los Andes (Colombia). Jeimy es Ingeniero y Magíster en Ingeniería de Sistemas y Computación por ese mismo claustro educativo; Especialista en Derecho Disciplinario por la Universidad Externado de Colombia; Ph.D. in Business Administration por la Newport University, (California, EE.UU.); Executive Certificate in Leadership and Management por la MIT Sloan School of Management (Massachusetts, EE.UU.); Egresado de los programas de formación ejecutiva Leadership in 21st Century: Global Change Agent y Cybersecurity: The Intersection of Policy and Technology ambos por la Harvard Kennedy School of Government, (Massachusetts, EE.UU.); y Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners. Jeimy Cano es el actual Director de la Revista "Sistemas" de la Asociación Colombiana de Ingenieros de Sistemas, ACIS.

1. Introducción

En una sociedad digitalmente modificada, las condiciones y retos para tener una vida plena han cambiado. Lo que comúnmente se hablaba sobre relaciones, compras y desarrollo personal en la sociedad tradicional, se ha transformado estableciendo nuevos parámetros e imaginarios que entran en tensión con los de muchos profesionales maduros, los cuales advierten la presencia de una nueva generación de individuos donde la vida se concibe desde la realidad de productos y servicios tecnológicamente enriquecidos y cuyas necesidades van más allá de lograr un hito particular en sus vidas.

La vida digitalmente plena es la expresión que se acuña en la actualidad. Una declaración que sitúa a la persona en una dinámica de información y flujo de mensajes, que establece la nueva dinámica de la vida de las personas: un mundo en la nube, instantáneo, móvil y muchas veces con sobrecarga de información. De acuerdo con estudios recientes, una vida digital plena está fundada en cuatro hábitos claves:

- protege tu privacidad;
- asegura tu información;
- abre tus posibilidades; y,
- mueve tu experiencia [10].

Estos son hábitos que articulan de forma concreta la experiencia particular de los sujetos, para ir más allá de la obsolescencia de los *commodities* que poco a poco se instalan en el escenario digital, acelerando de forma importante la necesidad de innovaciones discontinuas que vuelvan a repensar la experiencia del usuario final.

De igual forma se hace una lectura de la tradicional pirámide de necesidades de Maslow, en el contexto de la sociedad digital. Un estudio que ahora integra aplicaciones móviles, redes sociales, *me gustas* y en general, interacción digital como una forma de darle sentido a la vida, a las relaciones y realizaciones individuales, las cuales generalmente pasan por exposición, resistencia a las críticas y sobre manera, visibilidad global. En consecuencia, trascender, en esta nueva interpretación digital de Maslow, implica un compartir experiencias que beneficien a otros (por ejemplo, Waze, LinkedIn), creando una red de significados e intereses comunes donde el único objetivo es el bienestar colectivo.

Bajo estas nuevas lecturas sociales digitales, los miembros de juntas directivas deben ser alfabetizados con el fin de decodificar las nuevas dinámicas sociales, los intereses cruzados, ya no de sectores especializados, sino de comunidades particulares, y cómo los flujos de información masivos, establecen retos particulares donde cambia la percepción del riesgo dados los nuevos patrones de incertidumbre que pueden afectar tanto las actividades de las personas como las realidades humanas [2].

En este ejercicio, los miembros de junta deben entender que la práctica imperfecta [4] de sus roles en el contexto digital, es la oportunidad para desconectar lo que han aprendido, para construir y mejorar su capital político y desarrollar vías alternativas que les permitan gobernar la organización, ya no desde una lectura analógica de la realidad, sino desde la inestabilidad de los servicios y productos digitalmente modificados, como reto permanente para decidir y dirigir fuera de la zona cómoda de sus certidumbres [5].

Este breve documento reflexiona sobre la alfabetización digital de las juntas directivas respecto del nuevo entorno de ataques emergentes, la protección del valor de las empresas y cómo sobrevivir a la sobrecarga de la información, con el fin de tomar riesgos y decisiones inteligentes que respondan a las exigencias de sus clientes y al mismo tiempo funden las bases de una confianza imperfecta [7] donde el error es una oportunidad para construir relaciones transparentes y de largo plazo.

2. Desacoplando la nueva sociedad del riesgo

El riesgo tiene una connotación eminentemente social, donde su lectura depende al menos de cinco variables claves: percepción, valoración, gestión, contexto y experiencias previas [2].

Cada uno de estos elementos está enraizado en la dinámica social, mediado por la red de significados de individuos y comunidades, que al final del ejercicio hacen una lectura de la incertidumbre para tomar una decisión que le permita avanzar o no, sobre una materia en particular. En este sentido, lo que se etiqueta como riesgo en el contexto actual responde a

> “El riesgo tiene una connotación eminentemente social, donde su lectura depende al menos de cinco variables claves: percepción, valoración, gestión, contexto y experiencias previas”

una serie de condiciones o estado del mundo, que son leídas desde la subjetividad y juicios de las personas para tomar opciones que le permitan establecer un nivel de conformidad respecto de sus necesidades específicas.

La realidad de los miembros de juntas directivas tradicionales es que construyen la distinción de riesgo desde la esfera de la toma de decisiones, las cuales se fundan en la dinámica de variables como son las financieras, reputacionales, regulatorias, posicionamiento y panorama de amenazas, donde encuentran un lugar común para reflexionar y plantear opciones que le permitan a la empresa mantener su curso hacia los objetivos de negocio y capitalizar las capacidades empresariales en sus diferentes procesos.

La dinámica actual cuenta con menos espacios de estabilidad y consolidación, creando una ventana de oportunidad menos visible para las empresas en su ejercicio por conquistar un nuevo sector de negocio. El conocimiento y experiencia previos de los miembros de la junta, si bien son un capital valioso para motivar una postura escéptica de las apuestas corporativas internas, amenazas emergentes del exterior y normales desbalances estratégicos de los sectores, marcan una nueva diferencia para poder mantener una vista centrada en temas específicos, para ofrecer una postura o recomendación particular.

El incremento de la visibilidad de los ataques informáticos, mediados por el avance de la digitalización social, donde la densidad digital de conexiones e interacciones, permite “captar y medir las facetas de las personas, cosas y procesos” [1], establece un lindero hasta ahora desconocido e inexplorado, que permite aumentar la capacidad de las organizaciones para anticipar tendencias, fortalecer las relaciones con los clientes y sobre manera, crear mercados potenciales, escondidos y muchas veces ignorados en las tendencias de los datos recolectados.

Por tanto, dado el nuevo contexto digital, el cual es poco conocido por los tradicionales miembros de la junta directiva, se hace necesario completar la revisión de los otros aspectos claves del riesgo como son la percepción, valoración y gestión. De esta manera, se pueden conectar las experiencias previas de los ejecutivos, para que encuentren distinciones renovadas del riesgo de ciberseguridad, no solamente como una vista de las decisiones que deben tomar, sino como la comprensión y reconocimiento de las amenazas externas, para resignificar el concepto del riesgo más allá de los impactos de su materialización: una opción imperfecta para crear desbalances en el escenario de los retos empresariales y descubrir oportunidades para estar delante de la curva.

3. Juntas directivas: de la mentalidad analógica a la digital

La tradición de las juntas directivas está en el ejercicio de dirigir, orientar y asegurar la dinámica de las empresas de las cuales son parte. Una práctica que mientras las condiciones eran medianamente estables era válida y efectiva. Ahora, en un mundo por definición inestable, lo analógico del pensamiento y reflexiones de los miembros de junta crea una tensión en la experiencia ejecutiva, que provoca reacciones algunas veces defensivas u otras abiertas para aprender y equivocarse rápidamente como fundamento de una transición de una vista del mundo a otra.

En el mundo analógico el riesgo está contextualizado como una lectura de eventos del exterior que pueden comprometer la operación y por tanto, la dinámica de negocio. Las percepciones de las personas deben sujetarse a una visión del riesgo que desde afuera sugiere impactos en el desarrollo de las actividades de la empresa. El reconocimiento conjunto de la expresión de los eventos externos crea las etiquetas de valoración que son alimentadas desde las experiencias previas para concretar acuerdos sobre los impactos que una situación particular puede generar. El modelo causa-efecto es la norma que guía la gestión del riesgo en el imaginario colectivo de los miembros del cuerpo colegiado.

En el mundo digital el riesgo reviste al menos dos miradas complementarias, una primera desde el exterior que no define la construcción de la etiqueta *riesgo* completamente, sino que es asistida desde la experiencia modificada del mundo, donde es posible combinar posturas colindantes como:

- apoyarse en datos, pero confiar en la intuición;
- ser escéptico, pero abiertos de mente; y,
- mantener lo que se tiene, pero ser disruptivo [1].

Éstas crean una segunda vista más cosmopolita [11] que demanda una actualización permanente de habilidades y conocimiento para descubrir no solamente los impactos negativos de los posibles efectos de las situaciones adversas, sino las lecturas positivas de los eventos para crear espacios de discusión que retan las barreras de lo que se percibe desde el exterior, con las decisiones que al interior de la empresa se deben concretar para atender la incertidumbre que genera un contexto particular.

Un miembro de junta digitalmente modificado, entiende la inevitabilidad de la falla como el depredador que se encuentra en el mismo estanque que su presa, que le permite mantener fresca la dinámica de la lectura del entorno, combinando opciones, haciendo simulaciones y prototipos que le permitan anticiparse a los nuevos cambios y no esperar a que ellos se produzcan, sino más bien motivarlos para que ocurran de forma proactiva.

Un ciberataque estresa el modelo causa-efecto de la vista analógica y demanda superar la ilusión del control que la junta tiene respecto de la dinámica de la empresa ahora en un ecosistema digital, para tomar distancia y desconectar lo que conoce de la realidad, incorporar elementos dinámicos e inestables de las nuevas prácticas de negocio, las intencionalidades de los atacantes o la transnacionalidad del ciberdelito, entre otros, para reconectar en un nuevo modelo que explique de forma imperfecta lo que ocurre, creando siempre el margen para asumir el riesgo de aprender y desaprender en cada momento.

La lógica digital implica superar la postura mecanicista que explica el mundo y moverse hacia la vista sistémica relacional, que reconoce propiedades emergentes y acepta los errores como oportunidades para ver nuevos referentes de la realidad y crear significados que la expliquen de forma distinta, esto es, posturas plurales de actores hasta el momento desconocidos por los ejecutivos de la empresa.

> “ Un ciberataque estresa el modelo causa-efecto de la vista analógica y demanda superar la ilusión del control que la junta tiene respecto de la dinámica de la empresa ahora en un ecosistema digital […] ”

4. La alfabetización digital: currículo oculto de la complejidad, la incertidumbre y la ambigüedad

Las organizaciones modernas tratan de abordar el reto de mantenerse al día intentando construir dominios de conocimiento conocidos y estructurados para fundar prácticas que permitan resolver problemas definidos y situaciones repetitivas que generan demoras en los procesos y comprometen la efectividad de la empresa.

Sin perjuicio de lo anterior, las inestabilidades del entorno establecen referentes de conocimiento que se actualizan y renuevan conforme a la velocidad de los cambios o las discontinuidades que se presenten. En este sentido, la alfabetización digital (ver **figura 1**), entendida como ese “ejercicio de apertura cognitiva para reconocer y apropiarse de un mundo volátil, incierto, complejo y ambiguo mediado por la experiencia de lo digital”, establece un marco de aprendizaje que invita a la experiencia ejecutiva de las juntas para desarrollar una nueva sabiduría digital [9].

La complejidad, interpretada como el número de situaciones o eventos distinguibles por un observador que son atendidos por las distinciones previas del ejecutivo, constituye un motivo de ansiedad cuando aquel no es capaz de comprender las diferentes e inesperadas tendencias que surgen en el entorno, desafiando su capacidad natural para establecer una posición concreta y clara. En este contexto, el ejecutivo debe buscar respuestas fuera de sus propios linderos para conectar con la incertidumbre que provoca el *no saber* y así abrirse para explorar opciones antes impensadas.

La incertidumbre como maestra natural de los miembros de la junta establece, ahora, un nuevo marco de referencia que implica sacar a los cuerpos colegiados de su zona cómoda para llevarlos a “interrogar la realidad a partir de la propia experiencia, volver significativo lo sobreentendido, generar sentido a lo obvio, valorar las diferencias” [8], para repensar y situar nuevos aprendizajes nutridos desde la sorpresa, el desconcierto y lo inesperado. Lo incierto crea en los miembros de la junta una especial motivación que los reta a cruzar el umbral de sus propias restricciones analógicas, para habilitarlos en el escenario virgen de las posibilidades digitales.

La ambigüedad, esa incapacidad para poder establecer una lectura cierta de una situación por la variabilidad y volatilidad que la define, reconoce, en el ejercicio de gobierno, la práctica de un papel imperfecto de los miembros de la junta, habida cuenta que la necesidad de conocer y distinguir en medio de la dinámica empresarial los enfrenta a sus propios miedos internos; unos miedos que tratan de resolver desde esa disposición activa de conocer, no para interrogar las propuestas novedosas que habitan en lo digital, sino para desarrollar una postura vigilante en medio del ruido y las rarezas que se presentan en este momento y en el futuro.

En consecuencia, la construcción de la sabiduría digital requerida para afrontar la realidad digitalmente modificada, demanda habilidades especiales que permitan asumir un contexto de decisiones, mediado por la complejidad, la incertidumbre y la ambigüedad, como son:

- tener una visión transformadora: conocimiento del mercado y las tendencias, sabiduría de negocios y resolución de problemas;
- mirar hacia adelante: visión clara, una sólida estrategia y previsiones claves;
- comprender la tecnología: experiencia previa y alfabetización digital;
- estar orientado al cambio: mente abierta, adaptable e innovadora; y,
- disponer de fuertes habilidades de liderazgo: pragmático, focalizado y decisivo [3].

Con estos elementos, comprender las nuevas posibilidades de lo digital, así como los retos propios que implica asumir un ataque informático de proporciones no conocidas, configura una postura enriquecida de los cuerpos colegiados donde el *no saber* establece una disposición de apertura a nuevas experiencias, las cuales advierten momentos de mayor o menor complejidad, incertidumbre y ambigüedad, que marcarán la diferencia para superar *los saberes constituidos* y tomar decisiones ágiles e inteligentes.

Figura 1. La alfabetización digital.

5. Reflexiones finales

Si bien dentro de las amenazas que se identifican para las empresas, frente a la acelerada digitalización de productos y servicios, se encuentran la falta de agilidad, la complacencia, los productos obsoletos, la intensa competencia, las brechas de seguridad de la información, entre otras [3]. Los miembros de la junta deben avanzar rápidamente hacia

> “ En este contexto, el ejecutivo debe buscar respuestas fuera de sus propios linderos para conectar con la incertidumbre que provoca el ‘no saber’ y así abrirse para explorar opciones antes impensadas ”

la conquista de una *confianza en movimiento*, aquella que reconoce la dinámica del entorno y establece opciones que balancean la volatilidad y los inciertos que ocasionan las discontinuidades propias de la realidad.

En este escenario, la alfabetización digital de los miembros de la junta, no se funda necesariamente en su conocimiento del mundo digitalmente modificado, sino en su capacidad para leer en lo digital una forma de pensar distinta que los prepare mental y psicológicamente para estar atentos para repensar sus saberes previos y suspender el ejercicio del entendimiento de la realidad, para situarse al mismo tiempo como observador que distingue y como participante que decide.

Por tanto, la sabiduría digital necesaria, ahora, en los cuerpos directivos, que se funda en conectarse con otros, reconociendo sus fortalezas e influencias de experiencias previas; en reconocer las expectativas de las tendencias del entorno, compartiendo los entendimientos particulares de sus participantes; y en la inevitabilidad de la falla, como fundamento del aprendizaje y desaprendizaje permanente, define el contexto en el cual las amenazas informáticas y los ataques se convierten en realidades que iluminan el hacer de sus responsabilidades y les permite descubrir nuevos sentidos que repiensan la tradición de sus decisiones previas.

Conforme a lo anterior, los ciberataques, como eventos que rompen los límites del gobierno de los riesgos de las organizaciones modernas, demandan una lectura sistémica de la realidad que permita integrar diversos elementos y actores del entorno y de la dinámica empresarial, creando una capacidad emergente para leer la incertidumbre, la complejidad y ambigüedad que estas situaciones sugieren, con el fin de preparar de forma anticipada las respuestas ejecutivas que generen esa confianza en movimiento requerida por los diferentes grupos de interés en una sociedad atravesada por lo digital en todas sus esferas.

En definitiva, la alfabetización digital de los directivos establece un proceso educativo de equilibrio constante entre su capacidad para dar cuenta de las inestabilidades del entorno, en un contexto particular, y la complementariedad de sus habilidades gerenciales y políticas; lo que ha de permitir un sistema de formación que les facilite, al máximo, trazarse su propio itinerario de aprendizaje de acuerdo con su retos e intereses.

Referencias

“Cinco habilidades del líder digital”. *IESE Insight. No.18. Tercer trimestre, 2013*.

[2] E. Rosa, O. Renn, A. McCright. “The risk of society revisited. Social theory and governance”. *Philapdelphia, Pennsylvania. USA: Temple University Press, 2015.*

[3] G. Kane, D. Palmer, A. Nguyen, D. Kiron, N. Buckley. “Aligning the Organization for Its Digital Future”. *Sloan Management Review – Deloitte University Press*. *Summer, 2016*.

[4] J. Brown. *The imperfect board member: Discovering the seven disciplines of governance excellence*. San Francisco, CA. USA: Jossey-Bass, 2006.

[5] J. Cano. “Protección de la información en las juntas directivas. Una lectura política de la seguridad de la información”. *Blog IT-Insecurity*, *2016.* <http://insecurityit.blogspot.com.co/2016/12/los-hombres-son-criaturas-muy-raras.html>.

[7] J. Cano. “Protección de la información. Un ejercicio de confianza imperfecta”. *Blog IT-Insecurity, 2016(b)* http://insecurityit.blogspot.com.co/2016/09/proteccion-de-la-informacion-un.html>.

[8] J. Contreras, N. Pérez. La experiencia y la investigación educativa. En Contreras, J. y Pérez, N. (Compiladores) (2013) *Investigar la experiencia educativa*. Segunda Edición. Madrid, España: Ediciones Morata. 21-36, 2013.

[9] K. Dörner, D. Edelman. “What ‘digital’ really means”. *Mckinsey Quarterly. Julio, 2015* www.mckinsey.com/industries/high-tech/our-insights/what-digital-really-means>.

[10] Microsoft. “4 hábitos para una vida digital plena”. *Microsoft News, 2015.* <https://news.microsoft.com/es-xl/microsoft-presenta-4-habitos-para-una-vida-digital-plena/>

[11] S. Iñiguez. *Cosmopolitan Managers. Executive development that Works*. Londres, UK. Palgrave Macmillan, 2016.

En el camino hacia la resiliencia

Susana Asensio[1], Jose Valiente[2]

[1]Miembro de la Dirección Ejecutiva del Centro de Ciberseguridad Industrial (CCI); [2]Cofundador y actual Presidente del Centro de Ciberseguridad Industrial (CCI).

<{susana.asensio, jose.valiente}@CCI-es.org>

Resumen: *Como colofón a la monografía, los autores 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 infraestructuras 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.*

Palabras clave: *ciberresiliencia, cloud, estrategia tecnológica, fabrica 4.0, Industria 4.0, Inteligencia Artificial, Internet de las Cosas, IoT, nube, resiliencia, riesgos tecnológicos, transformación digital*

Autores

Susana Asensio es Miembro de la Dirección Ejecutiva del Centro de Ciberseguridad Industrial (CCI). Obtuvo su Grado en Ingeniería del Software en la Universidad Politécnica de Madrid (UPM). Es, asimismo, Ingeniera Técnica en Informática de Gestión por la misma universidad y Postgrado en Promoción y Gestión de Proyectos y Acciones Internacionales de I+D+i, también por la UPM; actividad, esta última, a la que ha dedicado la mayor parte de su carrera profesional en entidades como la propia UPM y, muy particularmente, la Asociación Multisectorial de Empresas de la Electrónica, las Tecnologías de la Información y la Comunicación, de las Telecomunicaciones y de los Contenidos Digitales (AMETIC). Especializada en la gestión de la I+D+i en los ámbitos de la Seguridad Digital y la Tecnología, Susana, ha moderado, coordinado y/o participado en numerosos grupos de trabajo y proyectos, nacionales e internacionales, relacionados con la identidad digital, los servicios de certificación digital, la factura electrónica, la protección de datos, la ciberseguridad industrial y las infraestructuras críticas. En este sentido, Susana es, además, cofundadora de la Red Paneuropea para la Cooperación en materia de Protección de Infraestructuras Críticas (EUCONCIP), con sede en Roma.

José Valiente es cofundador y actual Presidente del Centro de Ciberseguridad Industrial (CCI). Diplomado en Informática de Gestión por la Universidad Pontificia de Comillas, inició su carrera profesional hace más de dos décadas en el ámbito de la consultoría tecnológica, habiendo ocupado puestos de diversa responsabilidad en diferentes firmas del sector. Especializado en consultoría tecnológica y de seguridad (cuenta con múltiples certificaciones profesionales, tanto generalistas, como ligadas a productos) ha participado y dirigido proyectos, en los citados ámbitos, para la gran cuenta y la Administración Pública. Centrado en los últimos años en la Ciberseguridad Industrial, en 2013 fue uno de los fundadores de CCI, centro que hoy dirige. Habitual y reconocido conferenciante internacional en la materia, también escribe regularmente sobre dicha disciplina. Actualmente, José es, además, miembro de la Junta Directica de la Red Paneuropea para la Cooperación en materia de Protección de Infraestructuras Críticas (EUCONCIP), con sede en Roma.

1. Adaptarse o sucumbir

La transformación digital de las organizaciones proviene de la adopción de las tecnologías electrónicas, informáticas y/o telemáticas en su operativa diaria. Y, sobre todo, de la de sus nuevos paradigmas como la computación en la nube ("*cloud computing*", según su denominación inglesa), la movilidad, la Internet de las Cosas (que se comunican autónomamente a través de esa Red), lo social (las redes sociales), la analítica de *datos a lo grande* (del inglés, "*Big Data*") y, más recientemente, la Inteligencia Artificial; todos los cuales constituyen, a su vez, el mayor reto para las empresas y la sostenibilidad de sus negocios en el siglo XXI.

De hecho, puede afirmarse que la supervivencia de las organizaciones resulta, en general, cada vez más compleja e incierta. Y, por lo tanto, requiere de una enorme capacidad para adaptarse a la cambiante coyuntura y a la ambigüedad del mercado.

La avalancha tecnológica (alimentada por la aparición de multitud de nuevas soluciones digitales que, no obstante, han de integrarse con las existentes) ha convertido esta Era Digital en un terreno azaroso en el que la estrategia tecnológica y la capacidad de adaptación de la que se doten las organizaciones están siendo claves para garantizar la supervivencia de los negocios en el actual mercado global, complejo y cambiante. Claro ejemplo de ello, en el dominio industrial, es la adopción de un nuevo paradigma, la Industria 4.0, en el que cada vez se hace más relevante fabricar con una mayor orientación a la demanda, lo que lleva a una fabricación personalizada, de manera más flexible y, naturalmente, sin penalizar el precio final del producto.

Esa capacidad de adaptación y respuesta a los cambios dinámicos y a los retos y dificultades que proponen el mercado y el variable entorno tecnológico recibe el nombre de resiliencia. La resiliencia tecnológica permite afrontar la evolución, la dependencia y los riesgos de la tecnología.

Un reciente estudio conjunto de la *MIT Sloan Management Review* y la firma Deloitte [5] revela la deficiente madurez digital de las organizaciones estadounidenses y, por tanto, su escasa capacidad de resiliencia tecnológica. Especialmente en sectores como la ingeniería y la construcción, la industria, el farmacéutico, el sanitario, el alimentario o el sector público. Un 70% de las organizaciones que participaron en el estudio declararon estar en una fase temprana (inicial) o de desarrollo (incremento) de su madurez digital. Las principales barreras que se están

> “La Seguridad Digital en las organizaciones evoluciona hacia la Resiliencia Operativa”

encontrando son la falta de una estrategia tecnológica y el exceso de prioridades, como muestra la tabla de la **figura 1**.

En el caso de España, cabe pensar que la gran mayoría de las organizaciones carecen, también, de una estrategia tecnológica. Y en las que existe, se fundamenta únicamente en las recomendaciones que han recibido de sus proveedores tecnológicos, de aquellos que ellas consideran *estratégicos*, cuya principal meta, sin embargo, no es otra que incrementar las ventas de sus servicios y soluciones.

Muy al contrario del panorama que dibuja esa descripción de la situación actual, la resiliencia debe formar parte de la naturaleza misma de las organizaciones y estar implícita en su estructura, a través de la definición y el cumplimiento de un plan corporativo para garantizar la resiliencia, que incluya como pivote, su estrategia tecnológica. El plan debe ser adoptado y abordado de acuerdo con las dos dimensiones clave que conforman la resiliencia en toda organización (ver **figura 2**): adaptación y robustez.

- La adaptación. Ante una nueva coyuntura, la organización debe tener la capacidad de reaccionar y adaptarse (gracias, entre otros factores, a la adopción de procesos de mejora continua), compitiendo y operando conforme a las nuevas reglas del mercado y su demanda. Ésta es la situación propia del ámbito industrial, en el que sólo se puede ser competitivo a través de la transformación y conversión tecnológica y digital.
- La robustez. Ante una serie de sucesos, la organización debe ser capaz de recuperarse y seguir operando, como si nada hubiera sucedido.

