Información Tecnológica
Vol. 29(1), 3-10 (2018)
http://dx.doi.org/10.4067/S0718-07642018000100003

Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia

Raúl J. Martelo, Luis C. Tovar y Diego A. Maza
Universidad de Cartagena, Facultad de Ingeniería, Grupo de Investigación en tecnología de las comunicaciones e informática, GIMATICA, Avenida el Consulado, Calle 30, No 48 – 152, Cartagena, Colombia. (e-mail: rmartelog1@unicartagena.edu.co, ltovarg@unicartagena.edu.co, diegomazatapia@gmail.com)

Recibido Ene. 3, 2017; Aceptado Feb. 20, 2017; Versión final Mar. 13, 2017, Publicado Feb. 2018

Resumen

El objetivo principal de este trabajo consiste en proponer un modelo de seguridad, bajo el marco de trabajo Plan-Do-Check-Act (PDCA), que facilite el proceso de creación, registro y mantenimiento de Políticas de Seguridad Informática (PSI) a nivel lógico. Se toma como caso de estudio el laboratorio de redes de la Universidad de Cartagena, en Colombia. Para la creación de este modelo, se tuvo en cuenta las fases de desarrollo a nivel físico y lógico, las cuales dieron como resultado el modelo propuesto. Esto es una herramienta software de apoyo, que permite a las organizaciones identificar el estado de riesgo ante posibles amenazas que puedan afectar la integridad de su información. Se concluye que la aplicación del modelo orienta a las organizaciones en la definición de medidas que contribuyan a la disminución de riesgos para garantizar mayor estabilidad.

Palabras clave: seguridad informática; seguridad lógica; sistema de gestión; ISO 27001; PDCA

Basic Logical Safety Model. Study Case: The Network Laboratory of the University of Cartagena in Colombia

Abstract

The main objective of this paper is to propose a security model, under the framework of Plan-Do-Check-Act (PDCA), which facilitates the process of creation, registration and maintenance of Information Technology Security Policies to logical level. As a study case, the networks laboratory of the University of Cartagena in Colombia was considered. For the creation of this model the development phases to physical and logical level were taken into account, giving as a result the proposed model. That is a software support tool that allows organizations identifying risk status to potential threats that may affect the integrity of their information. It is concluded that the application of the model guides organizations in defining the measures that must be taken to reduce risks, guarantying higher stability.

Keywords: informatics security; logical safety; management system; ISO 27001; PDCA

INTRODUCCION

La información es un bien preciado para empresas, que luchan contra el cambio constante de la sociedad y competencia. Sánchez y Zúñiga (2011) afirman que una sociedad desinformada no tiene herramientas para enfrentar desafíos y que estas se obtienen de manera fácil y rápida gracias a los avances tecnológicos; por ello las empresas deben mantenerse informadas, con el objetivo de idear planes estratégicos para abordar inconvenientes que se puedan presentar. Lo anterior, además de brindar soporte para incrementar su nivel competitivo, favorece la calidad de sus servicios (Torres y Vásquez, 2011).Datos igualmente importantes para una organización son los obtenidos en la ejecución de procesos administrativos y productivos, proporcionándoles una visión general de la situación interna de la empresa para tomar decisiones que mejoren el rendimiento de la misma, por tal circunstancia estos deben ser precisos, seguros y estar disponibles, características alcanzadas con la seguridad de la información, la cual posee ese fin además de preservar los sistemas implicados en su tratamiento (ISO, 2011). Siendo ésta de valor, se debe tener cuidado al momento de tratarla, ya que las empresas presentan vulnerabilidades y pueden ser atacados por personas internas o externas a ella, que hurtan datos para su beneficio, lo que implica pérdidas económicas y credibilidad, estableciendo mecanismos de seguridad informática como solución para ello, reduciendo el riesgo de ataques virtuales.

