UNIVERSIDAD CENFOTEC

MAESTRÍA EN CIBERSEGURIDAD

Documento final de Proyecto de Investigación Aplicada 2

"IMPLANTACIÓN DE HIPAA EN COSTA RICA".

Alpírez Monge Esteban

Febrero, 2018

Dedicatoria y agradecimientos.

Terminar una etapa satisfactoriamente siempre es causa de alegría, es por esto que el presente trabajo quiero dedicárselo primeramente a Dios por darme salud y vida y en segundo lugar a mis padres por haberme ayudado económicamente durante todo el tiempo que fui estudiante de esta maestría; sin ellos nada de esto hubiese sido posible.

Tabla de Contenido

1. Contenido

2. Abstract o resumen ejecutivo

Este trabajo consiste en una propuesta de implementación del estándar HIPAA en Costa Rica. HIPAA trata el manejo de información de pacientes y cómo se debe administrar de forma segura.

Esta investigación se fundamenta en la revisión bibliográfica de fuentes enfocadas en distintas aristas de la seguridad; no solo a nivel del uso que una aplicación haría a la información, sino también la manera de almacenarla, accederla, permisos, perfiles, transporte y formato, entre otros.

Definir y analizar los puntos anteriores, permitirá luego de hacer un estudio en dos aplicaciones, de dos distintas instituciones, mencionar las brechas en la realidad costarricense para que este HIPAA sea adoptado.

3. Introducción

3.1. Objetivos

3.1.1. Objetivo general

Desarrollar una guía para la implementación del estándar HIPAA en empresas costarricenses dedicadas a la salud.

3.1.2. Objetivos específicos

Los objetivos específicos concernientes al presente trabajo de investigación serán los siguientes:

- Definir qué es HIPAA, cuál es su intención, cuáles son sus lineamientos y qué trata de asegurar.
- Interiorizar conceptos de HIPAA.
- Definir los requisitos mínimos para el cumplimiento de la norma, basados en los componentes de HIPAA.
- Tipificar las brechas para el cumplimiento de la norma con respecto al estándar HIPAA en dos entidades que procesen información de salud o pacientes. Se utilizan conceptos sin un proveedor específico.

4. Marco teórico

HIPAA, en español, por sus siglas en inglés entenderíamos que es la Ley de Responsabilidad y Transferibilidad de seguros médicos. Esta ley fue aprobada el 21 de agosto de 1996 por el Congreso de los Estados Unidos, pero entró en vigor el 14 de abril de 2003. Establece estándares para transacciones electrónicas de salud, además de alejarse de los registros engorrosos en papel y da un mayor énfasis en la seguridad y privacidad de los datos de salud.

HIPAA fue concebida con la intensión de regular y ser una reforma para algunos aspectos del mercado de seguros de salud y al mismo tiempo facilitar los procesos administrativos asociados a la salud. Está pensada para garantizar el derecho a la privacidad y confidencialidad.

Nos encontramos sin duda alguna en la era de la información, no hay forma de invalidar este hecho. Lo cual implica que un dato, un registro, una descripción es siempre valiosa para algún grupo u organismo. La información de salud, es quizá una de las más sensibles, debido a que compromete el estado mental o físico de un sujeto. Una condición anormal podría complicar un proceso de contratación o de hacerse pública la información de un paciente, este podría tener inconvenientes para contractar un seguro médico o peor aún, los mismos aseguradores podrían negarse rotundamente a brindar el servicio.

La importancia del punto anterior, quizá no suene tan alarmante en un país como el nuestro, donde la salud es administrada, al menos principalmente por una entidad gubernamental o donde los seguros no se le niegan a nadie, al menos actualmente. Pero en los Estados Unidos, donde la salud es controlada en su mayoría por el sector privado, obtener un seguro puede ser de vida o muerte.

No obstante, en nuestra realidad nacional esta información no carece de valor y con el auge de las aseguradoras privadas o los hospitales seculares, más de un individuo podría beneficiarse o perjudicarse, de hacerse pública una base de datos de pacientes y más aún, si estas cuentan con patologías. Hoy en día cuando un individuo solicita un seguro de salud, se preguntan sus padecimientos, los ya existentes reportados normalmente son excluidos del contrato y el asegurado deberá correr con ellos por su cuenta. Ahora bien, de ser públicos datos como patologías, padecimientos crónicos, historial de tratamientos o cualquier otra información de salud, estas aseguradoras podrían ser muy efectivas a la hora de garantizar o negar coberturas; esto repercute negativamente en la sociedad que requiere sus servicios.

Otro caso interesante sería analizar lo que una organización dedicada a préstamos o una entidad bancaria podría hacer con información sensible, manejada por una organización como la CCSS, donde se almacenan datos como nombre, apellido, números de teléfono, historial de salarios, cuotas, entre otros. Esta información no

solo le permitiría poder rechazar u aceptar un cliente, sino que le permitiría realizar estimaciones poblacionales muy útiles.

Costa Rica cuenta con legislación que protege los datos. Incluso existe un ente encargado de velar por la protección de los datos de los individuos, la PRODHAB (Por sus siglas Agencia de Protección de Datos de los Habitantes), entre sus objetivos tiene garantizar a cualquier individuo su autodeterminación informativa de vida o actividad privada. La ley 8968 trata todos estos temas con mayor detalle (PRODHAB, s.f.). Agregar una certificación adicional como HIPAA a la PRODHAB podría ser un tópico que daría valor y robustez al uso de información confidencial entre organizaciones de salud; sin embargo, es algo que tardaría muchos años e implicaría mucho esfuerzo. No obstante a corto plazo, brindar herramientas para la capacitación a individuos seculares que se encarguen de dar valor a la protección de datos mediante el cumplimento de HIPAA, es uno de los fines de esta investigación; proveer una guía que permita a organizaciones conocer su grado de madurez de HIPAA, lo cual reflejará su grado de protección de información de pacientes.

HIPAA hace hincapié explícito en la salvaguarda de la información protegida de salud, mejor conocida como PHI (Por sus siglas en inglés Personal Health Information).

La información de salud implica cualquier dato, ya sea verbal o registrado en cualquier medio, que es creado o recibido por un proveedor de salud, plan de salud, autoridad pública o privada de salud, empleador, asegurador, escuela o universidad.

¿Pero que es PHI? Si existe información presente, pasada o futura que denote una condición física o metal de algún individuo y esta permita identificarlo directamente o que de alguna forma ayude a hacerlo, entonces estaremos hablando de PHI.

Existen tres reglas básicas de HIPAA, la Regla de Privacidad de HIPAA que cubre PHI de cualquier tipo, ya sea física, verbal o virtual, pero la regla de seguridad es exclusiva de PHI de forma electrónica o ePHI (Por sus siglas en inglés Electronic Protected Health Information), finalmente la regla de notificación de violaciones de seguridad cubre el manejo de casos en los que existe incumplimiento en el manejo de información o si hubo una fuga de esta.

La clave para la protección de la información radica en estos aspectos:

- ¿Cómo se almacena la información?
    - Aquí se debe definir no solo las reglas de seguridad del o los repositorios de información, sino, quiénes tienen acceso al área física, qué controles deben haber para visitantes y los tipos de perfiles de acceso a la información, directamente en el repositorio.
    - Entre los controles de seguridad con que debe contar el área donde se almacene ePHI están:
        - Autenticación de doble factor: Si una persona dentro del data center o instalaciones físicas no está siendo escoltado, debe siempre portar un badge que lo identifique. Este badge, puede servir para identificarlo, pero también requerirá otro método, tal y como un código de acceso o un dispositivo biométrico.

