Recomendaciones sobre Seguridad y Privacidad Informática en el Tratamiento de Datos de Salud

Ana Sanchez Henarejos[1], Jose Luis Fernández Alemán[2], Ambrosio Toval Álvarez[2]

[1]Técnico Auxiliar de Informática de la Delegación del Gobierno en Murcia (España);
[2]Profesor del Departamento de Informática y Sistemas de la Universidad de Murcia (España).

Resumen / Abstract

Resumen. *Un reciente informe de la Agencia Europea de Seguridad de las Redes y de la Información, pone de manifiesto la tendencia creciente de los ataques a la información personal de salud. Estos ataques se ven agravados con la informatización de las historias clínicas de salud y la falta de conocimientos informáticos del personal que trabaja en los centros sanitarios. En este artículo, se pretende hacer una revisión de los estándares, normativa y recomendaciones nacionales e internacionales que incluyen buenos hábitos de seguridad y privacidad para los profesionales de entornos sanitarios.*

Abstract. *A recent report published by the European Network and Information Security Agency highlights the growing trend of the attacks on personal health information. The adoption of the electronic health record and the lack of computer skills exhibited by health professionals working in health centers are compounding these attacks. This article is intended to revise national and international standards, regulations and recommendations that include security and privacy practices for healthcare professionals.*

Introducción

En enero de 2013, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), publicó el informe Threat Landscape. Responding to the Evolving Threat Environment (1) que indica las tendencias en los ataques a sistemas y organizaciones del año 2012.

La principal amenaza a la información de salud que se identifica en el informe son las violaciones en la confidencialidad, de los datos. Los principales hallazgos en lo que a estas violaciones se refieren son las siguientes:

1. El año 2011 se caracterizó por ser el año de las violaciones de privacidad de los datos. La tendencia es que sigan en aumento.
2. En los últimos años, el número de violaciones en la privacidad de los datos detectados en las organizaciones sanitarias ha aumentado debido a la adopción de sistemas de historia clínica digital.
3. La mayor parte de violaciones de la privacidad de los datos se produce a consecuencia de mala praxis por parte de los trabajadores, además de por ataques externos.
4. 9 de cada 10 violaciones se podrían haber prevenido si las organizaciones hubiesen seguido buenas prácticas en la seguridad de los datos.
5. Entre enero y junio de 2012, el número de incidentes que comprometen la confidencialidad del sistema en organizaciones sanitarias casi se ha duplicado.
6. El 96% de todas las organizaciones sanitarias encuestadas en el informe han sufrido al menos una violación de datos en los últimos años.

Las amenazas a las que se enfrentan las organizaciones sanitarias son importantes, y dependen en gran medida de la política de seguridad de la organización y en especial de la formación de cada uno de los trabajadores en la materia.

Esta situación se agrava con la informatización de los sistemas sanitarios, provocando que la información pueda escapar más fácilmente del control de la organización.

Por tanto, es de vital importancia vigilar y actualizar los hábitos de seguridad del personal con acceso a los sistemas informáticos de la organización sanitaria.

Revisión de las recomendaciones de seguridad nacionales e internacionales en materia de buenas prácticas en seguridad informática

Esta sección revisará algunas de las recomendaciones, normas y estándares de seguridad aplicables a los entornos hospitalarios, y que pueden emplearse como referencia y orientación en materia de buenas prácticas de seguridad informática para el personal sanitario.

1. ISO 27002

El estándar ISO 27002 (2) es una guía de buenas prácticas para la gestión de la seguridad en la organización, que describe los objetivos de control o aspectos a analizar para garantizar la seguridad de la información, y las recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización.

2. ISO 27799

La ISO 27799 (3) es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.

La ISO 27799, hace especial hincapié en la concienciación y formación continua de los empleados y en la gestión adecuada de riesgos de seguridad en el entorno sanitario.

3. Health Insurance Portability and Accountability Act (HIPAA) Y The American Recovery and Reinvestment Act of 2009 (ARRA)

La normativa de Estados Unidos relativa a privacidad y seguridad de los datos sanitarios de salud, HIPAA (Health Insurance Portability and Accountability Act), (4, 5) surge en el año 1996.

En ella establecen unos principios de privacidad y seguridad requeridos para todos los datos de salud de cualquier hospital, con el fin de armonizar y homogeneizar la diversidad de políticas de seguridad disponibles en los distintos centros de salud americanos.

