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.

Consejo Editorial
Guillem Alsina González, Juan Hernández Basora, Albert Jové, Miguel García-Menéndez (presidente del Consejo), Francesc Noguera Puig, Jordi Roca i Marimón

Coordinación Editorial
Encarna Quesada Ruiz <encarna.quesada@ati.es>
Composición y autoedición
Impresión Offset Derra S. L.
Traducciones
Grupo de Lengua e Informática de ATI <http://www.ati.es/gt/lengua-informatica/>
Administración
Tomás Brunete, María José Fernández

Secciones Técnicas - Coordinadores
Accesibilidad
Emmanuelle Gutiérrez y Restrepo (Fundación Sidar), <emmanuelle@sidar.org>
Loic Martínez Normand (Fundación Sidar), <loic@sidar.org>
Acceso y recuperación de la Información
José María Gómez Hidalgo (Pragsis Technologies), <jmgomez@pragsis.com>
Enrique Puertas Sanz (Universidad Europea de Madrid), <enrique.puertas@universidadeuropea.es>
Administración Pública electrónica
Francisco López Crespo (MAE), <flc@ati.es>
Sebastià Justicia Pérez (Diputación de Barcelona) <sjusticia@ati.es>
Arquitecturas
Enrique F. Torres Moreno (Universidad de Zaragoza), <enrique.torres@unizar.es>
José Flich Cardo (Universidad Politécnica de Valencia, <jflich@disca.upv.es>
Auditoría SITIC
Marina Touriño Troitiño, <marinatourino@marinatourino.com>
Sergio Gómez-Landero Pérez (Endesa), <sergio.gomezlandero@endesa.es>
Derecho y tecnologías
Elena Davara Fernández de Marcos (Davara & Davara), <edavara@davara.com>
Enseñanza Universitaria de la Informática
Cristóbal Pareja Flores (DSIP-UCM), <cpareja@sip.ucm.es>
J. Ángel Velázquez Iturbide (DLSI I, URJC), angel.velazquez@urjc.es>
Entorno digital personal
Andrés Marín López (Univ. Carlos III), <amarin@it.uc3m.es>
Diego Gachet Páez (Universidad Europea de Madrid), <gachet@uem.es>
Estándares Web
José Carlos del Arco Prieto (TCP Sistemas e Ingeniería), <jcarco@gmail.com>
Gestión del Conocimiento
Joan Baiget Solé (Cap Gemini Ernst & Young), <joan.baiget@ati.es>
Gobierno corporativo de las TI
Manuel Palao García-Suelto (ATI), <manuel@palao.com>,
Miguel García-Menéndez (ITTi) <mgarciamenendez@ittrendsinstitute.org>
Informática y Filosofía
José Angel Olivas Varela (Escuela Superior de Informática, UCLM), <joseangel.olivas@uclm.es>
Roberto Feltrero Oreja (UNED), <rfeltrero@gmail.com>
Informática Gráfica
Miguel Chover Sellés (Universitat Jaume I de Castellón), <chover@lsi.uji.es>
Roberto Vivó Hernando (Eurographics, sección española), <rvivo@dsic.upv.es>
Ingeniería del Software
Luis Fernández Sanz, Daniel Rodríguez García (Universidad de Alcalá),
<{luis fernandez,daniel.rodriguez}@uah.es>
Inteligencia Artificial
Vicente Botti Navarro, Vicente Julián Inglada (DSIC-UPV), <{vbotti,vinglada}@dsic.upv.es>
Interacción Persona-Computador
Pedro M. Latorre Andrés (Universidad de Zaragoza, AIPO), <platorre@unizar.es>
Francisco L. Gutierrez Vela (Universidad de Granada, AIPO), <fgutierr@ugr.es>
Lenguajes Informáticos
Óscar Belmonte Fernández (Univ. Jaime I de Castellón), <belfern@lsi.uji.es>
Inmaculada Coma Tatay (Univ. de Valencia), <Inmaculada.Coma@uv.es>
Lingüística computacional
Xavier Gómez Guinovart (Univ. de Vigo), <xgg@uvigo.es>
Modelado de software
Jesus García Molina (DIS-UM), <jmolina@um.es>
Gustavo Rossi (LIFIA-UNLP, Argentina), <gustavo@sol.info.unlp.edu.ar>
Mundo estudiantil y jóvenes profesionales
Federico G. Mon Trotti (RITSI), <gnu.fede@gmail.com>
Mikel Salazar Peña (Area de Jovenes Profesionales, Junta de ATI Madrid), <mikelbxo_uni@yahoo.es>
Seguridad
Rafael Fernández Calvo (ATI), <rfcalvo@ati.es>
Miquel Sàrries Griñó (ATI), <miquel@sarries.net>
Redes y servicios telemáticos
Juan Carlos López López (UCLM), <juancarlos.lopez@uclm.es>
Ana Pont Sanjuán (UPV), <apont@disca.upv.es>
Robótica
José Cortés Arenas (Sopra Group), <joscorare@gmail.com>
Juan González Gómez (Universidad Carlos III), <juan@iearobotics.com
Seguridad
Javier Areitio Bertolín (Univ. de Deusto), <jareitio@deusto.es>
Javier López Muñoz (ETSI Informática-UMA), <jlm@lcc.uma.es>
Sistemas de Tiempo Real
Alejandro Alonso Muñoz, Juan Antonio de la Puente Alfaro (DIT-UPM),
<{aalonso,jpuente}@dit.upm.es>
Software Libre
Jesús M. González Barahona (GSYC-URJC), <jgb@gsyc.es>
Fernando Tricas García (Universidad de Zaragoza), <ftricas@unizar.es>
Tecnologías para la Educación
Juan Manuel Dodero Beardo (UC3M), <dodero@inf.uc3m.es>
César Pablo Córcoles Briongo (UOC), <ccorcoles@uoc.edu>.
Tecnologías y Empresa
Dídac López Viñas (Universitat de Girona), <didac.lopez@ati.es>
Alonso Álvarez García (TID) <aag@tid.es>
Tendencias tecnológicas
Gabriel Martí Fuentes (Interbits), <gabi@atinet.es>
Juan Carlos Vigo (ATI) <juancarlosvigo@atinet.es>
TIC y Turismo
Andrés Aguayo Maldonado, Antonio Guevara Plaza (Univ. de Málaga), <{aguayo, guevara}-@lcc.uma.es>

Las opiniones expresadas por los autores son responsabilidad exclusiva de los mismos. ***Novática*** permite la reproducción, sin ánimo de lucro, de todos los artículos, a menos que lo impida la modalidad de © o copyright elegida por el autor, debiéndose en todo caso citar su procedencia y enviar a ***Novática*** un ejemplar de la publicación.

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"

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*.