Las empresas están interesadas en fortalecer sus sistemas a la luz de las vulnerabilidades y de los ataques cibernéticos que se conocen día a día (Castro-Leon et al., 2015). Para esto, la seguridad informática contribuye al desarrollo, mientras mitiga el riesgo de pérdida de la información al utilizar dispositivos avanzados para la protección de datos, conocen las tecnologías actuales y se mantienen a la vanguardia. Lo anterior conlleva a ejecutar medidas de seguridad en búsqueda de ataques de software malicioso del lado del usuario final, con el fin de establecer un marco de seguridad en sistemas de información como parte fundamental en una organización, tal como expresan Wolden et al. (2015), los cuales por medio de la aplicación de la norma COBIT 5, buscan la efectividad de la Información en un marco de Seguridad para reducir ataques cibernéticos sobre el Sistema de Gestión en la Cadena de Suministro en organizaciones.

En el área de redes, también se han investigado los efectos de la virtualización en seguridad de la información aplicando la norma ISO 27001, reflejado en Li et al. (2015). Los resultados obtenidos, sugieren que la virtualización puede ser beneficiosa para algunos sectores industriales en el manejo de los asuntos de seguridad de la información. Estudios como los realizados en Kerr y Murthy (2013), muestran la importancia del marco COBIT en procesos de TI para un efectivo control interno sobre la información financiera en las organizaciones; estos autores, concluyen que los procesos de COBIT son importantes para mantener un control interno efectivo sobre la fiabilidad de la información financiera, que debe ser de gran interés y relevancia para ejecutivos, gerentes, y auditores en cualquier organización. En Martelo *et al*. (2015), se desarrolla un software para contribuir al control de los documentos generados a partir del proceso de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Dicho software permite recibir, administrar y organizar la documentación generada en el proceso de implantación del SGSI. Para soportar dicho software, diseñaron e implementaron un modelo que define acciones de gestión necesarias para la aprobación, revisión, actualización, estados y legibilidad en documentos durante el ciclo de vida del SGSI.

Sin embargo, así como crecen los mecanismos de la seguridad informática, aumentan el número de amenazas que se encuentran en el entorno virtual, las cuales evolucionan para lograr su objetivo, esto hace que surjan nuevos retos que se afrontan mediante la seguridad informática. Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza: Seguridad lógica, que hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático; y seguridad física: dentro de la seguridad informática hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas. Los mecanismos de seguridad física deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza (Hernández y Flórez, 2011).

La seguridad lógica para la protección de la información es vital, porque permite: restringir el acceso a programas y archivos mediante claves y/o encriptación; asignar las limitaciones correspondientes a cada usuario del sistema informático, esto significa, no dar privilegios extra a un usuario, sino solo los que necesita para realizar su trabajo; asegurarse de que los archivos y programas que se emplean son los correctos y se usan correctamente, por ejemplo, el mal uso de una aplicación puede ocasionar agujeros en la seguridad de un sistema informático; control de los flujos de entrada/salida de la información, esto incluye que la información enviada llegue al destino deseado, pero no cuenta con un modelo con el cual se guíen para la creación de un sistema de seguridad informático a nivel lógico, lo que no permite medir el nivel de protección que tiene una organización.

La aplicación de modelos de seguridad a nivel organizacional, para apoyar la toma de decisiones y la mejora en los procesos dentro de una organización, ha llevado a estudios como el de Guerrero y Gómez (2012), el cual demuestra que la gestión de riesgo y controles en sistemas de información no son una tarea exclusiva de expertos en tecnología de la información e ingenieros de software, sino, una labor que requiere de una perspectiva amplia, que aporte al aprendizaje y apropiación de procesos de cambio organizacional. A pesar de lo anterior, la política concerniente a la gestión de riesgos y controles de los sistemas de información, no logra tener la recepción adecuada por parte de la gerencia organizacional, debido a la falta de entendimiento de su sentido o propósito, y a la ausencia de procesos necesarios para la implementación adecuada (Guerrero y Gómez, 2011).

En Cowan (2011), se estudia cómo el hecho de poseer una certificación en ISO 27001, puede influir en la decisión de seleccionar un proveedor entre las empresas que participen u oferten en una licitación; esto ha llevado a que las organizaciones que deseen ganar nuevos negocios a través de licitaciones y ofertas, estén bajo presión para dar información clara sobre procesos internos en la gobernanza y seguridad de la información, ya que se podría elegir un proveedor sobre otro, basado únicamente en el cumplimiento de la normativa aplicable o el hecho de que posee la certificación.