En el año 2009, surge la Health Information Technology for Economic and Clinical Health y su objetivo es expandir la regla de seguridad y privacidad de HIPAA. Estas recomendaciones pretenden informar al paciente de sus derechos, describir qué medidas de seguridad física hay que tomar para proteger la confidencialidad e integridad de los datos, y qué buenas prácticas deben concurrir en el personal sanitario para evitar ataques de seguridad y accesos no autorizados.

4. Legislación de Protección de Datos Carácter Personal en España (LOPD y normativa de desarrollo)

Para el desarrollo del derecho a la intimidad, surge la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal (6) (LOPD). Su objetivo es garantizar y proteger intimidad personal y familiar y el pleno ejercicio de los derechos personales, en lo que se refiere al tratamiento de los datos personales. Asimismo, el Reglamento de desarrollo de la LOPD, R.D. 1720/2007 (7), establece la obligación para todas las organizaciones de poner en marcha diversas medidas destinadas a garantizar la protección de dichos datos.

Los datos personales de salud, se encuentran particularmente amparados por la normativa, que los trata como datos especialmente protegidos (artículo 7 LOPD). Como consecuencia de este tratamiento especial, deben ser protegidos con medidas de seguridad altas según lo establecido por el R.D. 1720/2007. Las medidas de seguridad altas, incluyen a su vez las de nivel medio, éstas a su vez las de nivel básico.

5. Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Para adaptar y delimitar la protección de datos de carácter personal al ámbito hospitalario surgió la Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (8). Esta ley, establece también los derechos y obligaciones de los profesionales y los centros y servicios sanitarios, pú-

blicos y privados en cuanto a información y documentación clínica se refiere.

En cuanto a las historias clínicas, la ley exige que se respete el carácter confidencial de las mismas y prohíbe que nadie no autorizado acceda a ellas. Así mismo, responsabiliza a los centros sanitarios del establecimiento de las políticas y normas de seguridad que garanticen el acceso legal a los datos de los pacientes.

La ley indica que las obligaciones del personal sanitario establecidas por la ley 41/2002 son las siguientes:

- El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.
- Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.
- El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

6. Esquema Nacional de Seguridad

El objeto del Esquema Nacional de Salud (ENS)(9) es el establecimiento de los principios básicos y requisitos mínimos de seguridad en la utilización de medios electrónicos de las Administraciones Públicas, permitiendo la adecuada protección de la información, con el fin de crear las condiciones de confianza necesarias en el uso de los medios electrónicos por parte de los ciudadanos. Establece el conjunto de elementos necesarios para garantizar una adecuada gestión de la seguridad de la información en las redes y sistemas involucrados en la prestación de servicios públicos de manera electrónica.

Además, exige que la seguridad comprometa a todos los miembros de la organización y que la política de seguridad sea conocida por todos los miembros de la organización administrativa.

7. Instituto nacional de tecnologías de la comunicación (Inteco).

El Instituto Nacional de Tecnologías de la Comunicación (INTECO) tiene como objetivo servir como instrumento para el desarrollo de la Sociedad de la Información, con el desarrollo de proyectos asociados a las TIC, mediante la investigación, prestación de servicios, realización de estudios estadísticos y la formación.

De entre las recomendaciones de INTECO de interés para los profesionales de la salud destacan las recomendaciones para la creación de una contraseña segura (10).

8. CCN-CERT.

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional. Pone a disposición de todos los miembros de las administraciones públicas, una serie de guías prácticas para la implantación del Esquema Nacional de Seguridad. Entre ellas, se encuentra la guía de seguridad que presenta las normas a las que ha de ajustarse la administración y sus trabajadores, en la utilización de los sistemas informáticos para un correcto uso de los mismos, para proteger los datos personales con los que se trabaja (11), y adaptarse así al ENS. Estas guías se deben tener en cuenta ya que los centros sanitarios deben cumplir el Esquema Nacional de Seguridad.

9. Políticas de seguridad del centro sanitario

Cada centro sanitario debe de tener disponible las políticas de seguridad que deben cumplir todos los usuarios de sistema informático del centro.

