Evaluación de la seguridad de la información en la Clínica Hispanoamérica de Pasto, basada en la norma ISO/IEC 27001

José Javier Villalba Romero
Róbinson Andrés Jiménez Toledo
Docentes de Ingeniería de Sistemas
Universidad Mariana

Álvaro Rodrigo Torres Burbano
Estudiante de Ingeniería de Sistemas
Universidad Mariana

Figura 1. Seguridad de la información.
Fuente: http://riskcontrol.com.co/content/riesgos-de-seguridad-de-la-informaci%C3%B3n

Desde que Internet se convirtió en una interconexión global, los incidentes en seguridad informática en las compañías han ido aumentando debido al inadecuado manejo de la información, la falta de conocimientos sobre la seguridad informática y/o la inexperiencia en la actualización de metodologías y normas que rigen la seguridad, como la Norma ISO/IEC 27001, ocasionando pérdidas millonarias. Por lo tanto, las empresas buscan alternativas para proteger y almacenar información de forma segura, dado que hoy en día corren un gran riesgo de pérdida de información.

Según una encuesta realizada por la Corporación Symantec, la cual desarrolla y comercializa software sobre seguridad de la información, el 73 % de las pequeñas y medianas empresas (Pymes) a nivel mundial han sido víctimas de ataques informáticos, realizados en un 36 % por ciberdelincuentes, lo cual afecta su seguridad y las convierte en un blanco informático vulnerable. Pero muchas veces, son los mismos empleados quienes hacen que el lugar donde ellos trabajan se vea involucrado, siendo el puente entre la información y el atacante al sistema informático, cuando conectan a las redes o computadores, dispositivos que podrían infectar estos sistemas o cuando ingresan por Internet a portales no permitidos, provocando que la información se vea comprometida y expuesta.

De acuerdo con el contexto anterior y teniendo en cuenta el avance tecnológico que tienen las empresas, se toma como caso de estudio la Clínica Hispanoamérica, empresa relativamente nueva en el contexto regional. Este proyecto pretende evaluarla para comprobar su estado actual y el manejo de la información, según los principios básicos de la seguridad de la información, que tiene por objeto proteger los sistemas informáticos frente a las amenazas a los que están expuestos. Cabe mencionar que la seguridad de la información maneja tres principios que son primordiales:

Figura 2. Principios de Seguridad de la Información.
Fuente: http://informaticaagmd25heidyvelazco.blogspot.com.co/2013/06/seguridad-de-la-informacion.html

Confidencialidad: es el proceso por el cual la información no se revela ni se pone a disposición de individuos, entidades o procesos no autorizados, y garantiza que solo los usuarios con autorización puedan acceder a ella; de lo contrario se viola la confidencialidad de la empresa.

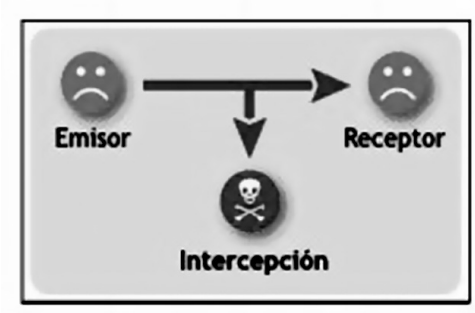

Figura 3. Confidencialidad.
Fuente: Escrivá, Romero, Ramada y Onrubia (2013).

Con la Figura 3 se muestra la violacion de confidencialidad, la cual se presenta cuando un atacante consigue un acceso a un equipo sin autorizacion, y controla todos los recursos del equipo.

Integridad: es el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Se enfoca en garantizar que la información no pueda ser modificada sin autorización de los altos jefes o encargados.

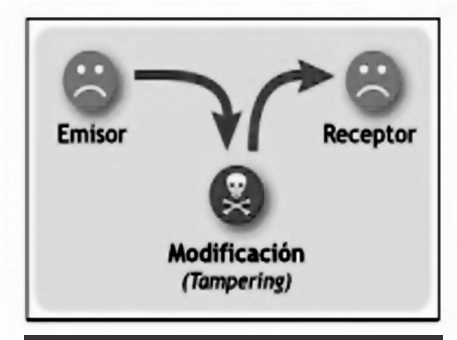

Figura 4. Integridad.
Fuente: Escrivá, Romero, Ramada y Onrubia (2013).

La Figura 4 muestra la violacion de la integridad, y ésta se presenta cuando un empleado modifica algún archivo o documento (base de datos) sin autorización, lo cual hace que el receptor reciba modificado el archivo o documento.