      Si se está visitando las instalaciones y no se le ofrece un badge temporal al visitante o si no se mantiene un registro de ingresos, se puede concluir fácilmente que la seguridad es ineficiente.

      Las instalaciones deben contar con video vigilancia y los registros de esta deben permanecer hasta por 90 días (HIPAA Compliant Hosting, 2012).

- ¿Qué Consideraciones técnicas se manejan?
    - HIPAA no define cómo se deben implementar controles a nivel técnico, pero sí indica qué se debe hacer; los aspectos más relevantes son:
        - Identificación única de usuario: Esta debe permitir llevar una bitácora de la actividad de aquellos que interactúen con los sistemas,
        - Procedimiento de emergencia: Debe existir un proceso de emergencia para poder acceder información sensible en caso de una eventualidad.

- Cierre de sesión automático: Siempre que se produzca inactividad por parte del usuario de un sistema que interactúe con ePHI, tal sistema deberá bloquearse.
- Cifrado y descifrado: Curiosamente este no es un aspecto obligatorio, pero sí recomendado.
- Controles de auditoría: Mecanismo para monitorear las actividades de los usuarios dentro de los sistemas (HIPAA Compliant Hosting, 2012).

- ¿Cómo trafica la información?
  - Por cuál medio viaja la información y cómo viaja a su destino, esto es que el método sugerido para garantizar la seguridad de la ePHI son los protocolos de comunicación; si esto no se cumple los datos se deben encriptar.
  - Otro factor muy llamativo de la implementación de HIPAA es el formato en el que debe viajar; esto es su interrelación con diferentes sistemas de información. HIPAA establece un estándar de tráfico de información a través de una estructura ASC X12. Esto significa que todos los sistemas que sigan HIPAA hablarían el mismo idioma, es un avance significativo en intercambio de información entre sistemas.
  - ASC X12 viene del Comité de Estándares Acreditados (Accredited Standards Committee), que desarrolla un estándar de intercambio de información para mercados nacionales y globales. X12 mantiene estándares y guías asociadas para múltiples tipos de comercio electrónico. HIPAA finalizó la transición de la versión ASC x12 4010 y 4010 A a la versión 5010 en 2009 (ANSI ASC X12 Standards Overview Tutorial).

- ¿Quién y cómo se accede la información?
  - Cada aplicación que administre, reciba o alimente información de salud deberá contar con un conjunto de usuarios y métodos para autenticación de estos. Un mecanismo que garantice que, quien está

ingresando es quien es y que el contenido que accede sea para el que está autorizado (HIPAA Compliant Hosting, 2012).

Todos los aspectos ya mencionados cubren los pilares básicos de la seguridad que son:

- Integridad.
- Disponibilidad.
- Confidencialidad.

5. Marco metodológico

5.1. Tipo de investigación

La presente investigación consiste en una recopilación de información bibliográfica y análisis de esta, con el fin de mostrar al lector los aspectos de HIPAA a considerar, para su aplicación. Consistirá además en un trabajo descriptivo sobre los aspectos más significativos a la hora de hablar del estándar, para que, sin mayor conocimiento previo, el lector pueda visualizar y entender estos aspectos y poder comprender qué se requiere para satisfacer los requerimientos de la norma.

Luego de esto se analizarán dos Sistemas relacionados con salud, para validar qué tan cercano o alejado se encuentra de las condiciones ideales para la implantación de HIPAA. Se describirán ambos entornos sin citar nombres, esto por una cuestión de privacidad y respeto a la información compartida. Este análisis contará con una descripción puntual de los puntos en los cuales cumple el ambiente con la realidad deseada y si este cumplimiento es parcial o total o completamente contrario.

Para cumplir con lo mencionado se utilizarán formularios o encuestas que serán respondidos por los administradores o responsables de los sistemas.

5.2. Alcance investigativo

El presente trabajo consiste únicamente en una investigación que arrojará resultados sobre la realidad de cumplimiento de la norma HIPAA en dos organizaciones nacionales. Se proponen aspectos que ayudarían a acercar el

cumplimento de la norma, pero no se implementará ninguna medida. El acatamiento o no de las recomendaciones o resultados quedarán a discreción de las organizaciones involucradas.

Esta investigación abarca únicamente aspectos de sistemas informáticos y no se refiere a cómo se administre la información física.

5.3. Población y muestreo

Como se ha mencionado, la herramienta que se utiliza es el formulario o encuesta para validar aspectos vitales de cumplimento de la norma.

La población elegida, son dos organizaciones nacionales que cuentan con Software de Salud.

5.4. Instrumentos de recolección de datos

Para la recolección de datos se utiliza el siguiente formulario o encuesta:

1) ¿Sabe o ha escuchado de HIPAA?

   [ ] Sí

   [ ] No

2) ¿Su sistema trabaja o almacena información personal de pacientes? Si este es el caso, indique el tipo (Puede marcar más de uno):

   [ ] Nombre y apellidos.

   [ ] Dirección.

   [ ] Patologías.

   [ ] Diagnósticos.

   [ ] Tratamientos.

[ ] Información de Seguro social (número de asegurado)

3) Si su sistema almacena información, ¿cómo lo realiza? (Puede marcar más de uno):

[ ] Base de datos.

[ ] Hojas de Excel.

[ ] Archivos de Word.

[ ] Física.

[ ] Otro. Mencione_____

4) ¿Con qué tipo de autenticación cuenta el sistema?

[ ] Un único usuario para cada persona que interactúa con el Sistema.

[ ] Una cuenta compartida para roles similares.

[ ] No existe autenticación.

[ ] Otro. Mencione. _____

5) ¿Con qué periodicidad se obliga al usuario a cambiar su contraseña?

[ ] Al menos una vez al mes.

[ ] Al menos una vez cada tres meses.

[ ] Al menos una vez cada seis meses.

[ ] El Sistema no obliga al usuario a cambiar su contraseña.

[ ] Otro _____

6) ¿Si el sistema fallase por una eventualidad, existen procesos de emergencia definidos para acceder la información?

   [ ] Sí.

   [ ] No

7) Si existe un periodo de inactividad por parte del usuario, ¿el sistema cierra sesión?

   [ ] Sí. Mencione el periodo de inactividad. _____

   [ ] No

8) Indique cuál es el mecanismo de protección de la información en tránsito.

   [ ] Protocolos de red.

   [ ] Encripción de datos.

   [ ] Los datos viajan sin protección.

   [ ] Otro. Mencione. _____

9) ¿Desde dónde es accesible el Sistema?

   [ ] Únicamente en equipos designados para su acceso.
   [ ] Desde cualquier equipo, pero dentro de una red segura.
   [ ] Desde cualquier equipo en cualquier ubicación.

10) ¿Qué datos de auditoría registra la aplicación? (Puede marcar más de uno)

   [ ] Usuario.

   [ ] Tipo de transacción.

[ ] Hora y/o fecha de transacción.

[ ] Hora y/o fecha de inicio de sesión.

