LA ADMINISTRACIÓN DE LOS SISTEMAS DE GESTOR DE BASE DE DATOS (SGBD'S) DE LOS SISTEMAS DE INFORMACIÓN Y SU INCIDENCIA EN EL CONTROL DE LAS SEGURIDADES DE LAS BASES DE DATOS

AUTORES: Patricio Navas Moya[1]

Rodolfo Matius Mendoza Poma[2]

Alexandra Lorena Alajo Anchatuña[3]

DIRECCIÓN PARA CORRESPONDENCIA: (matius.mendoza@utc.edu.ec)

Fecha de recepción: 08-10-2017

Fecha de aceptación: 02-03-2018

RESUMEN

En la actualidad las bases de datos almacenan información valiosa y confidencial. Una cantidad creciente de regulaciones obligan a las organizaciones a hacer auditorias del acceso a dicha información restringida y a protegerla de los ataques y la mala utilización. La administración de los sistemas gestores de bases de datos y como inciden sobre la seguridad de la información en las bases de datos. La presente investigación se basa en un análisis de las principales fortalezas y debilidades que pueden tener los Sistemas Gestores de bases de datos aplicando las buenas practicas que tiene COBIT 5 que es una herramienta que sirve para fortalecer las seguridades, mejorar los procesos dentro de las Tecnologías de la Información haciéndolos seguros y que se pueda garantizar la confidencialidad, integridad y disponibilidad de los datos. Los resultados muestran la eficiencia de la aplicación de estas normas, que además ayudan al desarrollo de una cultura de seguridad y optimización a la interna de una organización.

Palabras Clave: Amenaza; vulnerabilidad; riesgo; política de seguridad; Sistemas Gestores de Bases de Datos.

THE ADMINISTRATION OF DATABASED MANAGER SYSTEMS (DBMS) OF

[1]Ingeniero en Sistemas, Magister en Gestión de Bases de Datos, Docente de la Universidad de las Fuerzas Armadas Espe, Departamento de Electrica y Electronica, Carrera de Ingenieria de Software, Jefe de Laboratorio de Producción de Software e Investigación, Planificador las áreas de computación.

[2]Ingeniero en Sistemas, Magister en Sistemas Informáticos Educativos, Docente de la Universidad Técnica de Cotopaxi, Facultad de Ciencias Administrativas, Carrera de Secretariado Ejecutivo Gerencial, Administrador de la Plataforma MOODLE de la Facultad, Latacunga – Ecuador, E-mail: matius.mendoza@utc.edu.ec

[3]Ingeniera en Sistemas y Computación, Magister en Ciencias de la Educación Mención Planeamiento y Administración Educativa, Docente de la Universidad Técnica de Cotopaxi, Facultad de Ciencias Administrativas, Directora de la Carrera de Secretariado Ejecutivo Gerencial. Latacunga – Ecuador, E-mail: alexandra.alajo@utc.edu.ec

INFORMATION SYSTEMS AND ITS IMPACT ON THE CONTROL OF DATABASE SAFETY

DATABASES AND SECURITY CONTROL MANAGEMENT SYSTEM

ABSTRACT

At present, the databases store valuable and confidential information. An increasing number of regulations require organizations to make audits restricted access to such information and to protect it from attacks and misuse. The administration of management systems such as databases and how they affect the security of information in databases. This research is based on an analysis of the main strengths and weaknesses that can have Managers Database Systems applying the good practice that has COBIT 5, which is a tool that serves to strengthen the assurances, improve processes within Information Technology making them safe and that can guarantee the confidentiality integrity and availability of data. The results show the efficiency of the application of these rules, also help the development of a safety culture and internal optimization of an organization.

KEYWORDS: Threat; vulnerability; risk; security policy; Management Systems Databases.

INTRODUCCIÓN

El constante avance y cambio tecnológico hacen que las instituciones busquen nuevas formas de solucionar algunos inconvenientes de seguridad (Bugosen y Tejada, 2015) , que se van presentando tanto en la integridad, confidencialidad y la disponibilidad como pilar fundamental de la seguridad de la información (Carvajal y León, 2011).

La investigación está realizada en base a un análisis a las bases de datos universitarias su funcionamiento, forma de administración, construcción rendimiento entre otros parámetros que pueden ayudar a la optimización de procesos mediante los datos. El desarrollo de aplicativos en instituciones de educación superior ha hecho que se deba incrementar las seguridades por el fomento de la investigación que hacen más vulnerables todo tipo de información y más cuando se trata de académica, todos estos datos son guardados en bases de datos que obligan a los administradores y programadores por medidas necesarias para precautelar todo inclusive los procesos para adoptar las mejores prácticas de seguridad de la información y sus procesos.

DESARROLLO

Bases de Datos

Son conjuntos de datos almacenados sin redundancia que son innecesarias en un soporte informático y accesible simultáneamente por múltiples usuarios y aplicaciones. Los datos deben estar de forma estructurada y almacenada de forma totalmente independiente de las aplicaciones que la utilizan (De las paz, Mendoza, Lopez, Gozales y Lemahieu, 2015, pp. 89-103).

