Investigación en Discapacidad
Vol. 3, Núm. 4
Octubre-Diciembre 2014
pp 177-184

Implementación de la seguridad en el manejo de las imágenes médicas

Josefina Gutiérrez-Martínez,* Marco Antonio Núñez-Gaona,* Heriberto Aguirre-Meneses,* Ruth Evelyn Delgado-Esquerra*

* Departamento de Desarrollo Tecnológico. Instituto Nacional de Rehabilitación.

Dirección para correspondencia:
Dra. Josefina Gutiérrez Martínez
Av. México-Xochimilco Núm. 289,
Col. Arenal de Guadalupe,
México D.F. 14389
Tel: +52 (55) 5999 1000,
ext. 16154
E-mail: jgutierrez@inr.gob.mx

Recibido: 28 de abril de 2014.
Aceptado: 1 de noviembre de 2014.

Este artículo puede ser consultado en versión completa en:
http://**www.medigraphic.com/rid**

Abreviaturas
IS = Information systems.
PACS = Picture Archiving and Communication System.
DICOM = Digital Imaging and Communications in Medicine.
HIPAA = Health Insurance Portability and Accountability Act.
ISO = International Organization for Standardization.

Palabras clave: SI, PACS,DICOM, HIPAA, ISO/IEC27002, *Firewall*.

Key words: *IS, PACS, DICOM, HIPAA, ISO/IEC27002, Firewall.*

Resumen

La seguridad en los sistemas de información (SI) que administran las imágenes médicas generadas en una institución hospitalaria es un proceso continuo que tiene como fin conservar la confidencialidad, integridad, disponibilidad de las imágenes y protección de la identidad del paciente en los sistemas de almacenamiento y comunicación denominados PACS (por sus siglas en inglés). La seguridad de los datos es crítica en los procesos de almacenamiento y transmisión a través de una red, especialmente porque las políticas de seguridad de Intranet o Internet no son suficientes para garantizar la privacidad, autenticidad e integridad de las imágenes en formato DICOM. En este contexto, se han creado técnicas de protección como el filtrado a través de *firewall*, cifrado y encapsulamiento de datos para ofrecer una protección adicional. Sin embargo, estas técnicas no se aplican sistemáticamente a los PACS. La parte 15 del estándar DICOM (PS3.15) especifica perfiles y políticas de seguridad, así como medidas técnicas para las entidades de aplicación involucradas en el intercambio de información. En este trabajo se presentan los controles (indicadores), estándares (DICOM) y políticas (HIPPA) que rigen la implementación del diseño y construcción del PACS-INR con el fin de asegurar que las imágenes médicas y los datos del paciente que se utilizan en el Instituto Nacional de Rehabilitación sean transferidos, visualizados y almacenados bajo un esquema de seguridad y privacidad.

Abstract

Security inside institutional information systems in hospitals must guarantee confidentiality, integrity and availability of medical imaging as well as of patients' identity in PACS (patient administration and communication systems). Data in systems are not safe at all, since policies in security of internet or intranet are not enough to ensure absolute privacy, authenticity or integrity of imaging through the DICOM format. Firewall, encryption and encapsulation are procedures designed to provide additional protection of data. However, such procedures are not applied as an absolute rule. Part 15 of DICOM standard PS3.15 specifies profiles and security measures to the appropriate handling of information. In this paper, controls (indicators), standards (DICOM) and policies (HIPPA) are discussed about the design of our PACS-INR in order to ensure the storage, recovering and handling imaging information under a true security and privacy scheme.

Introducción

La seguridad y privacidad de la información son una obligación ética y legal de los gobiernos, las entidades militares, las instituciones financieras, los hospitales y las empresas privadas que deben resguardar información confidencial sobre sus empleados, clientes, productos, investigaciones y en particular la privacidad sobre la información de los pacientes.[1]

A pesar de las ventajas de los sistemas informáticos, el fácil acceso a las redes de comunicación incrementa el riesgo de propagación de la información, ya sea de manera intencional o no intencional.[2]

El objetivo de la seguridad en los sistemas de información (SI) que administran y almacenan datos, es prevenir el mal uso, destrucción y/o modificación de la información por medios no autorizados, así como la reducción o eliminación de riesgos.