Disponibilidad: es el acceso y utilización de la información y los sistemas de tratamiento de la misma, por parte de los individuos, entidades o procesos autorizados, cuando lo requieran, y garantiza que la información esté disponible cuando las personas la necesiten, sin importar la hora y la fecha.

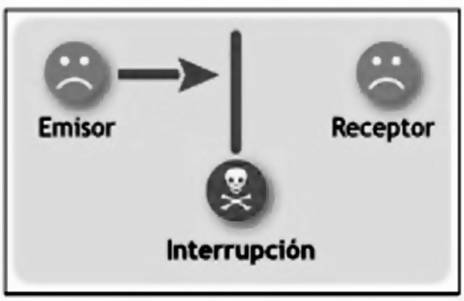

Figura 5. Disponibilidad.
Fuente: Escrivá, Romero, Ramada y Onrubia (2013).

La Figura 5 muestra la violacion de la disponibilidad, la cual se presenta cuando un servicio se cae y los usuarios no pueden utilizarlo, lo que genera pérdidas a la empresa.

En el contexto de esta investigación es importante resaltar la seguridad de la información, ente principal sobre el cual se va trabajar, aplicando los principios básicos que permiten analizar la empresa a estudio, identificar los riesgos y al final mitigarlos, manteniendo claves de seguridad y restricción a la información de usuarios no autorizados, conservando en su totalidad la información sin cambios de ninguna índole y haciendo que ésta esté disponible a los usuarios o trabajadores autorizados que le darán solo uso laboral, lo cual es muy aplicable a cualquier ámbito investigativo dentro de la seguridad informática en cualquier empresa de diferentes especialidades. Para ello se elabora unas fases que van representadas con una metodología que pretende analizar los riesgos que tiene la Clínica Hispanoamérica y así poder mitigarlos, distribuidas de la siguiente manera:

Fase 1: Familiarización con el entorno

Se realizará con el fin de familiarizarse con la Empresa en cuanto a la infraestructura tecnológica, mediante un estudio previo a la información que se desea evaluar de acuerdo con su importancia, utilizando las herramientas necesarias para el levantamiento de la información y así efectuar una planeación adecuada.

Fase 2: Planeación de las Actividades

En este punto se llevará a cabo la planificación de todo el proceso de la caracterización, con las siguientes actividades:

- Se realizará un estudio previo de la infraestructura tecnológica de la Clínica Hispanoamérica, obteniendo información de la misma.
- Se identifica el alcance y los objetivos de la evaluación a realizar.
- Se determina los recursos que se utilizará en la evaluación en la Clínica.
- Se elabora el plan de manejo.

Fase 3: Realización de las Actividades de Auditoría

En esta etapa se hará efectivos todos los planteamientos de la etapa anterior, con la aplicación de las metodologías y técnicas seleccionadas que garanticen el cumplimiento de los objetivos planeados. Las actividades serán:

- Identificar bajo los dominios de la Norma ISO/IEC 27001 los objetivos de control que se va a evaluar.
- Elaborar la matriz de riesgo, enfocad a la Norma ISO/IEC 27001.
- Identificar los hallazgos dentro del proceso que se va a evaluar.

Fase 4: Presentación del Informe Final

Etapa en la cual se realizará un informe final que contendrá los planes de mejora de acuerdo con los hallazgos existentes dentro de la evaluación de la información en la Clínica Hispanoamérica; el reporte se entregará al gerente con el fin de mejorar la seguridad dentro de ella.

Esta investigación pretende mejorar el manejo de la información de la Clínica, proporcionando planes de mejora que ayudarán a mitigar los riesgos y amenazas que surjan en la matriz de riesgos, y así, en un futuro poder certificarse bajo la Norma ISO/IEC 27001.

Bibliografía

Escrivá, G., Romero, R., Ramada, D. y Onrubia, R. (2013). Seguridad informática. Malaga, España: Editorial Mcmillan.

Quadstudio. (s.f.). Riesgos de seguridad de la información. Recuperado de http://riskcontrol.com.co/content/riesgos-de-seguridad-de-la-informaci%C3%B3n

Symantec. (2013). Encuesta Global de Pymes 2013. Recuperado de https://www.symantec.com/es/mx/about/page.jsp?id=smb-survey-2013

Subinet. (s.f.). Los 5 principios fundamentales de la Seguridad Informática. Recuperado de http://www.subinet.es/los-5-principios-fundamentales-de-la-seguridad-informatica/