Sistemas Gestores de Bases de Datos

En la actualidad los Sistemas Gestores de Bases de Datos (SGBD), permiten resolver problemas, brindando a los administradores de la información comodidad y eficiencia en el tratamiento de los datos. Entonces son un aporte a la selección adecuada de métodos existente los cuales ayudaran en la toma de decisiones por parte de los usuarios de los sistemas de información tratando de mitigar las causas en posibles efectos ya que ayudan en el control sobre la redundancia de los datos (Bleha, Slivinsky y Hussien, 1990, pp. 1217-1222.

Sistemas de Información

Los sistemas de información son un conjunto de elementos organizados, relacionados y coordinados entre sí, que facilitan el funcionamiento global de las empresas o de cualquier otra actividad humana para conseguir sus objetivos (Dorai y Kannan, 2011).

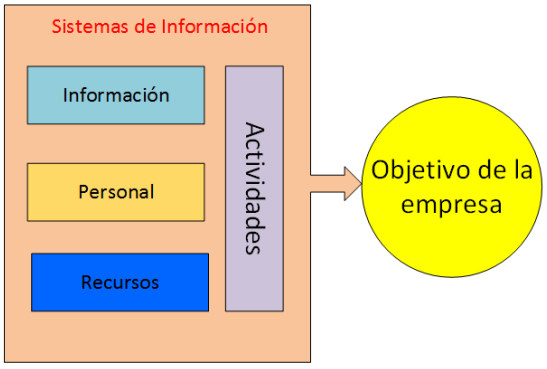

Figura 1: Sistemas de Información

Seguridad

En la actualidad hay que tener en cuenta que lo más importante son las seguridades de las bases de datos, el proceso de aplicar soluciones que interactúen con información sensible y que estas puedan ser confidenciales ya que incluye material que puede poner en riesgo la seguridad de las

instituciones, mediante mecanismos de cifrado y otras herramientas virtuales (Disterer, 2013).

COBIT

Significa Objetivos de Control para Tecnologías de Información y Tecnologías relacionadas, cuyo trabajo es el resultado de una investigación con expertos de varios países del mundo desarrollado por ISACA Al Omari, Barnes y Pitman, 2012).

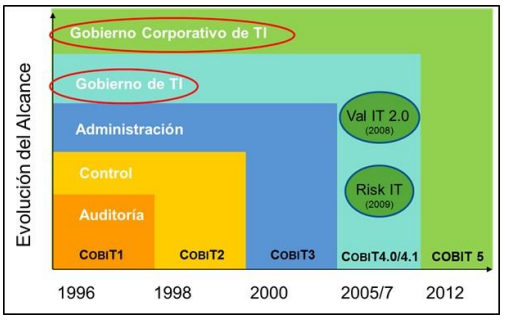

Figura 2. COBIT® 5(Isaca, 2012)

1. Configuraciones

1.1. Diseño de la solución

La administración de los SGBD está orientada a la evaluación de aspectos relacionados con la eficiencia, seguridad y productividad de las fortalezas y debilidades de las bases de datos de los sistemas de información.
Este modelo está basado de las buenas prácticas de los estándares:

Cobit 5 y la ISO/IEC 27001:2005

Separa la seguridad de la Información en dos procesos:

- Gestionar la seguridad
- Gestionar la seguridad de los servicios de la seguridad (Beckers, Beckers, Heisel, Heisel & Schmidt, 2012).

Cobit 5 y la ISO/IEC 38500:2008

Definen los procesos de la gestión de las Tecnologías de la Información (Preittigun, Chantatub, & Vatanasakdakul, 2012).

Cobit 5 y la ISO/IEC 31000:2009

Definen los principios de la gestión de riesgos, necesarios para poder implementar seguridades de la información (Preittigun, Chantatub, & Vatanasakdakul, 2012).

Cobit 5 y CMMI

Define controles para el desarrollo y la adquisición de software CMMI a través de sus procesos, cumple con dichos controles, por lo tanto, se complementan y en conjunto abarcan desde el desarrollo de software hasta la gestión de entrega y mantenimiento del mismo. Aunque la forma de evaluar la madurez se alinea según COBIT a lo que dice la norma ISO 15504 (Preittigun, Chantatub, & Vatanasakdakul, 2012).

Cobit 5 y la ISO/IEC 15504

Este estándar determina la capacidad de mejora del proceso de software, que básicamente es un modelo para la mejora y la evaluación del desarrollo y mantenimiento de los sistemas de información (Bartens, De Haes, Eggert, Heilig, Maes, Schulte, & Voß, 2014).

Basados en esos criterios la investigación se centrará en 3 ejes fundamentales para la investigación:

- Seguridad de la información
- Uso de identificadores de COBIT 5 para implementar la seguridad de la información en la práctica.
- Adaptación de COBIT 5 para la seguridad de la información al entorno institucional (Mera, 2014).