En Kerr y Murthy (2013), se estudia la importancia del marco COBIT en procesos de TI, para un efectivo control interno sobre la información financiera en las organizaciones. De igual forma, concluyen que los procesos de COBIT son importantes para mantener un control interno efectivo sobre la fiabilidad de la información financiera, el cual es objeto de interés y relevancia para ejecutivos, gerentes, y auditores en cualquier organización; mientras que Castro-Leon et al. (2015), presenta el enfoque metodológico de la asignatura Servicios y Seguridad del Grado de Informática y Servicios; proponen un enfoque basado en estrategias de ataque y defensa utilizadas en sistemas informáticos. A través del enfoque se aprende a diferenciar y a valorar el uso de las técnicas de seguridad conociendo qué aporta cada una en el cuadro global de la seguridad del sistema y de la información de la empresa. Teniendo en cuenta los estudios anteriores, se destaca la importancia que representan las PSI en las organizaciones, por lo tanto se realiza la presente investigación orientada a la seguridad lógica.

MODELO PLANTEADO

En esta sección se presenta el modelo propuesto, para facilitar el proceso de creación y registro de políticas de seguridad informática a nivel lógico en organizaciones. Luego de realizar el estudio de los diferentes modelos, normas y estándares existentes para el establecimiento de estas, Marrugo y Núñez (2012), plantean un modelo que apoya el proceso de Creación, Redacción, Clasificación y Registro de Políticas de Seguridad Informática en las Organizaciones, enfocado a la seguridad física. Este estudio sirvió como referencia para realizar el modelo de seguridad propuesto, teniendo en cuenta, las características similares que se podían conservar entre estos.

En la Figura 1, se pueden observar las cuatro etapas que abarca el modelo propuesto, las cuales, se encuentran organizadas de acuerdo al orden de trabajo del PDCA, lo que le permite al modelo estar en conformidad con un sistema de gestión.

Etapa 1: Planear: Identificar activos (lógicos), a proteger y de qué se intenta proteger. El encargado debe listar los bienes a asegurar de acuerdo con las categorías sugeridas; así mismo, los problemas presentes. La lista puede modificarse o transformarse en la medida que sea necesario reiniciar el ciclo al cumplirse la última etapa del proceso.

Etapa 2: Hacer: Implementar medidas de seguridad. Teniendo en cuenta la relación costo/eficiencia, realizar un plan de objetos y problemas a tratar, en el que se determinen políticas orientadas a rectificar la situación acorde a la alineación estratégica de la empresa.

Etapa 3; Monitorear: Determinar probables amenazas y revisar políticas. Una vez se han creado las políticas preliminares que cubren los problemas, visiblemente identificados en la empresa, se determinan probables amenazas que, igualmente, pueden causar daños a los bienes listados.

Etapa 4; Actuar: Revisar el proceso y aplicar correcciones o modificaciones necesarias. Esta etapa del proceso permite identificar claramente el cumplimiento de las políticas implementadas a través de una revisión general del mismo, verificando las políticas creadas, las estrategias de comunicación y ejecución de las mismas, la alineación estratégica aplicada, el cumplimiento de los requisitos fundamentales de seguridad informática preestablecidos, entre otros aspectos.

