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"

¿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.