RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE CONSULTA DE HISTORIA CLÍNICA A TRAVÉS DE LA WEB

Elkin Andrés Alquichides Fajardo
Universidad Piloto de Colombia
Bogotá, Colombia
andrewk_477@yahoo.com

Resumen: *Actualmente la información de historia clínica de las personas tiende a ser divulgadas sin su previa autorización, trayendo por objeto problemas legales. En el presente artículo se analiza y se da recomendaciones sobre el manejo de información sensible como los datos personales a través de la Web, buscando hallazgos de posibles vulnerabilidades y amenazas, garantizando que la información del usuario se encuentra segura. Estas recomendaciones se basan en experiencias desde la parte profesional que a su vez van ligadas al obligatorio cumplimiento de leyes y legislaciones Colombianas.*

Palabras Claves*: Dato sensible, Leyes, Normas, Riesgo, Seguridad de la Información, Servicio Web.*

Abstract: *Currently the information history of people tend to be disclosed if its authorization, bringing objective legal problems. In the present article it analyzes and gives recommendations on handling sensitive information such as personal data via the Web, looking for findings of possible vulnerabilities and threats, ensuring that user information is safe. These recommendations are based on experiences from the professional part which in turn are linked to the enforcement of laws and Colombian legislation.*

Keywords: *Sensitive data, Laws, Regulations, Risk, Information Security, Web Service.*

1 INTRODUCCIÓN

Hoy en día el manejo referente a los datos privados de las personas es importante, más si se trata de información confidencial de su estado de salud, el usuario tiene derecho al acceso a Consultar su Historia Clínica en cualquier momento y lugar. Gracias a las nuevas tecnologías estas consultas deben realizarse de forma segura, teniendo en cuenta los principios de la Seguridad de la Información, se debe garantizar que la información sensible esté libre de amenazas y vulnerabilidades.
Cada vez aparecen delincuentes informáticos que recolectan datos privados de los usuarios para fines maliciosos.
Para prevenir y proteger estos datos se deben realizar pruebas para encontrar posibles vulnerabilidades, esto se hace mediante ethical hacking, es una herramienta de prevención. Al finalizar estas pruebas el resultado se envía mediante un informe señalando las incidencias encontradas, para así tomar medidas inmediatas y prevenir riesgos que puedan afectar la información de los usuarios.

Es importante proteger estos servicios ya que las empresas día a día invierten en estos temas de seguridad ya que para ellos lo más importante es garantizar al usuario que el tratamiento de su información se está realizando de la mejor manera.

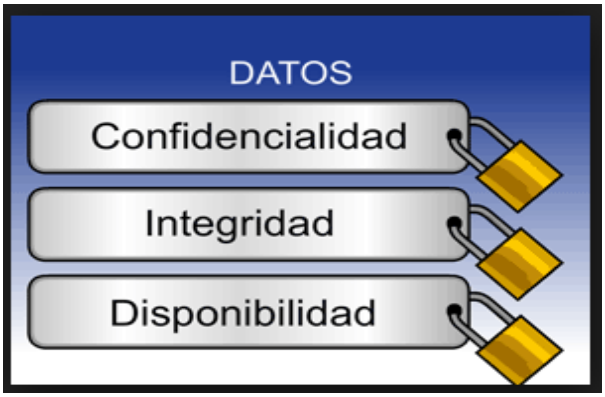

Figura 1 Principios de la Seguridad de la información.
(ISMS, 2011)

El propósito fundamental como experto de la Seguridad de la información es dar recomendaciones para la implementación de consulta de Historia Clínica a través de la Web, para ello es importante tener en cuenta varias normas, resoluciones y leyes que se rigen en Colombia, así respetar los derechos fundamentales que se rigen en la Constitución Política de Colombia de 1991 enmarcado en el **Titulo II. De los Derechos, las Garantías y los Deberes, articulo 15 "**Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".

También conocer y aplicar la siguiente reglamentación.