Para lograr este propósito se deben mantener los tres principios básicos referidos a la seguridad de la información,[3] que se muestran en la *figura 1* y que a continuación se mencionan:

La confidencialidad es definida por la Organización Internacional de Estandarización ISO (por sus siglas en inglés: *International Organization for Standardization)* en la Norma ISO/IEC27000,[4] como el mecanismo para garantizar que la información y los datos estén disponibles únicamente a personas o sistemas autorizados.

La disponibilidad es la característica, cualidad o condición del SI que permite el acceso autorizado a los datos en cualquier momento y de forma ininterrumpida a través de mecanismos de respaldo y soporte.

La integridad es la propiedad que busca conservar la información libre de modificaciones. Éstas pueden ser provocadas de forma malintencionada por personas o procesos no autorizados o accidentalmente. La integridad de un conjunto de datos se garantiza cuando se adjuntan códigos de verificación, asegurando que la información no ha sido alterada.[5]

Entre los retos a los que se enfrenta la seguridad informática está evitar el acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción de los datos.[6] En este contexto, se busca proteger la infraestructura y los datos contenidos en ella de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas, minimizar riesgos y exposición de la información e implementar un conjunto de controles que abarquen políticas y procedimientos.

La Gestión de Seguridad de la Información (GSI) es un proceso continuo que busca formar y mantener programas, controles y políticas que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información. Para crear sistemas de GSI eficientes es necesario determinar las vulnerabilidades y amenazas que se ciñen sobre cualquier información, considerando las causas de riesgo, la probabilidad de que ocurran y el impacto que puedan tener.

La GSI debe establecerse al mismo tiempo que se determina el diseño del sistema. En esta etapa también se deben identificar los esquemas de seguridad de forma rigurosa y oportuna para evitar situaciones de vulnerabilidad.[7] Se han realizado varios estudios sobre la seguridad para determinar la vulnerabilidad de los sistemas, especialmente en sitios de Internet orientados al comercio electrónico.

En 1996, con la herramienta de detección de intrusos SATAN, creada por Dan Farmer, se analizaron más de 2,000 sitios WEB, encontrándose que varios de esos sistemas estaban abiertos a ataques potenciales o accesos ilegales con probabilidad de causar daño.[8]

Por supuesto, los sistemas informáticos médicos no son ajenos a los tres principios básicos de seguridad de la información, así como a las disposiciones

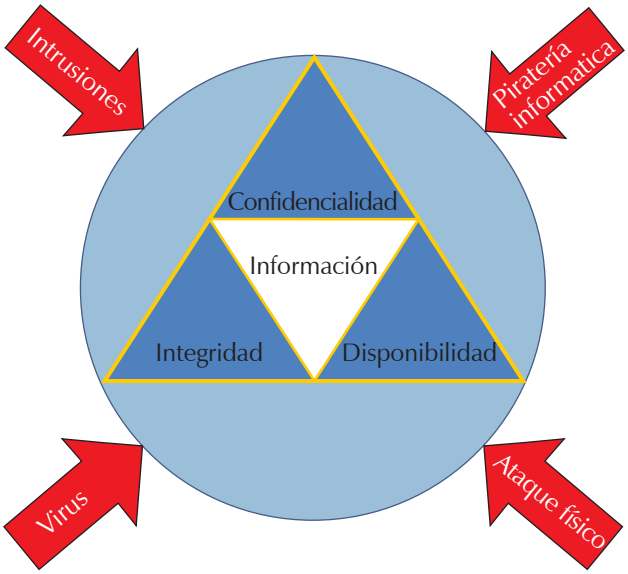

Figura 1. Principios básicos de la seguridad de información. La integración de los aspectos de confidencialidad, integridad y disponibilidad proporciona un esquema de seguridad de la información para prevenir intrusiones, ataques físicos, *hacking* y virus.

y normativas para el manejo de datos confidenciales de los pacientes. En este contexto, este trabajo introduce los aspectos de confidencialidad, integridad y disponibilidad, así como los estándares y protocolos de comunicación involucrados en los sistemas de información médica. Particularmente, el estudio se enfoca al sistema de almacenamiento de imágenes médicas del Instituto Nacional de Rehabilitación; denominado PACS-INR.