En el contexto actual, no resulta sencillo trazar una nítida línea divisoria entre el alcance de la resiliencia corporativa de la organización y su resiliencia tecnológica, ciberresiliencia o resiliencia digital. El hecho de que la continuidad de las operaciones de la organización, así como su competitividad dependan, hoy, directamente de la tecnología, de la automatización y de la eficiencia que ambas aportan, dificulta aventurar la referida división.

De la **figura 1** se desprende, además, que la segunda barrera más importante para lograr la madurez en la transformación digital de las organizaciones es su preocupación por la seguridad. En este sentido, son cada vez más las voces que defienden que la seguridad en la era de la transformación digital no debe estar basada de forma exclusiva en medidas de prevención o defensa, sino también en la capacidad de adaptarse y dar respuesta, tal y como indica el profesor e investigador Jeimy Cano (coautor, también, de esta monografía): “*Tarde o temprano las barreras definidas van a caer, tarde o temprano la organización será objeto de un incidente y para ello, la postura de seguridad por vulnerabilidad habilita a la organización para responder de manera ágil y eficaz, pues no estará distraída en el* qué dirán *del incidente, sino tomando acciones concretas que permitan entender, contener, recuperar y comunicar lo que ha ocurrido, para aprender rápidamente y aumentar su capacidad de resiliencia frente a eventos futuros*” [6].

2. Un nuevo enfoque en la mitigación del riesgo: la resiliencia tecnológica, más allá de la seguridad digital (el caso de la Industria 4.0)

Retomando la referencia al paradigma de la Industria 4.0, en un escenario de *fábricas 4.0* aparecen nuevos riesgos cibernéticos derivados de la nueva operativa industrial. La mayor interconectividad (interna y externa), el creciente uso de la nube como plataforma de computación, la proliferación de sistemas embebidos (que proporcionan inteligencia a sensores, materiales, máquinas o productos) y el desarrollo de nuevas aplicaciones de fabricación avanzada y personalizada, constituyen todos nuevas oportunidades; pero, también, potenciales nuevas debilidades. La aparición, tal y como se está detectando actualmente, de nuevos vectores de ciberataque más propios de los sistemas de información tradicionales tiene su origen en la adopción de estas nuevas tecnologías en el contexto industrial y en la creciente necesidad de conectar las redes que controlan el proceso industrial con las redes informáticas corporativas.

Además, todos estos riesgos se ven agravados por la falta de madurez tecnológica y la falta de una estrategia definida, ya mencionadas; lo cual, en muchos casos genera conflictos internos, bien por la asignación de responsabilidades a personal insuficientemente formado, bien por la propia necesidad de provisionar recursos (escasos) dedicados.

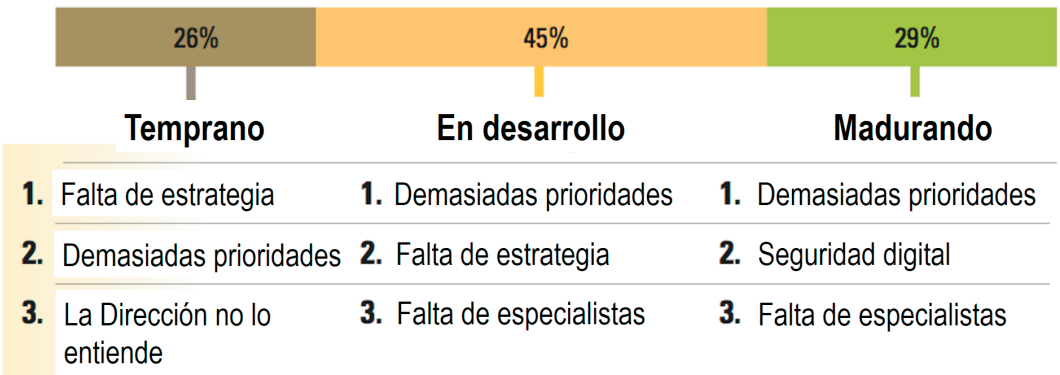

Figura 1. Barreras a la madurez digital de las organizaciones. Fuente: MIT Sloan Management Review/Deloitte.

> “En definitiva, definir y ejecutar un plan corporativo para la resiliencia tecnológica que garantice la continuidad del negocio, contribuya a fomentar la cultura de la seguridad digital y convierta la resiliencia tecnológica en una ventaja competitiva”

Ha de advertirse que, en el contexto industrial y, más acusadamente, en la Industria 4.0 se dan algunas diferencias a la hora de abordar la resiliencia tecnológica con respecto a otros entornos (ver **figura 3**):

- Se trata de un sector que, en su operativa principal, se ha mantenido históricamente aislado de la revolución digital, por lo que la adaptación táctica y organizativa a este nuevo entorno es, en muchos casos, conflictiva.
- Los periodos de adaptación tecnológica en los entornos industriales son lentos y deben implicar a todos los equipos organizativos de los cuales depende que la operativa de la organización evolucione de forma sostenible y eficiente.
- Habitualmente los incidentes en el entorno industrial (particularmente los más graves, que alcanzan la consideración de desastres) tienen un impacto muy elevado para el negocio y sus diferentes grupos de interés.
- De hecho, las operaciones y, por tanto, las consecuencias de cualquier perturbación en estos entornos tienen un gran componente físico. Los principales escenarios de desastre hacen referencia a amenazas de naturaleza física como incendios, inundaciones, sabotajes o destrucción de equipamiento/instalaciones.
- Los tradicionales enfoques, propios de otros sectores, para la contención y la recuperación tras una perturbación a menudo resultan no ser de aplicación en el ámbito industrial. Por ejemplo, en muchas ocasiones resultará inviable disponer de una localización alternativa donde ubicar el proceso industrial durante el periodo de recuperación, lo cual es una práctica habitual, institucionalizada, en los entornos de la informática corporativa.

Figura 2. Dimensiones de la resiliencia tecnológica.

Figura 3. Peculiaridades del contexto tecnológico industrial.

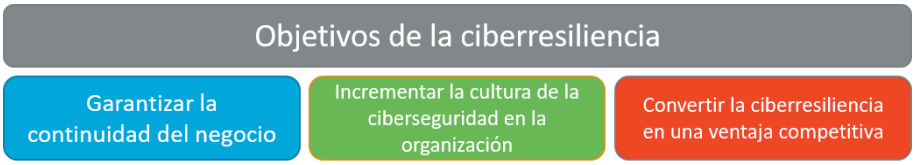

Figura 4. Objetivos de la resiliencia tecnológica en las organizaciones.

Las organizaciones industriales, cada vez más conscientes del impacto sobre el negocio del riesgo digital, comienzan a establecer algunos objetivos y a implantar ciertas buenas prácticas: 1) concienciar y formar al personal; 2) revisar y auditar la tecnología implantada (desde la arquitectura, hasta la configuración de dispositivos y sistemas, especialmente sus controles de acceso interno y externo) [1]; 3) establecer políticas y normas de uso de la tecnología, en ocasiones siguiendo sistemas de gestión de la seguridad que les permita aplicar medidas de seguridad según buenas prácticas [2]; etc.

Aunque muchas organizaciones han empezado a contemplar medidas de seguridad digital basadas en la evaluación y gestión de riesgos [3], son conscientes de que estas medidas no serán suficientes, y que deben estar preparadas para afrontar los nuevos retos tecnológicos y recuperarse de los incidentes. Ello supone, como apuntaba Jeimy Cano [6], que deberán preocuparse de sus capacidades de adaptación y resiliencia, es decir, de su capacidad para transformarse a las nuevas demandas del mercado, resistir, dar respuesta y superar cualquier perturbación relativa al uso de las tecnologías de operación. Bajo este principio se entenderán las necesidades de la organización para planificar, definir, desarrollar, gestionar y medir las oportunas prácticas y comportamientos que conduzcan la resiliencia (en sus dos dimensiones) de la organización. En definitiva, definir y ejecutar un plan corporativo para la resiliencia tecnológica que garantice la continuidad del negocio, contribuya a fomentar la cultura de la seguridad digital y convierta la resiliencia tecnológica en una ventaja competitiva (ver **figura 4**).

3. El *ciberecosistema* como factor global de la resiliencia tecnológica

Los tremendos avances aparecidos en las comunicaciones de datos durante los últimos años, han provocado que las organi-

> “ Todas esas estrategias abogan por una mayor cooperación internacional y subrayan, particularmente, la dimensión económica de la política de ciberseguridad ”

zaciones, disten mucho de estar aisladas, tanto en lo referente a la conexión de sus sistemas y redes, como a la relación con sus proveedores y subcontratistas. Existe pues, un complejo entramado de interconexiones con otras infraestructuras y con otros agentes, de manera que la interrupción del suministro de un servicio puede impactar en los servicios ofrecidos por otras instalaciones u operadores. Este fenómeno de interrelaciones e interdependencias, conocido tradicionalmente como la *empresa extendida* (¡no estás solo!), da lugar, hoy, al concepto de *ciberecosistema*, entendido como un componente externo de la capacidad de resiliencia de la organización.

La consultora EY define este nuevo concepto como “*una comunidad compleja de dispositivos interactivos, redes, personas y organizaciones, y el entorno de los procesos y tecnologías que apoyan estas interacciones*” [4]. Los componentes del *ciberecosistema* intercambian información constantemente entre sí dando lugar a composiciones más complejas (redes y organizaciones) que a su vez se relacionan generando un fuerte entramado de flujos de datos y sinergias, cuyo tremendo potencial, está aún por descubrir. Las vulnerabilidades de los sistemas y las aplicaciones que almacenan, procesan o transmiten la información privada y valiosa para la operación, frente a las amenazas de robo, parada, alteración o destrucción por parte de los delincuentes, u otros actores dañinos, aumentan continuamente. Perturbaciones localizadas pueden desencadenar rápidamente una secuencia en cascada de eventos que pueden causar desastres tecnológicos, a través de redes enteras y comunidades, es decir, *ciberecosistemas* completos.

A diferencia de los enfoques tradicionales de seguridad, el enfoque basado en *ciberecosistemas* implica la necesidad de proteger la operación y la información que más importa, independientemente de su ubicación.

Conscientes de ello, algunos Estados ya han implementado estrategias de ciberseguridad particulares en las que se reconoce que muchas funciones esenciales del Estado para la economía, la sociedad y el propio gobierno, dependen actualmente de este entramado de interrelaciones. Todas esas estrategias abogan por una mayor cooperación internacional y subrayan, particularmente, la dimensión económica de la política de ciberseguridad.

Además, en muchas de dichas estrategias estatales, aparece el término *resiliencia*, conduciendo a la conclusión de que alcanzar la auténtica resiliencia tecnológica ha de entenderse como un objetivo conjunto del Estado y las empresas, dado que no será factible conseguir la resiliencia de uno sin la de las otras, y a la inversa. Especialmente cuando existen sectores y actividades en manos de empresas privadas, que resultan estratégicos para los Estados, y que tienen una gran dependencia, en sus modelos de negocio, de las tecnologías digitales.

Referencias

[1] CCI. “Buenas prácticas para el Diagnóstico de la Ciberseguridad en Entornos Industriales 2014”. *Biblioteca del Centro de Ciberseguridad Industrial, noviembre de 2014.* <https://www.cci-es.org/informes-y-analisis-estategicos#>.

[2] CCI. “Guía Práctica para la Construcción de un Sistema de Gestión de la Ciberseguridad Industrial”. *Biblioteca del Centro de Ciberseguridad Industrial, marzo de 2016.* <https://www.cci-es.org/informes-y-analisis-estategicos#>.

[3] “Estado de la Ciberseguridad Industrial en España, evolución y futuro”. *Biblioteca del Centro de Ciberseguridad Industrial, octubre de 2016.* <https://www.cci-es.org/informes-y-analisis-estategicos#>.

[4] EY. “Achieving resilience in the cyber ecosystem”. *EY Global/Insights on governance, risk and compliance, diciembre de 2014.* <www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf>.

[5] G. Kane, D. Palmer, A. Nguyen Phillips, D. Kiron, N. Buckley. “Strategy, not technology, drives digital transformation. Becoming a Digitally Mature Enterprise”. *MIT Sloan Management Review/ Deloitte, 14 de julio de 2015.* <http://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/>.

[6] “La ilusión del control: Seguridad por vulnerabilidad”. *LinkedIn/Pulse, 23 de diciembre de 2016.* <https://es.linkedin.com/pulse/la-ilusi%C3%B3n-del-control-seguridad-por-vulnerabilidad-cano-ph-d-cfe>.

Benchmark de consultas de agrupamiento y ordenamiento difuso

Soraya Carrasquel[1], David Coronado[1], Ricardo Monascal[1], Rosseline Rodríguez[1,2], Leonid Tineo[1,2]

[1]Departamento de Computación y Tecnología de la Información, Universidad Simón Bolívar, Caracas (Venezuela); [2]Universidad Católica Nuestra Señora de la Asunción, Paraguay

<{scarrasquel, dcoronado, rmonascal, crodrig, leonid}@usb.ve>

Resumen: *Se han propuesto extensiones a SQL para soportar atributos cuyo dominio es un conjunto de etiquetas provisto de una relación de similitud, conocidos como atributos difusos Tipo 3. Dichas extensiones consideran la definición y manipulación de este tipo de dominios, así como consultas con ordenamiento y agrupamiento difuso. Mediante una arquitectura medianamente acoplada, estas nuevas funcionalidades fueron añadidas a PostgreSQL, surgiendo así fuzzydoDB. En este trabajo se presenta el análisis de desempeño de las consultas con ordenamiento y agrupamiento basado en atributos difusos Tipo 3, así como una base de datos experimental para este tipo de* benchmark*.*

Palabras clave: *Atributos difusos Tipo 3,* benchmark*,* GROUP BY*,* ORDER BY*, SGBD.*

1. Introducción

La mayoría de los sistemas gestores de bases de datos (SGBD) implementan el modelo relacional, que supone datos precisos, con valores perfectamente conocidos o ausentes. Sin embargo, en el mundo real, puede haber información parcial o imprecisa sobre valores de algunos datos. Una herramienta matemática que permite modelar este tipo de información es la teoría de conjuntos difusos [16].

La aplicación de esta teoría ha dado lugar al surgimiento del modelo relacional difuso generalizado GEFRED [10] y el modelo entidad relación extendido difuso Fuzzy EER [8]. Éste distingue cuatro tipos de atributos difusos: *Tipo 1*, datos precisos sobre los cuales se permiten consultas con etiquetas lingüísticas interpretadas como números difusos; *Tipo 2*, datos posibilísticos sobre dominios ordenados; *Tipo 3*, etiquetas lingüísticas no ordenadas provistas de una relación de similitud, y distribuciones de posibilidad sobre ellas; y *Tipo 4*, similar a los *Tipo 3* pero sin la relación de similitud.

Para los *Tipo 3*, sin distribuciones de posibilidad, se han estudiado sus implicaciones en consultas basadas en ordenamiento y agrupamiento [3][4]. Los resultados han sido implementados en una extensión [1] del SGBD MariaDB [9], la cual permite especificar y almacenar atributos *Tipo 3*, y procesar consultas que involucren estos atributos, particularmente ordenamiento y el agrupamiento difuso [3][4]. Esta extensión fue migrada a PostgreSQL y ampliada para dar soporte a otros tipos de datos difusos, esta nueva versión se llama *fuzzy*doDB [6]. Con esta extensión se planteó realizar el *benchmark* de consultas con atributos *Tipo 3*.

Fue necesario crear una base de datos experimental con atributos *Tipo 3* para este *benchmark*, pues, dado lo reciente de esta extensión, no existen bases de datos públicas que contemplen estos atributos. Aquí se presenta dicha base de datos experimental y se reporta el resultado del análisis de desempeño de *fuzzy*doDB, sobre ésta, en el procesamiento de consultas con agrupamiento y ordenamiento difuso.

Este artículo se organiza como sigue: En la **sección 2** se presenta el marco teórico, los dominios *Tipo 3*, y su uso en ordenamiento y agrupamiento difuso. En la **sección 3**, se describen algunos detalles relevantes de *fuzzy*doDB. En la **sección 4**, se explica la base de datos para el *benchmark*. En la **sección 5**, se muestran los detalles del diseño experimental. En la **sección 6**, se plantea el análisis de los resultados obtenidos en los experimentos. Finalmente, en la **sección 7**, se proponen las conclusiones y trabajos futuros.

2. Marco teórico

Un conjunto difuso F [16] es un subconjunto de un conjunto clásico X, caracterizado por una función de membresía $\mu_F: X \rightarrow [0,1]$, donde 0 es la completa exclusión, 1 la completa inclusión y hay elementos que pertenecen gradualmente (posiblemente). En bases de datos, este concepto permite expresar preferencias del usuario o particularidades del contexto al dar semántica a criterios vagos (o condiciones difusas), así como representar y manipular atributos de datos imprecisos (o difusos).

Para incluir consultas o datos difusos en SQL, se han propuesto varias extensiones. Una de ellas es FSQL [7], basada en GEFRED [10] y Fuzzy EER [8] que define cuatro tipos de atributos difusos. El *Tipo 3* consiste en un dominio formado por etiquetas, provisto de una relación de similitud.

Sea S un conjunto difuso en $X \times X$ caracterizado por $\mu_S: X \times X \rightarrow [0,1]$, S es una relación de similitud [4] si es reflexiva $\forall x \in X\ \mu_S(x,x)=1$, simétrica $\forall x,y \in X\ \mu_S(x,y)=\mu_S(y,x)$ y transitiva $\forall x,y,z \in X\ ((\mu_S(x,y)=1 \Rightarrow \mu_S(x,z)=\mu_S(y,z)) \wedge (\mu_S(y,z)=1 \Rightarrow \mu_S(x,z)=\mu_S(x,y)))$. S induce una partición difusa [3], $P_S=\{ S[x] \mid x \in X \}$, donde $S[x]$ se llama la clase difusa de x, con $\mu_{S[x]}(y)=\mu_S(x,y)$.

En trabajos previos [3][4] se proponen y formalizan extensiones a SQL para definir datos *Tipo 3* y su uso en consultas ordenadas y agrupadas, que se resumen a continuación.

2.1. Dominios de datos con relaciones de similitud

Un dominio *Tipo 3* se especifica así [4]: CREATE FUZZY DOMAIN *fd* AS VA-

μ_S	Europe	Oceania	Asia	Africa	Antarctica
Europe	1	0.4	0.9	0.8	0
Oceania	0.4	1	0.7	0.4	0.4
Asia	0.9	0.7	1	0.6	0.3
Africa	0.8	0.4	0.6	1	0.8
Antarctica	0	0.4	0.3	0.8	1

Tabla 1. Relación de similitud para CONTINENTS.

> “ Para incluir consultas o datos difusos en SQL, se han propuesto varias extensiones. Una de ellas es FSQL, basada en GEFRED y Fuzzy EER que define cuatro tipos de atributos difusos ”

LUES $l_1,\ldots,l_n$ [SIMILARITY { $(l_{il}, l_{jl})/v_1,\ldots, (l_{im}, l_{jm})/v_m$ }]. Donde *fd* es el nombre del dominio, $l_1,\ldots, l_n$ son las etiquetas en el dominio, $(l_{ik},l_{jk})/v_k$ es un par en la relación de similitud con grado de membresía v_k. Sólo es necesario especificar los pares de la relación base; los correspondientes a la reflexividad, simetría y transitividad están sobreentendidos; el resto tienen membresía cero.

Por ejemplo, así se especifica un dominio *Tipo 3* de continentes (ver **tabla 1**): CREATE FUZZY DOMAIN CONTINENTS AS VALUES (Europe, Oceania, Asia, Africa, Antarctica) SIMILARITY {(Europe, Oceania)/0.4, (Europe, Asia)/0.9, (Europe, Africa)/0.8, (Oceania, Asia)/0.7, (Oceania, Africa)/0.4, (Oceania, Antarctica)/0.4, (Asia, Africa)/0.6, (Asia, Antarctica)/0.3, (Africa, Antarctica)/0.8}.

2.2. Ordenamiento usando similitud

La cláusula ORDER BY se extendió así [4]: ORDER BY *criterio*$_1$,...,*criterio*$_o$, donde cada *criterio*$_i$ es de la forma: - k_i d_i siendo k_i un atributo y d_i un especificador de orden (ASC o DESC); - k_i START l_i siendo k_i un atributo difuso *Tipo 3*, l_i una etiqueta en el dominio de k_i. En este último caso, las tuplas se ordenan descendentemente por el grado de similitud del valor de k_i con l_i.

Por ejemplo, dada una tabla COUNTRY de nueve filas, con atributos name, region, continent y surfacearea, siendo continent un atributo *Tipo 3* del dominio CONTINENTS, la consulta SELECT name, region, continent, surfacearea FROM COUNTRY ORDER BY continent START Europe, produce como resultado la siguiente lista de registros ordenada según la relación de similitud de la **tabla 1**: [(France, Western Europe, Europe, 551500), (Spain, Southern Europe, Europe, 505992), (Armenia, Middle East, Asia, 29800), (Japan, Eastern Asia, Asia, 377829), (Algeria, Northern Africa, Africa, 2381741), (Ghana, Western Africa, Africa, 238533), (New Zealand, Australia and New Zealand, Oceania, 270534), (New Caledonia, Melanesia, Oceania, 18575), (Antarctica, Antarctica, Antarctica, 13120000)].

2.3. Agrupamiento usando similitud

Se extendió la cláusula GROUP BY así [3]: GROUP BY [SIMILAR] $k_1,\ldots,$ [SIMILAR] k_o, la palabra clave SIMILAR es opcional, sólo se usa si k_i es *Tipo 3* y se quiere considerar la partición difusa inducida por su relación de similitud.

Por ejemplo, dada la tabla COUNTRY (subsección anterior), el atributo continent es *Tipo 3*, su relación de similitud (ver **tabla 1**) induce la partición difusa {{Europe/1, Asia/0.9, Africa/0.8, Oceania/0.4}, {Oceania/1, Asia/0.7, Africa/0.4, Antarctica/0.4, Europe/0.4}, {Asia/1, Europe/0.9, Oceania/0.7, Africa/0.6, Antarctica/0.3}, {Africa/1, Antarctica/0.8, Europe/0.8, Asia/0.6, Oceania/0.4}, {Antarctica/1, Africa/0.8, Oceania/0.4, Asia/0.3}}.

La consulta: SELECT continent, COUNT(*) FROM COUNTRY GROUP BY SIMILAR continent; produce: [(Europe, 6.2), (Oceania, 5.4), (Asia, 4.7), (Africa, 6.2), (Antarctica, 4.0)]. COUNT se calculó según el operador $\sum count$ de Zadeh [17], se usó por ser el más sencillo [3].

3. SGBD extendido *fuzzy*doDB

En esta sección se describe brevemente *fuzzydo*DB [6], su arquitectura y catálogo. Para más detalles, se recomienda consultar el trabajo dedicado al prototipo inicial [1].

La versión actual incluye todas las variantes de atributos difusos según se proponen en Fuzzy EER [8]. En *fuzzy*doDB los *Tipo 3* no permiten el uso de distribuciones de posibilidad. Se ha extendido la clasificación con un *Tipo 5* que son distribuciones de posibilidad sobre *Tipo 3*. A continuación se describe la porción correspondiente a los atributos *Tipo 3*.

3.1. Catálogo difuso

Los metadatos correspondientes a dominios *Tipo 3* se incluyen en el catálogo relacional de objetos de la base de datos. Para ello, se define un esquema de base de datos compuesto de cuatro tablas: DOMAIN, LABEL, SIMILARITY y COLUMN.

DOMAIN (domainId, tableSchema, domainName) contiene los dominios *Tipo 3*, donde domainId es la clave primaria autogenerada, también identificado por su domainName dentro de una base de datos (tableSchema).

LABEL (labelId, domainId, labelName), almacena las etiquetas (labelName) de los dominios de datos difusos, referenciado por domainId, con clave primaria autogenerada labelId, y (domainId, labelName) una clave alterna.

SIMILARITY (label1Id, label2Id, value, derived) contiene los pares de etiquetas (label1Id, label2Id) que conforman una relación de similitud, indicando su grado de membresía (value) y el atributo derived que indica si el par pertenece a la relación base o fue derivado por reflexividad, simetría y transitividad; label1Id y label2Id son claves foráneas a LABEL.

COLUMN (tableSchema, tableName, columnName, domainId) contiene la definición de columnas cuyo tipo es un dominio difuso (domainId), el cual se identifica por su nombre (columnName), junto con el nombre de la tabla (tableName) y base de datos (tableSchema) a la que pertenece; (tableSchema, tableName, columnName) **es la clave primaria y domainId es una clave foránea a DOMAIN.**

3.2. Arquitectura

Para extender la funcionalidad de un SGBD se han propuesto tres arquitecturas: acoplamiento fuerte, acoplamiento débil y acoplamiento medio [15]. En *fuzzy*doDB [1][6] se usa una arquitectura medianamente acoplada (ver **figura 1**), que consiste en una implementación intermedia donde la lógica fue programada en el lenguaje nativo del SGBD original.

Esta extensión posee una capa externa programada en Java que implementa los esquemas de traducción del lenguaje extendido a SQL [2]. La capa externa es un mediador que consta de tres módulos [1]: el *front-end* es un analizador sintáctico o *parser* de SQL extendido que genera un árbol sintáctico abstracto (AST); el *core* es un traductor que transforma un AST del lenguaje extendido a un AST del lenguaje nativo; el *back-end* (*deparser*) es un generador de código que toma el AST y escribe la instrucción en SQL.