- **Resolución 1995 de 1999**, establece todas las normas para el manejo y custodia de Historia Clínica.
- **Ley Estatutaria 1751, articulo 10. Derechos y deberes de las personas, relacionados con la prestación del servicio de salud, numeral g**, "A que la historia clínica sea tratada de manera confidencial y reservada y que únicamente pueda ser conocida por terceros, previa autorización del paciente o en los casos previstos en la ley, ya poder consultar la totalidad de su historia clínica en forma gratuita y a obtener copia de la misma".
- **Ley Estatutaria 1581 de 2012,** disposiciones generales para la protección de datos personales.

2 METODOLOGÍA

Para este caso recomiendo utilizar la metodología **MAGERIT.**

Magerit- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Es una metodología que se utiliza para analizar los riesgos soportados por las TIC, se lleva mediante guías informales, aproximaciones metódicas y herramientas de soporte, el objetivo principal de este método es analizar los riesgos para saber cuan seguros o inseguro esta le compañía.

2.1 ANÁLISIS DE RIESGO

Los aspectos más importantes en el análisis de riesgo son los siguientes:

- Definir que quiero proteger.
- Establecer importancia de la protección.
- Determinar las probabilidades de amenazas.
- Implementar controles que protejan mis activos (tangibles/intangibles).
- Realizar seguimiento y dar mejoras.

2.2 TRATAMIENTO DEL RIESGO

El tratamiento del riesgo se realiza de la siguiente manera:

- Eliminar el riesgo, se debe eliminar los activos a los que el riesgo está asociado.
- Transferir el riesgo, se valora la subcontratación del riesgo externamente.
- Asumir el riesgo, no tomar medidas de protección contra el riesgo.
- Mitigar el riesgo, aplicar medidas de seguridad.

2.3 NORMAS INTERNACIONALES

También recomiendo aplicar los controles de las siguientes normas internacionales como ISO 27001, ISO 27002, ISO 27005 e ISO 31000.

2.4 RECOMENDACIONES ANTES DE LA IMPLEMENTACIÓN

Una vez realizado el análisis de riesgo y haber definido la importancia de saber la información que quiero proteger, además teniendo en cuenta las amenazas y vulnerabilidades que se puedan presentar me permito dar las siguientes recomendaciones antes de implementar y/o poner en marcha el nuevo sistema de consulta de Historias Clínicas para la Compañía:

- Segmentar la información, es decir que quiero mostrar.
- Realizar pruebas a la aplicación antes de salir a producción.
- Asegurar y realizar pruebas de penetración del servidor donde se aloje el servidor.
- Controlar quien tiene acceso a estos datos.
- Generar logs de auditoria, saber quién, cuando y donde genero la información.
- Los datos solo pueden ser consultados por mayores de edad.
- Definir un sistema de autenticación, puede ser Key chain, es un sistema de gestión de contraseñas, también se conoce como llavero allí se almacenan diferentes tipo de datos, como contraseñas, servidores FTP, SSH, recursos compartidos de red, redes inalámbricas, certificados de autenticación.
- La información del usuario debe ser descargada mediante un archivo tipo PDF.
- El documento PDF debe solicitar el número de documento del usuario para abrir el archivo.
- Manejar certificados SSL.
- Manejar un consecutivo de consultas.
- Manejar claves seguras.
- No manejar sesiones simultaneas
- Confirmación de datos básicos, preguntas de seguridad.
- Registro de usuario y contraseña.
- Acuerdo de confidencialidad Bajo ley.
- Establecer criterios de búsqueda para aquellos pacientes que requieran una historia clínica más detallada ejemplo: consultas pre anestésico, hojas de uci, hojas quirúrgicas, notas de enfermería, conciliación de medicamentos, medicamentos administrados.

2.5 RECOMENDACIONES DESPUÉS DE LA IMPLEMENTACIÓN

Ahora bien, es importante realizar seguimiento mediante métodos que me permitan continuar con el buen funcionamiento de la aplicación. La metodología que recomendaría para controlar estos riesgos es la

metodología de **MAGERIT** mencionada el punto anterior, al igual que se deben llevar a cabo los controles establecidos en las siguientes normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000.