[ ] Hora y/o fecha de fin de sesión.

[ ] Otro. Mencione _____

[ ] La aplicación no registra auditorías.

11)Si la aplicación registra auditoría, qué acciones registra:

[ ] Inserciones.

[ ] Eliminaciones.

[ ] Cambios a registros.

[ ] Otro _____

12)¿Qué tipo de borrado realiza la aplicación?

[ ] Lógico.

[ ] Físico.

13)¿Quién almacena la información de pacientes registrada en el Sistema?

[ ] El propietario de la aplicación.

[ ] Un tercero.

14)¿Qué métodos de seguridad implementa quien almacena la información para visitantes? (Puede marcar más de uno)

[ ] Bitácoras de entrada para visitantes.

[ ] Identificación o badge para visitantes.

[ ] Escolta de visitantes.

[ ] Vigilancia mediante cámaras de video.

[ ] No se utiliza ningún método de vigilancia en áreas de acceso público.

15)¿Qué métodos de seguridad implementa. quien almacena la información? ¿Para quiénes tienen acceso permanente?

[ ] Autenticación mono factor.

[ ] Autenticación poli factor.

[ ] Identificación visible.

[ ] Vigilancia mediante cámaras de video en áreas de acceso interno.

[ ] No se cuenta con vigilancia para personas con acceso permanente.

16)La información se almacena de forma:

[ ] Encriptado.

[ ] Texto plano.

17)¿Con cuántas otras aplicaciones se intercambia u obtiene información de pacientes el sistema en cuestión?

[ ] Uno o dos.

[ ] Más de dos.

[ ] Ninguno.

18)Si la aplicación intercambia u obtiene información con otros sistemas, ¿qué calificación le daría a la seguridad implementada por los otros sistemas?

[ ] La seguridad es similar a la del sistema que administró.

[ ] La seguridad es superior a la del sistema que administró.

[ ] La seguridad es inferior a la del sistema que administró.

[ ] No conozco los controles que implementan los otros sistemas.

19)¿Qué estándar utiliza la aplicación para administrar u comunicar la información?

[ ] XML.

[ ] ASC X12.

[ ] Otro. Menciónelo _____

[ ] La aplicación no utiliza ningún estándar

20)¿Qué tan frecuentemente se realizan respaldos a la información?

[ ] Diariamente.

[ ] Semanalmente.

[ ] Mensualmente.

[ ] No se realizan respaldos.

[ ] Otro _____

21)Si se realizan respaldos, estos se almacenan de forma:

[ ] Encriptado.

[ ] Texto Plano.

22)¿Qué tan frecuentemente se realizan auditorías a la seguridad de las instalaciones donde se almacena la información?

[ ] Al menos una vez cada 3 meses.

[ ] Al menos una vez cada 6 meses.

[ ] Al menos una vez al año.

[ ] No se realizan auditorías de seguridad.

[ ] Otro _____

23)¿En cuántos sitios se almacena de forma distribuida la información de pacientes?

[ ] En un solo sitio.

[ ] Al menos dos sitios.

[ ] Más de tres sitios.

[ ] No estoy al tanto.

5.5. Estrategia de desarrollo de la propuesta

La propuesta comenzará con una recopilación de la información obtenida a través del formulario o encuesta y su comparación con el marco teórico de la presente investigación; todo esto será procesado y se elaborarán conclusiones sobre los resultados encontrados.

6. Análisis del diagnóstico

Luego de aplicadas y respondidas las encuestas, con los resultados obtenidos, se desarrolla esta sección al analizar los resultados.

Tal y como se mencionó, las encuestas fueron aplicadas a los administradores de dos sistemas relacionados con salud. La idea radica en verificar qué tan cercano o

alejado se encuentran los sistemas para cumplir con HIPAA. De ahora en adelante, debido al respeto a la privacidad de ambas instituciones, se hace referencia a la primera empresa como “Escenario uno” y la segunda como “Escenario dos”.

6.1. Conocimiento de HIPAA

La primera pregunta pretendía visualizar de manera muy superficial si los encargados de estas aplicaciones conocían sobre HIPAA.

Esto con el fin de saber si conocía el estándar, ya que un individuo con conocimiento sobre este, sería un elemento de influencia sobre las decisiones y la metodología de aplicar para un acercamiento a la aplicación del estándar.

En un entorno ideal, un recurso con conocimiento de este estándar, que labore con una aplicación de salud, sería un excelente candidato para aplicar la norma, al menos en un aspecto.

De esta forma en el escenario uno, se obtuvo una respuesta afirmativa sobre el conocimiento de HIPAA. En contraste, en el escenario dos se obtuvieron resultados negativos. Como sentido común se esperaría un mayor cumplimiento por parte del Sistema del administrador del primer escenario. No se quiso profundizar más en el conocimiento sobre HIPAA de los encuestados para no influenciar sus posteriores respuestas.

6.2. Tipo de información y almacenamiento

Un detalle trascendental en HIPAA es la información sensible, para determinar si es un caso que concierne a HIPAA, debemos validar la información que procesa. Recordemos que para HIPAA son relevantes los datos asociados a condiciones físicas o mentales de individuos y que esta pueda ser asociada a un paciente real, con su nombre y apellido.

Será de nuestro interés averiguar si se guarda información personal; o sea, los datos que permiten identificarnos como individuos únicos frente a la sociedad, tales como nombre, apellido y dirección física.

En el escenario uno, se registran datos tales como nombre y apellidos del paciente, además del número de seguro social. El escenario dos, además de registrar la información ya mencionada, también toma la dirección del domicilio.

A nivel de información personal, ambos escenarios almacenan información sensible y que permite diferenciar a dos sujetos e identificarlos. Hasta el momento ambos casos son dignos de estudio.

Ahora veremos si se registran valores que denoten condiciones mentales o físicas. En el escenario uno se obtuvo que el sistema solo administra información sobre diagnósticos, que son juicios clínicos sobre el estado psicofísico de una persona. El diagnóstico médico permite establecer a partir de síntomas, signos y hallazgos de exploraciones complementarias, qué enfermedad padece o podría padecer un paciente (ECURED, s.f.).

El escenario dos almacena igualmente diagnósticos, pero va mas allá y trabaja con tratamientos y patologías. La patología define la rama de la medicina que se ocupa del estudio de las enfermedades; el término se ha ampliado y convertido en inventario de enfermedades (Patología - Definición, s.f.).

Hasta aquí se puede asegurar que ambos casos son útiles para continuar este estudio; sin embargo, el escenario dos es el más rico para el estudio, pues maneja información mucho más sensible y confidencial.

También resulta relevante analizar cómo se almacena la información. Aquí vemos que en el escenario uno se cuenta unicamente con su base de datos y un repositorio de imágenes. El escenario dos tiene a su disposición información digital como base de datos, hojas de excel y archivos de word; no obstante cuenta también con información física.

Del punto anterior, se nota que el escenario uno trabaja únicamente con información digital, mientras que el dos con física y electrónica. Para el cumplimiento de HIPAA, toda la información debe estar protegida, ya sea el medio que se almacene; sin embargo, para efectos del presente trabajo, el enfoque solo se centrará en información digital.