Fundamentos

La ingeniería de software y su enfoque en seguridad

La ingeniería de Software representa la aplicación de un enfoque metodológico, sistemático y cuantificable al diseño, desarrollo, operación y mantenimiento del software y hardware de los sistemas informáticos. Integra métodos matemáticos y ciencias de la computación para lograr soluciones costo-efectivas, con el objetivo de elaborar productos de software de calidad confiables, utilizables, seguros, robustos y con alto costo-beneficio.[9]

El diseño de los componentes o elementos de software involucra metodologías que toman en con-

sideración, de forma iterativa e incremental, los requerimientos del usuario, la arquitectura del sistema, las técnicas y las herramientas de implementación. Un punto clave es describir desde etapas tempranas del diseño los requisitos funcionales del sistema, el análisis de dependencias e identificación de requisitos no funcionales (seguridad, fiabilidad y rendimiento).

El enfoque para desarrollar *frameworks* (marco del sistema)[10] dirigidos a la administración de la seguridad se basa en ingeniería de software e integración del modelo de negocios; propone definir, analizar, modelar y mapear los ataques a los cuales el sistema pueda ser susceptible, identificando el entorno operativo y definiendo el tipo de seguridad adecuado para su implementación.

Como se mencionó anteriormente, un aspecto fundamental en la seguridad de los sistemas es la detección de intrusos. En Hossein[11] se analizan diferentes estrategias (evasión pública, evasión basada en debilidades arquitectónicas, evasión basada en el modelo TCP/IP) relacionadas con la estructura de los sistemas para la detección de intrusos IDS (por sus siglas en inglés *Intrusion Detection System);* presenta los nuevos patrones de ataque, las técnicas de prevención y seguimiento, discute las vulnerabilidades, los defectos de seguridad, y los problemas sistémicos para eliminar defectos y reducir intrusiones.

La seguridad de la información en los sistemas informáticos médicos

Un sistema informático médico (SIM) es aquel que maneja, procesa y transfiere información (metadatos-texto, imágenes, video) con el fin de mejorar la gestión y procesos clínicos (diagnóstico y tratamiento), la asignación y control eficiente de los recursos en la unidad hospitalaria para la toma de decisiones en el cuidado de la salud.[12] Los principales riesgos asociados con la información médica son la divulgación de un contenido no autorizado y la alteración de la información de forma intencional, teniendo como consecuencia un diagnóstico y tratamiento erróneos.[3]

Entre las estrategias metodológicas que se han utilizado para la seguridad en sistemas informáticos médicos está TROPOS, la cual se ha aplicado para modelar el proceso de análisis de seguridad de un sistema denominado *eSAP*,[13] que se diseñó para evaluar la efectividad del cuidado a distancia de los adultos mayores. El *eSAP* lo comparten varias dependencias de salud en Inglaterra, con el objetivo de estandarizar la evaluación y el diagnóstico, y generalizar la terapéutica clínica.

Entre las recomendaciones más importantes de estas estrategias está la implementación de acciones tales como: hacer copias de seguridad y recuperación automática, resguardo remoto de copias cifradas y establecer políticas de seguridad; todas ellas encaminadas a asegurar la información en caso de desastres, reducir riesgos y potenciar la productividad.