Los controles de gestión y seguimiento para esta aplicación de acuerdo a los resultados del análisis de riesgos son los siguientes:

- Manejar sistemas de autenticación.
- Realizar pruebas de penetración, tanto internas como externas, el Software que recomendaría para estas pruebas es NESSUS, es una aplicación de seguridad para aplicaciones Web.
- Tener controles en capas, sirve para detectar y bloquear ataques tempranos al servidor.
- Implementar defensa en profundidad, como secuestros de sesión.
- Almacenamiento de logs.
- Encriptar la información de la red.
- Crear reglas al servidor de autenticación.
- Utilizar herramientas de análisis de vulnerabilidades.
- Clasificar las vulnerabilidades:
  - Criticas
  - Altas
  - Medias
  - Bajas
  - Informativas
- Capacitación y sensibilización al usuario interno.
- Crear políticas para la protección del servidor Web.
- Limitar el tiempo de inactividad.
- Limitar la cantidad de ingresos fallidos.

- Usar nmap para saber si existen ataques.
- Descargar las últimas versiones de los navegadores.
- Control de Acceso regular, manejar derechos de acceso, se define a través de grupos. Las cuentas de usuario se generan de forma automática.
- Stateful firewall, el objetivo principal es el filtrado de paquetes, esto se hace a través de un firewall de arquitectura que examina cada paquete, por ejemplo de puede dejar solo para que examine el encabezado y/o también el contenido a través de la capa de aplicaciones.
- Inline intrusión, se puede controlar mediante sistemas de prevención de intrusos (IPS), que se pueden controlar mediante el host, los objetivos principales de este mecanismo es de escanear los dispositivos de red, suplantaciones.

- Correlación de eventos, es manejar una gestión de accesos e identidades a sistemas, la gestión de documentos y la gestión de evidencias, la idea es recopilar toda esta información y mantener un objetivo específico que es la garantizar una seguridad eficiente.

2.6 MECANISMO DE SOLUCIÓN

Una vez definido los controles que se recomiendan utilizar para mitigar el riesgo es viable adoptar un modelo enfocado en el manejo de procesos se puede realizar mediante ciclos continuos como PHVA.

Los controles a evaluar son los siguientes:

2.6.1 Manejar sistema de autenticación

Propongo implementar métodos de autenticación, lo importante es garantizar que el usuario establecido es realmente el que ingresa, los mecanismos de control de acceso son:

- Doble autenticación
- Códigos Captcha

"El NIST (*National Institute of Standards and Technology*) provee entre otras, las recomendaciones para implementar sistemas de autenticación. La seguridad en la autenticación, la divide en cuatro niveles, de los cuáles **el tercer nivel hace referencia a la protección de acceso a la red de forma remota mediante factor de múltiple autenticación**. Este estándar reúne, además, las **características que deben tener los sistemas para garantizar la seguridad en la autenticación**, describiendo su uso y tipos de acuerdo al factor de protección elegido (credenciales, Tokens, procesos de autenticación, *assertions*)." (Amaya, s.f.)

Planear	*Hacer*	*Verificar*	*Actuar*
Definir política de seguridad	*Establecer políticas de control de acceso*	*Actualización de la norma*	*Mejoramiento continuo de la Seguridad*
Llevar a cabo mecanismos de control de acceso	*Implementación de sistemas de autenticación, se recomienda utilizar doble autenticación y/o códigos captcha*	*Realizar pruebas de fuerza bruta, verificación de reglas del Firewall*	*Mejoramiento continuo de la Seguridad*
Identificar y evaluar los riesgos	*Aplicar los 7 controles de la Norma ISO 27002, Dominio 11*	*Realizar listas de chequeo*	*Mejoramiento continuo de la Seguridad*

Figura 2 Procesos de Gestión.
Fuente: El Autor

2.6.2 Realizar pruebas de penetración

Existen varios programas que tienen como funcionalidad la búsqueda de amenazas y vulnerabilidades, algunas

de estas aplicaciones son gratuitas y otras no, las herramientas más importante para este tipo de evaluación son:

- Nessus
- Acunetix
- Open Vas

Además recomiendo utilizar la herramienta de pruebas para proyectos de seguridad para la Web conocida como OWASP.