Como parte del análisis a la información, el siguiente punto relevante es saber quién almacena la información digital que utiliza la aplicación. Entre las posibles opciones tenemos que puede ser el propietario del sistema o un tercero. Hoy en día, no es de extrañar que para transferir riesgos y disminuir costos operativos, se contrate a un externo para que administre los servidores, ya sea operativos, base de datos o

repositorios. En ambos casos es el mismo propietario de la aplicación quien se asegura de la seguridad y la administración del contenedor de la información.

Que el mismo propietario sea el encargado de almacenar la información tiene su ventaja en el hecho que se sabe qué sucede con los datos. En el caso de que fuese un externo, siempre existirá un margen de ignorancia o sosobra sobre qué tan protegida está la infomación o si alguien no autorizado tiene acceso a ella. En la siguiente sección se expone el nivel de seguridad que se implementa en las instalaciones donde se almacena la información.

6.3. Seguridad del sistema

Lo más importante por proteger dentro de HIPAA, es la información de pacientes. Cualquier dato que permita identificar a un sujeto. Es por esto, que dentro de la encuesta realizada, se hicieron preguntas que permitieran medir qué tan protegida o susceptible se encuentra la información desde varias aristas.

Esta sección se enfoca en validar desde la aplicación en sí, algunas métricas de seguridad que permitan una sana interacción del usuario con el sistema.

Lo primero es validar el tema de usuarios. Todo individuo que ha trabajado con aplicaciones sabe lo importante que es tener un acceso único; esto es que cada individuo que interactúa con el sistema tenga los privilegios para hacerlo. Toda la información es sensible, pero cuando se habla de información de salud y personal, la importancia de su protección pareciera intuitivo.

Parte importante del estudio es validar si primeramente el acceso estaba regulado por puerta de inicio; esto es un portal de primera mano que validara que solamente individuos autorizados accedieran al sistema. Esto es que no existiera una entrada donde cualquier individuo pudiera navegar a través de los datos, libremente. Una vez validado el primer punto, lo siguiente es verificar si cada usuario existente dentro del sistema, tenía una cuenta única; esto es, que no existen cuentas comunales, cada actor es único e identificable.

Para ambos escenarios, se encontró con la agradable sorpresa que existe un único usuario para cada persona que interactúa con el sistema. Con esto se garantiza

que hay una validación inicial, donde cada individuo cuenta con un usuario y una contraseña que debe ingresar y que el sistema debe validar para ver si tiene permisos y sobre qué contenido los tiene.

Con este punto inicial ya aclarado, lo próximo en indagar será lo concerniente al posible compromiso de cuentas. Es importante recordar que el hecho de tener un usuario y una contraseña no es razón para despreocuparse del acceso de actores no deseados. Las cuentas pueden comprometerse ya sea por decisión propia o mediante acciones delictivas de espionaje. Un ejemplo de compromiso por decisión propia, podría ser si un usuario del sistema da por deseo propio su contraseña, para que un tercero tenga acceso; se da por sentado, que esta es una situación reprochable que nunca debe suceder, pero que en un ambiente humano podría darse. Otro ejemplo es que un usuario apunte su contraseña en una hoja de papel o en algún sitio visible y esta sea usurpada. Una acción delictiva o de espianaje, podría ser el uso de Sniffers, key Logers, virus, etc.

Uno de los métodos más sencillos y automáticos para proteger cuentas comprometidas es el cambio de contraseñas en periodos de tiempo razonable. De esta forma, si el usurpador cambia la contraseña, el usuario autorizado levantará una alerta al ver que no puede accceder a su sesión y si el usuario auténtico la cambia, el usurpador dejará de tener acceso, ya que no tendrá la nueva contraseña.

En el escenario uno, tendremos que el sistema no obliga al usuario a cambiar su contraseña. En el escenario dos por el contrario sí se fuerza a realizar un cambio de contraseña, en una periodicidad semestral. HIPAA no indica nada sobre cuál es la periodicidad adecuada, pero en un conceso de buenas prácticas, según investigación en varios sitios Web, se recomienda que el cambio de contraseña se realice al menos una vez cada tres meses. Aquí podemos ver que el escenario uno está completamente a merced de una suplantación de identidad, en el escenario dos, se estará protegido, mas no como realmente se debiera estar.

Otro caso de interés a nivel de seguridad es de los periodos de inactividad, ya sea que el usuario se encuentre en un área privada y personal o que por el contrario se halle en un cubículo compartido, siempre debe cerrarse la sesión de un usuario que lleva algún periodo sin interactuar con la aplicación. Esto porque un tercero que encuentre la aplicación abierta y, dentro de un , podrá manipular o visualizar

información para la cual no está autorizado; se pasa por alto cualquier tipo de seguridad de mayor nivel, ya preexistente.

Así pues, en aplicación del entorno uno se encontró que bajo ningún tiempo de inactividad, el sistema se encarga de cerrar la sesión del usuario activo. En el escenario dos sí existe un tiempo que puede ser configurado, pero que actualmente se mantiene como quince minutos sin interacción.

6.4. Protección de datos en tránsito y acceso al sistema

Como parte del cumplimiento de HIPAA, se requiere que los datos en tránsito se encuentren protegidos de terceros. Para esto no se especifica ningún método en específico según el estándar, incluso la información podría ir desencriptada en el tanto exista algún otro mecanismo que se asegure de proteger los datos.

Es por esto que se cuestionó la forma de protección de los datos para ambos escenarios; de esto se obtuvo que en el escenario uno los datos viajan sin protección alguna, pero al indagar desde donde es accesible el sistema se descubrió que únicamente lo es desde ciertos dispositivos asignados para este uso.

Así pues, en el escenario uno nos encontramos que mientras la información transita en texto plano, el sitema únicamente es accesible dentro de dispositivos designados propiamente para este fin. Esto crea un ambiente de peligro medio, ya que, si bien es cierto los datos podrían ser vulnerados, únicamente personas autorizadas podrían acceder a la red interna. Así bien si los datos fuesen vulnerados, sería por una persona con previo acceso al Sistema; claro está si la seguridad perimetral es robusta; esto es que a la red que maneja esta información solo pueden entrar individuos realmente autorizados. Este tema se verificará más adelante.

Ahora analizamos el escenario dos, según la encuesta realizada, los datos se encuentran protegidos mediante protocolos de red. Ahora bien, sabemos que en su forma más simple, un protocolo puede ser definido por las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Pueden ser implementados mediante software, hardware o híbridos (Protocolos de red, s.f.).

Luego de esto se preguntó igualmente desde dónde es accesible el sistema; se respondió que desde cualquier ubicación en cualquier equipo. Debido a que el sistema es accesible, incluso desde una ubicación externa, se solicitó la dirección

para su acceso externo; al realizar un intento de ingreso al sistema, se descubrió que los datos pueden ser capturados por un sniffer cualquiera. Así que debido a que no se pueden realizar pruebas dentro de la red interna, no queda más que asumir que dentro de esta hay protocolos que protegen la información, pero al utilizarse de forma externa no los hay. Así pues, con estos resultados podemos asumir que el escenario dos tiene una seria debilidad con sus datos en tránsito y estos no se hallan realmente protegidos.