Los estándares en la informática médica

Los estándares definen un conjunto de reglas que se deben cumplir como requisitos mínimos para garantizar la calidad de un producto, proceso o servicio. La importancia de su aplicación es garantizar la interoperabilidad entre sistemas, permitiendo el uso de diversas tecnologías y diferentes marcas, así como el desarrollo de sistemas eficaces, contemplando un lenguaje específico universal y aspectos de seguridad y privacidad.[14]

En el ámbito de los SIM, la seguridad de la información médica está protegida por la legislación y estrictas reglas éticas. La HIPAA (por sus siglas en inglés; *Health Insurance Portability and Accountability Act)*[15] es una Ley Federal conocida como Ley de «Portabilidad» y Responsabilidad, constituida por primera vez como Ley Pública 104-191 en 1996 en los Estados Unidos e instituida oficialmente el 14 de abril del 2003, obligando a los fabricantes de los SIM a cumplirla en abril del 2005. Esta ley introduce los mandatos del gobierno de Estados Unidos en el desarrollo de una ley nacional sobre privacidad, estándares de seguridad y de transacciones electrónicas para reducir violaciones y accesos ilícitos a la información de salud.

La HIPAA propone mejores prácticas para proteger la confidencialidad, integridad y disponibilidad de la información; en concreto, responde a las necesidades especiales de gestión de seguridad de información del sector salud y sus entornos operativos.

Existen dos estándares para el manejo de la información hospitalaria: HL7[16] (por sus siglas en inglés *Health Level Seven Inc);* ésta es una organización internacional donde se definen los modelos de comunicación para estandarizar el intercambio de información médica entre aplicaciones como el expediente clínico electrónico en el dominio médico, administrativo y de asistencia, por medio del cual se define la arquitectura de documentos clínicos (informe de alta, resumen de diagnóstico, informe de análisis clínicos, citas, farmacia, entre otros). DICOM[17] (por sus siglas en inglés *Digital Imaging and Communications in Medicine*), por su parte, es un estándar cuyo objetivo es asegurar la interoperabilidad entre equipos y sistemas de imáge-

nes médicas heterogéneos, el cual considera la adquisición, transferencia almacenamiento y visualización de imágenes médicas. El estándar DICOM controla en su totalidad el manejo de información relacionada con las imágenes médicas, incluyendo las reglas para transferir las imágenes médicas con seguridad cuando se usan los protocolos de comunicación ISO-OSI y TCP/IP (por sus siglas en inglés ISO /*Open System Interconnection y Transmition Control Protocol/Internet Protocol* respectivamente).[13]

La seguridad en los sistemas PACS

Hoy en día, en las unidades hospitalarias donde se generan anualmente miles de estudios de imagen se dispone de un PACS. Este sistema integra equipos que generan la imagen (modalidades), dispositivos de almacenamiento, servidores de base de datos y visualizadores.[18] Por lo general, estos dispositivos son heterogéneos, así que deben regirse por estándares de interoperabilidad (por ejemplo; DICOM y HL7) para el intercambio de la información a través de una red local o servicio remoto. Los componentes del PACS donde la seguridad de la información es más vulnerable son la red de comunicación (Intranet o el Internet) y el sistema de almacenamiento, como se muestra en la *figura 2*.[19]

El diseño e implementación de los PACS debe integrar esquemas de seguridad para prevenir intrusiones, ataques físicos, piratería informática y virus que puedan corromper las imágenes médicas. Las incidencias de violación en la seguridad se presentan de forma casi cotidiana en estos sistemas,[20] en especial aquellos cuyo acceso es a través de Internet. Es de vital importancia asegurar que los datos e imágenes correspondan al paciente correcto. El PACS debe contar con un sistema robusto de almacenamiento, que a través de un modelo normalizado entidad-relación contenga privilegios de acceso a la información.

Estandarización de la estructura de información en las imágenes DICOM

Un archivo DICOM válido (denominado IOD) contiene información diversa, que va desde los parámetros de adquisición de la imagen (modalidad, marca del equipo, tipo de estudio, técnica empleada) hasta los datos del paciente (identidad y demográficos) necesarios para su correcta identificación.

Para que un IOD se comparta entre entidades de aplicación (EAs) a través de los servicios DICOM (almacenamiento, consulta, recuperación) debe cumplir con la sintaxis y la semántica definidas en el modelo de información DICOM (MID). En este sentido, cualquier modificación de la información puede ocasionar que se aborte la comunicación. En la *figura 2* se muestra la asociación entre dos entidades de aplicación: la primera es un visualizador de imágenes y la segunda un sistema de almacenamiento.