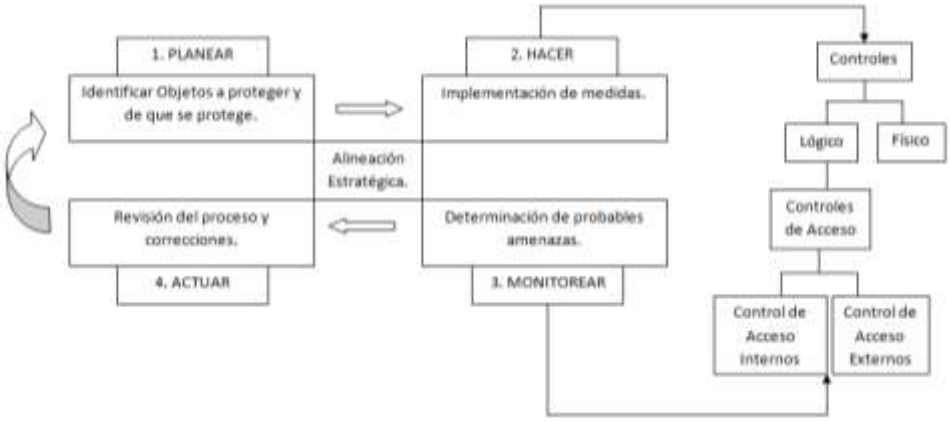

Fig. 1: Esquema Básico de Seguridad Lógica (EBAS–L) propuesto

De lo anterior, se efectúa un análisis con el propósito de aplicar correcciones necesarias en la identificación de activos a proteger, nuevas amenazas y problemas no tenidos en cuenta, o por lo menos, no priorizados en la escala de gravedad, y que deben estarlo de acuerdo a los riesgos e impactos hallados en el análisis de riesgos de la etapa anterior (monitorear). Si los resultados son satisfactorios, se implantará la mejora de forma definitiva, y si no lo son, habrá que decidir si realizar cambios para ajustar los resultados o, en su defecto, desecharla. Como núcleo del modelo, se encuentra la alineación estratégica, cuya finalidad es tener en cuenta el plan de negocios de la empresa al momento de la creación e implementación de PSI, de forma tal, que contribuya a cumplir con las metas del negocio sin dejar de lado los objetivos de seguridad propuestos, es decir, las medidas de seguridad sugeridas no pueden entorpecer el buen funcionamiento de la organización. En el modelo MBAS-L propuesto, entre las etapas hacer y monitorear, se definen los requisitos fundamentales de seguridad, los cuales, hacen referencia a los controles de seguridad que permiten monitorear el cumplimiento de las políticas definidas, los cuales pueden ser a nivel lógico y físico; esta investigación se enmarca en los controles a nivel lógico.

Como se observa en el modelo existen controles de acceso de los cuales se listan: (1) Identificación y Autenticación: Identificación es cuando el usuario se da a conocer en el sistema; autenticación es la verificación que hace el sistema de la identificación; (2) Roles: los derechos de acceso se agrupan de acuerdo a un rol determinado y, el uso de los recursos, se restringe a las personas autorizadas a asumir dicho rol. Cambiar de rol implicaría salir del sistema y reingresar; (3) Transacciones: al acceso se le establece una determinada cantidad de transacciones; una vez el sistema detecta que se completaron las transacciones permitidas, el acceso termina y, en este caso, el usuario no tiene más oportunidad de operar; (4) Limitaciones de Servicio: son restricciones que dependen de parámetros propios de utilización de la aplicación, o que son preestablecidos por el administrador del sistema; (5) Modalidades de acceso: se pueden considerar como ciertos privilegios que se tiene sobre la información; pueden ser de lectura, escritura, ejecución, borrado, creación y búsqueda; (6) Ubicación y Horario: el acceso a determinados recursos del sistema, puede estar basado en la ubicación física o lógica de los datos o personas; estos, a su vez, pueden ser Controles de Acceso Internos: los cuales determinan lo que un usuario puede o no hacer con los recursos del sistema; (7) Palabras claves: son comúnmente asociadas a la autenticación y se utilizan para proteger datos y aplicaciones; (8) Encriptación: esta información solo puede ser descifrada por quien posea la clave apropiada para hacerlo; (9) Listas de control de acceso: registro de usuarios, computadoras y procesos, a quienes se les han otorgado ciertos privilegios para usar algún recurso del sistema; (10) Limites sobres las interfaces de usuario: conjunto de listas que restringen funcionalidades específicas; (11) Etiquetas de seguridad: son denominaciones que se dan a los recursos; una vez ha sido hecha, ya no puede ser cambiada; (12) Controles de Acceso Externos: son una protección contra la interacción de nuestro sistema con los sistemas, servicios y personas externas a la organización; (13) Dispositivos de control de puertos: autorizan el acceso a un puerto determinado del computador; (14) Puertas de seguridad: permiten filtrar o bloquear el acceso entre redes.; y (15) Autenticación basada en Host: proporciona el acceso según la identificación del computador donde se origina el requerimiento de acceso.