"OWASP (acrónimo de Open Web Application Security Project, en inglés 'Proyecto abierto de seguridad de aplicaciones web') es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera"
(http://es.wikipedia.org/wiki/Open_Web_Application_Security_Project, 20113)

2.6.2.1 Nessus

En esta implementación recomiendo utilizar Nessus , es una herramienta que realiza el escaneo de vulnerabilidades, allí me permite crear políticas y reglas de escaneo, además que su funcionalidad es cliente servidor, acepta solo conexiones HTTPS, no permite conectarse a HTTP sin cifrar.

Se puede operar bajo cualquier sistema operativo, el escaneo se puede realizar tanto a la Web como a la red. Además clasifica las vulnerabilidades en críticas, altas, medias, bajas, informativas. Los resultados me permite descargarlos mediante archivos PDF y HTML.

También se puede utilizar como modelo de autenticación ya que maneja software de cifrado PGP, esto es muy utilizado en cajeros automáticos y pines. Nessus realiza auditorias mediante credenciales, el análisis de estos resultados determinan si las contraseñas son correctas. Además se recomienda utilizar adecuadamente una herramienta que muestre la información de la red, estado de los puertos y servicios de los sistemas operativos esta herramienta de búsqueda puede ser Nmap.

Planear	*Hacer*	*Verificar*	*Actuar*
Definir el Plan de Seguridad	*Implementación de una herramienta de escaneo.*	*Realizar Pen Test*	*De acuerdo a los hallazgos encontrados en las pruebas se debe tomar medidas correctivas para prevenir cualquier amenaza*
Definición de reglas del Servidor WEB	*Implementar las restricciones de seguridad de los Servicios Web*	*Evaluar las reglas implementadas*	*Mejoramiento continuo de la seguridad*
Definición de la exposición de datos sensibles	*Implementar un almacenamiento de contraseñas convertidas en MD5*	*Realizar pruebas para descifrar contraseñas*	*Realizar ajustes necesarios de acuerdo a los resultados obtenidos*

Figura 3 Procesos de Gestión.
Fuente: El Autor

2.7 CIFRAR LA INFORMACIÓN

Cifrar la información es un mecanismo que protege los datos importantes para ese caso son los antecedentes clínicos de los pacientes, se hace mediante una fórmula matemática o algoritmo y una llave que convierte los datos en un texto plano fácil de entender para el usuario. Por lo general estas llaves son una larga cadena de números protegidos mediante un sistema de autenticación como claves, dispositivos biométricos y huellas digitales.

Hoy en día la información que se transmite a través de la Web es vulnerable si los datos no están cifrados, un mecanismo de protección importante en línea es el uso de HTTPS o conexiones seguras, muchos navegadores traen por defecto esta protección, cabe destacar que se debe revisar las últimas actualizaciones de los mismos.

Si la conexión se realiza a través de una red Wi-Fi pública se recomienda utilizar red cifrada. WPA2 es un sistema de cifrado bastante fuerte y uno de los más usados por los Oficiales de la Seguridad de la Información. Para cifrar la información es considerable tener en cuenta:

- Usar algoritmo como AES (Advance Encryption Standard) son sistemas de cifrado para dominios públicos.
- Respaldar la información confidencial de forma segura, en caso dado que el usuario pierda la llave o clave solo pueda ser recuperada por el propietario de los datos.
- El cifrado no funciona contra virus, troyanos o ingeniería social, para esto es bueno mantener la seguridad de los dispositivos de almacenamiento.

2.8 SEGURIDAD EN LA NUBE

La nube es un modelo que reduce los costos a las empresas, proporciona al usuario el acceso a la información en cualquier momento y lugar, este servicio se realiza a través de un proveedor. Las principales ventajas de este modelo son las siguientes:

- Independiente de la ubicación
- El servicio es medible
- Autoservicio bajo demanda

Lo más importante es que la información está bajo el control del proveedor, ya que ellos mismos tienen mejores procesos de seguridad en la información garantizado la confidencialidad e integridad de los datos de los usuarios y estableciendo políticas de privacidad.