A pesar de que el MID utiliza esencialmente las mismas estructuras de codificación de datos desde hace 30 años, ha demostrado ser eficiente para soportar la integridad y confidencialidad de la información contenida en las imágenes médicas.[19] El esquema del MID está definido en la parte cinco del estándar DICOM (PS 3.5); como complemento del MID se deben considerar tanto los perfiles de seguridad especificados en DICOM así como las recomendaciones emitidas por la HIPPA.

Dentro de las medidas que define DICOM para la seguridad de la información están los esquemas de anonimato, cifrado y compresión de datos.

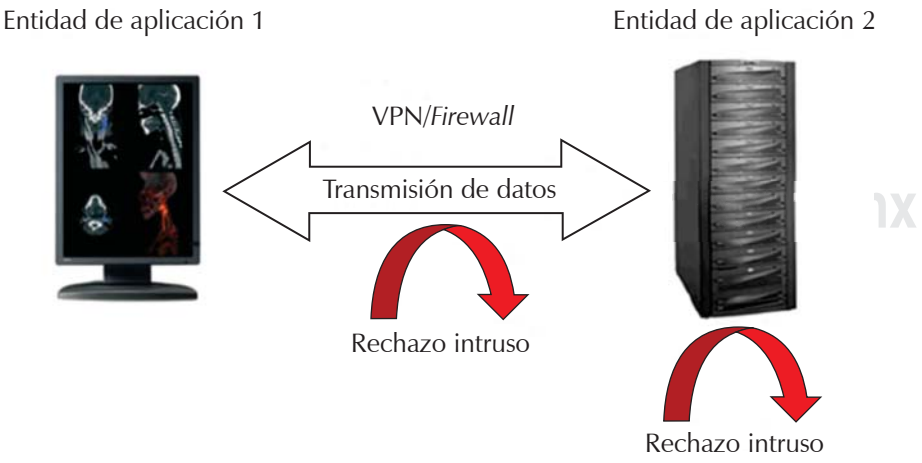

Figura 2.

Protección de datos entre las entidades de aplicación (1 y 2) a través de *Firewall* y VPN's o entornos locales. Adaptado de Pianykh.[19]

Anonimato. La información presentada en el visualizador de imágenes médicas se puede restringir de tal manera que se asegure el anonimato de datos (en particular la identidad del paciente), como se puede mostrar en la *figura 3*.

Cifrado. Existen métodos de cifrado y seguridad en la información así como algoritmos especializados que permiten la recuperación de la información en su formato original a través de una clave.

Compresión. Se deben emplear algoritmos de compresión de imágenes DICOM que garanticen una recuperación de los datos originales.

Los perfiles de seguridad definidos en la parte 15 del estándar DICOM[17] son:

- Perfiles de usuario: Define cómo una EA puede tener acceso al sistema mediante el uso de atributos y otros perfiles de seguridad como acceso remoto, firma digital, etcétera.
- Perfiles de conexiones: Describe los mecanismos de autenticidad de las EAs y los métodos de cifrado de la información.
- Perfiles de firma digital: Define los mecanismos para incluir una firma digital en el conjunto de datos asociado a las imágenes y cuál es el propósito de la misma.
- Perfiles de seguridad en el almacenamiento: Define las especificaciones de acceso y la protección de las imágenes.
- Perfiles de manejo de direccionamiento de red: Define servicios para asignar y gestionar los parámetros IP para una EA de forma remota mediante DHCP (del inglés *Dynamic Host Configuration Protocol)*.
- Perfiles de sincronización de tiempo: Define servicios para sincronizar los relojes en varios equipos, empleando NTP (del inglés *Network Time Protocol)*.
- Perfiles de confidencialidad en los atributos: Indica cómo cifrar los datos de la cabecera de las imágenes.
- Perfiles de administración de configuración de aplicaciones: Explica cómo se almacena la información en un servidor de base de datos LDAP (de sus siglas en inglés *Lightweight Directory Access Protocol)*, qué campos se requieren y cuál es su formato.