RESULTADOS

Con el fin de dar cumplimento al objetivo principal de este artículo, se desarrolló un modelo de apoyo al proceso de creación y registro de políticas de seguridad a nivel lógico, el cual permite a la organización la creación, aplicación y apropiación de la seguridad informática como una de las claves principales de su negocio, sin descuidar las metas del mismo; así mismo permite un seguimiento, a través de auditorías, del cumplimiento de cada uno de los controles existentes en la organización, implementados a partir de las políticas presentes en dicha empresa.

El modelo fue implementado mediante una herramienta software que contaba con las siguientes características: 1) La integración de los módulos de usuarios, núcleo y auditorias, que permite realizar seguimiento continuo de las políticas se seguridad informática en la organización, y establecer compromiso en los partícipes del proceso de implantación; 2) Módulo usuarios, para el control de los privilegios (permisos), que tendrá cada uno de los agentes que interactúen con el sistema; 3) Módulo núcleo, permite la opción de gestionar, en cualquier momento, toda la información referente a, activos a defender, amenazas a neutralizar, controles a implementar, empresas, metas del negocio y políticas de seguridad, la cual, es necesaria para el funcionamiento del sistema; por otro lado, también se manejará la opción de buscar Información previamente gestionada, de las características anteriores, para su validación o corrección; 4) Módulo auditoria, brinda la opción de gestionar toda la información referente a las auditorias, las cuales, permiten verificar de manera continua y detallada la situación actual, de una organización a nivel de seguridad, en cuanto al porcentaje de cubrimiento y de riesgo de las políticas de esta, así como sus respectivas calificaciones, que son el fundamento principal para implementar el sistema; también se ofrece, una calificación descriptiva del cumplimiento de los controles implementados, y se manejará la opción de buscar Información previamente gestionada de las características anteriores para su consulta, validación o corrección.

Con el fin de validar el modelo planteado se simuló un escenario en los laboratorios de redes del programa de Ingeniería de Sistemas de la Facultad de Ingeniería de la Universidad de Cartagena, en el que se utilizó el modelo planteado teniendo en cuenta los diferentes escenarios que se pueden presentar en una organización. A continuación, se presenta el modelo básico de seguridad lógica mediante la ejecución de las siguientes etapas:

Etapa 1: Planear: Como primer paso se identificó qué activos se querían proteger, de esta relación se determinaron cuáles eran los activos lógicos y físicos.

Etapa 2: Hacer: una vez finalizada la lista de chequeo se establecieron las políticas a implementar y sus respectivos controles que aplican. Se debe tener en cuenta que una política aplica uno o más controles para poder ser implementada.

La Tabla 1 muestra las políticas propuestas, con los respectivos controles que se deben aplicar para llevarse a cabo.

Tabla 1: Lista de políticas con los controles que deben aplicarse

Código política	*Política*	*Controles que Aplican*
1	Verificar que no existan Keylogger en PCs con información critica	3
2	Evitar Intentos seguidos errados en claves del sistema	1,2,12
3	cambiar clave de acceso al sistema periódicamente	2,12
4	Utilización de Firewalls, VPNs y Conexiones seguras (SSL).	1,5,6,4,9
5	Instalar Software de análisis de vulnerabilidad y Fingerprints para archivos.	11
6	Manejo de ataques potenciales de ingeniería social.	12

En la Tabla 2 se muestra la tabla con los controles propuestos.

Tabla 2: Lista de controles propuestos.