6.5. Bitácoras y datos de auditoría

Entre los controles técnicos que establece HIPAA está el manejo de auditorías; esto es un monitoreo de actividades por parte de los usuarios. No es de extrañar este apartado, ya que HIPAA hace incapié explícito en la salvaguarda de la información. Imaginemos que alguien con acceso pudiera registrar valores a su antojo, luego de por ejemplo realizar un diagnóstico a un paciente para favorecer o perjudicar a este; de suceder esto, se perdería todo el valor de la aplicación.

Por lo anteriormente mencionado, es menester llevar una bitácora de acciones realizadas; HIPAA no establece qué tan profundo o superficial debe ser este control. No obstante, es importante definir quién realiza la operación, especialmente si es una modificación; sin embargo, operaciones como inserciones y eliminaciones no deberían quedar desatendidas. El borrado lógico es otra gran herramienta de , ya que nos garantiza poder tener un histórico de valores asignados, de lo contrario la información eliminada sería irrecuperable.

Debido a lo mencionado en el parrafo anterior es que dentro de la encuesta realizada se preguntó por cuáles datos de auditoría se registran dentro del sistema. En el escenario uno, producto de este cuestionamiento, se obtuvo que no se registra ningún tipo de bitacoreo; esto implica que los usuarios pueden interactuar libremente con el sistema sin temor a poder ser identificados en caso de error. Sin embargo, según se consultó, solo un par de personas tienen acceso al sistema; no obstante esto no deja de ser una debilidad fuerte en la integridad de los datos.

En el escenario dos, por el contrario, se obtuvo que la aplicación registra datos de auditoría tales como:

- Usuario que realiza la acción.

- Tipo de transacción.
- Hora y fecha de transacción.
- Hora y fecha de inicio de sesión.
- Hora y fecha de fin de sesión.

El escenario dos también almacena los datos:

- Valor anterior.
- Nuevo valor.

Como se puede ver, en este escenario se hace una mejor labor de auditoría que, al menos en este aspecto, daría un alto grado de cumpliento a la norma. Además, las transacciones que bitacorea son inserciones, eliminación de registros y edición de estos.

Otro punto de interés, ya mencionado, es el tipo de borrado, en el escenario uno no se permite realizar ningún tipo de borrado; esto tiene su lado positivo, ya que la información no podrá ser eliminada por conveniencia; no obstante, no garantiza integridad en los datos, debido a la carencia de bitácoras para las otras operaciones.

En el escenario dos, sobre este mismo punto, se obtuvo que la aplicación realiza unicamente borrados lógicos. Hasta quí podemos ver que el escenario dos a nivel de datos de auditoría, sí cumple con el estándar.

6.6. Interacción y seguridad en otros sistemas

La informacion almacenada y en tránsito no es únicamente responsabilidad del sistema primario que la administra; si los datos son compartidos con otra aplicación, es también su responsabilidad velar por la salvaguarda de la información.

Por lo mencionado en el parrafo anterior es que se preguntó con cuantas aplicaciones externas se relacionaba el sistema; en el escenario uno se respondió que con ningún otro Sistema.

En el escenario dos se descubrió que el Sistema se enlaza u obtiene información de uno o dos sistemas. Al indagar sobre la seguridad de estos otros sistemas, el encuestado respondió que la seguridad de estos otros, es similar a la del sistema en cuestion. De ser esto cierto, se estaría frente a dos sistemas con control de usuarios, uso de bitácoras para acciones, seguridad mediante protocolos dentro de redes internas, pero sin seguridad en redes externas.

Con base en esto, se asumirá para el escenario dos, que todas las fortalezas que apliquen para él, lo serán también para los otros Sistemas y aquellos puntos identificados como debilidades también lo serán para ellos.

En caso contrario, no se hará ningún análisis sobre las aplicaciones con las que se relacione el escenario uno, ya que este opera en un ambiente aislado.

6.7. Estándar de comunicación

La comunicación con otros sistemas o al menos la previsión para hacerlo es uno de los aspectos de HIPAA. La norma intenta estandarizar la forma como se trabajan los datos, de tal forma que ods o más Sistemas que cumplan con HIPAA, puedan hablar de forma transparente sin mayor interacción o modificación de programadores.

En este momento cabe preguntarse: ¿Cómo puede ser esto posible? La respuesta es sencilla, mediante una estructura ya definida de tráfico de información, donde se establecen cabeceras de mensajes, atributos de estos, entre otros.

Existe multitud de estándares, pero si se desea cumplir con HIPAA, el formato que se debe adoptar es ASC X12; este fue desarrollado por el comité de estándares acreditados.

Ahora bien, como parte del presente estudio para analizar el cumplimiento de HIPAA se procedió a incluir en la encuesta si se utilizaba algún estándar en el sistema en cuestión. Los resultados arrojados fueron los siguientes:

- Escenario uno: Se utiliza es estándar DICOM. Este formato fue creado en 1983 por el ACR (American College of Radiology) y la NEMA (National Eletrical Manufacturers Association). Este estándar consiste en normas que hacen que el almacenamiento y la comunicación de las informaciones

médicas se haga en eun formato electrónico único. Este formato va orientado a tomografías, resonancias magnéticas y radiografías.

- Escenario dos: Se utiliza formato XML, sin embargo sin estructura estándar.

Con respecto al escenario uno, se puede asumir que sí cumple, debido a que no tiene comunicación con otros sistemas; el escenario dos claramente no cumple, debido a que al comunicarse con otros sistemas, no lo hace mediante ASC X12.

6.8. Seguridad en las instalaciones

La salvaguarda de la información es un punto clave en HIPAA, su centro y su eje. Ya se analizó el tráfico de información y la seguridad aplicada a este. Es necesario abordar también la protección de los repositorios físicos de la información; esto es la seguridad perimetral de los data centers.

En esta sección se procederá a analizar cuál es el tipo de seguridad de los sitios donde se almacena la información para con los visitantes y para aquellos que tienen acceso recurrente a las instalaciones. Esto con la finalidad de validar con qué madurez se administran los accesos.

Iniciando como de costumbre con el escenario uno, primeramente se cuentan con al menos dos sitios donde se almacena la información. En estos dos sitios se cuenta con bitácoras para los visitantes, donde deben registrar sus datos personales para poder ingresar; estos datos son validados contra una identificación válida y al día para cotejar los datos brindados. Además de esto, los visitantes son escoltados por alguien con acceso permanente durante toda la estancia de la visita.

Aunque estas dos medidas son significativas, vemos una deficiencia en falta de Badges de identificación para visitantes; de esta forma se complica identificar una visita de un recurrente. Además, no existe monitoreo de cámaras de video, de tal forma que las acciones no quedan registradas en ningún medio.

El acceso a personas con acceso permanente es libre, no existe ningún tipo de validación fuera de un agente de seguridad que impida el acceso de aquellos que no

le son conocidos, a menos que vayan escoltados y se hayan registrado con anterioridad.

Para concluir con el escenario uno, se preguntó qué tan frecuentemente se realizan auditorías a la seguridad perimetral para validar que las normas de seguridad se estén aplicando y analizar si podrían hacer mejoras a la seguridad existente. Producto de esta pregunta se descubrió que no se realiza ninguna auditoría a la seguridad.

Ahora se realiza el mismo análisis anterior, solamente que para el escenario dos. En este caso, la información se registra en más de tres sitios, todos administrados por el administrador del sistema, no terceros.