La HIPAA

Esta ley ha emitido una serie de recomendaciones de seguridad para proteger la información generada en los equipos médicos y que será transmitida a través de una red de comunicación. A continuación se enuncian las más importantes.[19]

1. Las imágenes médicas (así como otros datos confidenciales), deben residir en servidores dedicados *(Figura 3)*.
2. Se deben implementar mecanismos de respaldo de las imágenes de forma periódica (diario, semanal o mensual).
3. El acceso remoto a la información debe hacerse a través de una red privada virtual (VPN) con acceso restringido y controlado *(Firewall) (Figura 3)*.

Mecanismos de seguridad implementados en el PACS-INR

En el Instituto Nacional de Rehabilitación (INR) se diseñó desde hace varios años (2004) el PACS-INR de alto desempeño, confianza y eficiencia para la transferencia y almacenamiento de imágenes médicas en formato DICOM, soportando imágenes que se generan en las Áreas de Tomografía, Resonancia Magnética, Ultrasonido, Medicina Nuclear y Radiología de la División de Imagenología del INR. Actualmente está en producción, se encuentra instalado en áreas médicas del Instituto donde se requiere el diagnóstico y consulta de imágenes, soportando a 245 usuarios concurrentes aproximadamente.

Cuenta con un sistema de almacenamiento de alta disponibilidad (24 horas, 365 días del año) que utiliza un «framework validado (tecnología EMC^2)» y redundante en los datos, que lleva a cabo un respaldo en tiempo real, utilizando una arquitectura CAS/DAS para asegurar una solución costo-efectiva con mecanismos de alta seguridad.[21] Esta tecnología CAS/DAS ofrece al sistema la capacidad WORM (de sus siglas en inglés *Write Once Ready Many)* para la protección de los datos utilizando el algoritmo de cifrado con dispersión, denominado HMAC-SHA-512. Esta solución

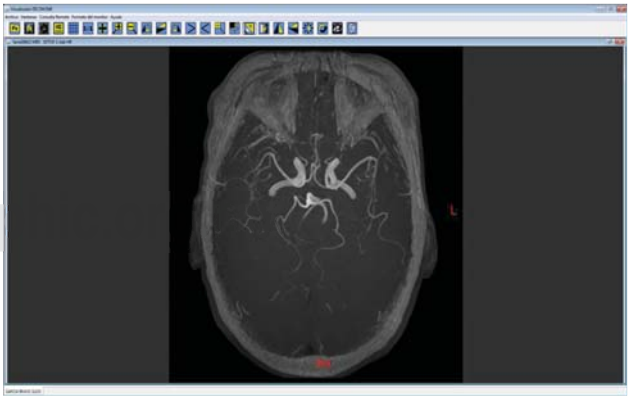

Figura 3. Anonimato de datos del paciente en el despliegue de una imagen DICOM.

automatiza y maximiza la utilización de la información a bajo costo minimizando los riesgos.

En el *cuadro I* se muestran los perfiles de seguridad referentes a la parte PS3.15 DICOM y las recomendaciones HIPPA que el PACS-INR da cumplimiento.

Discusión

La seguridad de la información de los SIMs se refiere a cuestiones tales como el acceso en tiempo durante la consulta, recuperación rápida durante el tiempo de inactividad del sistema y el aseguramiento de la integridad de los datos que certifique información médica correcta, oportuna y confiable, sin dejar a un lado la protección de la privacidad del paciente.

Es necesario implementar controles de eficiencia para asegurar una correcta gestión de la seguridad de la información. Éstos se pueden dividir en: a) cumplimiento de estándares y legislación, b) uso de indicadores del desempeño del sistema, y c) percepción del usuario final (médico).