Código Control	*Control*
1	Identificación, autenticación y autorización para usuarios.
2	Restricción de acceso a programas y archivos.
3	Restricción de modificación de programas y archivos que no correspondan.
4	Seguridad en uso de datos, archivos y programas correctos en y por procedimiento correcto.
5	Información transmitida sea recibida por el destinatario al cual ha sido enviada.
6	Información recibida igual a información trasmitida.
7	Sistemas alternativos secundarios de transmisión entre diferentes puntos.
8	Pasos alternativos de emergencia para la transmisión de información.
9	Utilizar barreras firewall
10	Tunning en la base de datos.
11	escanear con antivirus equipos de cómputos
12	Normas de asignación de cuentas (Prioridades).

Etapa 3: Monitorear: Las políticas creadas se le asignaron una serie de controles, para verificar el cumplimiento de estos en el módulo de auditoría se procedió a calificar cada uno teniendo en cuenta los criterios de la Tabla 3:

Tabla 3: Criterios de calificación

Calificación de los Controles	
Criterio	*Puntaje*
El control no aplica	N
El control es redundante	R
El control es efectivo, es clave y no se cumple o no se conoce	1
El control es efectivo, no es clave y no se cumple o no se conoce	2
El control no es efectivo y se cumple	3
El control es efectivo, no es clave y se cumple	4
El control es efectivo, es clave y se cumple	5

Cada calificación tenía como objetivo medir que tan apropiado estaba el personal de la política de seguridad y cuál era su cumplimiento. En la Tabla 4 se muestra la calificación que se le proporcionó a los controles en la auditoría realizada.

Tabla 4: Lista de controles con las respectivas clasificaciones.

Código Control	*Control*	*Calificación*
1	Identificación, autenticación y autorización para usuarios.	5
2	Restricción de acceso a programas y archivos.	4
3	Restricción de modificación de programas y archivos que no correspondan.	5
4	Seguridad en uso de datos, archivos y programas correctos en y por procedimiento correcto.	3
5	Información transmitida sea recibida por el destinatario al cual ha sido enviada.	4
6	Información recibida igual a información trasmitida.	3
7	Sistemas alternativos secundarios de transmisión entre diferentes puntos.	N
8	Pasos alternativos de emergencia para la transmisión de información.	N
9	Utilizar barreras firewall	3
10	Tunning en la base de datos.	N
11	Escanear con antivirus equipos de cómputos	4
12	Normas de asignación de cuentas (Prioridades).	3

Una vez realizada toda la auditoria, donde fue asignado un puntaje para cada control, se procedió a calcular el porcentaje de cubrimiento de cada política, mediante la siguiente operación: se realizó una sumatoria de todas las calificaciones que se le asignaron a los controles, esto se dividió entre el total de controles existentes menos el número de controles que no aplican a la política, que se quería valorar, por 5 que es el valor de la calificación más alta.

Calculado el porcentaje de cubrimiento se pudo identificar el grado de riesgo en que se encuentran cada uno de los activos que estaban protegidos mediante las políticas auditadas, y tomar decisiones que permitieran, mantener o eliminar la política dependiendo cual fuera el caso, en la Tabla 5 se puede observar cómo se determinó el grado de riesgo, donde C es el porcentaje de cubrimiento calculado.

Tabla 5: Significado grado de riesgo

GRADO DE RIESGO	
% DE RIESGO = (1 - C)	
%	SIGNIFICADO
0,00 a 9,99	Los controles son adecuados
10,00 a 39,99	Los controles son suficientes
40,00 a 59,99	El control es débil
60,00 a 79,99	El control es deficiente
80,00 a 99,99	El control no opera

Tabla 6: Vista EBAS–L: Modulo Auditoria

Política	*Fecha*	*Cubrimiento (%)*	*Riesgo (%)*
Verificar que no existan Keylogger en PCs con información critica	2/02/2017	49%	51%
Evitar Intentos seguidos errados en claves del sistema	2/02/2017	32%	68%
cambiar clave de acceso al sistema periódicamente	2/02/2017	43%	58%
Uso de Firewalls, VPNs y Conexiones seguras (SSL).	2/02/2017	25%	75%
Instalar Software de análisis de vulnerabilidad y Fingerprints para archivos.	2/02/2017	52%	48%
Manejo de ataques potenciales de ingeniería social.	2/02/2017	57%	43%