Durante el análisis sintáctico se genera la lista de columnas *Tipo 3* a ser traducidas. Para ello, se recorren las expresiones de las cláusulas SELECT, WHERE, ORDER BY y GROUP BY, y se busca cada columna en el catálogo difuso. Luego se invoca al traduc-

> “ En *fuzzy*doDB se usa una arquitectura medianamente acoplada que consiste en una implementación intermedia donde la lógica fue programada en el lenguaje nativo del SGBD original ”

tor, que utiliza el catálogo para generar un AST correspondiente a la sentencia traducida al lenguaje nativo de SQL, de acuerdo a los esquemas de traducción [2].

Posteriormente, se recorre de nuevo el AST para localizar expresiones que involucren columnas *Tipo 3*. Estas columnas son sustituidas en el AST por la columna de la tabla LABEL que contiene la etiqueta conocida por el usuario. Si esta sustitución se realizó en la cláusula SELECT, se asegura que la expresión mantenga su alias o el nombre por el cual se accede al valor en el resultado.

La generación de código realiza el proceso inverso (*deparser*) para transformar el AST en un string SQL. Finalmente, se envía el string SQL al manejador para que sea ejecutado, obteniendo el resultado de la instrucción original.

4. Base de datos experimental

El pgfoundry.org [11] es anfitrión de varios proyectos de software relacionados con PostgreSQL [12].

Para probar el prototipo *fuzzy*doDB se buscó uno de los ejemplos de bases de datos allí publicados. De entre las disponibles, se escogió la base de datos *World*.

Ésta es una base de datos de prueba encontrada en la documentación oficial de MySQL, la cual fue migrada a PostgreSQL por esta organización [11]. El interés de tomar una base de datos de este sitio obedece al hecho que son recursos disponibles públicamente y conocidos por la comunidad de desarrollo de PostgreSQL. Sin embargo, estas bases de datos no incluyen atributos difusos que es justamente la funcionalidad añadida por *fuzzy*doDB. De manera que para la base de datos experimental a usar en este trabajo se hizo imperativo el realizar modificaciones a la base de datos *World*, con el fin de incluir atributos difusos.

4.1. Modelo lógico

La base de datos *World* [11] posee tres tablas: COUNTRY, CITY y COUNTRYLANGUAGE. A éstas se realizaron modificaciones con el fin de incluir atributos difusos. A continuación, se describe el modelo lógico de la base de datos *World* modificada. Se colocan en cursiva los atributos difusos correspondientes a las modificaciones realizadas. Los dominios difusos se presentarán en la siguiente subsección.

COUNTRY (code, name, *continent*, region, surfacearea, indepyear, population, lifeexpentacy, gnp, gnpgold, localname, governmentform, headofstate, capital, code2) contiene la información acerca de los países del mundo con 239 registros, donde code es la clave primaria y capital es una clave foránea que referencia a CITY. Se modificó el atributo *continent* para que fuera del nuevo dominio difuso *Tipo 3* FUZZYCONTINENT.

CITY (id, name, countrycode, district, population, cars, *ePopulation*), contiene la información sobre ciudades de esos países con 4079 registros, donde id es la clave primaria y countrycode es una clave foránea que referencia a COUNTRY. Se agregó una nueva columna denominada *ePopulation* la cual contiene datos del dominio difuso *Tipo 2* FUZZYPOPULATION.

COUNTRYLANGUAGE (countrycode, language, isofficial, percentage) contiene los idiomas hablados en cada país con 985 registros, donde la clave primaria es (countrycode, language) y countrycode es una clave foránea que referencia a COUNTRY.

4.2. Dominios difusos

Se definieron dominios difusos, uno *Tipo 2* y el otro *Tipo 3*. Para este último, se mostrará la definición en SQL extendido pues este dominio es el objeto de este trabajo.

FUZZYPOPULATION: permite representar valores estimados para la cantidad actual de habitantes de una ciudad. Si bien la base de datos original tiene por cada ciudad un valor de población (*population*), dado que la población real es un dato cambiante, en un momento podría no tenerse el valor preciso, por lo que tiene sentido modelar esta información con un atributo difuso *Tipo 2*.

FUZZYCONTINENT: existen siete continentes en la base de datos, éstos pueden considerarse con cierta similitud entre ellos, por lo que puede modelarse como *Tipo 3*. En este caso, la similitud que se ha representado tiene que ver con cercanía geográfica, donde los grados de similitud se han puesto en forma arbitraria. Tal definición de similitud se justifica por ser un estudio experimental y el propósito aquí es enfocarse en el tema de desempeño.

Estos valores pueden cambiarse por otros dependiendo de las preferencias del usuario,

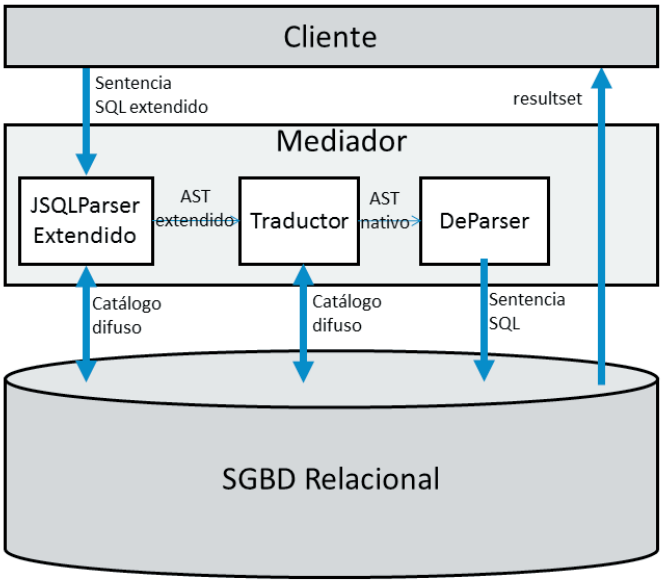

Figura 1. Arquitectura de *fuzzy*doDB. Fuente [1].

> “ Para la base de datos experimental a usar en este trabajo se hizo imperativo el realizar modificaciones a la base de datos *World*, con el fin de incluir atributos difusos ”

captando mejor la semántica que se quiera adoptar para la relación de similitud entre continentes.

La definición del dominio difuso sería CREATE FUZZY DOMAIN FUZZYCONTINENT AS VALUES (Europe, Oceania, Asia, North America, Africa, Antarctica, South America) SIMILARITY {(Europe, Oceania)/0.4, (Europe, Asia)/0.9, (Europe, North America)/0.5, (Europe, Africa)/0.9, (Europe, Antarctica)/0.2, (Europe, South America)/0.3, (Oceania, Asia)/0.7, (Oceania, North America)/0.2, (Oceania, Africa)/0.4, (Oceania, Antarctica)/0.8, (Oceania, South America)/0.4, (Asia, North America)/0.3, (Asia, Africa)/0.6, (Asia, Antarctica)/0.5, (Asia, South America)/0.3, (North America, Africa)/0.4, (North America, Antarctica)/0.2, (North America, South America)/0.9, (Africa, Antarctica)/0.3, (Africa, South America)/0.3, (Antarctica, South America)/0.6}.

5. Diseño experimental

Se realizó un estudio de desempeño experimental usando un modelo estadístico formal [5][14]. La idea de este método es explicar la influencia de diversos factores considerados en los valores observados de los experimentos. La importancia de un factor es medida por la proporción del total de variación en la respuesta que es explicada por el factor. En el análisis de desempeño se persigue mostrar resultados con el menor número de experimentos.

Se adoptó un diseño factorial $2^{(k+2)}$ [5][14] donde k es el número de factores utilizados, para cada factor se consideran únicamente dos niveles. Además, se realizaron cuatro réplicas por cada una de las pruebas para obtener mayor precisión, esta es la razón del exponente (k+2). Se consideraron dos factores relevantes (k=2) para explicar el comportamiento del sistema.

Hay dos grupos de experimentos, cada uno con un experimento para ordenamiento y otro para agrupamiento. El primer grupo considera el impacto del tipo de atributo en el SGBD extendido, mediante los factores: volumen (*V*) y tipo de atributo (*A*). El factor *A* se refiere al atributo involucrado en la cláusula que se está experimentando, el cual puede ser preciso (A_1) o *Tipo 3* (A_2). El segundo grupo considera el impacto de la extensión del SGBD respecto al original en consultas con atributos precisos, mediante los factores: volumen (*V*) y SGBD (*S*). El factor *S* puede ser PostgreSQL original (S_1) o PostgreSQL extendido (S_2), es decir *fuzzy*doDB.

En todos los experimentos se usa la tabla CITY. El volumen de datos original de esta tabla era 4079 tuplas que ocupaban 298 KB. Este volumen resultó ser poco representativo para los fines del análisis de desempeño. Para aumentar el volumen se hicieron réplicas de los datos. Se consideró el factor volumen (*V*) con dos niveles: el bajo (V_1) con 32632 registros (2413 KB) y el alto (V_2) con 30128 filas (9.713 KB).

Se elaboraron cuatro consultas experimentales. Para el ordenamiento y agrupamiento difuso se tomó el atributo *continent* de la tabla COUNTRY. Fue necesario hacer las consultas sobre las tablas CITY y COUNTRY, combinadas mediante la clave foránea countrycode y la clave primaria code. Para el ordenamiento y agrupamiento clásico se tomó el atributo district que está en la tabla CITY, sin embargo, a fin de tener igualdad de condiciones, en las consultas clásicas se usa también la combinación de las tablas CITY y COUNTRY.

Las consultas experimentales son:

- SELECT district FROM CITY, COUNTRY WHERE countrycode=code ORDER BY district;
- SELECT *continent* FROM CITY, COUNTRY WHERE countrycode=code ORDER BY *continent* START Europe;
- SELECT district, count(*) FROM CITY, COUNTRY WHERE countrycode=code GROUP BY district;
- SELECT *continent*, count(*) FROM CITY, COUNTRY WHERE countrycode=code GROUP BY SIMILAR *continent*;

Todas estas consultas se usan en el primer grupo de experimentos, donde se varía el tipo de atributo. Para el segundo grupo de experimentos, en el cual lo que se varía es el SGBD, se tomaron únicamente las consultas que usan atributos precisos.

Para la corrida de los experimentos, se fijaron las características del hardware, la carga del computador y las conexiones. Las pruebas se realizaron en una máquina VIT P2400 que posee un procesador Intel Core i3-3110M a 2.4 GHz, una memoria RAM de 1.8GB y un disco duro de 150 GB. El disco estaba particionado para alojar dos sistemas de operación y las pruebas se realizaron sobre el sistema operativo Ubuntu 14.04 LTS de 32 bits. La verdadera capacidad de la máquina es de 320 GB de disco duro y de 2 GB de RAM. En cuanto a la carga de la máquina, en el momento de realizar las pruebas se tenía únicamente como proceso operativo el SGBD. Las conexiones a las bases de datos trabajaron sobre el servidor local de la máquina.

Para garantizar igualdad de condiciones entre las corridas de los experimentos, antes de ejecutar cada consulta, se limpiaba la memoria caché del SGBD.

La variable observada en el estudio fue el tiempo de ejecución (*T*) de las consultas medido en milisegundos, obtenido con el comando “time”.

Este diseño experimental se corresponde con el modelo aditivo $T=T'+\beta_1 A+\beta_2 V+\beta_3 AV+\varepsilon$, para el primer grupo de experimentos, y $T=T'+\beta_1 S+\beta_2 V+\beta_3 SV+\varepsilon$, para el segundo grupo de experimentos.

6. Análisis de los resultados

En esta sección se presentan los resultados de los experimentos realizados (ver **tabla 2**) y su análisis descriptivo. Se utilizó el software estadístico R para las pruebas de ajuste del modelo aditivo, obteniendo las tablas ANOVA.

6.1. Análisis de varianza

Para el primer grupo de experimentos, según las correspondientes ANOVA (ver **tabla 3**), se obtuvo: En las consultas con ordenamiento, tanto el factor volumen como el tipo de atributo, influyen de manera significativa, así como su interacción, aunque en menor grado. En el caso de las consultas con agrupamiento, ninguno de los factores influye significativamente.

En cuanto al segundo grupo de experimentos, según la **tabla 3**, se obtuvo: Para las

> “En el caso de consultas con agrupamiento, la gráfica muestra que no hay crecimiento significativo del tiempo de ejecución con el aumento del volumen de datos. Adicionalmente, los tiempos promedio son similares para ambos tipos de atributos”

Atributo	Volumen	Réplica	ORDER BY	GROUP BY
Preciso	Bajo	R1	6660	4525
		R2	9063	4968
		R3	6764	4378
		R4	7904	4489
	Alto	R1	14705	4504
		R2	14861	5288
		R3	16044	4629
		R4	14455	4687
Difuso	Bajo	R1	6133	4242
		R2	5963	5634
		R3	6110	4264
		R4	6108	4390
	Alto	R1	11900	5063
		R2	11121	4895
		R3	11218	5093
		R4	10707	4769

(a)

SGBD	Volumen	Réplica	ORDER BY	GROUP BY
Original	Bajo	R1	5594	3466
		R2	5264	3393
		R3	4693	2860
		R4	5091	2996
	Alto	R1	9437	3807
		R2	8458	4193
		R3	8625	4090
		R4	10128	3404
Extendido	Bajo	R1	6660	4525
		R2	9063	4968
		R3	6764	4378
		R4	7904	4489
	Alto	R1	14705	4504
		R2	14861	5288
		R3	16044	4629
		R4	14455	4687

(b)

Tabla 2. Tiempo de ejecución (ms) observado. (a) Resultados de experimentos del primer grupo. (b) Resultados de experimentos del segundo grupo.

Grupo	Consulta	ANOVA
Atributo	ORDER BY	Df Sum Sq Mean Sq F value Pr(>F) A 1 28079401 28079401 55.60 7.67e-06 *** V 1 158168352 158168352 313.21 5.79e-10 *** A:V 1 5109860 5109860 10.12 0.00791 ** Residuals 12 6059970 504997
	GROUP BY	Df Sum Sq Mean Sq F value Pr(>F) A 1 48620 48620 0.294 0.598 V 1 259590 259590 1.568 0.234 A:V 1 18360 18360 0.111 0.745 Residuals 12 1986903 165575
SGBD	ORDER BY	Df Sum Sq Mean Sq F value Pr(>F) S 1 68748972 68748972 109.67 2.17e-07 *** V 1 130416400 130416400 208.05 6.08e-09 *** S:V 1 11675889 11675889 18.63 0.001 ** Residuals 12 7522298 626858
	GROUP BY	Df Sum Sq Mean Sq F value Pr(>F) S 1 5358068 5358068 53.353 9.42e-06 *** V 1 777483 777483 7.742 0.0166 * S:V 1 257810 257810 2.567 0.1351 Residuals 12 1205128 100427
		Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Tabla 3. ANOVA de cada uno de los cuatro experimentos realizados.

consultas con ordenamiento, ambos factores, SGBD y volumen de datos, son altamente significativos, mientras que la interacción lo es un poco menos. Para el caso de las consultas con agrupamiento, el factor realmente significativo es el SGBD.

6.2. Análisis descriptivo

6.2.1. Experimentos según tipo de atributo

Para las consultas con ordenamiento, la gráfica de la **figura 2(a)** muestra que el crecimiento del tiempo de ejecución aumenta según el volumen de datos donde la tendencia es más fuerte para atributos precisos.

Esto puede explicarse porque en el caso de consultas con atributos precisos, las tuplas se ordenaron en base a cadenas de caracteres correspondientes a los valores de la columna district, mientras que en el caso de atributos difusos se ordenan en base al grado de similitud de la etiqueta para el atributo *continent* respeto al valor Europe, los cuales son números reales. El ordenamiento de secuencias de caracteres es mucho más costoso que el ordenamiento de números reales.

Cabe mencionar que la escogencia del atributo district para este experimento fue intencional. En el caso de haber diseñado *continent* como un atributo clásico, éste sería una cadena de caracteres. Por otro lado, aun siendo *continent* un atributo difuso, en caso de no usar la opción START de la cláusula ORDER BY, tendría que ordenarse como cadena de caracteres.

Dada la significancia de influencia de los factores volumen y tipo de atributo, así como su interacción, y el comportamiento antes descrito, se podría concluir que para consultas ORDER BY, a la medida que crece el volumen de datos, el desempeño es mejor con atributos difusos que con atributos precisos.

En el caso de consultas con agrupamiento, la gráfica de la **figura 2(b)** muestra que no hay crecimiento significativo del tiempo de ejecución con el aumento del volumen de datos. Adicionalmente, los tiempos promedio son similares para ambos tipos de atributos. Se concluye que el desempeño de *fuzzy*doDB para consultas con GROUP BY es igual si el agrupamiento es difuso o preciso.

6.2.2. Experimentos según SGBD

Para las consultas con ordenamiento, la gráfica de la **figura 2(c)** muestra que el crecimiento del tiempo de ejecución aumenta según el volumen de datos donde la tendencia es más fuerte para el caso del manejador extendido. Hay una diferencia entre el tiempo de ejecución de las consultas sobre el manejador extendido que va aumentando a medida que el volumen crece. Esto se explica por el impacto del procesamiento adicional generado por la extensión.

En el caso de las consultas con agrupamiento, la gráfica de la **figura 2(d)** muestra que no hay crecimiento significativo del tiempo de ejecución con el aumento del volumen de datos. Los tiempos promedios para SGBD extendido son mayores que para el original, sin embargo, la diferencia en este caso pareciera ser relativamente constante, lo cual corrobora la significancia del factor SGBD.

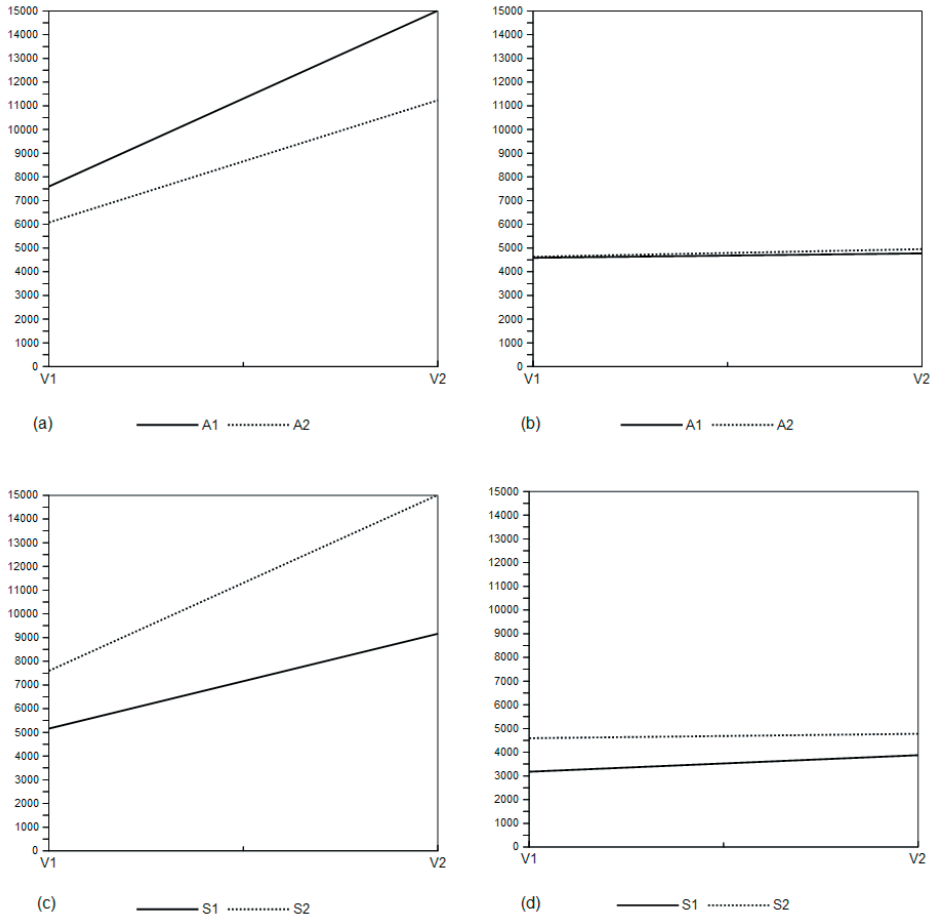

Figura 2. Promedio de tiempo de ejecución (ms), gráficas de interacción de factores. (a) Volumen-Atributo en consulta ORDER BY. (b) Volumen-Atributo en consulta GROUP BY. (c) Volumen-SGBD en consulta ORDER BY. (d) Volumen- SGBD en consulta GROUP BY.

7. Conclusiones y trabajos futuros

Este trabajo reporta un *benchmark* de consultas con ordenamiento y agrupamiento difuso sobre atributos *Tipo 3* en *fuzzy*doDB, una extensión con acoplamiento medio de PostgreSQL. A partir de una base de datos pública llamada *World* , se creó una base de datos experimental con atributos difusos que permite evidenciar funcionalidades de *fuzzy*doDB y puede ser usada en futuros *benchmark* con atributos difusos.

Se observó que para las consultas ORDER BY, a mayor volumen de datos, el ordenamiento difuso es mejor que el del ordenamiento preciso de etiquetas. Esto se debe a que el orden se realiza en base a grados de similitud y no en base a cadenas de caracteres. En el caso de consultas con la cláusula GROUP BY, el tiempo de ejecución de agrupamiento difuso es igual al preciso. Estos resultados sugieren que es razonable la inclusión de atributos difusos en los SGBD.

Se evidenció que la extensión degradó el desempeño del SGBD. Esto se debe a que todas las consultas pasan por el mediador, generando sobrecarga en el procesamiento. Este es el costo por más funcionalidad en una arquitectura de acoplamiento medio. Para evitar este costo, habría que implementar la extensión con una arquitectura de acoplamiento fuerte, lo cual sería mucho más complejo en términos de desarrollo pues involucra una intervención a código abierto.

Sólo se consideraron atributos *Tipo 3* y consultas con ordenamiento y agrupamiento sencillo. Se plantea a futuro hacer *benchmark* con otros tipos de atributos difusos y consultas más complejas.

Agradecimientos

Muchas gracias a nuestros alumnos en Miniproyecto de Desarrollo de Software de los últimos tres años, quienes contribuyeron con la implementación y pruebas de *fuzzy*doDB. Hablar de *World* y ordenamiento nos hace reflexionar que "*Tú ya eras Dios aun antes que las montañas se formaran y que crearas la tierra y el mundo. Tú eras y siempre serás Dios*" (Salmos 90:2).

Referencias

[1] S. Carrasquel, A. Gyomrey, S. Moreau, R. Rodríguez, B. Stornelli, C.Timaury, L. Tineo. "Extensión de MariaDB para ordenamiento y agrupamiento difuso". *Novática. Revista de la Asociación de Técnicos de Informática*, *Nº 229*, pp. 92-97, 2014.

[2] S. Carrasquel, R. Monascal, R. Rodríguez, L. Tineo. "Processing of Queries with Fuzzy Similarity Domains". *Handbook of Research on Innovative Database Query Processing Techniques*, L.Yan, Ed. Hershey, USA: IGI Global, 2016, pp. 88–128.

[3] S. Carrasquel, R. Rodríguez, L. Tineo. "Consultas con Agrupamiento basado en Similitud". *Ingeniare. Revista chilena de ingeniería*, *vol. 22 Nº 4*, pp. 517-527, 2014.

[4] S. Carrasquel, R. Rodríguez, L. Tineo. "Consultas con Ordenamiento basado en Similitud". *Telematique Vol. 12, N° 1*, pp. 24-45, 2013.

[5] O. Castejón. *Diseño y Análisis de Experimentos con Statistix*. Fondo Editorial Biblioteca Universidad Rafael Urdaneta, 2011.

[6] D. Coronado, S. Carrasquel, R. Monascal, R. Rodriguez, L. Tineo. "Portal de fuzzydoDB". *Memorias de la Tercera Conferencia Nacional de Computación, Informática y Sistema*. pp. 328–332. Caracas, Venezuela, octubre 2015.

[7] J. Galindo. "FSQL (Fuzzy SQL) A Fuzzy Query Language". Universidad de Málaga. <www.lcc.uma.es/~ppgg/FSQL/>.

[8] J. Galindo, A. Urrutia, M. Piattini. *Databases: Modeling, Design and Implementation*. Idea Group Publishing Hershey, USA, 2006.

[9] MariaDB Foundation. *MariaDB* <mariadb.org/>.

[10] J. Medina, O. Pons, A. Vila. "GEFRED: A Generalized Model of Fuzzy Relational Databases". *Information Sciences*, *Vol. 77, no. 6*, pp. 87-109, 1994.

[11] PostgreSQL Development Group. " *Forge*", 2014. <pgfoundry.org>.

[12] PostgreSQL Web Team. "*Pgfoundry* <wiki.postgresql.org/wiki/Pgfoundry>.

[13] R Core Team. "*R: A language and environment for statistical computing*". R Foundation for Statistical Computing, Vienna, Austria, 2015 <http://www.R-project.org/>.

[14] J. Raj. *The Art of Computer Systems Performance*, John Wiley & Sons, Inc, 1991.

[15] R. Timarán. "Arquitecturas de Integración del Proceso de Descubrimiento de Conocimiento con Sistemas de Gestión de Bases de Datos: un Estado del Arte". *Ingeniería y Competitividad Universidad del Valle, Colombia, vol. 3, no. 2*

[16] L. A. Zadeh. "Fuzzy Sets". *Information Control* , pp. 338-353. 1965.

[17] L. A. Zadeh. "A computational approach to fuzzy quantifiers in natural languages". *Computer Mathematics with Applications*. , pp. 149-183. 1983.