El acceso a visitas se realiza al registrar una bitácora con datos personales del visitante, cotejado contra una identificación al día; las visitas deben ser identificadas debidamente con un Badge que lo caracterice como tal durante toda su estadía en las instalaciones; no obstante, no se aplica la escolta por parte de un individuo con acceso permanente, pero sí cuenta con vigilancia mediante cámaras.

Aquellos individuos que cuentan con acceso permanente requieren de autorización mono factor, que consiste en deslizar su badge por ciertas áreas de acceso restringido y en todas las instalaciones se cuenta con vigilancia mediante cámaras de video.

7. Propuesta de solución

En el capítulo anterior, se validaron los resultados obtenidos del formulario respondido por los administradores de dos Sistemas relacionados con Salud, que administran información de pacientes.

En esta sección se procede a proponer una solución para poder acercar estos sistemas a un cumplimiento del formato HIPAA.

Primeramente el conocimiento en HIPAA, es importante que los relacionados con el Sistema conozcan sobre el estándar y que exista un líder técnico que guíe los cambios. Luego de modificado el Sistema y que esté alineado con la norma, vele para que los posteriores desarrollos continúen cumpliendo. Esta recomendación

aplica para ambos escenarios, debido a que, si bien en el escenario uno el encargado conoce sobre HIPAA, es quizá este el que menos cumple. Así que no solo consiste en conocer sino guiar para que las propuestas se alineen.

Debido a que la protección de los datos es el punto más fuerte de HIPAA, es menester enfocarse en la seguridad. Ambas aplicaciones al menos cuentan con un portal de inicio que valida quién entra al Sistema y verifica sus permisos para administración de contenido. No obstante el tema de compromiso de cuentas, es bastante sensible. De ser comprometida una cuenta en el escenario uno, esta podría pasar por tiempo indefinido de esta forma, sin que nadie lo note. Ya que nunca se fuerza el cambio de contraseña, un punto a favor es que el Sistema solo es accedido desde ubicaciones designadas. Esto implica que si un tercero está obteniendo información no autorizada, es posible observarlo y denunciarlo; no obstante el Sistema debería estar implementado de tal forma que prevenga esto. La medida propuesta para esto es implementar un cambio periódico de contraseñas en un intervalo no mayor a tres meses.

A nivel de cambio de contraseñas en el escenario dos, se encontró un entorno más seguro, ya que cuenta con cambio de contraseña semestral; esto no es una periodicidad recomendada. Por conversación con el encargado del sistema, se descubrió que este permite configurar el tiempo para cambio de contraseña; así que realizar este cambio no requeriría mayor esfuerzo.

Continuando con la seguridad en el sistema, los tiempos de inactividad son un detalle que compromete la información, de no ser tratados de forma correcta. Basta solo imaginarse un Sistema como el que se está analizando, desbloqueado para acceso, sin necesidad de introducir un usuario; toda la seguridad que se haya implementado cae por tierra por un descuido así.

En el escenario uno, como parte de esta propuesta, está el integrar bloqueo o desactivación de la cuenta por un tiempo mayor a diez minutos. De tal forma, si un usuario autorizado se ausenta del equipo por este tiempo, el sistema procederá a cerrar su sesión y si un tercero llegase al equipo en cuestión este no podría interactuar ilegalmente.

En el escenario dos, se cuenta con un sistema que cierra sesión luego de un tiempo de inactividad mayor a quince minutos. HIPAA realmente no establece un tiempo máximo de no interacción con el sistema, mientras exista la opción, así que quince minutos, dependiendo de la situación particular de este escenario, podría ser un tiempo correcto y prudencial. Sin embargo, como parte de esta propuesta está en disminuir a 10 minutos el tiempo para evitar compromisos innecesarios.

Continuando con la seguridad, pero en esta ocasión centrándose en los datos en tránsito, se descubrió que la información se trafica sin protección alguna en el escenario uno; no obstante, existe una contraparte y es el hecho que la información solamente se accede desde ciertos dispositivos. Sin embargo, este hecho no opaca la necesidad de algún tipo de protección, ya que la única forma que podría cumplir la norma una situación así, es que hubiese una conexión dedicada entre el servidor y los nodos de acceso. Debido a que este no es el caso, algún tipo de seguridad debe ser implementada, pues el estándar no cierra las posibilidades a una única solución; pero debe existir, ya sean certificados, protocolos de transferencia segura como https o inscripción mediante Software o Hardware.

En el escenario dos, se mencionó que los datos se encuentran protegidos por protocolos de red; esto implica que existen medidas de software o hardware que regulan cómo viaja la información para que esta llegue segura a su destino. Esto daría un cumplimiento a la norma; no obstante debido a que la página puede ser accedida desde cualquier sitio, al implementar una pequeña red y un sniffer se pudieron capturar los datos de autenticación en el portal. Esto implica que al menos en acceso remoto, la aplicación es susceptible a robo de información; por esta razón, es que se propone, como parte de este estudio, la implementación de un protocolo de transferencia segura como Https, no solamente para el acceso externo, sino también para el interno. De esta forma, se garantiza un túnel de protección que garantiza que la información viajará de forma segura.

Las bitácoras y el registro de datos de auditoría son temas que no deben quedar desatendidos, si se quiere cumplir con el estándar; no obstante, son consideraciones fundamentales de seguridad que aseguran integridad de los datos. Como se observó en el análisis de resultados, en el escenario uno no se registra

ningún tipo de datos de auditoría; esto es inconcebible y ciertamente una falla de proporciones considerables a nivel del cumplimiento con HIPAA.

Como propuesta, por parte de este estudio, es el registro de datos de auditoría, al menos para las operaciones de inserción y edición; en este sistema en particular, debido a que no existe borrado, la edición de valores resulta crítica. Los valores propuestos, que deben registrarse son:

- Nombre de usuario.
- Fecha y hora de la operación.

Adicionalmente se formula el registro del cambio de valores:

- Valor anterior.
- Nuevo valor.

De implementarse esta propuesta, la aplicación del escenario uno, a nivel de auditorías podría cumplir con HIPAA; desgraciadamente en el punto en que se encuentra actualmente, es deficiente y requiere un esfuerzo considerable para su cumplimento.

El escenario dos es distinto en este aspecto; para empezar, si se registran datos de auditoría, se registra quién realiza la acción, el tipo de esta, la fecha y hora de la acción, además de la fecha y hora de inicio y fin de sesión.

Además de los datos anteriormente mencionados, registraron el valor nuevo y el anterior. Por todas estas razones, el escenario dos sí cumpliría con HIPAA a nivel de manejo de bitácoras y registro de datos de auditoría.

HIPAA, en casi todos los aspectos, no obliga la adaptación de algo en particular para su cumplimento; sin embargo, la única forma de garantizar una comunicación nítida, transparente y sencilla entre sistemas es forzar la implementación de un estándar único. El estándar elegido por HIPAA es ASC X12, que consiste en una serie de encabezados y estructuras muy particulares.

El escenario uno no interactúa con otros sistemas, por lo tanto el formato de comunicación no existe, ya que no interactúa con otros sistemas. Internamente

utiliza DICOM. Esto no sería una falta al cumplimiento de HIPAA, ya que ASC X12 se utilizaría para comunicarse con otros sistemas. Así pues se puede decir que el escenario uno, debido a que no tiene comunicación con otros sistemas no incumple con la norma; pero la propuesta de llegar a interactuar hipotéticamente con otras entidades externas, sería que lo hiciera mediante el formato ASC X12.