Discusión

Un problema de confidencialidad, integridad o disponibilidad de los datos sanitarios de carácter personal en la organización sanitaria puede tener una repercusión grave tanto en el ámbito asistencial como en el ámbito organizativo. La Agencia Española de Protección de Datos ha sancionado con multas tipificadas como graves varios hospitales y clínicas en España. Como ejemplo podemos citar la infracción cometida por una clínica que filtró un fichero Excel con datos de 3000 pacientes en el programa Emule, lo cual le costó 6000 euros (12).

Un estudio que evalúa el estado de las medidas de privacidad y seguridad en los diferentes estados miembros de la Unión Europea (13) concluye que en España uno de cada 3 hospitales viola la LOPD. Además:

- 40% de los hospitales públicos, y 15% de los privados, no tienen registro de acceso a la historia clínica o a los archivos físicos de información.
- Sólo un tercio de los hospitales estatales llevó a cabo una auditoria de seguridad.
- 64% de los hospitales públicos no cumplen la LOPD.
- Veinte hospitales privados se enfrentan a multas de entre 60.000 y 300.000 euros.

Los resultados de este estudio están avalados por un estudio del 2010 de la Agencia Española de Protección de datos (14) y por otro de 2011 del Instituto Nacional de Tecnologías de la Comunicación (INTECO) (15).

Conclusiones

Es primordial para las organizaciones sanitarias mantenerse actualizado en lo que a las recomendaciones, estándares y normativa de seguridad de los datos personales de salud se refiere. Además es necesario que se transmita la preocupación en este ámbito a todos los trabajadores de la organización para evitar errores humanos que comprometan el sistema informático del centro. En este trabajo se recopilan las principales fuentes a la que acudir para actualizar estos contenidos, y preparar material formativo para educar a los trabajadores.

Bibliografía

1. ENISA. ENISA Threat Landscape. Responding to the Evolving Threat Environment. European Network and Information Security Agency. 2012. Available from: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport.

2. ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management.

3. ISO 27799:2008. Health informatics — Information security management in health using ISO/IEC 27002 (ISO 27799:2008). Brussels: European Committee for standarization (CEN); 2008. p. 70.

4. HealthIT. Guide to Privacy and Security of Health Information. The office of the Nacional Coordinator for Health Information Technology. Department of Health and Human services. USA. Available from: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

5. United States Congress. HIPAA Handbook for Behavioral Health Staff: Understanding the Privacy and Security Regulations. 2009.

6. LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Madrid 1999. Available from: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf.

7. REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Available from: http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf.

8. LEY 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Madrid 2002. Available from: http://www.boe.es/boe/dias/2002/11/15/pdfs/A40126-40132.pdf.

9. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Madrid2010. Available from: http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf.

10. INTECO. Recomendaciones para la creación de una contraseña segura [20 de Noviembre de 2012]. Available from: http://cert.inteco.es/Proteccion/Recomendaciones/Crear_una_contrasena_segura/.

11. CCN-CERT. Guía de seguridad (CCN-STIC-821)(borrador) Esquema Nacional de Seguridad. Normas de seguridad. 2012. Available from: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/821-Normas_de_Seguridad_en_el_ENS/821-Normas_de_seguridad-081112.pdf.

12. Resolución: R/02386/2010 de la Agencia Española de Protección de Datos. 2010. Available from: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2010/common/pdfs/PS-00379-2010_Resolucion-de-fecha-26-11-2010_Art-ii-culo-9-LOPD.pdf.

13. Kierkegaard P. Electronic health record: Wiring Europe's healthcare. Computer Law & Security Review. 2011;27(5):503-15.

14. Agencia Española de Protección de Datos. Informe de cumplimiento de la LOPD en Hospitales Madrid 2010. Available from: http://www.agpd.es/portalwe-

bAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/octubre/INFORME_HOSPITALES.pdf.

15. INTECO, Madrid APD. Estudio sobre la privacidad y la seguridad de los datos personales en el sector sanitario español Madrid 2010. Available from: http://www.inteco.es/file/pILW9PPN9b_MIxpjOX2pMw.

RevistaeSalud.com es una publicación electrónica que intenta promover el uso de TICs (Tecnologías de la Información y las Comunicaciones) con el propósito de mejorar o mantener la salud de las personas, sin importar quiénes sean o dónde estén.

Edita: FESALUD – Fundación para la eSalud
Correo-e: cperez@fesalud.org
ISSN 1698-7969