El rol del conocimiento propio en la organización

Joan Baiget i Solé
Doctor en Sociedad de la Información y el Conocimiento; socio sénior de ATI

<joan.baiget.sole@gmail.com>

Resumen: *En un mundo globalizado, los bienes tangibles están (cada vez más) al alcance de las organizaciones en mayor igualdad de condiciones. Para diferenciarse competitivamente, las empresas pueden recurrir a los bienes intangibles, entre ellos el conocimiento. No obstante, se advierte un gap entre la importancia que éstas otorgan al conocimiento y la valoración que las propias empresas hacen de su Gestión del Conocimiento. Contribuir al análisis de este gap es el objeto de la presente tesis.*

Palabras clave: *Competitividad, conocimiento propio, Gestión del Conocimiento, escenarios del conocimiento, sostenibilidad, trayectorias de aprendizaje, ventajas competitivas.*

1. Estado del arte

Desde hace ya décadas que el conocimiento y su gestión se hallan situados en una parte central del mundo de la gestión, de los sistemas de información, del '*Strategic Management*' y, en definitiva, de un buen puñado de disciplinas que se esfuerzan en dar respuestas a las nuevas realidades, y necesidades de gestión y desarrollo de la sociedad y, en ella, de las empresas actuales que ven en el concepto del conocimiento una transformación no sólo radical sino también crítica, necesaria e imprescindible para el futuro de la sociedad[1].

Podemos considerar que ha existido un cierto auge de esta actividad, en torno al conocimiento y su gestión, a partir de los inicios de la década de los 90, con un punto álgido asociado a la emblemática publicación de "*The Knowledge Creating Company*" por parte de los conocidos iconos de la Gestión del Conocimiento (GC) Nonaka y Takeuchi [1].

Esta referencia imprescindible y popular no debe hacernos perder de vista que la discusión académico-teórica sobre GC tiene antecedentes muy anteriores con pioneros emblemáticos como Daniel Bell [2] que ya en 1973 evidenciaba la magnitud social de los cambios basados en el conocimiento, presagio de una auténtica revolución.

Además de refinadas aproximaciones desde el *management* como las de Boisot – Macmillan [3], existen aproximaciones a la Gestión del Conocimiento desde perspectivas TIC (Tecnologías de la Información y las Comunicaciones), como las de McClellan y Dorn [4] o desde perspectivas auspiciadas por el concepto de *"Organizational Learning*" [5], entre otras.

El conocimiento, también por la esencia humana de su naturaleza, se ha abordado desde vertientes filosóficas, o *pseudo*-filosóficas, hasta confeccionar (con tantas perspectivas posibles) una extensa trama de aproximaciones en su tratamiento, cuyos extremos difieren conceptualmente hasta casi el infinito y cuyas fronteras interiores pueden incluso parecer difusas.

La justificación académica del conocimiento y su gestión no es un proceso banal atendiendo a la rica historia de estudiosos del conocimiento que han llenado de una interesante literatura estas últimas décadas. No puede hacerse una recopilación (por exhaustiva que ésta sea) que no corra el riesgo de dejar fuera de ésta nombres, importantes o no, que hayan contribuido de manera significativa en la identificación y evolución conceptual de esta nueva disciplina.

Tal vez un buen resumen, no exento del problema mencionado, pueda atribuirse al profesor Manuel Riesco [6] en su revisión de autores y conceptos que durante las últimas 3 décadas han contribuido al fenómeno de la cristalización de la Gestión del Conocimiento.

De él extraemos algunos de los momentos álgidos para la construcción de la nueva Gestión del Conocimiento. En su cronología de hechos históricos relevantes se propone un (siempre teórico) inicio de era con la aportación de Itami por su concepto de "*Mobilizing Intangible Assets*" (1980). Efectivamente, es no sólo la identificación de los activos intangibles sino también su *movilización* lo que fundamenta y justifica que exista un importante activo llamado "conocimiento" que requiere de una no menos importante "Gestión", cuyo concepto enfatiza Masuda para aplicarlo a una sociedad emergente, "*Managing the Information Society*" (1980) [7].

No menos pioneras son las aportaciones de K. Erik Sveiby en "*The Know-How company*" (1986) [8] y las de Peter Druker identificando dos aspectos característicos de las nuevas organizaciones: su estructura en red, "*The Networked Organization*" (1988) y la importancia de un aprendizaje distinto para una realidad distinta, el "*Organizational Learning*" (1989) [9], concepto ampliamente estudiado por un importante número de autores que lo han elevado casi al concepto de sub-disciplina.

Otro pilar fundamental imprescindible de esta nueva disciplina son las aportaciones de Peter Senge (1990) [10] y sus contribuciones en el ámbito del aprendizaje organizacional con su gran aportación conceptual que moldeó una revolución en el *management*: "*The Learning Organization*".

Pocos conceptos han calado tan hondo en el ámbito del *management* como el de "*Learning Organization*", a pesar de que otras muchas aproximaciones han sido propuestas en discursos paralelos en la búsqueda de una explicación lo más real posible de los importantes cambios que sucesivamente se iban concretando, de manera ràpida y persistente, en la cambiante realidad social.

Así, "*Brain Power*" (Steward, 1991), "*Relational Organization*" (P. Keen, 1991), "*Cluster Organization*" (Quinn, 1991), "*Intelligent Enterprise*" (J. Brian, 1992), "*Virtual Corporation*" (Davidow & Malone, 1992) o "*Re-engeenering Corporation*" (Hammer & Champi, 1994) son intentos de capitalizar ese cambio interpretándolo con el foco específico del investigador.

Un punto de inflexión en el impacto de esta nueva realidad en el *management* y su entronque en las organizaciones lo podemos situar en el momento en que se concreta una nueva figura en la estructura organizativa con rango de "*Manager*".

Esto sucedió en 1991 cuando el primer CKO (*Chief Knowledge Officer*, Leif Edvinson) institucionalizó al Responsable de la Gestión del Conocimiento en el seno de las organizaciones, a pesar de que (como veremos en el resultado de los distintos estudios) este rango no está aún presente en la mayoría de las organizaciones, si bien su función empieza a consolidarse.

> “El capital intelectual se focaliza con claros objetivos de medición, de manera que deviene en unas propuestas más ‘estáticas’, mientras que la Gestión del Conocimiento se focaliza en la acción para la optimización de resultados basado en una óptima utilización y gestión de este tipo de activos”

La aparición del CKO fue el significativo resultado de un largo trayecto con numerosas aportaciones académicas y del *management* de las últimas décadas, pero también de algunas más tempranas en la línea del pensamiento, como las de Polanyi [11] y su foco en la “dimensión tácita” del conocimiento que le entrona como pionero y precursor de este concepto.

También cabe hacer una ineludible referencia a Karl Popper [12] por su temprana colaboración al núcleo conceptual de la Gestión del Conocimiento, con mención especial para su idea de los “3 mundos”, que representan: el mundo real a nivel de la existencia, el de nuestro pensamiento y aquel que va conformándose a medida que la humanidad convierte conocimientos en documentación explícita (planteamientos muy paralelos a los “Escenarios del Conocimiento” de este propio doctorando.

Casi a la par, existen los primeros intentos de formalizar un corpus teórico-practico de la Gestión del Conocimiento. Wiig nos habla ya en 1993 de “*Knowlewdge Management Foundations*” [13]. Y también surgen los primeros principios teóricos que intentarán (atendiendo a la importancia del conocimiento en las organizaciones) algunas estrategias para su medición. Ya en 1994, Stewart habla de “*Intellectual Capital*”, concepto que consolidarán Edvinson y Malone en 1997 [14].

Estos intentos de comprensión y medición del capital intelectual van emparentados con la idea de un conocimiento intangible como activo de las entidades, pero si bien en un principio se utiliza como paralelismo a la Gestión del Conocimiento, en realidad evolucionará como disciplina propia y se alejará de la investigación académica asociada a ésta.

El capital intelectual se focaliza con claros objetivos de medición, de manera que deviene en unas propuestas más “estáticas”, mientras que la Gestión del Conocimiento se focaliza en la acción para la optimización de resultados basado en una óptima utilización y gestión de este tipo de activos, como ejemplariza la conocida obra de Davenport y Prusak, “*Working Knowledge*” [15].

El primer informe público sobre capital intelectual (CI) de obligada referencia es el de Skandia, desarrollado en 1994 y entronizado posteriormente por Edvinsson [16].

El capital intelectual, en su proceso de independizarse (en forma figurada) de la disciplina de la Gestión del Conocimiento, ha dejado un buen número de modelos como el *Balanced Scorecard* [17], el *Intangible Assets Monitor* [18] o hasta los más recientes como el *Intellectual Capital Benchmarking System* [19] originado en 2001 y perfeccionado hasta la re-edición de 2012. Todos ellos inciden en la medición más que en el “flujo” de este capital, si bien sus resultados podrán ser utilizados para una reformulación estratégica.

Pero si existe un punto de inflexión en la Gestión del Conocimiento, éste lo representa la publicación de “*The Knowledge-Creating Company*” en 1995 [20]. Los profesores Nonaka y Takeuchi sientan las bases de lo que será la más prolífica aportación de un modelo de Gestión del Conocimiento, el Modelo SECI (Socialización, Externalización, Combinación, Internalización), las cuatro posibles combinaciones entre el conocimiento explícito y el conocimiento tácito.

Según nos dice Sveiby [21], en su desarrollo, la Gestión del Conocimiento bebe de tres distintas fuentes que a la postre configurarán dos diferentes corrientes de pensamiento sustancialmente alejadas la una de la otra en la dimensión pragmática del conocimiento y su gestión.

Estos orígenes son el japonés, por un lado, con los trabajos del profesor Ikujiro Nonaka sobre la innovación en las organizaciones que se remontan a inicios de la década de los 80 y con las aportaciones del también japonés Hiroyuki Itami que introduce el concepto de activos intangibles por las mismas fechas.

El segundo origen se sitúa en EEUU con las investigaciones acerca de la Inteligencia Artificial (AI) aportando una dimensión tecnológica a la incipiente disciplina de la Gestión del Conocimiento y cuyo representante principal sería el profesor Karl Wiig.

Finalmente, un “autoproclamado” origen sueco (aunque algo más tardío, década de los 90) situaría a K.E. Sveiby como un pionero en la investigación sobre la estrategia de las organizaciones asociada a la Gestión del Conocimiento.

De estos tres orígenes florecen dos corrientes principales: una “oriental” y otra “occidental”, atendiendo lógicamente a sus respectivos orígenes pero muy diferenciadas no por razón de origen sino por posicionamiento intelectual, foco y contexto en donde se originan cada una de ellas.

La corriente oriental y la occidental se diferencian por un reducido pero contundente número de características en las que divergen. Éstas son:

- La corriente oriental ensalza el conocimiento tácito, mientras que la corriente occidental prioriza el conocimiento explícito.
- La corriente oriental ve el conocimiento como un proceso dinámico, mientras que la corriente occidental trata el conocimiento como un objeto.
- La corriente oriental asocia el conocimiento a las Personas, mientras que la corriente occidental se centra en la implantación de soluciones TI (Tecnologías de la Información).
- La corriente oriental traza el objetivo de la generación de beneficio, mientras que la corriente occidental trabaja el conocimiento para la reducción de costes.
- La corriente oriental focaliza la creación de conocimiento y la innovación, mientras que la occidental se centra en el “reúso” del conocimiento.
- La corriente oriental trabaja los aspectos intangibles (conocimiento tácito, reputación, lealtad…), mientras que la corriente

> “Como disciplina aún emergente, en un escenario cambiante, la Gestión del Conocimiento requiere reflexión y análisis, investigación en definitiva, para aportar nuevos elementos teóricos que permitan una mejora de su práctica”

occidental pone énfasis en el ciclo del conocimiento (captura, catalogación, distribución, compartición…).

Pero esta diferenciación de enfoques no obvia que existan unos mitos comunes a evitar acerca de la Gestión del Conocimiento, de manera que la Gestión del Conocimiento no es sólo:

- Aprender (*learning*).
- Implantar procedimientos.
- Capturar el conocimiento de la cabeza de los empleados.
- Distribuir adecuadamente la información.
- Una función a delegar en RRHH o TI.
- Un añadido a la gestión habitual.
- Una manera de invertir en TI.

Todos estos errores conceptuales se han encontrado con frecuencia presentes en la realidad de las organizaciones si bien han ido evolucionando con el tiempo.

2. El rol del conocimiento propio en la organización

La perspectiva de la empresa basada en el conocimiento (*Knowledge Based View of the Firm*), como evolución a este nuevo contexto de paradigmas anteriores, como la empresa basada en recursos (*Resources Based View of the Firm*), dinamiza unas corrientes de pensamiento a la vez que implica unas nuevas prácticas empresariales que se retroalimentan entre sí, si bien no aún en la medida necesaria.

Como disciplina aún emergente, en un escenario cambiante, la Gestión del Conocimiento requiere reflexión y análisis, investigación en definitiva, para aportar nuevos elementos teóricos que permitan una mejora de su práctica.

Esta tesis doctoral pretende contribuir a este noble objetivo investigando acerca del rol del conocimiento propio (idiosincrásico) en la organización, para la creación de valor en una economía global.

Para ello tomará como base de partida una década de estudios de Gestión del Conocimiento (IESE, Capgemini, UOC) para revisar la investigación académica en relación al conocimiento propio (*Firm Specific Knowledge*), lanzar y validar (o refutar) las hipótesis de trabajo para obtener unas conclusiones novedosas al respecto y sentar (a la vez) precedentes para nuevas investigaciones de campo.

Juntamente con el profesor Rafael Andreu (IESE) lanzamos la hipótesis principal, según la siguiente forma:

> ***“El desarrollo del Conocimiento Propio en una Organización contribuye a obtener Ventajas Competitivas sostenibles en el tiempo”***

En base a esta hipótesis principal, declaramos las siguientes sub-hipótesis:

> **Sub-hipótesis 1ª:**
> ***“La importancia otorgada al Conocimiento Propio en una empresa debería correlacionarse con el nivel de Liderazgo de ésta”.***

> **Sub-hipótesis 2ª:**
> ***“Los Tipos de Aprendizaje e incorporación de Conocimiento que utilizan las empresas deberían ser coherentes –en relación al Conocimiento Propio- con sus Practicas de Gestión del Conocimiento”***

En el enunciado de esta última sub-hipótesis existe tanto la creencia que debe darse coherencia entre incorporación de conocimiento (aprendizaje) y prácticas de Gestión del Conocimiento, como la sospecha de que podemos encontrarnos un “*gap*” o disfunción entre estos aspectos críticos de gestión, que representaría (entendemos) incidir en la brecha entre la teoría y la práctica de la GC en las Organizaciones.

Algunos resultados (*en la escala de Likert, de 1 a 5*):

- El liderazgo (4,1 de media) y la importancia del conocimiento propio (CP) (4,0 de media) son altos y se correlacionan (según análisis realizado anteriormente)[2].
- La proporción del conocimiento propio no requiere ser alta (3,5 media).
- La Gestión del Conocimiento no es adecuada (2,7 de media) a pesar que se considera que contribuye a la competitividad (3,9 de media) y que sus ventajas competitivas son duraderas en el tiempo (4,0 de media).
- La incorporación de conocimiento (3,3 de media en preguntas cerradas) se realiza básicamente con recursos externos y las prácticas que declaran no son las que más aportan al CP (35% de empresas fomentan el CP).
- La creación de conocimiento (3,7 de media en preguntas cerradas) incluye un ‘*mix*’ de recursos internos y externos y las prácticas que declaran apuntan a una potencial creación de CP (61,3% de empresas fomentan el CP).
- La transmisión de conocimiento (3,6 de media en preguntas cerradas) tiene un claro componente de prácticas con potencial para la creación de un conocimiento propio (62,5 % de empresas fomentan el CP).
- De acuerdo con el “*gap*” que apuntábamos como previsible entre la importancia y los mecanismos de desarrollo del conocimiento propio y las prácticas de Gestión del Conocimiento, y que se ha confirmado con la no validación de la segunda hipótesis, observamos que en las Prácticas de Gestión del Conocimiento declaradas sólo el 43,6% de empresas declaran unas prácticas que son lógica y fácilmente potenciadoras de un conocimiento propio diferenciado e idiosincrásico.

Lo primero que podemos anticipar en estas conclusiones de la investigación es que los objetivos esperados al inicio de este trabajo se han cumplido, y además creemos que se han cumplido de manera ampliamente satisfactoria.

Efectivamente, la importancia estratégica que se otorga al conocimiento propio (*firm specific knowledge*) corre paralela al lideraz-

> “ La importancia estratégica que se otorga al conocimiento propio (*firm specific knowledge*) corre paralela al liderazgo de las empresas estudiadas y a la percepción declarada de sostenibilidad de este conocimiento como ventaja competitiva ”

go de las empresas estudiadas y a la percepción declarada de sostenibilidad de este conocimiento como ventaja competitiva.

En ésto consistía precisamente el hecho de probar la primera sub-hipótesis declarada:

> “*La importancia otorgada al conocimiento propio en una empresa debería correlacionarse con el nivel de liderazgo de ésta*”.

La primera sub-hipótesis se ha probado. Éste era, no obstante, un objetivo que se intuía y empíricamente fácil de demostrar y era, en la práctica, la estrategia de cimentar un punto de partida como base para la investigación más de fondo: la segunda sub-hipótesis.

La segunda sub-hipótesis enfocaba la probación de un concepto que (de manera opuesta a la primera sub-hipótesis) se preveía intuitiva y experimentalmente difícil de probar y, aún más, difícil de no encontrar lagunas importantes que dificultasen seriamente el optimismo necesario para su futuro proceso de probación.

La segunda sub-hipótesis era ésta: “*Los tipos de aprendizaje e incorporación de conocimiento que utilizan las empresas deberían ser coherentes –en relación al conocimiento propio- con sus practicas de Gestión del Conocimiento*”. La segunda sub-hipótesis se ha refutado, pero ésta era la expectativa e incluso parte de la estrategia planteada.

La probación de la primera sub-hipótesis y la no-probación de la segunda nos servirán de base para argumentar acerca del ‘*gap*’ más importante y significativo que han aportado una década de estudios sobre Gestión del Conocimiento: el conocimiento se considera estratégico pero su gestión se hace ineficientemente.

3. Conclusiones

A modo de conclusiones podemos decir:

- El conocimiento propio se reconoce como factor importante para la obtención de ventajas competitivas sostenibles en el tiempo que permiten a la organización situarse en la zona de liderazgo del sector en donde operan.
- Pero existe un significativo ‘*gap*’ entre la importancia que las empresas otorgan a su conocimiento y la valoración que las propias empresas hacen de su gestión a la hora de implantar sus propias prácticas de Gestión del Conocimiento.
- El análisis de los datos demuestra que en las empresas las prácticas de Gestión del Conocimiento no se encuentran alineadas respecto a los esfuerzos de aprendizaje que contribuyen a la configuración de su conocimiento propio y que les permitiría la obtención de ventajas competitivas sostenibles en el tiempo.
- Orientar dichas prácticas a los esfuerzos de aprendizaje pasa por entender la importancia del proceso de generación de conocimiento (modelo SECI).
- Pero el modelo SECI (Nonaka-Takeuchi), a pesar de algunas extensiones estratégicas del modelo desarrolladas (por ej. SECI, Ba y Leadership), no contiene suficientes elementos que ayuden a la necesaria reflexión para la implantación.
- Las *trayectorias de aprendizaje* (R. Andreu) pueden aportar el punto de reflexión sobre la importancia del adecuado “*mix*” de conocimiento externo e interno para la configuración de un adecuado conocimiento propio.
- Los *escenarios del conocimiento* (J. Baiget) pueden ayudar a orientar y concretar las prácticas necesarias para gestionar el conocimiento a nivel individual y ayudar también a la reflexión estratégica a nivel organizativo.

Ante la realidad del persistente desencuentro de la Gestión del Conocimiento en la práctica de las empresas y los esfuerzos teóricos académicos para su eficiente gestión, se hace imprescindible una iniciativa académica que concilie las muchas aportaciones teóricas ya existentes hasta converger en un simple “modelo de recomendaciones” que desde la teoría oriente la práctica y la implantación de la Gestión del Conocimiento en las empresas.

Referencias

[1] I. Nonaka, H. Takeuchi. *The knowledge-creating company : how Japanese companies create the dynamics of innovation*, Oxford University Press, New York, 1995.

[2] Daniel Bell. *The Coming of Post-industrial Society: A Venture in Forecasting*. New York: Basic Books, 1973.

[3] Max Boisot, Ian Macmillann. *Crossing Epistemological Boundaries: Managerial and Entrepreneurial*. UOC-Internet Interdisciplinary Institute (IN3) Working Paper, 2004. <http://www.analisi.cat/index.php/in3-working-paper-series/article/viewFile/n4-boisot-macmillan/n4-boisot-macmillan>, Último acceso: 6 de marzo de 2017.

[4] J.E. McClellan, H. Dorn. *Science and Technology in World History: An Introduction*. The Johns Hopkins University Press, Baltimore and London, 1999.

[5] S. Sieber, R. Andreu. Organizational Learning and Knowledge Management: where is the link? En Yogesh Malhota (ed.). *Knowledge management and Business Model Innovation*. Idea Group Publishing, abril 2001. ISBN-13: 978-1878289988.

[6] Manuel Riesco González. *El Negocio es el Conocimiento*. Ed. Díaz de Santos, 2010.

[7] Yonehi Masuda. *The information society as a post-industrial society*. Basil Blakwell, 1980.

[8] Karl Erik Sveiby. *The Know-How company*, 1986.

[9] Peter Druker. *The coming of the New Organization*. Harvard Business Review, 1988.

[10] Peter Senge. *Fifth Discipline: The Art and Practice of the Learning Organization*. Doubleday Business, 1st edition, agosto 1990.

[11] M. Polany. *The Tacit Dimension*. The University of Chicago Press, 1966.

[12] K.R. Popper. *Objective Knowledge: An Evolutionary Approach*. Oxford University Press, 1972. ISBN-13: 978-0198750246.

[13] Karl Wiig. *Knowledge Management Foundations: Thinking about Thinking – How People and Organizations Create, Represent, and Use Knowledge*. Arlington, TX: Schema Press, 1993.

[14] L. Edvinsson, M.S. Malone. *Intellectual Capital: Realizing Your Company's True* ***Value by Finding its Hidden Brainpower*****. New York: Harper Business, 1997.**

[15] T. Davenport, L. Prusak. *Working knowledge: How organizations manage what they know*
ton: Harvard Business School Press, 1998.

[16] L. Edvinson. "Developping Intellectual Capital at Skandia". *Long Range Planning Volume 30, Issue 3*, June 1997, pp. 320-321, 366-373.

[17] R.S. Kaplan, D. Norton. *The Balanced Scorecard: Translating Strategy into Action*. Harvard Business School Press; Edición: First Edition, 1 de septiembre de 1996. ISBN-13: 978-0875846514.

[18] Karl Erik Sveiby. Intangible Assets Monitor. *Journal of Human Resource Costing & Accounting 2(1)*: pp. 73-97, December 1997.

[19] J.M. Viedma. ICBS Intellectual Capital Benchmarking System. *Journal of Intellectual Capital*, MCB University Press, U.K, 2001.

[20] I. Nonaka, H. Takeuchi. *The Knowledge-Creating Company*. Oxford University Press, 1995. ISBN-13: 9780195092691.

[21] Karl Erik Sveiby. *Knowledge Management – Lessons from the Pioneers*
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.474.3743&rep=rep1&type=pdf>.Último acceso: 6 de marzo de 2017.

Notas

[1] Este artículo es un extracto de la tesis doctoral del autor cuya lectura tuvo lugar en marzo de 2015. La tesis doctoral completa puede descargase desde: <http://www.tesisenred.net/bitstream/handle/10803/306604/Tesis_Doctoral_Joan_Baiget.pdf>.

[2] Se ha realizado un análisis detallado, más allá del coeficiente de correlación y la covarianza calculados en las bases de datos por métodos puramente estadísticos y que no colman el análisis pretendido aquí.

Roberto José Fernández García
Ejecutivo de Cuentas en Telefónica; Estudiante de doctorado; Socio sénior de ATI

<rfernandez.casa@gmail.com>

El éxito de Bitcoin: La economía de la deep web

Resumen: *Bitcoin empezó con idea de desarrollar un proyecto de software libre que permitiese el funcionamiento de una moneda sustentada de manera colectiva por la red, permitiendo hacer pagos instantáneos a cualquier parte del mundo sin intermediarios. Se trata una divisa descentralizada que opera a través de tecnología P2P. Al no existir una autoridad central ni intermediación de ninguna institución financiera, los encargados de la gestión de las transacciones y de la creación del dinero son los propios usuarios de Bitcoin. Pero la no adopción del dinero virtual, Bitcoin por ejemplo, por parte de los bancos centrales mundiales se justifica por los lentos procesos de regulación y los escasos incentivos al cambio. Los bancos centrales inciden en los casos de financiación de actividades ilícitas, blanqueo de capitales, etc. para tirar por tierra la propuesta. Ha sido Japón, quien en febrero de 2016 ha considerado a Bitcoin como una divisa corriente (en vez de mercancía) volviendo a situarse a la vanguardia de la regulación de las divisas digitales. Aunque la imagen de Bitcoin ha sufrido por ser la moneda empleada en Silk Road y por la bancarrota de su principal agencia de cambio, Mt. Gox, hoy cotiza por encima de los 420$ y su futuro se presenta halagüeño. El dinero electrónico sólo está empezando pero parte con muchos intereses creados ¿hasta cuándo las resistencias al cambio?*

Palabras clave: *Bitcoin, dinero electrónico, Mt.Gox, Ruta de la Seda, Satoshi Nakamoto, web profunda*.