El escenario dos sí tiene relación con otros sistemas y no lo hace mediante el formato ASC X12, así pues el escenario dos incumple y no solo eso, todos los sistemas que interactúan con el posiblemente también. Por lo tanto, la propuesta aquí es que todos los sistemas, incluyendo el que se encuentra en estudio, implementen el formato propuesto por HIPAA para realizar sus transacciones.

El punto final por analizar es el acceso y seguridad en las instalaciones; HIPAA protege tanto los datos en tránsito como aquellos que están almacenados. Por esto, los controles perimetrales y el control de acceso, debe estar monitoreado para aquellos sitios que fungen como data center.

El escenario uno tiene un proceso de atención a visitas que, si no es perfecto, al menos es aceptable, la única deficiencia analizada es que aquellas personas que son visitantes no poseen ninguna característica especial que los identifique como tales. La propuesta en este aspecto es una vez que los votantes son registrados, se les otorgue un badge distintivo que los identifique como visitas en todo momento.

Como parte de los controles solicitados por HIPAA es que debe existir vigilancia mediante cámaras de vigilancia tanto para aquellas personas con acceso como visitantes como para aquellos con acceso permanente y que las grabaciones se mantengan por al menos 90 días. Debido a que no existe ningún monitoreo por cámara, se recomienda la instalación de cámaras de vigilancia en las áreas de recepción para llevar un control de quiénes entran y salen, además de cámaras en las áreas críticas, como por ejemplo donde se encuentren los servidores, además que las grabaciones sean almacenadas por noventa días.

El acceso para permanentes es casi inexistente, si realmente desean cumplir con HIPAA; esta es muy explícita en qué se requiere de un proceso al menos de dos factores. Para este caso, se recomienda el uso de Badge de acceso con puertas lectoras y también un sistema biométrico que lea huellas digitales, al menos en la

entrada principal y en las áreas de acceso a los servidores donde se almacene la información.

El escenario dos, tiene un sistema más estricto y la única deficiencia encontrada es el acceso mono factor para aquellos individuos con acceso permanente. La recomendación en este caso es contar con accesos de al menos dos factores en la entrada principal y donde se encuentren los servidores. Los dos factores recomendados son el uso de Badge de acceso en puertas con lectoras de estos, además un sistema biométrico que lea huellas digitales para estos dos lugares críticos.

Como parte de la propuesta de esta investigación, se ofrece una plantilla para calcular el cumplimiento de HIPAA en un Sistema; si todas las respuestas son “Sí”, estaremos frente a un Sistema que cumple con HIPAA, de lo contrario se deberán abordar las áreas que den negativo.

El sistema es relevante para HIPAA	Sí	No
El sistema registra información personal (nombre, apellidos, dirección, correo, número de identificación, etc.).		
El sistema registra datos médicos (patologías, historial de medicamentos, diagnósticos, número de asegurado).		
Si al menos una casilla no fue marcada en esta sección, entonces el sistema no necesita cumplir con HIPAA		
Confidencialidad		
El sistema cuenta con un usuario único para cada individuo que interactúa con el sistema.		
El sistema cuenta con una contraseña para cada usuario.		
El sistema fuerza el cambio de contraseña en una periodicidad establecida.		

El sistema cierra sesión, luego de un periodo de inactividad.		
El sistema tiene algún método de protección de datos en tránsito (encripción, protocolos de red, certificados, canales seguros, etc.).		
¿El sitio donde se almacena la información cuenta con bitácoras de entrada para los visitantes?		
¿El sitio donde se almacena la información provee un distintivo para los visitantes, mientras visitan las instalaciones?		
¿En el sitio donde se almacena la información, se asigna una escolta a los visitantes durante todo el tiempo en que encuentren en las instalaciones?		
¿El sitio donde se almacena la información cuenta con vigilancia mediante cámaras de video, para las áreas accedidas por visitantes?		
¿El sitio donde se almacena la información cuenta con autenticación al menos de dos factores para acceder a los críticos?		
¿En el sitio donde se almacena la información, se solicita algún método de identificación visible, para aquellos con acceso permanente?		
¿En el sitio donde se almacena la información, registran esta de forma encriptada?		
¿Los respaldos estos se almacenan encriptados?		
Disponibilidad		
¿En caso de eventualidad, existen procesos de emergencia establecidos para acceder la información?		
¿Se realizan respaldos a la información con una periodicidad menor a un mes?		
Integridad		
El Sistema registra datos de auditoría (Tipo de acción realizada, usuario que realiza la acción, fecha y hora de la acción, valor anterior y valor		

actual).		
El sistema realiza un borrado lógico.		
¿El sistema se comunica con otros sistemas a través del formato ASC X12? (Si el sistema no se comunica con otros, omita esta pregunta).		

8. Conclusiones y recomendaciones

8.1. Conclusiones

El propósito de HIPAA es la protección de la información sensible de pacientes; si tuvieramos que resumir en una frase, el objetivo del estándar sería esa. La protección de la información es algo de mucho valor en la sociedad moderna; vivimos en una era donde estar informado es dinero. La información permite a las entidades validar la calidad de un cliente, dar un norte más efectivo a la planeación y visión de la empresa.

Conocer datos financieros es útil, pero si a esto le sumamos conocer historial médico personal y no porcentual, nos da una idea de los peligros latentes. Basta imaginar un inividuo con padecimientos crónicos tratando de conseguir trabajo, pero debido a que su información es de dominio público, no es dificil visualizar que su situación no va a mejorar, ya que entre dos candidatos, uno sin padecimientos llevará la ventaja competitiva.

Es por esto que la ley de protección de datos es necesaria y vital; sin embargo, una organización de este calibre es reactiva. La aplicación de estándares que protejan la información son medidas preventivas. Debido al poder de esta proactividad, en la protección de datos, es que un estándar como HIPAA es tan llamativo. Así como las organizaciones financieras se preocupan por proteger su información con estándares como PCI, las organizaciones médicas deberían preocuparse igualmente de velar por sus datos.

Producto de esta investigación, se notaron fuertes brechas para el cumplimiento de HIPAA; sin embargo, quizá el punto más fuerte y preocupante es la falta se seguridad para información en tránsito. Para ambos escenarios, de encontrase en la misma red, sin mucho conocimiento y unicamente con un sniffer un intruso podría hacerse con información sensible y hasta capturar las credenciales de acceso. Se concluye que la implantación de seguridad durante el tráfico de datos y credenciales es un punto clave que debe ser implementado para todos los sistemas que administren información sensible; no es posible que la información esté desprotegida a ese nivel.

Se encontró en ambos casos que la sociedad costarricense es confiada y no da la importancia necesaria a la seguridad; la información en ambos escenarios se halla vulnerable al estar en tránsito. En el escenario uno, se halló también una deficiencia administrativa al adminitrar el acceso tanto para visitantes como para individuos con acceso permanente. Este escenario se puede trasladar a otros casos reales, donde podemos encontrar un exceso de confianza o no se le da importancia a las normas de seguridad perimetral.

Capturar información con auditoría es otro punto muy importante que garantiza la transparecia e integridad de la información. Permite ver los cambios en los registros, para que, si hubo una manipulación indebida, esta quede registradas.