En este sentido, el servidor del sistema de almacenamiento es responsable de asegurar la confianza, integridad y disponibilidad de los datos almacenados en el PACS-INR; sólo se pueden almacenar imágenes que son adquiridas de las EAs (equipos de imagen-TC, RM, US, RX) autorizadas. Por otro lado, se encarga de la recuperación cuando ocurren desastres en el archivo radiológico digital a través de contraseñas y cifrado. Cuando este sistema está en modo de fallo, se ejecutan procesos manuales para restablecer el estado normal e identificar el problema (por ejemplo, errores en la conectividad de la base de datos, riesgo de integridad de los datos a través de EMC DiskXtender, falta de disponibilidad de los sistemas de archivo, problemas con tráfico de la red, o falla en la conectividad con la EA, entre otros).

Para cumplir con las recomendaciones definidas por las organizaciones internacionales se han establecido los siguientes indicadores:

1. Disponibilidad del sistema PACS-INR (No. de días funcionando/365) x 100).
   En el periodo de enero-junio de 2014 el PACS-INR tuvo una disponibilidad promedio del 98.89, calculada a partir de un total de 181 días. La cantidad de minutos en estado activo fue de 260,536 contra 284 minutos de inactividad, cuya diferencia arroja un total de 180.80 días de funcionamiento neto.

Cuadro I. Estrategias de seguridad implementadas en el PACS-INR.

Estándar	Estrategia	Específico	Descripción
DICOM	Perfil de seguridad	Usuario	Nombre del usuario (médico), dirección IP y puerto
		Conexiones	Autorización de las 245 EAs
		Almacenamiento	Encapsulamiento por modalidades y sistemas de archivos, base de datos asociada y aplicaciones EMC[2]
		Red	Asignación estática de IP para las 245 EAs
		Confidencialidad en los atributos	La información se separa de acuerdo a la estructura del archivo DICOM
	Anonimato	No muestra datos	Se mantiene oculta la identidad del paciente
	Cifrado	Integridad y disponibilidad	Se aplica el algoritmo HMAC-SHA-512-bit
	Copiado	No hay copia remota	Réplica automatizada, por medio del sistema CAS/DAS[21]
HIPPA	Acceso	Local	No se permite el acceso vía internet, ya que no se cuenta con una VPN
	Almacenamiento	Local	Sólo en servidores dedicados
		Acceso Restringido	Sólo se almacenan imágenes provenientes de una EA autorizada
	Respaldo	Automático	Semanal

Cuadro II. Mensajes generados a partir de intentos de intrusión al PACS-INR.

Mensaje	Causa	Fecha	Hora
C-MOVE-RESPONSE Failure - Refused: Move Destination unknown.	Entidad de Aplicación no autorizada.	21/01/2014 13/03/2014 15/03/2014 16/05/2014	11:26 am 13:54 pm 09:15 am 10:35 am
C-MOVE-RSP Study Root Query/Retrieve Information Model - MOVE SOP Class, status #c000H[Failure: Unable to process]	Dirección IP no válida.	09/03/2014 17/06/2014 17/06/2014	07:40 am 10:27 am 10:29 am

2. Incidentes (#interrupciones, %usabilidad, %estudios correctamente identificados). Es importante resaltar que sólo usuarios autorizados tienen acceso al PACS-INR, manteniendo así la seguridad de la información contenida en las imágenes DICOM e impidiendo la extracción no autorizada de datos. Para identificar intrusos se utiliza una tabla de ruteo que valida la dirección IP, el puerto y nombre de la entidad de aplicación solicitante. En el primer semestre del 2014 se identificaron cuatro intentos de intrusión al sistema por entidades de aplicación no autorizadas y tres más por direcciones IP no válidas, a través del mecanismo de copia ilegal del visualizador DICOM-INR. Esto fue identificado por los registros generados, definidos por las políticas de seguridad del PACS INR, impidiendo la recuperación de imágenes médicas *(Cuadro II)*.

Por último, el PACS-INR está alineado a las especificaciones establecidas en el estándar DICOM incluyendo las medidas de seguridad de parte PS3.15, así como de las recomendaciones propuestas por la HIPPA. La perspectiva del PACS-INR en referencia a la seguridad de la información radica en el análisis de los requerimientos para dar cumplimiento al estándar ISO/IEC 27002.