1. Introducción

En los últimos años, el incremento de ancho de banda en las comunicaciones, la capacidad de los dispositivos móviles, el desarrollo masivo de aplicaciones, el crecimiento vertiginoso de las comunidades virtuales, la compartición de conocimiento, etc. han desembocado en una economía conducida a través de Internet. Actualmente, programas "robots" o "*bots*" escuchan las tendencias bursátiles con el fin de realizar operaciones automáticas y muy rápidas a nivel mundial.

En este entorno donde van surgiendo nuevos modelos de negocio *e-Business*, se ha hecho necesaria una divisa virtual y descentralizada para pagos instantáneos, intercambio de bienes y servicios, etc., y con costos de transacción mínimos.

Esta divisa no dispone de una autoridad central o intermediación de una institución financiera, por lo que son sus propios usuarios colectivamente, la red abierta P2P (*peer to peer*), los encargados de la gestión de las transacciones y de la creación de dinero. Bitcoin (BTC) es el tipo de divisa más generalizado, aunque existen otras.

Por otra parte, la *Deep Web*, el lado oscuro de Internet, es una red de webs de no fácil acceso al usuario común, donde pululan todo tipo de *hackers*, agentes del gobierno, altos cargos militares y las peores lacras de la sociedad. Para entender la *Deep Web* o "web profunda" [1] lo primero que debemos saber es que las páginas que todo el mundo visita día a día: Google, Wikipedia, Amazon y tantas otras, pertenecen a la *surface web* o "web superficial".

En la *Deep Web* se puede encontrar información que roza la ilegalidad o bien es completamente ilegal, páginas, foros, *wikis*, manuales, anuncios y artículos sobre: venta de órganos, venta de drogas, venta de armas, compra de artículos robados, *hackers*, contratación de sicarios, *ebooks* de todo tipo, pedofilia, necrofilia, zoofilia, violación y demás parafilias, canibalismo, guerrillas, asesinatos, secretos corporativos, documentos clasificados de empresas o gobiernos, terrorismo mundial, tráfico de seres humanos y un gran etcétera.

El caso de éxito "Silk Road" (La Ruta de la Seda) [2] ofrecía, través de la red anónima TOR, una plataforma para la venta de narcóticos en línea, realizando transacciones por medio de *bitcoins* (ver **figura 1**).

Era la web más grande de su tipo, llegando a facturar millones de dólares cada mes. El FBI encontró a su fundador, Ross Ulbricht, lo capturó y dejó el sitio cerrado.

2. Dinero electrónico

2.1. Historia del dinero

El dinero se intercambia en transacciones para compras de bienes y servicios, facilitando el comercio de un bien por otro. Un buen dinero debe ser transportable, divisible (las fracciones de bitcoins se denominan *satoshis*), corriente, escaso (tendiendo a una cota máxima: 21 millones en el caso de bitcoins) y no necesita tener valor intrínseco. El valor de cada unidad de dinero se determina por el equilibrio entre la oferta y la demanda.

El dinero puede ser físico (oro, plata, platino, monedas/billetes, perlas, etc.), electrónico (PayPal, WebMoney, e-gold, etc.), o virtual (Bitcoin, Litecoin, etc.).

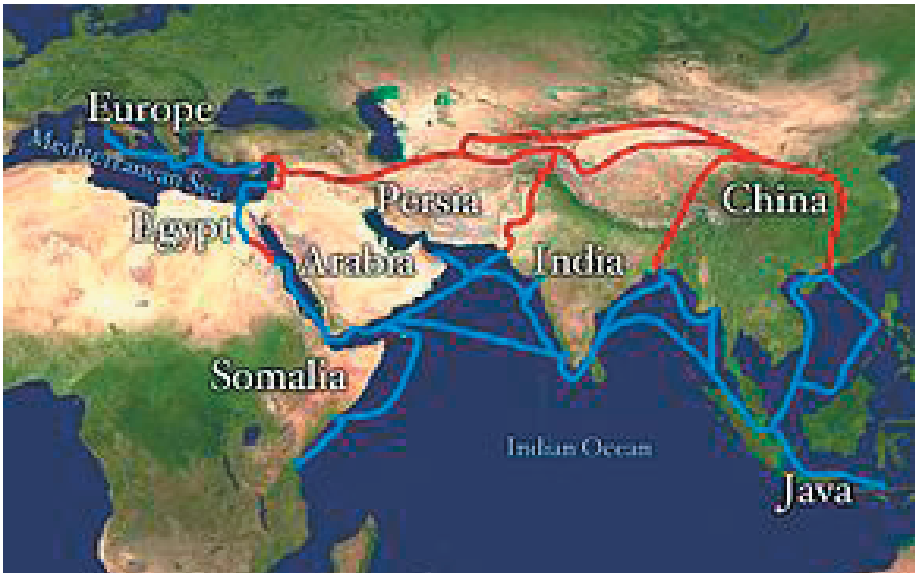

Figura 1. La Ruta de la Seda. Fuente: Wikipedia [3].

> “ En este entorno donde van surgiendo nuevos modelos de negocio *e-Business*, se ha hecho necesaria una divisa virtual y descentralizada para pagos instantáneos, intercambio de bienes y servicios, etc., y con costos de transacción mínimos ”

El dinero presenta propiedades como las siguientes:

- Es una unidad de cuenta con valor definido; en Bitcoin quizás con alta variabilidad.
- Es un medio de intercambio.
- Es un almacén de valor no perecedero.
- Es difícil de falsificar.
- Permite transacciones rápidas.
- Previene el doble gasto (Se han constatado casos en transacciones rápidas con bitcoins).
- Permite cierto grado de anonimato. Bitcoin lo permite.

2.2. Aspectos técnicos e institucionales

Según el Banco de España, se entiende por dinero electrónico [4] el valor monetario representado por un crédito exigible a su emisor:

a) Almacenado en un soporte electrónico.
b) Emitido al recibir fondos de un importe cuyo valor no será inferior al valor monetario emitido.
c) Aceptado como medio de pago por empresas distintas del emisor.

El dinero electrónico ha tenido que dar solución a los siguientes cinco puntos:

1) Implantación técnica. Productos basados: bien en software, utilizando un cliente específico para PC, *smartphone*, etc. (sistemas *software-based*: Paypal o pagos a través del teléfono móvil: Telefónica-BBVA) o bien en hardware, incluyendo un chip en una tarjeta de plástico (VISA Cash, Blue American Express).
2) Requisitos institucionales. Habitualmente en una transacción con dinero electrónico encontraremos cuatro agentes prestadores de servicio: el proveedor del dinero electrónico, la red de operadores, los vendedores de hardware y software especializado y los encargados de compensar las transacciones con dinero electrónico[1].

Desde el punto de vista normativo, los proveedores son el elemento más importante, ya que el dinero electrónico supone un pasivo en sus balances. Por el contrario, los operadores y vendedores no son más que proveedores en el ámbito técnico. Finalmente, la compensación la llevan a cabo bancos o compañías especializadas.

3) Método de transferencia de valor. Tradicionalmente, sólo eran permitidos los pagos de consumidor a proveedor, hoy es posible realizar transacciones P2P[2] en las que el propio sistema consolida la transacción.
4) Registro de las transferencias. En la mayoría de los casos, las operaciones se registran en una central de base de datos controlada. En el caso de operaciones P2P, sólo se grabarán y podrán ser controladas si el consumidor contacta con su operador de dinero electrónico.
5) Divisa de valor almacenado. Antiguamente, en la mayoría del dinero electrónico, el valor guardado sólo figuraba en la moneda nacional. En la actualidad, es posible pagar y registrar el valor almacenado en diferentes divisas, entre ellas Bitcoin.

2.3. Aspectos regulatorios

Cuando el Tribunal de Justicia de la Unión Europea decidió que el Bitcoin era una moneda más, hubo cierta esperanza de que quedara fuera de las manos de nuestros gobernantes.

Pero la Unión Europea quiere controlar las criptomonedas, con el argumento del terrorismo. El problema es que técnicamente no hay forma de controlarlas, así que la única regulación posible es prohibirlas y combatir su uso:

- No permitir a los comercios aceptarlas.
- Intentar identificar a las personas que las usan.

Bitcoin permite cierto anonimato (aunque las transacciones son públicas) y eso pone en riesgo los controles de capitales. Si se sigue extendiendo su uso parece seguro que la Unión Europea va a intervenir fiscalizando las transacciones financieras.

Los principales problemas de carácter regulatorio para la adopción del dinero electrónico son los siguientes:

1) Un lento proceso de regulación. La aparición de nuevos sistemas de pago guarda una estrecha relación con la política monetaria, pero no debe suponer un riesgo para el consumidor. Por este motivo, el marco legal y reglamentario debe evolucionar en el mismo sentido y celeridad: prevaleciendo la protección al consumidor y garantizado la viabilidad del sistema de pagos en el futuro.
2) Necesidad de una coordinación internacional. Los nuevos sistemas, especialmente los basados en software, no requieren de ninguna base geográfica, lo que aumenta considerablemente los riesgos.

La Unión Europea ya ha empezado a legislar para garantizar la viabilidad y la seguridad de los medios de pago del futuro. La Directiva Comunitaria 2000/46 establece que estas instituciones serán tratadas como entidades de crédito en lo que a exigencias de reservas mínimas y tendrán acceso a la refinanciación ofrecida por el Banco Central.

Desde 2011, en España su regulación está contenida en la Ley 21/2011, de 26 de julio, de dinero electrónico.

3) Pocos incentivos para el cambio, ya que aún es necesario disponer de dinero tradicional para efectuar compras en el mundo real. El dinero electrónico se parece a las tarjetas prepago, en las que el usuario debe poner dinero en una tarjeta con un chip integrado antes de poder utilizarla para pagar.

Las entidades de dinero electrónico, conocidas como EDE, están reguladas en el Ley 21/2011. Estas entidades se dedican a emitir dinero electrónico que es admitido como medio de pago por empresas distintas a la entidad emisora. Una de las entidades más conocidas es Paypal.

Además de las entidades bancarias existen dos EDE’s en España, [5] (MoneyToPay y YoUnique Money) que, junto con otras autorizadas en la Unión Europea, pueden operar en España.

> “Con Bitcoin no hay entidades en las que confiemos. No hay un banco que nos asegure que ‘este dinero es real’. En su lugar, la validez de Bitcoin reside en su tecnología, en todas las técnicas que aseguran que funciona como si fuese una moneda real”

3. El Bitcoin

3.1. Nacimiento e historia

Internet ha transformado muchas cosas, y una de ellas es nuestra forma de ver el dinero. Éste ha pasado de ser algo físico a ser un bien intangible, un número en una página. Creemos que está ahí porque confiamos en la entidad emisora y sabemos que lo gestionan como si fuese dinero físico y tangible.

Con Bitcoin no hay entidades en las que confiemos. No hay un banco que nos asegure que “este dinero es real”. En su lugar, la validez de Bitcoin reside en su tecnología, en todas las técnicas que aseguran que funciona como si fuese una moneda real.

La idea pionera de David Chaum data de 1982, con el desarrollo *e-cash*, y fue en 2007 cuando Satoshi Nakamoto concibió Bitcoin con el objeto de desarrollar un proyecto de software libre que permitiese el funcionamiento de una moneda sustentada de manera colectiva por la red y que permitiera pagos instantáneos a cualquier parte del mundo sin intermediarios.

La/s identidad/es bajo el seudónimo de Satoshi Nakamoto son todo un misterio. Se cree que el nombre fuese creado expresamente para el proyecto con la finalidad de proteger la verdadera identidad/es del autor/es y la red Bitcoin. Empezó a trabajar en el proyecto en 2007, para ir reduciendo su participación en 2009 y desaparecer en 2010.

3.2. Diferencias entre dinero electrónico y dinero virtual

El dinero virtual, como Bitcoin, puede considerarse un tipo específico de dinero electrónico utilizado para transacciones en el ciberespacio [6].

El Banco Central Europeo establece similitudes y diferencias entre el dinero electrónico y el dinero virtual en cuanto a:

- Formato del dinero: ambos son digitales.
- Supervisión: el dinero electrónico sí lo tiene, mientras que el dinero virtual no.
- Tipos de riesgo: el dinero electrónico presenta principalmente riesgos operacionales mientras que en el dinero virtual los riesgos son legales, de crédito, de liquidez y operacionales.
- Estatus legal, el dinero electrónico está regulado, mientras que el dinero virtual no lo está.
- Unidad de cuenta, el dinero electrónico es dinero tradicional (euros, dólares, etc.) con estatus de moneda de curso legal, mientras que el dinero virtual es dinero criptográfico inventado (bitcoins) sin estatus de moneda de curso legal.
- Aceptación: el dinero electrónico es por compromiso del expendedor, mientras que el dinero virtual se utiliza dentro de una comunidad virtual específica.
- Expendedor: el dinero electrónico lo establece legalmente una institución de dinero electrónico (VISA o MasterCard), mientras que el dinero virtual surge a través de estructuras descentralizadas abiertas, de software libre, no financieras.
- Canjear fondos: El dinero electrónico está garantizado (por valor), mientras que el dinero virtual no está garantizado.
- Suministro: en el dinero electrónico está fijado, mientras que en el dinero virtual no lo está, depende de las decisiones del expendedor.

3.3. Aspectos teóricos y prácticos en relación con el dinero virtual

Bitcoin/BTC puede considerarse bajo tres prismas:

1) Moneda virtual o forma innovadora de establecer dinero digital a través de Internet. Con un sistema de pago de código abierto, basado en una red P2P abierta, descentralizado, que utiliza transacciones irrevocables y fundamentado en *Proof-of-Work*/PoW.
2) Un nuevo tipo de sistema de pago o medio de intercambio privado virtual basado en PoW, persona a persona, que no necesita ni de autoridad-banco central, ni de expedidor, ni de sistema de reserva que controle el suministro de BTCs, ni de terceras partes de confianza o TTP para posibilitar o supervisar las transacciones *online*.
3) Protocolo criptográfico para procesos financieros en nuevos modelos de *e-Business* y *e-Commerce*, con un crecimiento importante en el área de la criptografía financiera.

Tal y como funciona BTC [7], el envío es instantáneo y toda operación puede ser monitorizada en tiempo real.

Para hacer uso de Bitcoin necesitaremos descargarnos un cliente de software libre que contiene: pares de claves para cada dirección, transacciones desde o hacia tus direcciones, las preferencias del usuario, etc.
El cliente se podrá descargar en:

1) PCs/Macs (Bitcoinqt, Armony, Bitcoinspinner, etc.). Proporcionan control total de su monedero, y exigen hacer copias de seguridad y proteger el dinero.
2) Móviles (Coinbase, Bitcoin-wallet, etc.). Permiten tener bitcoins en el bolsillo, se puede pagar o intercambiar monedas escaneando un código óptico QR o utilizando tecnología RF NFC (a través de un *smartphone* o *smartcard*).
3) Monederos web. Permiten utilizar bitcoins en cualquier lugar. Se debe elegir un proveedor de servicios de monedero web para almacenar sus bitcoins. Para aceptar bitcoins se necesita poner la dirección BTC en el sitio web.

3.4. Implementación técnica

La compleja tecnología de Bitcoin *garantiza que se pueda usar como moneda* sin que cualquiera pueda crear dinero, asegurando que sólo puedes gastar tu dinero una vez, y controlando la introducción de nuevas monedas en el mercado.

Esta completa tecnología comienza por la definición técnica de dos términos: *Hash y firma digital*.

En el caso de Bitcoin, el algoritmo es SHA256. Definimos *hash* como un objeto (cadena de texto, número,… representado en bits) de *identificación única y constante,* como nuestra huella dactilar. Tiene la peculiaridad de que es una función “de una vía”, desde el objeto es muy fácil obtener su *hash* y si tienes el *hash* es extremadamente difícil obtener el objeto original del que proviene.

> “La compleja tecnología de Bitcoin *garantiza que se pueda usar como moneda* sin que cualquiera pueda crear dinero, asegurando que sólo puedes gastar tu dinero una vez, y controlando la introducción de nuevas monedas en el mercado”

Firma digital:. Bitcoin utiliza ECDSA, firma digital de curva elíptica. La firma digital certifica que eres tú quien ha creado, verificado, o aceptado ese objeto. Para ello se usan dos claves: pública y privada. La clave privada se “combina” con el mensaje a firmar y se obtiene la firma.

Para verificar la firma, se “combina” la clave pública del firmante con la firma, que debería dar como resultado el mensaje original.

3.4.1. Las bases: transacciones y bloques

Una transacción es el envío de bitcoins de un usuario a otro, que tiene entrada y salida: de donde viene el dinero y a dónde va. Su ID (identificación) es un *hash* combinado del ID de las entradas y del ID del destinatario (su clave pública).

Así se fija de forma inequívoca quién es el destinatario y de dónde han salido las monedas. Después, ese ID se firma con la clave privada del emisor de la transferencia, quedando certificado que el dinero lo ha transferido su propietario.

Las transferencias *se agrupan en bloques,* que además contienen: un sello de tiempo, un número de verificación y el ID del bloque anterior. De esta forma, se genera una cadena de bloques (*Blockchain*), con toda la historia de transferencias de bitcoins (ver **figura 2**).

Los bloques los generan los *mineros*, y antes de crearlos verifican la validez de todas las transferencias (evitar que un usuario transfiera más de una vez la misma divisa). Una transferencia que se ha quedado fuera de la cadena de bloques no es válida, y del mismo modo una transferencia dentro de la cadena se considera válida sin más operaciones.

Cuando un nodo genera un bloque, lo emite al resto de nodos. Éstos verifican que el bloque esté construido correctamente y que sus transferencias sean válidas. Si el bloque es correcto, empezarán a trabajar con ese nuevo bloque como el final de la cadena.

Puede ocurrir que haya *dos ramas de la cadena*: un nodo ha emitido un bloque y en el mismo momento otro nodo ha emitido otro bloque distinto. En este caso, se conservan las dos ramas hasta que una de ellas sea más larga: ésta será la que se mantenga, y la otra se desechará.

Lo indicado funcionaría si todos los nodos que están creando bloques fuesen honestos. Pero sabemos que un nodo malicioso podría crear un bloque con una transferencia inválida (con dinero gastado dos veces) y después generar más bloques de forma masiva.

Al generar bloques válidos rápidamente, la transferencia inválida queda enterrada en la cadena. Cuando el resto de los nodos reciban esta cadena, que será la más larga de todo el entorno, verificarán como mucho los últimos bloques, darán la rama como válida y *esa transacción inválida pasará desapercibida*.

Es por esto que se hace necesario desarrollar un método que evite la generación de bloques indiscriminadamente y que obligue a los nodos a invertir tiempo en generar el bloque.

Este método se llama *proof-of-work* y consiste en encontrar el número de verificación, *nonce,* de tal forma que el *hash* del bloque sea menor que un determinado valor objetivo. El algoritmo búsqueda de ese número es prueba y error: empezamos en cero y calculamos el *hash*. Si es menor que el objetivo, perfecto, lo hemos encontrado. Si no, aumentamos en uno el *nonce* y volvemos a verificar. La probabilidad de encontrar un *nonce* válido es de $1/(2*10^{16})$. El valor objetivo se elige de tal forma que se tarde unos 10 minutos en generar un bloque. De esta forma, no pueden generar bloques rápidamente para ocultar transacciones.

El siguiente obstáculo es *el espacio de almacenamiento de toda la historia de transacciones:* guardar toda la cadena de bloques sin desperdiciar disco.

Para verificar una transacción, tenemos que comprobar que las entradas de monedas ya han sido verificadas. Normalmente, los clientes verifican varias transacciones atrás y consideran que el resto son válidas.

Es decir, se necesita una forma de guardar las transacciones y comprobar que están en los bloques: cada bloque contiene el *hash* combinado de las transferencias. Verificarlo es tan sencillo como coger el *hash* de la transferencia a verificar, combinarla con el resto de *hashes* de las transferencias del bloque y comprobar que tenemos la misma salida.

El problema surge cuando mantenemos muchas transferencias que no nos sirven para nada. Supongamos que, en un bloque, se ha gastado y verificado el dinero de todas las transferencias menos una. No vamos a necesitar el resto para verificar nada porque no vamos a llegar a tanta profundidad en la cadena. Sin embargo, tenemos que mante-

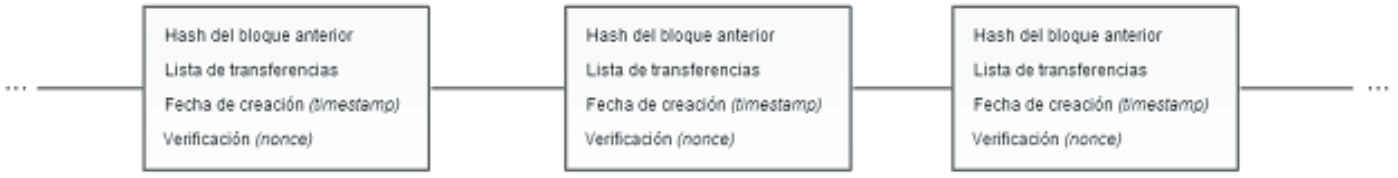

Figura 2. Cadena de bloques. Fuente: Wikimedia Commons.

> “ Cuando un nodo genera un bloque, lo emite al resto de nodos. Éstos verifican que el bloque esté construido correctamente y que sus transferencias sean válidas. Si el bloque es correcto, empezarán a trabajar con ese nuevo bloque como el final de la cadena ”

nerlas para que al verificar esa transferencia que no ha sido gastada, el *hash* siga siendo el mismo.

La solución pasa por usar un árbol de *hashes* o un árbol Merkle. Los *hashes* de las transferencias se van combinando dos a dos en forma de árbol binario. Así, cuando no necesitamos dos hermanos (comparten el mismo padre), podemos borrarlos y quedarnos con el nodo padre sin perder la posibilidad de verificar el resto de nodos del árbol. Esto reduce considerablemente el espacio necesario y permite quedarnos sólo con las transferencias más recientes y olvidarnos del resto.

En la **figura 3** podemos ver el funcionamiento de un árbol *hash*. Los recuadros verdes son los *hashes* que generamos, y los grises los que guardamos. Los sombreados no los usamos, así que no hace falta guardarlos.

3.4.2. Generación/minado de bitcoins

BTC es una moneda sin una entidad central que controle la inflación ni la generación de más dinero en el mercado. Será nuevamente la técnica la encargada de controlar la generación de monedas (con equipos específicos para ese propósito y varios procesadores gráficos o GPUs).

Cuando un nodo crea un bloque, además de todas las transferencias que haya verificado incluye otra más: una transferencia sin entradas. Cada vez que se verifica un bloque, se introducen nuevas monedas en el sistema. La tasa a la que se liberan nuevos BTC’s está controlada de tal forma que cada 4 años se reduce en el 50%. Así, está calculado que el número de BTC’s nunca pasará de los 21 millones.

Esto es un incentivo para los nodos de la red: cuantos más bloques verifiquen, más BTC’s ganan. Este enfoque hace más rentable ser un nodo honesto que uno malicioso.

Finalmente permite controlar el aspecto de “escasez” como requisito para considerar una divisa como BTC’s.

3.5. Ventajas e inconvenientes de la utilización de bitcoins

El principal reclamo de Bitcoin es su absoluta independencia con respecto al Estado o institución financiera. Al no estar sujeto a legislaciones nacionales, el uso de esta moneda como fondo para tus ahorros puede ser conveniente para evitar corralitos o devaluación de la moneda.

Las principales ventajas son las siguientes: [8]:

Permite el intercambio libre de dinero a nivel mundial simplemente con un equipo conectado a Internet.

- La identidad del usuario puede permanecer en todo momento en el anonimato. La dirección se genera aleatoriamente y no está ligada a ningún dato personal.
- Las transacciones son completamente públicas. Disponemos de webs donde puedes ver los movimientos en tiempo real o hacer seguimiento de una cuenta concreta. Por ejemplo: <https://www.biteasy.com>.
- Debido a que los pagos tienen un carácter irreversible, la reputación de los usuarios es algo básico para generar confianza a la hora de operar.
- Seguridad: En una transacción entre A y B, el cifrado con la clave pública asegura que B es el destinatario de la misma, y la firma con la clave privada, asegura que A es el emisor. El resto de los nodos de la red validan las firmas criptográficas y el valor de la transacción antes de aceptarla.
- Crecimiento sostenido. La oferta de bitcoins se limitará en el tiempo hasta un total de 21 millones. En 2033 se habrán generado casi todos los que van a estar en circulación (ver **figura 4**). Este límite no puede ser superado y el ritmo de creación no puede ser incrementado.
- Moneda descentralizada. No hay una autoridad central que la controle, es decir, ninguna institución o estado puede generar BTCs. Algo que sí hacen los bancos centrales con sus monedas, provocando procesos inflacionistas o pérdidas de valor.
- Los costes por transacción son casi nulos.
- Se pueden comprar o vender BTC en mercados de intercambio de divisas, basadas en la reputación de cada usuario.