Dentro del estudio se encontraron resultados divididos, ya que en un escenario, sí se realiza un adecuado uso de bitácoras, pero en el otro no. Comúnmente en los desarrollos, el manejo de bitácoras se suele ver como algo extra, por lo cual no es de extrañar que en el resultado final la presencia de estas se omita.

Otro punto para la adecuada implantación de HIPAA y un punto que quizá es el unico que tiene nombre dentro del estandar es la aplicación de ASC X12. HIPAA establece, en la mayoría de los casos, qué se debe hacer, pero no cómo debe hacerse, a excepción de este caso donde especfica claramente cómo debe ser la comunicación entre sistemas. Si bien es cierto, esto garantiza que la unificación, con un nuevo sistema, debería ser considerablemente sencilla. En nuestro escenario nacional, donde practicamente nadie conoce ASC X12 y donde todos los sistemas involucrados deben aplicarlo, requeriría un gran retrabajo. Esto, en especial en escenarios como el número dos, donde la aplicación se relaciona con al menos tres

sistemas; todos estos deberían replantear su forma de comunicación. El punto positivo es que las siguientes integraciones deberían ser cada vez más sencillas y transparentes.

Producto de este trabajo, se descubrió que la sociedad costarricense no conoce siquiera el estándar ASC X12; este es un punto clave si se desea implementar el estándar. En ambos escenarios se manifestó no solo la falta de aplicación del formato, sino tambien un desconocimiento total de este.

Luego de analizados los escenarios, se nota que hay bastante trabajo pendiente. HIPAA proporciona confidencialidad, disponibilidad e integridad a los datos, confidencialidad en el acceso, integridad en las transacciones y disponibilidad de los datos. La aplicación del estándar es una manera proactiva de proteger la información sensible en sistemas de salud, que hoy parecieran no dar la importancia que se merecen los datos que administra. Dado lo vital de la infomación administrada por las aplicaciones analizadas, las conclusiones de esta investigación se inclinan a afirmar la utilidad de este estándar y de los beneficios para las instituciones que lo apliquen. Estarían cumpliendo con la normativa de seguridad de la información vigente en el país, de forma proactiva; además de brindar un mejor entorno a la población, al respetar su privacidad.

Al iniciar esta investigación, no se tenían expectativas muy altas; el conocimiento de años en desarrollo de aplicaciones, permite conocer los puntos débiles del desarrollo en Costa Rica. Siendo sinceros, el tema de la seguridad de la información es un tema que se encuentra en pañales en nuestro país. El desarrollo se realiza para tener un producto estable en el menor tiempo posible. Aspectos como control de acceso, controles de auditoría, seguridad de datos en tránsito, se tienden a ver como aspectos adicionales que generan costos. El escenario uno pareciera ser un espejo de las espectativas iniciales al comenzar este trabajo; no obstante, el escenario dos, sin cumplir a cabalidad con todos los requisitos para cumplir con HIPAA, muestra una mayor madurez en temas de seguridad.

Producto del análisis realizado, se confeccionó el formulario de cumplimiento de HIPAA; si una entidad puede responder afirmatvamente a todos los apartados, puede saber que primeramente la información que administra su información, es relevante para el estándar y segundo que su sistema se encuentra en cumplimiento

con este. Al mismo tiempo, la herramienta permite validar deficiencias y qué aspectos mejorar. Si bien es cierto, el cumplimiento del estándar no es obligado por el momento, de llegar a serlo, una entidad que halla seguido el formulario, sabrá que puede optar por la acreditación sin mayor inversión; además, que sabe que está cumpliendo con los tres pilares de la seguridad, que son integridad, disponibilidad y confidencialidad.

Todas las aplicaciones que trabajan con datos de salud, deberían contar con herramientas que protejan la información que administran; el impacto para la sociedad es bastante negativo si este tipo de información se hace pública. Organizaciones como la CCSS o el INS deben ser en extremo cautelosas, ya que además de manejar información de salud, que ya es confidencial y muy sensible, conocen información financiera como historial de salarios, pensiones, etc. La adaptación de HIPAA en instituciones como las mencionadas, proveería un marco robusto, que, además de dar renombre a la organización, velaría como un guardián proactivo para que la información esté segura contra amenazas, tanto externas como internas. El aporte de la adaptación de este estándar, crearía una sociedad más segura, ya que la información no sería traficada libremente como en ocasiones sucede hoy en día, cuando empresas financieras ofrecen créditos preaprobados, ya que conocen todo su historial financiero.

El objetivo general de esta investigación se cumplió con el formulario de cumpliento de HIPAA, una herramienta capaz de medir las fortalezas y debilidades de un Sistema contra los requisitos de HIPAA. Los objetivos especifícos se cumplieron al definir HIPAA y la interiorización de los conceptos básicos, que se encuentran fusionados dentro de este trabajo. Con todo esto se definieron los requisitos para el cumplimiento de la norma, los cuales fueron el insumo para generar el formulario de cumplimiento de HIPAA. Finalmente, en el análisis del diagnóstico se documentaron las brechas de las entidades seleccionadas para su cumplimiento. Así pues se cumplen todos los objetivos propuestos inicialmente y de forma satisfactoria.

8.2. Recomendaciones

Al iniciar esta sección, quizá pareciera estar sobreentendido, pero la implantación del estandar HIPAA es muy recomendado para organizaciones que administran información sensible. Esto es información personal que puede dar detalles privados sobre condiciones de salud, ya sea física o mental, de pacientes. Organizaciones financieras no dudarían en aplicar un estándar que los proteja de forma proactiva, ya que sus intereses económicos estarían protegidos.

En el caso de la salud, el valor no es tangible. Sin embargo, existe legislación que deben cumplir aquellas entidades que administren bases de datos con información sensible; además, leyes de delitos informáticos que penalizan a individuos que intercepten información sobre la intimidad de otro. HIPAA vendría a implementar controles para proteger a las entidades que almacenan la información y al mismo tiempo previene que los datos sean leídos por terceros no autorizados.

Seguir la guía planteada por la actual investigación, garantizará un ambiente más seguro, salvará a multiples individuos de caer presos por sanciones, por no cuidar sus bases de datos o por acceder a datos para los cuales no están autorizados.

Para los dos entes aquí analizados, se recomienda atender a los puntos explicados en la propuesta de la solución, según el nivel de cumplimiento que deseen tener de la norma. Mirando más allá de la implementación del estándar, las recomendaciones planteadas dan un mayor grado de madurez y organización, que son grandes valores agregados a la seguridad.

9. Trabajos a futuro

Luego de realizada esta investigación, sería muy llamativo tener escenarios en los cuales aplicar el formulario generado, producto de esta investigación y quizá pulir un poco más las brechas encontradas en esta investigación. Aunque se encontró un escenario deficiente y otro moderadamente robusto, aunque no lo suficiente para cumplir con HIPAA a cabalidad, sería de interés analizar más casos.

10. Bibliografía

ANSI ASC X12 Standards Overview Tutorial. (s.f.). GXS.

HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules. (Agosto de 2016). Obtenido de Centers for Medicare & Medicaid Services: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf

HIPAA Compliant Hosting. (2012). Online Tech.

HIPAA Implementation Guide. (2000). See beyond.