Esto fortalecerá la calidad del sistema y permitirá establecer controles estandarizados con el fin de auditar la gestión de la seguridad de la información del PACS-INR.

Bibliografía

1. Cushman R. Information and medical ethics: Protecting patient privacy. IEEE Technology and Society Magazine. 1996; 15 (3): 32-39.
2. Hodge JG, Gostin LO, Jacobson PD. Legal issues concerning electronic health information: privacy, quality, and liability. JAMA. 1999; 282: 1466-1471.
3. Lim E. Data security and protection for medical images. In: Biomedical information technology by dagan feng. Ed. Elsevier, 2008, pp. 249-257.
4. International Standard ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements. Disponible en: http://www.iso27000.es/iso27000.html
5. International Standard ISO/IEC 7498-2. Information technology, Open Systems Interconnection, Basic Reference Model-Part 2: Security Architecture, International Organization for standardization: 1989. Disponible en: http://www.iso.org
6. Zio E. Reliability engineering: old problems and new challenges. Reliability Engineering & System Safety, 2009; 94 (2): 125-141.
7. Anderson R. Security engineering: a guide to building dependable distributed systems, 2nd Edition. Wiley Computer Publishing, 2008.
8. Metcalf L, Spring J. Passive detection of servers; software engineering institute technical report. CERT division. 2003; pp. 29.
9. Sommerville I. Software engineering. Addison-Wesley, 9th Edition 2011.
10. Alotaibi Y, Fei L. A novel framework to model a secure information systems. International Conference on Information and Computer Applications. 2012; 24: 84-89.
11. Jadidoleslamy H. Weakness, vulnerabilities and elusion strategies against intrusion detection systems. International Journal of Computer Science & Engineering Survey. 2012; 3 (4): 15-25.
12. ISO/TR 20514:2005. Health informatics-electronic health record-definition, scope and context 2005. Disponible en: http://www.iso.org/iso/home/store/catalogue tc/catalogue detail.htm?csnumber=39525
13. Mouratidis H, Giorgini P, Gordon M. When security metes software engineering: a case or modelling secure information systems. Information Systems. 2005; 30: 609-629.
14. Hammond E, James C. Standards in Medical Informatics En: Biomedical. Informatics: Computer Applications in Health Care and Biomedicine, 3rd Edition 2006; pp. 265-311.

15. HIPAA Security Standard. Health Insurance Portability and Accountability 2003. Disponible en: http://www.cms.hhs.gov/hipaa/ hipaa2/regulations/security/03-3877.pdf
16. HL7 Health Level Seven Standards Version 3.0. An application protocol for electronic data exchange in health care environments. 2003. Disponible en: http://www.hl7.org/implement/standards/index.cfm?ref=nav
17. DICOM. Digital Imaging and Communications in Medicine Standard, Part 1: Introduction and Overview. National Electrical Manufacturers Association PS. 3.1-3.18, 2009.
18. Gutiérrez J, Martínez A, Núñez MA, Baltazar R, Delgado R, Muñoz JE et al. Sistema PACS-CNR: Una propuesta tecnológica. Revista Mexicana de Ingeniería Biomédica. 2003; 24 (1): 77-85.
19. Pianykh O. Digital Imaging and Communications in Medicine (DICOM) Cap 11. DICOM Media and Security Springer 2nd Edition. 2012, pp. 243-262.
20. Krens R, Spruit M, Urbanus N. Evaluating Information Security Effectiveness with Health Professionals. In: Fred AA, Filipe JJ, Gamboa H (Eds.) Communications in Computer and Information Science 274, BIOSTEC 2011; pp. 324-334.
21. Gutiérrez-Martínez J, Núñez-Gaona MA, Aguirre-Meneses H, Delgado-Esquerra RE. A software and hardware architecture for a high-availability PACS. J Digit Imaging. 2012; 25 (4): 471-479.