En la Tabla 6 se visualizan los resultados de las auditorías realizadas a las políticas de la organización, los cuales permiten comprobar (en porcentajes de cubrimiento y riesgo), el nivel de eficiencia con respecto a la implementación de una política y los controles que esta conlleva: Se presentan las características para las auditorias gestionadas: Política, conjunto de guías a las cuales se le pretende hacer la auditoria por parte del usuario; Fecha, hace referencia a la fecha de creación de la auditoria, para el caso de estudio la fecha es la misma ya que la auditoria se realizó el mismo día para todas las políticas; Porcentaje de cubrimiento, indica que tan efectivo son los controles con respecto a las políticas implementadas; Porcentaje de riesgo, hace referencia a qué tan deficientes son los controles con respecto a las políticas implementadas; Significado, es la calificación descriptiva del nivel de riesgo.

Etapa 4: *Actuar*: Una vez finalizada la auditoria y calculado él porcentaje de cubrimiento, se pudo identificar el grado de riesgo en que se encuentran cada uno de los activos que estaban protegidos mediante las políticas auditadas, se estableció un marco de políticas y controles que estén orientados a rectificar la situación acorde a la alineación estratégica de la empresa, como se puede observar, los controles son débiles y deficientes.

CONCLUSIONES

De los resultados obtenidos, se pueden enunciar las siguientes conclusiones sobre el modelo y la herramienta que lo soporta:

1) Permite identificar el estado de riesgo de la organización ante amenazas que pueden afectar la integridad de la información; 2) Para implementar las PSI, debe existir un apoyo de las directivas, de forma tal, que favorezca la apropiación de su importancia en todo el personal de la organización; 3) La aplicación del modelo orienta a las organizaciones en la definición de medidas que contribuyan a la disminución de riesgos para garantizar mayor estabilidad; 4) Modelo de trabajo cíclico. 5) las auditorias permiten identificar si una política ha cumplido con su finalidad en la organización; 6) niveles de riesgo altos alertan a la organización de incumplimiento de las PSI por parte del personal involucrado.

REFERENCIAS

Castro-Leon, M., F. Boixader, M. Taboada, D. Rexachs y E. Luque. Servicios y seguridad, un enfoque basado en estrategias de ataque y defensa, Enseñanza y Aprendizaje de Ingeniería de Computadores. Revista de Experiencias Docentes en Ingeniería de Computadores, (5), 39-48 (2015)

Cowan, D. External pressure for internal information security controls. Computer Fraud & Security, 2011 (11), 8-11 (2011)

Guerrero, M.L. y L.C. Gómez. Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional. Estudios Gerenciales, 28(125), 87-95 (2012)

Guerrero, M.L. y L.C. Gómez. Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información. Estudios Gerenciales, 27(121), 195-215 (2011)

Hernández, J. y J. Flórez. Seguridad física y lógica en el manejo de la información policial. Revista Logos, Ciencia & Tecnología, 3(1), 222-233 (2011)

ISO/IEC 17799, Information technology -- Security techniques -- Code of practice for information security

management (2005)

Kerr, D.S. y U.S. Murthy. The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey. Information & Management, 50(7), 590-597 (2013)

Li, S.H., D.C. Yen, S.C. Chen, P.S. Chen, W.H. Lu y C.C. Cho. Effects of virtualization on information security. Computer Standards & Interfaces, 42, 1-8 (2015)

Martelo, R.J., J.E. Madera y A.D. Betín. Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información Tecnológica, 26(2), 129-134 (2015)

Sánchez, E. y L. Zúñiga, La importancia de contar con información precisa, confiable y oportuna en las bases de datos. Revista Nacional de Administración, 2(2), 145-154 (2011)

Torres, M. y C. Vásquez. Contribución de la información en la calidad de los servicios. Enlace Revista Venezolana de Información, Tecnología y Conocimiento, 8(1), 55-70 (2011)

Wolden, M., R. Valverde y M. Talla. The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System. IFAC-PapersOnLine, 48(3), 1846-1852 (2015)