Para la seguridad de la nube existen varias amenazas, una de las más frecuentes son las filosóficas y de procedimiento, esto se soluciona implementando gestión de riesgos, gestión de identidades, protección de la información y uso de estándares. La seguridad en la nube se lleva mediante tres niveles de servicios (IaaS, PaaS y SaaS) son controlados y operados por el operador de servicio. Además es bueno implementar soluciones de modelado para controlar lo que es privado y público.

3 RECOMENDACIONES

Es importante que las organizaciones manejen la responsabilidad en el tratamiento de los datos personales, las personas encargadas de este tratamiento deben implementar medidas que cumplan con los principios de la seguridad de la información, para esto existen guías o instrumentos que validan bajo fundamentos básicos para la gestión de datos personales.

La Superintendencia de Industria y Comercio en mayo del 2014 lanzo la Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability). Es un programa que está encaminado en la construcción de planes integrales para la gestión de datos personales, está dirigido a quienes estén sometidos a las empresas que manejen banco de datos, esta guía la pueden descargar en el siguiente link: (http://www.sic.gov.co/drupal/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada).

En Colombia existe un directorio público que administra el tratamiento de los datos personales, se conoce como el Registro Nacional de Bases de Datos, es administrado por la Superintendencia de Industria y Comercio, todo el tema de regulación y registro está a cargo del Gobierno Nacional, cualquier incumpliendo o falla acarrea las sanciones pertinentes.“Superintendencia de Industria y Comercio (SIC) impuso multas por un valor total de $1.892 millones a 46 empresas que violaron el Habeas Data (protección de datos personales). Se presentaron además 4.889 quejas y se impartieron 153 órdenes administrativas de eliminación, corrección o actualización de información en bases de datos.” (Cubillos, 2015).

4 CONCLUSIONES

De acuerdo al análisis y búsqueda realizada referente al manejo de datos personales se encuentra que somos vulnerables a diferentes situaciones tanto de suplantaciones como de engaño, esto se puede mitigar siempre y cuando autoricemos que información queremos divulgar.

La información que contiene la Historia Clínica es de carácter personal, solo es de interés al titular, por ello es importante dar un adecuado tratamiento para que los datos que se transmiten a través de la Web lleguen de forma segura.

También es importante educar al usuario, es decir generar campañas de sensibilización y generar confianza, mostrarle que riesgos puede obtener en la mala utilización de la herramienta de consulta de Historia Clínica.

Cabe mencionar que en Colombia existen Leyes que regulan el tratamiento de la información, también es responsabilidad de las empresas prestadoras de servicios de salud que cumplan con la custodia de la Historia Clínica, ya que el usuario tiene derecho a saber su estado de salud en cualquier momento y por cualquier medio.

Antes y después de realizar la implementación es importante realizar pruebas de Ethical Hacking, Ingeniería Social y Auditorias s internas para mitigar el riesgo.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] COLOMBIA, EL CONGRESO, Ley estatutaria 1581 de 17 de Octubre de 2012, por el cual se dictan disposiciones generales para la protección de datos personales.

[2] CERTICAMARA, ABC Para proteger los datos personales, Ley 1581 de 2012 Decreto 1377 de 2013. [En línea] {Diciembre 2013}. https://www.colombiadigital.net/entorno-digital/articulos-de-contexto/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html.

[3] WELIVESECURITY, La autenticación en el compliance de los principales estándares mundiales. http://www.welivesecurity.com/la-es/2013/04/25/autenticacion-compliance-principales-estandares-mundiales/.

[4] Metodologia para la gestion de la seguridad informatica. http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

[5] Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability), disponible en: www.sic.gov.co/drupal/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada.

[6] NIST, Special Publication 800-63-2. http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf.

[7] Figura 1, Principios de la seguridad de la información, ISMS 2011. http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=7&id_tema=63.

[8] Figura 2 Procesos de Gestión. Fuente el autor.

[9] Figura 3 Procesos de Gestión. Fuente el autor.

6 AUTOR

Elkin Andrés Alquichides Fajardo
Ingeniero de Sistemas, egresado de la Fundación Universitaria Panamericana
Estudiante de Seguridad Informatica en la Universidad Piloto de Colombia
Actualmente me desempeño como Administrador del Sistema en Clinica Colsanitas
Junio 2015.