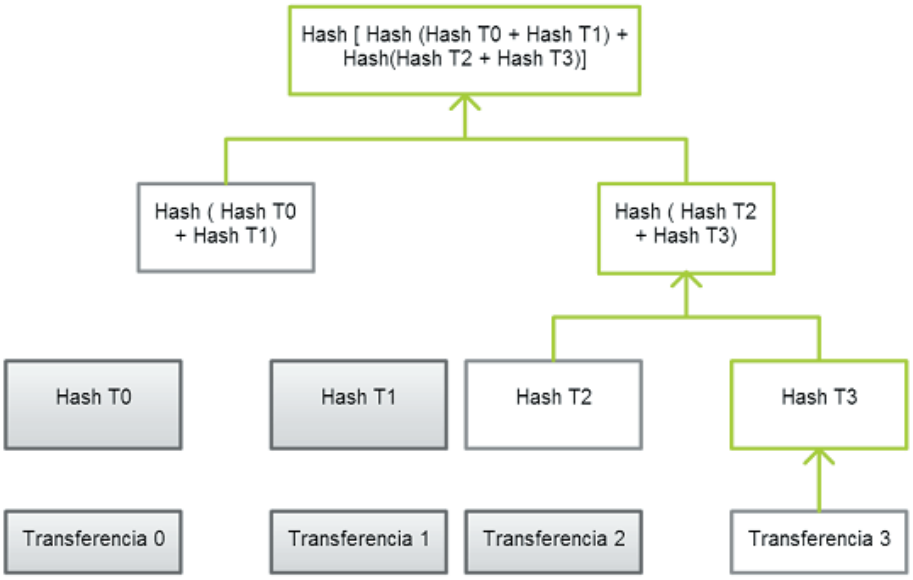

Figura 3. Árbol hash. Fuente: Wikimedia Commons.

> “La Autoridad de Servicios Financieros de Japón planea designar a la divisa virtual Bitcoin como una moneda corriente, con el fin de reforzar la protección de sus usuarios y facilitar su uso”

Los principales inconvenientes son los siguientes [9]:

- Financiación de actividades ilícitas y/o blanqueo de capitales. Debido al carácter descentralizado, la transmisión del valor monetario se produce directamente entre el ordenante y el beneficiario de la operación. Ésto dificulta la identificación y alerta temprana en actividades ilícitas.
- Efectos reputacionales negativos. El empleo generalizado de sistemas de pago electrónicos por parte de redes de crimen organizado deteriora la confianza del público.
- Tendencias oligopolísticas en la creación de la moneda virtual. La asignación asimétrica de unos recursos monetarios favorece a aquellos con mejores conocimientos técnicos y en recursos informáticos, frente a los mecanismos de mercado.
- Posibles transacciones fraudulentas. Desajustes en el ritmo de actualización de software de los distintos nodos de la red, han ocasionado puntualmente la aceptación de transacciones duplicadas. A posteriori rechazadas en otros puntos de validación.
- Impacto sobre la estabilidad de los precios. El uso de BTC’s podría llegar a afectar a la demanda de los pasivos de un banco central, impactando en el nivel general de precios de la economía y la efectividad de las medidas de política monetaria.
- Impacto sobre la estabilidad financiera. Las plataformas privadas de intercambio de BTC’s por monedas de curso legal, están marcadas por la elevada volatilidad de las cotizaciones debido a movimientos especulativos.
- No dispone de derecho de reembolso. Debido a su configuración, a modo de cadena de transacciones, el traspaso de bitcoins entre usuarios es firme e irreversible. Ésto impide poder disfrutar de un mecanismo de protección equivalente.

3.6. El futuro de Bitcoin

La Autoridad de Servicios Financieros de Japón ha promovido para 2016 [10] un nuevo marco legal para las entidades que ofrezcan servicios relacionados con divisas virtuales. Éstas deberán someterse a la supervisión de las autoridades japonesas y así prevenir nuevos casos como el escándalo en 2014 de Mt.Gox[3], a raíz del cual, Japón aprobó una normativa pionera para tipificar esta criptomoneda[4] como una mercancía y no como una divisa.

La Autoridad de Servicios Financieros planea designar a la divisa virtual Bitcoin como una moneda corriente, con el fin de reforzar la protección de sus usuarios y facilitar su uso. El cambio permitirá que el Bitcoin sea empleado como una forma de pago equivalente a otras unidades monetarias, además de que las divisas virtuales sean intercambiadas por monedas de curso legal sin control de ningún banco o autoridad monetaria.

El objetivo es responder a la creciente demanda de estas divisas, garantizar la protección de sus usuarios y facilitar el desarrollo del sector tecnológico, en especial las transacciones comerciales y financieras a través de Internet.

Nuevamente, Japón se sitúa a la vanguardia de la regulación de las divisas digitales, pues la nueva normativa será aprobada por la Dieta[5] durante la actual legislatura, según Nikkei.

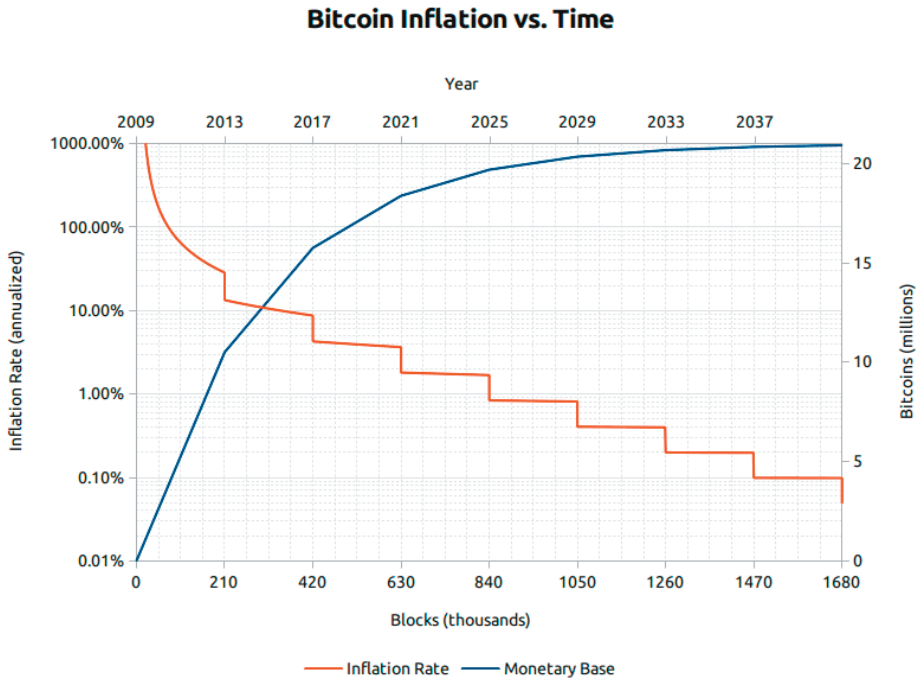

Figura 4. Gráfico sobre los bitcoins generados en el tiempo Fuente: Wikimedia Commons.

4. Otras monedas virtuales

El equipo jamaiquino [11] clasificado para las Olimpíadas de Invierno de Rusia en Sochi 2014 recaudó $25.000 en la moneda virtual Dogecoin en apenas unas pocas horas, con la finalidad de recaudar fondos para participar en el evento.

Conocer cuántos tipos de monedas virtuales existen en la actualidad es complicado. El portal web Coinmarketcap[6] registra la capitalización bursátil de una lista de 78 divisas en tiempo real. Entre ellas destacamos:

- **Litecoin**: En circulación desde el 2011. Ha llegado a cotizarse algunos días en 0,05$ y 48$. Utiliza el mismo sistema de Bitcoin, si bien la confirmación de las transacciones se produce con mayor rapidez (<3 minutos) y el proceso de *mining* puede realizarse con equipos de menor capacidad.
- **Peercoin**: Disponible desde 2012. Seguridad y eficiencia energética son parte de la oferta de esta divisa. Se denomina

"ecológica", pues la verificación de las transacciones por el método "*proof-of-stake*" (operaciones para probar que son los legítimos propietarios de la moneda) es más sencilla que la de Bitcoin "*proof-of-work*", que con algoritmos complejos hacen que la computadora trabaje excesivamente. Además, elimina el proceso colectivo de *mining*, identificado como un fallo en Bitcoin ya que su propósito es obtener ganancias, lo que va en contra de sus "principios democráticos".

- **Quark**: Creado en 2013, su buen desempeño llevó a esta divisa a aumentar su valor en 500%, en solo una semana. Su cualidad principal es la seguridad. Utiliza seis funciones *hash* diferentes para proteger la información frente a una sola que utiliza Bitcoin. Las transacciones son mucho más rápidas y los envíos de dinero dentro de la red Quark son gratuitos a diferencia de Bitcoin.

Referencias

[1] Taringa! *Deep Web (Niveles, y que contiene cada uno)*. <http://www.taringa.net/posts/offtopic/16047905/Deep-Web-Niveles-y-que-contiene-cada-uno.html>. Último acceso: 30 de marzo de 2017.

[2] Platzi. *Silk Road, su historia y colapso*. <https://youtu.be/bHmZmpSdSjQ>.

Último acceso: 30 de marzo de 2017.

[3] Wikipedia. *Silk Road*. <https://es.wikipedia.org/wiki/Silk_Road>. Último acceso: 30 de marzo de 2017.

[4] Banco de España. *Eurosistema. Entidades Dinero Electrónico*. <http://www.bde.es/bde/es/secciones/normativas/Regulacion_de_En/Estatal/Entidades__de_d_be3472d6c1fd821.html>. Último acceso: 30 de marzo de 2017.

[5] Andbank. *¿Qué son las entidades de dinero electrónico?* www.andbank.es/observatoriodelinversor/que-son-las-entidades-de-dinero-electronico/>. Último acceso: 30 de marzo de 2017.

[6] Javier Areitio Bertolín. Análisis de Bitcoin: Sistema P2P de pago digital descentralizado con moneda criptográfica virtual. *Novática nº222, marzo-abril 2013*, pp. 34-41. <http://www2.ati.es/novatica/2013/222/nv222sum.html>.

Último acceso: 30 de marzo de 2017.

[7] Finanzas para todos. *Bitcoin: origen, funcionalidades y riesgos de la moneda virtual.* <http://www.finanzasparatodos.es/es/secciones/actualidad/bitcoin.html>. Último acceso: 30 de marzo de 2017.

[8] Javier Hernando. *¿Qué es Bitcoin y por qué se habla tanto de ello últimamente?* United Explanations, Economía, 19/02/2013. Último acceso: 30 de marzo de 2017. <http://www.unitedexplanations.org/2013/02/19/que-es-bitcoin-y-por-que-se-habla-tanto-de-ello-ultimamente/>. Último acceso: 30 de marzo de 2017.

[9] Sergio Gorjón. *Divisas o Monedas Virtual: El caso de Bitcoin.* Banco de España EuroSistema, enero 2014. <http://www.bde.es/f/webpcb/RCL/canales/home/menu-botonera/noticias/2014/Enero/pdf/Nota_informativa_Bitcoin_enero2014.pdf>. Último acceso: 30 de marzo de 2017.

[10] Agencia EFE. *Japón considerará al Bitcoin como divisa para fomentar su uso y su seguridad.* EFE Tokio, 24 febrero 2016. <http://www.efe.com/efe/america/economia/japon-considerara-al-bitcoin-como-divisa-para-fomentar-su-uso-y-seguridad/20000011-2848609>. Último acceso: 30 de marzo de 2017.

[11] BBC. *No solo Bitcoin: cuáles son las otras monedas digitales*. 22 enero 2014. <http://www.bbc.com/mundo/noticias/2014/01/140122_tecnologia_monedas_digitales>. Último acceso: 30 de marzo de 2017.

[12] El Mundo. *La compañía de intercambio de bitcoins Mt.Gox se declara en quiebra en Japón*. 28 febrero 2014. <http://www.elmundo.es/tecnologia/2014/02/28/53105fd3268e3eaf138b456d.html>. Último acceso: 30 de marzo de 2017.

Notas

[1] *Clearers*.

[2] *Peer-to-Peer*.

[3] La empresa Bitcoin Mt Gox se lanzó en marzo de 2011 por Karpeles y fue la compañía más grande en el mercado de Bitcoin en su momento, llegando a manejar alrededor del 70% de las transacciones en todo el mundo. En febrero de 2014, se declaró en quiebra y reveló la desaparición de una enorme cantidad de esta moneda virtual [12].

[4] Forma de pago que tiene en la encriptación de datos el respaldo de su valor material.

[5] Parlamento nipón.

[6] <http://coinmarketcap.com>.

A continuación presentamos las habituales referencias que desde 1999 nos ofrecen los coordinadores de las Secciones Técnicas de nuestra revista.

Sección Técnica: *"Acceso y recuperación de información"* (José María Gómez Hidalgo, Enrique Puertas Sanz)

Tema: *Noticia: Cuadrante Mágico de Gartner para Plataformas de Análisis de Datos*

La firma de consultoría tecnológica Gartner ha publicado recientemente el llamado Cuadrante Mágico (Magic Quadrant) de plataformas de Análisis de Datos para el 2017. El informe ha evaluado un total de 16 empresas que ofrecen herramientas de análisis y minería de datos utilizando 15 criterios. Como consecuencia de esta evaluación, se han colocado a cada una de las 16 empresas en uno de los 4 posibles cuadrantes, basados en la visión del negocio y su capacidad de ejecución. Los cuadrantes en los que se pueden englobar las empresas son "líderes", "visionarios", "nichos" y "contendientes".

Hay que mencionar que este estudio no ha incluido lenguajes y plataformas de código abierto como Python o R que, aunque juegan un papel muy importante en el dominio de Data Science, la metodología empleada por Gartner no las incluye, por lo que este informe evalúa sólo a los proveedores de soluciones comerciales.

Analizando el estudio, 4 empresas aparecen como líderes del mercado, dominando el panorama de herramientas de Análisis de Datos: IBM, SAS, KNIME y Rapidminer. Ésta última es la que obtiene un mayor crecimiento en cuanto a su posición en el mercado.

Además, en este estudio del 2017 aparecen 5 nuevas empresas que no aparecían en el estudio del 2016: MathWorks, H2O.ai, Dataiku, Domino Data Lab, y Teradata.

Másinformaciónen:<https://www.gartner.com/doc/3606026/magic-quadrant-data-science-platforms>.

Tema: *Noticia: Un investigador consigue romper el sistema reCAPTCHA de Google usando APIs de reconocimiento de voz*

ReCAPTCHA es un servicio gratuito de Google que protege los sitio webs del *spam* y del abuso por parte de *bots*. Este sistema, concebido para distinguir humanos de programas informáticos, es usado por millones de sitios web en internet.

Un investigador ha encontrado una vulnerabilidad en la última versión de *reCAPTCHA* que permitiría que *spambots* se salten los sistemas *reCAPTCHA* utilizados en millones de sitios web de internet, y ha desarrollado, como prueba de concepto, un *script* para ilustrar el funcionamiento.

El *script* funciona para la versión más reciente de *reCAPTCHA* (versión 2), que utiliza también desafíos de audio como comprobación alternativa si hace clic en un botón situado en la parte inferior de la ventana emergente *reCAPTCHA.* El agujero que permite explotar esta debilidad se basa en el diseño que ha hecho Google de *reCAPTCHA*, y que permite a los usuarios de navegadores antiguos la opción de descargar el audio del *challenge*. Esto permite descargar los audios al ordenador local y, usando la *API* de reconocimiento de voz propia de Google, obtener la transcripción correcta del audio, la cual puede ser enviada de nuevo al sitio web para resolver el *captcha*.

Más información en: <https://github.com/eastee/rebreakcaptcha>.

Tema: *Demostración: Cómo construir un Chatbot con Watson*

La Inteligencia Artificial está de plena actualidad. Quizá las dos tecnologías que más han contribuido a ello son el *Deep Learning* y los *Chatbots*. Y de éstas, la segunda es especialmente interesante porque su visibilidad es directa para los usuarios finales, y porque su explosión se ha producido como consecuencia de la victoria del sistema *Watson* de IBM en "*Jeopardy*!", uno de los concursos televisivos más importantes en EE.UU.

Cada vez más, las empresas están descubriendo el potencial de los *Chatbots*. Estos programas son capaces de interactuar con los usuarios a través de un diálogo en lenguaje natural, y proporcionar ayuda automática en entornos como las compras online o los servicios de envío de noticias. Por ejemplo, en el primer caso pueden automatizar tareas de atención al cliente que antes debían realizar seres humanos de una manera mucho más costosa desde el punto de vista económico.

Pero no olvidemos que el primer *Chatbot* claramente reconocible, el programa Eliza desarrollado por Joseph Weizenbaum y que simula la conversación con un psiquiatra, data de 1966, y sólo ahora se está produciendo la popularización de este tipo de sistemas. Ello se debe en parte a que se ha simplificado notablemente su desarrollo gracias a la existencia de *APIs* como la del propio Watson, disponibles en la nube (*Cloud*).

En la referencia de IBM que mencionamos aquí se explica precisamente como realizar la implementación rápida de un *Chatbot* en inglés capaz de dar soporte a los clientes de una tienda online para la devolución de los productos que han adquirido en la misma. Utilizando las capacidades de Watson o de otras plataformas en inglés y en otros idiomas, es posible desarrollar *Chatbot* para gran cantidad de tareas con un esfuerzo relativamente pequeño.

Más información en: New York Times: Computer Wins on 'Jeopardy!': Trivial, It's Not <http://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html>.

IBM: Build a chatbot in ten minutes with Watson. <https://www.ibm.com/blogs/watson/2016/12/build-chat-bot/ >.

Tema: *Recurso: Conexiones gráficas entre entidades textuales con XPack Graph de Elasticsearch*

En referencias precedentes, hemos mencionado en varias ocasiones dos de las plataformas de búsqueda más populares hoy en día, *SOLR* de Lucidworks y *Elastic Search* de Elastic. Ambas están basadas en una de las tecnologías de búsqueda *opensource* denominada *Lucene*, diseñada para proporcionar altos niveles de rendimiento en entornos distribuidos tipo *Big Data*.

Una de las características que hace más interesantes estas plataformas es el conjunto de extensiones y herramientas periféricas que les acompañan, incluyendo herramientas de visualización como *Banana* en *SOLR* y *Kibana* en *Elastic Seach*, y otras más específicas del análisis de datos como el paquete *Graph* incluido en la extensión *XPack* de Elastic para Kibana.

El paquete *Graph* permite el desarrollo de visualizaciones operativas en forma de grafo sobre los conceptos que se han almacenado en los índices de Elastic, y la explotación de sus relaciones para ofrecer funcionalidades prácticas para los usuarios finales. Por ejemplo, es posible almacenar transacciones electrónicas de una tienda online en Elastic, y visualizar qué productos se compran juntos con más

frecuencia para ofrecer a los usuarios finales recomendaciones de compra personalizadas en base a sus compras precedentes y a lo que adquieren otros clientes. Como además se puede realizar este análisis de forma gráfica, podemos por ejemplo descubrir relaciones imprevistas entre productos de manera fácil y efectiva.

Más información en: Lucidworks <https://lucidworks.com/>. Elastic <https://www.elastic.co/>. XPack Graph de Elasticsearch <https://www.elastic.co/guide/en/x-pack/current/xpack-graph.html>.

Sección Técnica: *"Administración Pública electrónica"* (Francisco López Crespo, Sebastià Justicia Pérez)

Tema: *Congreso Nacional de Innovación y Servicios Públicos 2017 (CNIS)*

Este mes de febrero se celebró una nueva edición del congreso. Sin duda la administración pública tiene el reto de adecuarse al contexto socio productivo imperante en nuestra sociedad que no es otro que la tecnificación digital de los procesos administrativos y competencias públicas. Llevamos años donde esta directriz ha sido asumida en mayor o menor grado por nuestras administraciones y todo cabe decirlo, con éxito dispar.

Un acicate auto impuesto para lograr este objetivo han sido las leyes de procedimiento administrativo y de régimen jurídico de las administraciones 39/2015 y 40/2015. Estos desarrollos legislativos pretenden ser impulsores de la digitalización total del transaccionado público. Se residualiza progresivamente el modo operativo anterior analógico (presencial, que se mantiene por cuestiones de seguridad jurídica, para en un plazo de tres o cuatro años poder hacer posible una declaración de total implementación del procedimiento electrónico).

En este congreso CNIS <www.cnis.es> podemos ver excelentes ponencias que versan sobre los diferentes aspectos tecnológicos y organizativos tendentes a la total asunción digital. Recomendamos el visionado de algunas de ellas, para poder tomar el pulso de esta iniciativa pública con el necesario partenariado empresarial en muchos casos.

Una cita ineludible son los premios sectoriales. Al margen de los magníficos proyectos presentados podemos inferir la máxima de "dime qué premias y te diré qué promueves". Se podría objetar que quizás falten algunos ámbitos en los que asimismo poder haber instituido galardones. Con todo, creemos que dentro de las limitaciones, dan una muy buena radiografía de por dónde transita la transformación del modo operativo público y dónde se pone el énfasis. Los premios **CNIS 2017 a las Administraciones Públicas son los siguientes:**

1. Premio proyecto consolidado en **Interoperabilidad**
2. Premio proyecto consolidado en **Seguridad**
3. Premio mejor **Plan de Innovación**
4. Premio mejor **Acción Formativa Innovadora**
5. Premio mejor **Innovación Social**
6. Premio mejor proyecto consolidado de **Transformación Digital/Administración Electrónica**
7. Premio mejor proyecto de **Smart Cities**
8. Premio mejor proyecto en **Gobierno Abierto: Transparencia, Participación Ciudadana y Colaboración**
9. Premio mejor **Gestión innovadora de Redes Sociales**
10. Premio mejor **Estrategia de Servicios en la Nube**
11. Premio mejor **Estrategia móvil/App pública**
12. Premio **Proyecto europeo más innovador**
13. Premio mejor **Iniciativa de Compra Pública Innovadora**
14. Premio mejor proyecto de **Colaboración Público Privada** (Premio a la administración y a la empresa).

Creemos que podemos sentirnos satisfechos y con un cierto grado de confiabilidad en los rectores públicos, ya que lo público está no sólo acompañando el paradigma informacional que rige nuestra sociedad, sino que podríamos atrevernos a decir que, de forma desacomplejada, lo lidera, si no en todos, sí en muchos ámbitos de desarrollo. Sitúa así en el foco inversor y suministro de recursos, los elementos susceptibles de provisión de valor público, ya sea en su vertiente de prestación ciudadana ya sea en su rol de promotor del fomento de actividades económicas.

Hay una parte estructural y de cumplimiento normativo. Los esquemas nacionales de seguridad e inter operabilidad ENS y ENI respectivamente, han sido hilos argumentales desde 2010 para conferir a los sistemas de información públicos, estándares de confiabilidad y de intercambio asegurado protegiendo la inversión y promoviendo de esta manera los desarrollos informáticos. Se sigue potenciando los modelos de nube computacional en cuanto a economías de escala que generan los canales de comunicación cada vez más dotados de ancho de banda.

Se promueve asimismo la movilidad que asegure la ubicuidad en la relación ciudadanía y administración. Caso específico es el lugar de trabajo digital, alternativamente conocido como tele trabajo cuyos pilotos operativos comienzan a funcionar en algunas, todavía pocas, administraciones. Otro ámbito infra estructural es el de la licitación pública que agilice y dote de transparencia al hecho contractual tan en el foco social por las lamentables noticias de corrupción ocurridas en estos últimos años y que salpica, día sí día también, la crónica judicial de los informativos. Esperemos que la transición digital contribuya a erradicar esta lamentable lacra.

Vemos asimismo un especial hincapié en la innovación, premiándose diferentes perspectivas de la misma. Se pretende en esta revolución tecnológica que vivimos, auspiciar iniciativas de provisión de valor en la tecnificación digital, más allá del simple traslado a una automatización informatizada de los procesos públicos.

Por último, cabe destacar tres focos de negocio público de incidencia particularizada. La promoción del hecho participativo a partir de las posibilidades del voto electrónico y los canales virtuales, el despliegue exponencial de las ciudades inteligentes como modelos de gestión avanzada de nuestras urbes y los foros públicos virtuales concretados en las llamadas redes sociales que han venido a identificarse como el pulso social y político de nuestra era.

Tema: *La Generalitat Valenciana celebra el V Congreso de Software Libre*

La Generalitat Valenciana celebrará el V Congreso de Software Libre de la Comunitat Valenciana los días 5 y 6 de mayo, en la Universitat Jaume I de Castellón, con la participación de expertos nacionales e internacionales**.** El encuentro persigue promover el uso de las Tecnologías de la Información y la Comunicación a través del software libre y sensibilizar sobre sus ventajas. Además, servirá para conmemorar el décimo aniversario de LliureX, la distribución libre valenciana desarrollada por la Generalitat e implantada en los centros educativos.

El objetivo es ofrecer un foro de encuentro para la presentación de soluciones de código abierto y el intercambio de experiencias sobre su uso, no sólo en los centros educativos sino, también, en otros

ámbitos, para recoger las inquietudes y retos planteados por los distintos usuarios.

En 2005 la Generalitat comenzó a implantar la primera versión de LliureX en los centros escolares y, a día de hoy, está instalado en más de 120.000 ordenadores del sistema educativo valenciano. LliureX es una distribución GNU/Linux de descarga gratuita lliurex.net, disponible en valenciano y castellano, que cada año cuenta con una nueva versión mejorada y múltiples novedades. Además, su uso ha supuesto un ahorro a la administración de más de 36 millones de euros.

La versión actual ofrece un sistema operativo y las últimas versiones de más de 400 aplicaciones y recursos, como la suite ofimática LibreOffice 4.2 y el traductor y diccionario valenciano Salt, además de aplicaciones para la edición audiovisual y de páginas web, la enseñanza de idiomas multimedia, etc.

Actualmente, esta distribución se encuentra implantada en todos los centros educativos públicos valencianos y la UJI. Por otra parte, en 2014 se comenzó a implantar esta solución en el resto de departamentos de la Administración valenciana, para el uso de los empleados públicos, ya que cuenta con distintas variantes como la de Pyme, para empresas y entornos laborales.

Para el congreso, se ha puesto en marcha una página web (congreso.lliurex.net) en la que se irá informando de todas las novedades y en la que, además, los interesados pueden proponer a la organización aquellas ponencias que consideren que serían de interés para los asistentes.

Sección Técnica: *"Derecho y Tecnología"* (Elena Davara Fernández de Marcos)

Tema: *El TS admite como prueba para el despido el uso de las imágenes captadas por las cámaras de videovigilancia*

Se centra el debate sobre si en un proceso judicial por despido disciplinario, podía ser admitido como medio probatorio el video captado por las cámaras de vigilancia, y que servirían a la empresa para justificar el despido; es por ello que mediante la sentencia del Tribunal Supremo (TS) No. 77/2017 de 31 de enero de 2017, donde ha sido ponente el magistrado José Manuel López García, se acepta que las grabaciones deben ser admitidas como medio de prueba en el proceso judicial**.**

Tanto el Juzgado de lo social nº 15 de Barcelona como el Tribunal Superior de Justicia de Cataluña habían declarado el despido improcedente y no se admitieron las grabaciones como medios de prueba, por considerar que se violaba la protección de datos del trabajador, aun cuando se había informado de manera previa a los empleados sobre la instalación de las videocámaras, pues no se especificó que la finalidad era para vigilar el efectivo cumplimiento de sus funciones laborales. Por su parte, el TS, en su sentencia, establece que no se requiere el consentimiento expreso de los trabajadores para el uso de las imágenes que se obtienen de las cámaras instaladas por seguridad y/o para el control laboral, ya que el consentimiento de los trabajadores se debe entender implícito, y que solamente en el caso de que la instalación de esas cámaras busquen un objetivo distinto que al de seguridad y vigilancia laboral, se requerirá el consentimiento expreso de los trabajadores**.**

Más información en: <http://noticias.juridicas.com/actualidad/jurisprudencia/11728-el-ts-admite-como-prueba-para-el-despido-el-uso-de-las-imagenes-captadas-por-las-camaras-de-videovigilancia/#.WMAmSTVoHss.twitter>.

Tema: *El Tribunal de Justicia considera que no existe derecho al olvido en relación con los datos personales recogidos en el registro de sociedades*

El Tribunal de Justicia de la Unión Europea (TJUE) se ha pronunciado con respecto a los datos personales recogidos en el registro de sociedades, debido a las cuestiones prejudiciales planteadas por el Tribunal de Casación de Italia, cuando éste estaba conociendo la demanda que interpuso el señor Don Salvatore Manni, contra la Cámara de Comercio de Lecce, debido a que al demandante se le había adjudicado, en su calidad de administrador único de una sociedad, un contrato de construcción de un complejo turístico en Italia, pero como ya constaba en el registro de sociedades que en otra sociedad, en la que igualmente había sido administrador único en el año 1992, y que había sido declarada en concurso de acreedores y liquidada en el 2005, por lo que debido a esta información no lograba el desarrollo deseado (esto es, suficientes ventas) de los inmuebles de dicho complejo**.**

Al respecto, el TJUE respondió que los datos personales que se encuentran en el registro de sociedades no son desproporcionados con los derechos fundamentales reconocidos en la Carta de Derechos Fundamentales de la Unión, de vida privada y de protección de datos; ya que estos datos de carácter personal son limitados**.**

No obstante, ello no excluye que en situaciones concretas, de manera excepcional, los datos personales puedan limitarse, aunque reitera que en el caso del Sr. Manni, no se encuentra justificada su omisión, ya que los interesados o potenciales compradores, tienen el derecho de acceder legítimamente a la información del registro.

Más información en: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2017-03/cp170027es.pdf?platform=hootsuite>.

Tema: *Twitter presenta las actualizaciones que refuerzan su red social para hacerla segura y combatir el acoso*

La red social Twitter presentó una actualización de su plataforma, con la que busca mejorar las medidas de seguridad de potenciales amenazas, usos y contenidos abusivos, así como herramientas más sencillas para denunciar *tuits* abusivos. Todo esto para dar cumplimiento a los principios de la compañía**.**

Dentro de estas medidas, todo usuario que haga uso no debido de sus cuentas, podrá ser limitado o suspendido de su servicio por un tiempo, trayendo consigo esta actualización, la gran novedad que inclusive, la red social, podrá identificar cuentas con comportamientos abusivos, sin que éstos hayan sido denunciados por otro usuario.

A los usuarios se les otorga diversas opciones para activar y desactivar notificaciones, basadas en un filtro bajo diversos criterios con relación a otras cuentas, como aquéllas que no tienen foto de perfil, correo electrónico o número de teléfono no verificados.

Más información en: <http://www.europapress.es/portaltic/socialmedia/noticia-twitter-presenta-actualizaciones-refuerzan-red-social-hacerla-segura-combatir-acoso-20170301150239.html>.

Tema: *La AEPD publica la guía "Protección de datos y administración de fincas" para facilitar a este sector el cumplimiento de la normativa*

La Agencia Española de Protección de Datos ha hecho pública una guía de protección de datos y administración de fincas. Este tema era una de las cuestiones que más se consultaba a la AEPD.

Dentro de esta guía se incluyen, para su mejor entendimiento, conceptos básicos como puede ser la inscripción de ficheros y el futuro registro de actividades, así como de qué manera organizar las relaciones entre propietarios, comunidad y administradores. De igual manera, se incluye lo necesario para saber tratar la información de propietarios con pagos pendientes, acceso a la documentación de la comunidad y lo que se requiere para instalación de cámaras de videovigilancia.

Por otra parte, y debido a que el Reglamento General de Protección de Datos, será aplicable a partir del 25 de mayo de 2018, esa guía ya recoge los aspectos pertinentes y adaptaciones necesarias para el cumplimiento del mismo**.**

Más información en: <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_02_23-ides-idphp.php>.

Sección Técnica: *"Enseñanza Universitaria de Informática"* (J. Ángel Velázquez Iturbide, Cristóbal Pareja Flores)

Tema: *Libro*

Joel Grus. *Data Science from Scratch*. O'Reilly, 2015.

Es inútil ya decir que vivimos en un mundo poblado por datos. Datos abiertos, datos de redes sociales, los datos de los sensores en las vías públicas, los que proporcionan nuestros móviles según sea nuestra posición, *big data*, sistemas de recomendación, minería de datos, análisis de datos, inteligencia de negocios, etc. Los datos están ahí, y todo el mundo quiere poder extraer de ellos no ya información sino valor neto, para las decisiones empresariales, para...

El libro que traemos aquí hoy es la mejor introducción que conocemos a todos estos temas, partiendo de cero, o casi, ya que únicamente se salta el lenguaje vehicular que adopta (*Python*), del que hace una introducción suficiente para seguir leyendo, aunque insuficiente para el dominio con maestría de un lenguaje de programación.

Estamos usando este libro como complemento de una asignatura que no vamos a describir aquí, pero que admite plantear trabajos o proyectos (excursiones les estamos llamando nosotros) a mundos diversos como son los que recogía en el primer párrafo de esta breve reseña.

He aquí el contenido: *Introduction. A crash course in Python. Visualizing data. Linear Algebra. Statistics. Probability. Hypothesis and inference. Gradient descent. Getting data. Working with data. Machine learning. K-nearest neighbors. Naive Bayes. Simple linear regression. Multiple regression. Logistic regression. Decision trees. Neural Networks. Clustering. Natural language processing. Network analysis. Recommender systems. Database and SQL. MapReduce. Go forth and do data science*.

Nos parece un libro recomendable porque es realmente ameno, porque cada uno de sus cortos capítulos contiene el kit necesario para preparar aplicaciones que funcionan, con la teoría mínima necesaria y las referencias para profundizar más, y realmente al leer estos capítulos apetece profundizar más en ellas. Confesamos nuestro entusiasmo con todos estos temas, y este libro ha jugado su papel en poner el atractivo de cada una de estas técnicas al alcance de los estudiantes (y de los ya iniciados), de una manera divertida pero seria y eficaz.

Sólo nos asusta un asunto: con este material, si nuestros estudiantes no disfrutan y aprenden un montón, ya no tenemos excusa alguna.

Sección Técnica: *"Gestión del Conocimiento"* (Joan Baiget Solé)

Tema: *Publicación*

A. Bennet, D. Bennet. *The Profundity and Bifurcation of Change Part V: Living the Future.* MQIPress <http://mqipress.com/change/>.

Resumen: "Living the Future" (Marzo 2017) es la quinta entrega de la obra titulada "The Profundity and Bifurcation of Change". En esta obra se desarrolla la teoría del llamado "Intelligent Social Change Journey" (ISCJ), entendido éste como "el viaje del cuerpo, la mente y el corazón, que va de la pesadez de las extrapolaciones lineales causa- efecto, hacia la fluidez de co-evolucionar con nuestro entorno y a la ligereza de respiración de pensamiento y sentimientos en la realidad". A pesar de lo esotérico que pueda parecer esta frase, sus autores -especialmente Alex & David Bennet- hunden sus raíces en la Gestión del Conocimiento, con un pasado de trabajo en la NASA y posteriormente con títulos como "Knowledge Mobilization in the Social Sciences and Humanities". Su viaje no deja de ser algo que algunos (tengo el honor de incluirme) proponemos y que postula la evolución consciente del Conocimiento (y su gestión) hacia la Sabiduría. Un vistazo a sus publicaciones puede abrir una perspectiva insólita (pero no menos interesante) a este mundo del Conocimiento que pugna por abrirse camino entre la tecnología y las ciencias sociales.

Los autores: Alex & David Bennet, son un matrimonio de avanzada edad con una larga trayectoria en el mundo de la Gestión del Conocimiento. Son Co-fundadores de Mountain Quest Institute <http://www.mountainquestinstitute.com/#home.html>, con Arthur Shelley, Theresa Bullard y John Lewis, y autores de un buen número de publicaciones. Tuve el placer de conocerlos personalmente en la Gala de los Premios MAKE (*Most Admired Knowledge Enterprise*, Sao Paulo, 2009). Su compromiso con el Conocimiento y su Gestión les hace ser un referente de prestigio en este ámbito.

Sección Técnica: *"Gobierno corporativo de las TI"* (Miguel García-Menéndez, Manolo Palao)

Tema: *La Seguridad Digital como freno*

No hay mejor argumentación sobre el beneficio de abordar una determinada actividad dentro de una empresa, para quien se encuentra al frente de ésta, que su reflejo positivo en la cuenta de resultados. Las actividades que giran en torno a lo digital no son una excepción. Sin embargo, a la dificultad intrínseca de mostrar el valor que puede generar un activo intangible (los digitales tienden a serlo), hay que sumar el escaso número de fuentes de referencia que, tradicionalmente, se han ocupado de este tema. En 2004, el Centro para la Investigación de los Sistemas de Información (CISR, por sus siglas en inglés), del MIT, publicó los resultados de un estudio [4] sobre el papel (el uso) de los sistemas de información dentro de las organizaciones y la atención que se les prestaba, desde los órganos de gobierno de las distintas entidades analizadas (más de doscientas cincuenta empresas). La principal conclusión del trabajo realizado por los profesores Peter Weill y Jeanne Ross fue que las organizaciones que, dentro de un determinado sector (por ejemplo, el industrial), aplicaban las tecnologías digitales con mayor diligencia, y que además lo hacían en el contexto de un adecuado marco general de gobierno corporativo que rigiese el devenir de la entidad en todas sus vertientes, podrían llegar a alcanzar rentabilidades que superasen en un 20% las logradas por aquellos de sus iguales (sus competidores) que no aplicasen con igual eficacia las herramientas tecnológicas y cuyos órganos de gobierno no prestasen la misma atención a su debida dirección y control. Una

posterior actualización del trabajo [5], realizada en 2009, les permitió corroborar que "el éxito (económico) en la economía digital iría a parar a las empresas que resultasen más 'sabias' a la hora de aplicar la tecnología".

Más recientemente, en 2014, el Centro para el Negocio Digital (CDB, por sus siglas en inglés), también del MIT, a través de su programa "Iniciativa sobre la Economía Digital" abordó nuevamente el tema [1], logrando actualizar la cifra dada por Weill y Ross. En esta ocasión, los profesores George Westerman y Andrew McAfee, junto al consultor francés Didier Bonet, determinaron que los procesos de digitalización firmemente gobernados (dotados de un sistema de gobierno corporativo riguroso) podrían suponer para una empresa un 26% más de rentabilidad que la de la media de su sector.

Piense, por ejemplo, en el sector industrial y en las posibilidades que ofrece y ofrecerá en los próximos años, impulsado por la corriente "Industria 4.0". La firma de servicios profesionales Oliver Wyman, por boca de su responsable mundial para los sectores de Automoción y Fabricación, Thomas Kautzsch, cifra en 1,25 billones de euros (1,4 billones de dólares) el aumento agregado, en sus márgenes, que podrán lograr en el horizonte de los próximos años (hasta 2030) aquellas empresas industriales que digitalicen sus procesos operativos [6]. Kautzsch apunta a los procesos pre- y post-producción (diseño, desarrollo, ventas, distribución, …) como los más rentables una vez digitalizados.

Todas esas cifras hacen pensar que la Sociedad se encuentra en el umbral mismo de lo que va a ser el verdadero progreso. Se está viendo en todos los sectores, no sólo en el industrial. Sin embargo, esas mismas cotas de rentabilidad requieren de algún tipo de garantía. Requieren ser salvaguardadas. Es el principio del "Equilibrio del Valor" [2]: "a partir del establecimiento de una determinada estrategia corporativa, han de ponerse en marcha dos fuerzas (sólo aparentemente) contrapuestas: una, en el sentido de crear valor para la organización (aportación de valor); y otra, en el sentido de preservar el valor creado (mitigación del riesgo de destrucción de valor)". Parece razonable interpretarlo como un principio básico de la responsabilidad corporativa que recae sobre quienes están al frente de las organizaciones, cuya primera misión ha de ser velar por la sostenibilidad del valor en el tiempo; es decir, en suma, por la perdurabilidad de las propias organizaciones [3].

Parece, igualmente, razonable identificar en ese principio de "Equilibrio del Valor" (en sus dos fuerzas), tanto a la digitalización, cuanto a la ciberseguridad (más aún, a la ciberresiliencia). La actual ola transformadora, por vía de lo digital, tiene en la creación de valor su más reconocida ventaja. En igual medida, y lejos de constituir un obstáculo a esa creación de valor, la ciberseguridad ofrece su contribución al valor, preservando el valor creado. En palabras del consultor japonés William H. Saito, el papel de la ciberseguridad para la organización es equivalente al que juega el mecanismo de frenos en el famoso tren bala de Shinkansen: "En 1964, (el nuevo tren) fue ensalzado por su velocidad; pero, francamente, cualquiera puede construir un tren rápido. Fueron las innovaciones en el sistema de frenos las que hicieron posible esas nuevas velocidades. Los frenos no están ahí para ralentizar el movimiento del tren, sino que son ellos los que le permiten ir más rápido que los trenes convencionales, al garantizarles a los maquinistas el control que ejercen sobre la marcha" [7].

Inigualable metáfora que permite hacer una interpretación de la ciberseguridad, en positivo, como elemento que, bajo la supervisión del pertinente órgano de gobierno (y control), actúa (en este caso, como en el ejemplo del tren) de garante de la buena marcha de la organización. Una afirmación que no puede adquirir mayor sentido en el mundo industrial, donde la convergencia de lo lógico y lo físico (lo "ciberfísico") constituye el principal exponente de riesgo para las personas, el medioambiente, el patrimonio y, en última instancia, para la pervivencia de los procesos, de las operaciones y, por extensión, del propio negocio.

En definitiva, retomando el símil del tren bala, puede decirse que para ir verdaderamente rápido (para que una empresa industrial progrese), con garantía de poder repetir la proeza (de manera sostenible), lo que se necesita es disponer de unos buenos frenos (una buena seguridad digital).

Referencias

[1] G. Westerman, A. McAfee, D. Bonnet. "Leading Digital: Turning Technology into Business Transformation". *7 de octubre de 2014.* <https://www.amazon.es/Leading-Digital-Technology-Business-Transformation/dp/1625272472>.
Último acceso: 30 de marzo de 2017.
[2] M. García-Menéndez. "Confianza en, y valor de, los sistemas de información". *Blog "Gobernanza de TI", 1 de enero de 2010*. <https://gobernanza.wordpress.com/2010/01/01/confianza-en-y-valor-de-los-sistemas-de-informacion/>.
Último acceso: 30 de marzo de 2017.
[3] M. García-Menéndez. "Continuidad del Negocio y Auditoría de Sistemas (por Manolo Palao)". *Blog "Gobernanza de TI". Presentación del Texticulillo™ (nº 12) homónimo, de Manolo Palao, en su edición para "Gobernanza de TI"*, *15 de octubre de 2010.* <https://gobernanza.wordpress.com/2010/10/15/continuidad-del-negocio-y-auditoria-de-sistemas-por-manolo-palao-2/>.
Último acceso: 30 de marzo 2017.
[4] P. Weill, W.R. Jeanne. "IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*". 1 de mayo de 2004.* <https://www.amazon.es/Governance-Performers-Decision-Superior-Results/dp/1591392535>.
Último acceso: 30 de marzo de 2017.
[5] P. Weill, W.R. Jeanne. "IT Savvy: What Top Executives Must Know to Go from Pain to Gain". *1 de junio de 2009.* <https://www.amazon.es/Savvy-What-Executives-Must-Know/dp/1422181014>.
Último acceso: 30 de marzo de 2017.
[6] T. Kautzsch. "Become digitally lean. Manufacturing is leading a Digital Industrial Revolution". *Oliver Wyman, "Ten Digital Ideas from Oliver Wyman", idea número 4, Junio de 2016.* <http://www.oliverwyman.com/insights/publications/2016/jun/new-digital-ideas/become-digitally-lean.html#.WD65R_nhDdM>.
Último acceso: 30 de marzo de 2017.
[7] W.H. Saito. "It's Time To Think Of Cybersecurity As A Business Enabler". *Forbes Magazine, 1 de julio de 2016.* <http://www.forbes.com/sites/williamsaito/2016/07/01/its-time-to-think-of-cybersecurity-as-a-business-enabler/>.
Último acceso: 30 de marzo de 2017.

Sección Técnica: *"Lenguajes de Programación"* (Oscar Belmonte Fernández, Inmaculada Coma Tatay)

Tema: *Rust, el lenguaje de programación creado por Mozilla*

Rust, el lenguaje de programación creado por Mozilla en 2010, ha llegado a su versión 1.15. Según un informe de *StackOverflow*, es el lenguaje de programación más amado entre los desarrolladores.

Este lenguaje de programación tiene una sintaxis cercana al lenguaje de programación C, al que intenta sustituir en la programación de sistemas, según se encuentra en su página web <http://www.rust-lang.org>.

Una de sus principales virtudes es la rapidez en la ejecución del código generado, lo que hace de él un excelente candidato para de-

sarrollar aplicaciones computacionalmente costosas, en particular, algoritmo de aprendizaje sobre grandes volúmenes de datos.

Algo realmente atractivo del lenguaje es su inferencia de tipos, de gran ayuda al escribir código en lenguajes de tipado fuerte, como es el caso de *Rust.* Otro lenguaje con una muy cuidada inferencia de tipos es *Scala,* con el que también comparte la herencia múltiple a través de *traits*.

Muy de agradecer es la abundante documentación en línea que se proporciona para el aprendizaje de este lenguaje de programación, y como era esperable de una fundación como Mozilla.

Tema: *StackOverflow Developer Survey Results*

El sitio web al que todo programador acude en busca de ayuda es, sin lugar a dudas, *StackOverflow*. Analizando los datos generados en esta web los responsables de *StackOverflow* han generado un interesante informe, que, como todos ellos, hay que asimilar en su justa medida.

Además de lo ya comentado sobre *Rust* como lenguaje de programación más amado por los desarrolladores, proporcionan otros datos interesantes, y algunos de ellos conocidos, como el bajo porcentaje de mujeres que trabajan en TIC. Otro dato curioso es el porcentaje de usuarios de *StackOverflow* que se consideran a sí mismos, al menos parcialmente, como autodidacta (69%) frente a los que tienen una titulación universitaria (35%).

Más información en: <http://stackoverflow.com/insights/survey/2016>.

Sección Técnica: *"Seguridad"* (Javier Areitio Bertolín, Javier López Muñoz)

Tema: *Libros*

■ **C.J. Brooks, P. Craig, D. Short.** *Cybersecurity Essentials*. Sybex. ISBN 1119362393, 2017.
■ **K. Mayes, K. Markantonakis.** *Smat Cards, Tokens, Security and Applications*. Springer. 2nd Edition. ISBN 3319504983, 2017**.**
■ **L. Brotherston, A. Berlin.** *Defensive Security Handbooks: Best Practices for Securing Infrastructures*. O`Reilly Media. ISBN 1491960387, 2017.
■ **R. Leenes, R.V. Brakel, S. Gutwirth, P.D. Hert**. *Data Protection and Privacy: (In)visibilities and Infrastructures*. Springer. ISBN 3319507958, 2017.
■ **R. Messier.** *Network Forensics*. Wiley. ISBN 1119328284, 2017.
■ **S.M. Muyeen, S. Rahman**. *Communication, Control and Security Challenges for the Smart Grid*. IET (The Institution of Engineering and Technology). ISBN 1785611429, 2017**.**
■ **W. Allsopp.** *Advanced Penetration Testing: Hacking the World's Most Secure Networks*. Wiley. ISBN 1119367689, 2017**.**
■ **W.J. Schunemann, M.O. Baumann.** *Privacy, Data Protection and Cybersecurity in Europe*. Springer. ISBN 3319536338, 2017**.**

Tema: *Congress – Conferences – Forum*

■ **Securmática 2017**. XXVIII Congreso Global de Ciberseguridad, Seguridad de la Información y Privacidad: "La Ciberseguridad aterriza en la alta dirección". Del 25 al 27 de Abril 2017. Campo de las Naciones, Madrid.
■ **CYBERSEC'2017** (3rd European Cybersecurity Forum 2017). 9 y 10 de Octubre del 2017. Krakow, Polonia**.**
■ **ISSA (Information Systems Security Association) 2017**. International Conference. Del 9 al 11 de Octubre del 2017. San Diego. California, USA.
■ **Cyber Security EU 2017**. 18 de Octubre del 2017. Leeds, UK.
■ **Black Hat Europe 2017**. 4 y 5 de Diciembre del 2017. Londres, UK.

Sección Técnica: *"TIC y Turismo"* (Andrés Aguayo Maldonado, Antonio Guevara Plaza)

Tema: *Boletín SICTUR*

Gracias al acuerdo entre la Sociedad Mercantil Estatal para la Gestión de la Innovación y las Tecnologías Turísticas, S. A (SEGITTUR) y las veintiséis Universidades que forman REDINTUR, la Red Universitaria de Postgrados en Turismo surgió el proyecto SICTUR, el Sistema de Información de la Investigación Científica en el Turismo, cuyo fin es el de promover la investigación científica y tecnológica en la industria turística a través de Internet.

En la actualidad, el sistema recoge información relativa a más de 2.600 usuarios con perfil de investigador activo, es decir, que figuran en alguna publicación en turismo, pertenecientes a alguno de los más de 250 grupos de investigación registrados. En cuanto a las publicaciones científicas recogidas, podemos resaltar los más de 3.800 artículos publicados en 1.150 revistas, las más de 3.500 contribuciones en congreso o las más de 560 tesis doctorales.

Con el objetivo de difundir mejor la oferta científica y tecnológica entre usuarios y clientes externos, se publica el Boletín SICTUR. Editado por REDINTUR, este boletín compila y difunde las últimas novedades de la producción científica realizada por las Universidades españolas en el ámbito de la investigación turística.

Este mes de marzo se cumplen cuatro años desde que se editase el primer número de este boletín, que mensualmente es enviado a más de 5.000 investigadores en turismo de todas las partes del mundo.

El boletín SICTUR correspondiente al mes de marzo incluye los siguientes apartados:

■ Proyecto de investigación *"SurfiNg Routes In a Sustainable Europe"*.
■ Breve reseña de los últimos artículos académicos de turismo publicados en revistas nacionales e internacionales.
■ Noticias de interés para investigadores y docentes en turismo.
■ Sinopsis del libro "¿Existe un modelo turístico canario?".
■ Resumen de la tesis doctoral "Las variables experienciales como determinantes de la calidad de vida, la satisfacción y la lealtad del turista en el contexto del turismo gastronómico".
■ Relación de congresos científicos de turismo y sus fechas límites para el envío de comunicaciones o *abstracts*.
■ Llamada a autores para capítulos de libros y revistas académicas.

La base de datos SICTUR puede consultarse a través de su página web <http://www.sictur.es>.

El problema del robot de exploración de Marte

Julio Javier Castillo, Diego Javier Serrano, Marina Elizabeth Cárdenas
Laboratorio de Investigación de Software MsLabs, Dpto. Ing. en Sistemas de Información, Facultad Regional Córdoba - Universidad Tecnológica Nacional (Argentina)

<jotacastillo@gmail.com>,
<diegojserrano@gmail.com>,
<ing.marinacardenas@gmail.com>

Este es el enunciado del problema 2 que fue planteado en la Octava Competencia de Programación de la Facultad Regional de Córdoba (Universidad Tecnológica Nacional, Argentina) UTN-FRC celebrada en noviembre de 2016.

Un barco tiene rota su brújula, por lo tanto luego de realizar cada giro se desconoce hacia donde está avanzando. Sin embargo el capitán de este barco sabe correctamente cuántos grados gira cada vez que lo hace y está seguro de que el puerto desde donde salió le permite iniciar su recorrido exactamente hacia el norte. Se requiere un programa que reciba la dirección y ángulo de cada giro e informe el punto cardinal hacia el que está dirigido. Para ello el programa debe informar el punto cardinal con una precisión de 22,5°, es decir, según la siguiente rosa de los vientos, que se presenta en la **figura 1**.

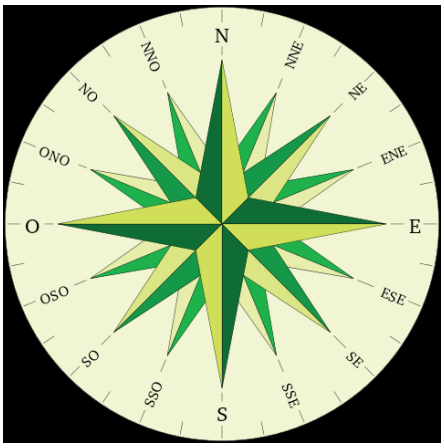

Figura 1. Rosa de los vientos.

En caso de que el barco no finalice apuntando exactamente a uno de los 16 puntos cardinales indicados, se debe informar el más cercano.

Entrada

La entrada inicia con una línea con la cantidad de casos de prueba C. Luego se presentan C casos, cada uno de los cuales presenta una línea conteniendo un número entero G indicando la cantidad de giros y luego G líneas. Por cada giro se ingresa una letra B o E, indicando si el giro fue a babor (izquierda, sentido antihorario) o estribor (derecha, sentido horario) respectivamente y luego un número entero A con la cantidad de grados que giró.

$$0 < C < 10^4$$
$$0 < G < 10^8$$
$$0 \leq A < 360$$

Salida

Por cada caso de prueba se debe informar una cadena con la sigla del punto cardinal hacia el que el barco está más orientado (una de {N, NNE, NE, ENE, E, ESE, SE, SSE, S, SSO, SO, OSO, O, ONO, NO, NNO}).

Ejemplo de entrada

```
2
3
B 45
B 45
B 0
5
E 15
E 15
B 10
B 10
E 5
```

Ejemplo de salida

```
O
NNE
```

Julio Javier Castillo, Diego Javier Serrano, Marina Elizabeth Cárdenas
Laboratorio de Investigación de Software MsLabs, Dpto. Ing. en Sistemas de Información, Facultad Regional Córdoba - Universidad Tecnológica Nacional (Argentina)

<jotacastillo@gmail.com>,
<diegojserrano@gmail.com>,
<ing.marinacardenas@gmail.com>

El problema del robot de exploración de Marte

El enunciado de este problema apareció en el número 237 de ***Novática*** (julio-octubre 2016, p. 78).

El problema consiste en codificar un algoritmo que sea capaz de controlar remotamente un robot. El control del mismo debe hacerse de manera tal de evitar las posiciones de peligro y en el caso de que uno de los desplazamientos ponga en riesgo la misión se debe informarlo por consola.

El problema aclara también, que cualquier posición fuera del área de trabajo del robot se considera como no segura. Es por ello que los controles de los límites de las matrices deben hacerse constantemente en cada paso de un desplazamiento. Aunque el problema no lo indica, asumimos que el descenso del robot ha sido exitoso y que, por ello, siempre partimos de una posición segura.

El problema se resuelve con dos lenguajes de programación alternativos: Java y Python. La solución en Java muestra el uso de una sola clase, con el método estático main que permite realizar la lectura y rellenado de la matriz de exploración, la cual se conoce que será cuadrada y binaria. Seguidamente, se realiza la lectura de la cantidad de casos de prueba a analizar, y a través del empleo de una estructura repetitiva se procesan cada uno de estos casos de prueba. Luego, es necesario analizar la secuencia de movimientos de cada desplazamiento partiendo del centro de la matriz. Ya que los casos de prueba vienen separados entre sí por una ",", es necesario realizar un split (división) del String para obtener cada uno de los movimientos del desplazamiento. Esta información nos permite comenzar a recorrer la matriz, y esto se refleja en el ciclo for anidado, puesto que el algoritmo procesa un caso de prueba a la vez.

En la implementación, el par (x,y) representa inicialmente el centro de la matriz y un ciclo for permite recorrer esta matriz en alguna de las cuatro direcciones permitidas y con una determinada cantidad de movimientos (longitud). Cada movimiento en un paso se refleja en la actualización de los valores de las coordenadas x e y, en la dirección que corresponda.

Si en algún momento se detecta una posición insegura, el algoritmo lo refleja mediante el cambio de valor de la bandera seguro. Esto es realizado controlando que las posiciones se mantengan en el rango de la matriz y siempre que no se cumpla la condición "area[x][y] == 1".

Si en algún momento se detecta una posición no segura para ese desplazamiento, entonces se interrumpe su procesamiento, se informa esa situación y se prosigue con el análisis del siguiente desplazamiento.

La segunda solución propuesta implementa el mismo algoritmo pero con el lenguaje de programación Python. Se utiliza el script principal y cuatro funciones que simplemente permiten actualizar la posición del desplazamiento, y que es representada por una tupla de dos componentes.

Notamos que el área se crea utilizando listas por comprensión, y que los movimientos se almacenan en una lista de funciones. Esta lista puede ser indizada y mediante una tupla de dos elementos como argumentos, es posible invocar a las funciones de dirección para que actualicen el sentido del desplazamiento.

Este problema también podría ser abordado empleando un enfoque basado en grafos, pero se lo resuelve con un enfoque matricial puesto que naturalmente se representa como una matriz, y además, su recorrido se reduce a simples desplazamientos en formas de filas o columnas.

A continuación se presentan las soluciones en ambos lenguajes de programación.

Solución en Java:

```
import java.util.Scanner;

public class RobotExplorador {

    public static void main(String[] args) {

        Scanner sc = new Scanner(System.in);
        int[][] area;
        int tamaño = sc.nextInt();

        area = new int[tamaño][tamaño];

        for (int i = 0; i < tamaño; i++) {
              for (int j = 0; j < tamaño; j++) {
                area[i][j] = sc.nextInt();
            }
        }

        int c = sc.nextInt();
        sc.nextLine();
```

```
        int x, y, distancia, direccion, longitud;
        for (int i = 0; i < c; i++) {
            x = y = (tamaño-1) / 2;
            boolean seguro = true;
            distancia = 0;
            String l = sc.nextLine();
            String[] linea = l.split(",");

            for (String movimiento : linea) {
              String []tok = movimiento.trim().split(" ");
              direccion = Integer.parseInt(tok[0]);
              longitud =  Integer.parseInt(tok[1]);


                for (int j = 0; j < longitud && seguro; j++) {
                    switch (direccion) {
                        case 0: x--; break;
                        case 1: x++; break;
                        case 2: y++; break;
                        case 3: y--;
                    }

x < 0 || y < 0 || x >= tamaño || y >= tamaño || area[x][y] == 1)
                        seguro = false; break;
                }
                distancia += longitud;
                if (!seguro) break;
            }
        System.out.println((seguro) ? distancia : "NO SEGURO");
        }
    }
}
```

Solución en Python:

```
def arriba(x, y): return x-1,y
def abajo(x, y): return x+1,y
def izquierda(x, y): return x,y+1
def derecha(x, y): return x,y-1

movimiento = [arriba, abajo, izquierda, derecha]

tamaño = int(input())
area = [None] * tamaño

for i in range(tamaño):
    area[i] = [int(x) for x in input().split()]

c = int(input())

for i in range(c):
    movimientos = [x.strip().split() for x in input().split(",")]
    x = y = (tamaño - 1) // 2
    seguro = True
    distancia = 0
    for m in movimientos:
        direccion = int(m[0])
        longitud = int(m[1])

        for j in range(longitud):
            x, y = movimiento[direccion](x, y)
if (not 0 <= x < tamaño) or (not 0 <= x < tamaño) or area[x][y] == 1:
                seguro = False
                break

        distancia += longitud
        if not seguro: break

    print(distancia if seguro else "NO SEGURO")
```

Coordinación Editorial

Conclusiones de la 5ª edición del estudio "Estado actual y futuro del software en España 2017"

SoftDoit ha presentado el pasado 14 de marzo la 5ª edición del estudio "Estado actual y futuro del software en España 2017", realizado en colaboración con ATI (Asociación de Técnicos de Informática).

El estudio muestra la situación actual de la implantación del software en todo el territorio español y analiza tanto el estado actual de las soluciones informáticas más utilizadas por las empresas españolas, como las expectativas y líneas futuras. En la realización del estudio han participado cerca de 150 empresas de toda España, casi un 44% de ellas pymes de menos de 50 empleados, y casi un 25%, con más de 1.000 trabajadores en plantilla.

Entre las conclusiones principales destacan:

- El ERP es el software más utilizado por las empresas (80%).
- Windows es el sistema operativo más implantando en las empresas (93%), seguido de Linux (40,4%) y de IOS (27%).
- Las soluciones a medida superan las estándares, siendo las más utilizadas (66,4%).
- La confianza de las empresas en la nube aumenta ligeramente respecto al estudio anterior (66%, frente a un 64,4%.), aunque solo un 13% utiliza esta modalidad de alojamiento de forma exclusiva.
- La satisfacción de las empresas con sus soluciones de software desciende (42,5%, frente a un 52% de hace un año).
- El 70,5% de las empresas prevé crecer a lo largo de este año, siendo menos optimista un 21,2% que afirma que se mantendrá.

Más información: <https://www.softwaredoit.es/estudios>.

Programación de Novática

Por acuerdo del Consejo Editorial de ***Novática***, el tema de la segunda monografía de 2017 será:

Nº 239 (marzo – junio 2017): *"Salud y tecnología".*

Socios institucionales de ati

Según los Estatutos de ATI, pueden ser socios instituciones de nuestra asociación *"las personas jurídicas, públicas y privadas, que lo soliciten a la Junta Directiva General y sean aceptados como tales por la misma".*

Mediante esta figura asociativa, todos los profesionales y directivos informáticos de los socios institucionales pueden gozar de los beneficios de participar en las actividades de ATI, en especial congresos, jornadas, cursos, conferencias, charlas, etc. Asimismo los socios institucionales pueden acceder en condiciones especiales a servicios ofrecidos por la asociación tales como Bolsa de Trabajo, cursos a medida*, mailings*, publicidad en Novática, servicio ATInet, etc.

Para más información dirigirse a <info@ati.es> o a cualquiera de las sedes de ATI. En la actualidad son socios institucionales de ATI las siguientes empresas y entidades:

AGROSEGURO, S.A.

COSTAISA, S.A.

FUNDACIÓ PRIVADA ESCOLES UNIVERSITÀRIES GIMBERNAT

FUNDACIÓN TALENTO MATEMÁTICO Y CIENTIFÍCO

INSTITUT D'ESTUDIS CATALANS

INSTITUT MUNICIPAL D´INFORMÀTICA

INSTITUTO MADRILEÑO DE FORMACIÓN

KRITER SOFTWARE, S.L.

MASTER.D Master Distancia,S.A.

ONDATA INTERNATIONAL, S.L.

UNIVERSIDAD DE ALCALÁ DE HENARES (UAH)

UNIVERSIDAD EUROPEA DE MADRID

UNIVERSITAT DE GIRONA

UNIVERSITAT OBERTA DE CATALUNYA

INSTITUTO DE LA MUJER

SEACEPTANIDEAS.COM

Hoja de subscripción a Novática (2017)
(revista digital de la Asociación de Técnicos de Informática)
Novática Subscription Form (2017)
(Online journal and magazine published by Asociación de Técnicos de Informática)

Revista de la Asociación de Técnicos de Informática

www.ati.es/novatica

Formulario de suscripción en línea disponible en https://www.ati.es/suscripcionnovatica / Online Subscription Form available at https://www.ati.es/novaticasubscription

Todos los datos son obligatorios a menos que se indique otra cosa / All the data must filled in unless otherwise stated

Una vez cumplimentada esta hoja, se ruega enviarla a / Please fill in this form and send it to:
e-mail novatica.subscripciones@atinet.es o/or ATI, C/ Àvila 50, 3a planta, local 9 - 08005 Barcelona, España / Spain

Nota importante / Important Notice: Novática es una revista que se publica solamente en formato digital, de aparición trimestral, es decir cuatro números al año[1] / Novática is a digital-only publication that appears quarterly, i.e. four issues per year[1].

►**Cuota anual: 50 Euros** (IVA incluido – este impuesto se aplica solamente a residentes en España) / **Annual fee: 50 Euros** (VAT applicable only to subscribers that reside in Spain)

- El suscriptor es una empresa o entidad __ o una persona física __ (marcar con X lo que corresponda) /
- The subscriber is an organization (business, university, government, etc) __ or a person __ (mark your option with X)

- Datos del suscriptor empresa o entidad / Data of organizational subscriber

Empresa o entidad / Organization	Sector / Business
Dirección / Address	
Localidad / City	Cód. Postal / Post Code
Provincia / Country	
Datos de la persona de contacto / Data of contact person	
Nombre y apellidos / Full name	
Correo electrónico / E-mail address[1]	Teléfono / Phone

- Datos del suscriptor persona física / Data of personal subscriber [2]

Apellidos / Last name	
Nombre / First name	
Localidad / City	Cód. Postal / Post Code
Provincia / Country	Teléfono / Phone
Correo electrónico / E-mail address[1]	

- Datos bancarios para domiciliación del pago / Bank account data for payment (si desea pagar por otro método contacte por favor con novatica.subscripciones@atinet.es **/** if you want your payment to be made using a different method please contact novatica.subscripciones@atinet.es)

Nombre de la entidad bancaria / Name of the Bank (if the bank is not located in Spain please provide also BIC Code)

……..

IBAN:

Cód. país/Country Code	Cód. Banco/Bank Code	Cód. oficina / Branch Code	DC/CD	Núm. Cuenta / Account number

- NIF para su factura / Tax ID for invoice ……

Firma / Signature Fecha / Date ……..

Mediante su firma la persona que ha cumplimentado este impreso declara que todos los datos contenidos en el mismo son ciertos y acepta todos los términos y condiciones del servicio de suscripción a Novática / Along with his/her signature the person filling in this form declares that all the data provided are true and accepts all the terms and conditions of the Novática subscription service

Nota sobre protección de datos de carácter personal / Data Protection Notice: *De conformidad con la LO 15/99 de Protección de Datos de Carácter Personal, le informamos de que los datos que usted nos facilite serán incorporados a un fichero propiedad de Asociación de Técnicos de Informática (ATI) para poder disfrutar de los servicios que su condición de suscriptor de Novática socio le confiere, así como para enviarle información acerca de nuevos servicios y ofertas que ATI ofrezca en relación con sus publicaciones. Si usted desea acceder, rectificar, cancelar u oponerse al tratamiento de sus datos puede dirigirse por escrito a secregen@ati.es. / ATI is fully compliant with the Spain Data Protection Law (LO 15/99). You can enact your rights to access, cancellation or opposition writing to secregen@ati.es.*

[1] Una vez validados por el servicio de suscripciones de Novática los datos de este formulario, Vd. recibirá la información sobre el procedimiento para acceder a la zona de la Intranet de ATI donde se almacenan los números publicados por nuestra revista / Once the data in this form have been validated by the Novática subscription staff you will receive the information about the procedure required to access the ATI Intranet area where the issues edited by our journal are stored.

[2] Si Vd. es profesional informático o estudiante de Informática, o simplemente una persona interesada por la Informática, debe tener en cuenta que la revista Novática es solamente uno de los diferentes servicios que los socios de ATI reciben como contrapartida de su cuota anual, de forma que, muy probablemente, le será más beneficioso hacerse socio que suscribirse únicamente a la revista. Por ello le recomendamos que se informe sobre qué es ATI y sobre los servicios que ofrece en http://www.ati.es/ o en info@ati.es.

Hoja de solicitud de inscripción en ATI (2017)

(Asociación de Técnicos de Informática)

www.ati.es

La solicitud puede hacerse también mediante una hoja online disponible en http://www.ati.es/sersocio

Todos los datos son obligatorios a menos que se indique otra cosa
Una vez cumplimentada esta hoja, se ruega enviarla por correo electrónico a secregen@ati.es,
o por correo postal a ATI, Calle Ávila nº 50, 3ª Planta, local 9 - 08005 Barcelona

► **Solicito inscribirme como:** **Socio de número** ☐ (88€)* **/ Socio junior** ☐ (28€)* **/ Socio jubilado** ☐ (28€)* / **Socio adherido** ☐ (60€)*

(Para inscribirse como **socio estudiante** se ruega utilizar la hoja de inscripción específica disponible en http://www.ati.es/estudiantes - ver en la siguiente página información detallada sobre ATI y los diferentes tipos de socios)

*** Nota importante:** la cuota cubre el año natural, de 1 de enero a 31 de diciembre. Las inscripciones a socios de número realizadas de 1 de julio a 31 de octubre tienen una reducción de cuota del 50% y todas las cuotas son gratuitas si se realizan del 1 de noviembre al 31 de diciembre. En este último caso, si se desea acceder a descuentos en servicios ofrecidos por terceros no se aplicarán reducciones a la cuota anual de asociado, que deberá abonarse en su totalidad.

- Datos personales del solicitante

Apellidos		
Nombre		
Domicilio	Nº	Piso
Localidad	Código Postal	
Provincia	Teléfono	
Dirección de correo electrónico [1]		
Fecha de nacimiento	DNI	

- Datos de la empresa o entidad donde trabaja (si es autónomo indíquelo en el campo "Empresa o entidad")

Empresa o entidad	Sector
Puesto actual	Depto.
Dirección	Nº
Localidad	Código Postal
Provincia	Teléfono

- Domiciliación de la cuota anual (ATI se encarga de su envío al banco o caja)

Nombre de la entidad bancaria: _____

IBAN:

Cód. país	Cód. Banco	Cód. oficina	D.C.	Núm. Cuenta

- Datos complementarios (si necesita más espacio para estos datos continúe en otra hoja)

Títulos superiores o medios que posee y centros otorgantes: .....
.....
.....
Resumen de experiencias profesionales: .....
.....
.....
Número de años de experiencia profesional informática: .....

- Presentado por los Socios de número (**)

(**) Esta información no es necesaria para solicitar inscribirse como socio junior, estudiante o adherido; para inscribirse como socio de número o jubilado, si el solicitante no conoce a ningún socio de número que pueda presentarle, la Secretaría General de ATI le contactará para determinar otra forma fehaciente de acreditar su profesionalidad.

1) Apellidos y Nombre ..... Nº de socio ..... Fecha .../.../..... Firma

2) Apellidos y Nombre ..... Nº de socio ..... Fecha .../.../..... Firma

Firma del solicitante Fecha _____

Mediante su firma el solicitante declara que todos los datos incluidos en esta solicitud son ciertos.

Nota sobre protección de datos de carácter personal: *De conformidad con la LO 15/99 de Protección de Datos de Carácter Personal, le informamos de que los datos que usted nos facilite serán incorporados a un fichero propiedad de Asociación de Técnicos de Informática (ATI) para poder disfrutar de los servicios que su condición de socio le confiere, así como para enviarle información acerca de nuevos servicios, ofertas y cursos que ATI ofrezca y puedan resultar de su interés. Sus datos podrán ser comunicados a aquellas instituciones, sociedades u organismos, con los que ATI mantenga acuerdos de colaboración, relacionados con el sector de los seguros, la banca y la formación para el envío de información comercial. Si usted desea acceder, rectificar, cancelar u oponerse al tratamiento de sus datos puede dirigirse por escrito a secregen@ati.es.*

☐ *No deseo recibir información comercial de ATI ni de terceras entidades colaboradoras de ATI.*
☐ *No deseo recibir información comercial de terceras entidades colaboradoras de ATI.*
☐ *No autorizo la comunicación de mis datos a terceras entidades colaboradoras de ATI.*

[1] Una vez validados por la Secretaría de ATI la hoja de inscripción y los documentos requeridos, y aceptada su solicitud, Vd. recibirá en esta dirección de correo la información sobre el procedimiento para poder utilizar todos los servicios de la red ATINET (ver reverso).

www.ati.es

Una asociación abierta a todos los informáticos

Una asociación útil a sus socios, útil a la Sociedad

Creada en 1967, **ATI (Asociación de Técnicos de Informática)** es la asociación profesional más numerosa, activa y antigua de las existentes en el Sector Informático español, con sedes en Barcelona (sede general), Madrid y Valencia. Cuenta con más de 3.000 socios, que ejercen sus funciones como profesionales informáticos en empresas, universidades y Administraciones Públicas, o como autónomos.

ATI, que está abierta a todos profesionales informáticos independientemente de su titulación, representa oficialmente a los informáticos de nuestro país en Europa (a través de CEPIS, entidad que coordina a asociaciones que representan a más de 400.000 profesionales informáticos de 32 países europeos) y en todo el mundo (a través de IFIP, entidad promovida por la UNESCO para coordinar trabajos de Universidades y Centros de Investigación), y pertenece a la CLEI (Centro Latinoamericano de Estudios en Informática). ATI tiene también un acuerdo de colaboración con ACM (*Association for Computing Machinery*).

En el plano interno tiene establecidos acuerdos de colaboración o vinculación con Ada Spain, ASTIC (Asociación Profesional del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado), Hispalinux, AI2 (Asociación de Ingenieros en Informática), Colegios de Ingenierías Informáticas de Cataluña y con RITSI (Reunión de Estudiantes de Ingenierías Técnicas y Superiores de Informática).

Tipos de socio

√ Socios de número: deben acreditar un mínimo de tres años de experiencia profesional informática (o dos años si se posee un título de grado superior o medio), *o bien* poseer un título de grado superior o medio relacionado con las Tecnologías de Información, *o bien* haber desarrollado estudios, trabajos, o investigaciones relevantes sobre dichas tecnologías

√ Socios estudiantes: deben acreditar estar matriculados en un centro docente cuya titulación dé acceso a la condición de Socio de Número (la hoja específica de inscripción para socios estudiantes está disponible en http://www.ati.es/estudiantes)

√ Socios junior: profesionales informáticos con una edad máxima de 30 años y que no sean estudiantes

√ Socios jubilados (Aula de Experiencia): socios de ATI que, al jubilarse y cesar su actividad laboral, deciden continuar perteneciendo a ATI colaborando con su experiencia con la asociación

√ Socios adheridos: profesionales informáticos que no cumplan las condiciones para ser Socios de Número o también personas que, no siendo profesionales informáticos, quieran participar en las actividades de ATI

√ Socios institucionales: personas jurídicas, de carácter público o privado, que quieran participar en las actividades de ATI (para más información sobre esta modalidad se ruega ponerse en contacto con la sede general de ATI)

¿Qué servicios ofrece ATI a sus socios?

Mediante el pago de una cuota anual, los socios de ATI pueden disfrutar de la siguiente gama de servicios:

√ Formación Permanente
- Cursos, Jornadas Técnicas, Mesas Redondas, Seminarios,
- Conferencias, Congresos
- Secciones Técnicas y Grupos de Trabajo sobre diversos temas
- Intercambios con Asociaciones Profesionales de todo el mundo

√ Servicios de información
- Revista trimestral **Novática** (decana de la prensa informática española)
- Red asociativa **ATInet** (IntrATInet, acceso básico gratuito a Internet, correo electrónico con dirección permanente, listas de distribución generales y especializadas, foros, blogs, página personal, …)
- Servidor web http://www.ati.es, pionero de los webs asociativos españoles.

√ Servicios profesionales
- Asesoramiento profesional y legal
- Peritajes, diagnósticos y certificaciones
- Bolsa de Trabajo
- Emisión en España del certificado profesional europeo EUCIP (*European Certification of Informatics Professionals*)
- Emisión en España del certificado ECDL (*European Computer Driving License*) para usuarios

√ Servicios personales
- Los que ofrece la Mutua de los Ingenieros (Seguros, Fondo de pensiones, Servicios Médicos)
- Los que ofrece la Caja de Ingenieros (gozar de las ventajas de ser socio de esta caja cooperativa)
- Promociones y ofertas comerciales

¿Dónde está ATI?

√ **Sede General y Capítulo de Catalunya** – Calle Avila 50, 3a planta, local 9, 08005 Barcelona - Tlfn. 93 4125235; <secregen@ati.es>

√ **Capítulo de Andalucía** - <secreand@ati.es>

√ **Capítulo de Galicia** - <secregal@ati.es>

√ **Capítulo de Madrid** – Gutierre de Cetina, 24 28017 Madrid - Tlfn. 91 4029391; <secremdr@ati.es>

√ **Capítulo de Valencia y Murcia** – Universidad Politécnica de Valencia. Asociación de Técnicos de Informática. Edificio 1H – ETSINF. Camino de Vera, s/n 46022 Valencia / <secreval@ati.es>

√ **Revista Novática** – Gutierre de Cetina, 24 28017 Madrid – Tlfn. 91 4029391 / <novatica@ati.es>

Acreditación Europea de habilidades informáticas

Líder internacional en certificación de competencias TIC

11.409.855 Candidatos ECDL / ICDL

41 Idiomas

148 Países

24.000 Centros autorizados

45 millones de exámenes

http://www.ecdl.es
info@ecdl.es / 934125235