2. Implementación

Para la implementación de políticas de seguridad hay que prever muchos aspectos referentes a como se encuentran estructurado los comités de seguridad en las organizaciones y cuáles podrían ser los planes de contingencia en caso de presentarse problemas de seguridad:

- Los principios, las políticas y los marcos son el medio para convertir el comportamiento deseado en orientación práctica para la gestión diaria.
- Los procesos describen un conjunto organizado de prácticas y actividades para lograr ciertos objetivos y producir en conjunto de resultados que sustentan el logro de las metas generales.
- Las estructuras organizacionales son entidades claves en la toma de decisiones en una institución.
- Los servicios, la infraestructura y las aplicaciones incluyen la infraestructura, la tecnología y las aplicaciones que brindan a la empresa servicios y procesamiento de TI.
- Las habilidades y las competencias están vinculada a las personas y son requeridas para la finalización exitosa de todas las actividades y para la toma de decisiones correctas y aplicar medidas correctivas (Moya, & Véliz, 2013).

En base a lo expuesto y tomando en cuenta a las buenas prácticas de COBIT se plantea la creación de comités de seguridad.

Figura 3: Comité de Seguridad de la Información

Las mejores prácticas deben ser tomadas en cuenta según el número de equipos y usuarios, pero casi nunca se lo puede cumplir, por lo que se debe plantear algunas alternativas de acuerdo a la realidad de la mayoría de las organizaciones. Que para este caso se formara un comité de seguridad de la información quienes se encargaran de la integridad de la información, procurando siempre que con el constante crecimiento de las instituciones de educación superior se podría llegar a formas más comités, de prevención de alteraciones o eliminación de información.

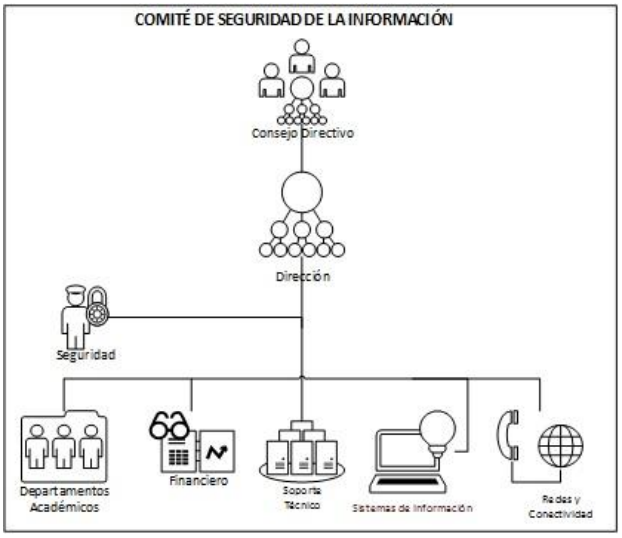

Figura 4: Comité de seguridad Universitaria

El esquema planteado se refiere al comité de seguridad planteado el mismo que debe tener gran injerencia dentro de las IES (Instituciones de Educación Superior). El comité debería siempre actuar como eje asesor dentro de estas instituciones, ya que son las que deben determinar cuándo se debe proceder y de qué manera en caso de alguna novedad en las seguridades. Para poder cumplir con las funciones que deben tener para garantizar la seguridad de la información se plantea una matriz en la que se debe cumplir con las especificaciones y normas vigentes.

TAREAS DE SEGURIDAD DE LA INFORMACIÓN	Seguridad de la Información	Bases de Datos	Redes de Datos	Soporte	Desarrollo
Administración	A	A	M	B	M
Políticas, procesos y estándares	A	A	A	A	A
Estrategia	A	A	A	B	M
Evaluación de riesgos (Definición)	M	M			B
Evaluación de riesgos (Ejecución)	M	A	A	B	A
Gestión de seguridad de la información	A	A	A	B	M
Arquitectura de seguridad	A	M	M	M	M
Tecnología de Seguridad	A	M	M	B	M
Desarrollo seguro	B	M	B	B	A
Operaciones y entrega de servicios	M	A	B	A	B
Gestión de proyectos	M	A	A	A	B
Auditoría, revisión y monitorio	A	M	A	M	M
Respuesta a incidentes	A	A	A	A	M
Entorno legal y normativo	A	A	A	A	A
Conocimiento, educación y capacitación	A	A	A	A	A
Nomenclatura: **A:** Alta **M:** Media **B:** Baja					

Tabla 1: Tareas de seguridad de la Información

3. Procesos

Los procesos tienen la propiedad de describir un conjunto organizado de prácticas y actividades para lograr ciertos objetivos y producir un conjunto de resultados respaldando el logro de las metas generales relacionadas con TI.

La Administración de seguridad de la información platea unos procesos de seguridades que están basados en componentes.

PRINCIPIO	OBJETIVO	DESCRIPCION	ESTADO	EVIDENCIA
Soporte a la Organización				
Concentrarse en la Administración	Garantizar que la seguridad de la información se integre a las actividades del negocio	Las personas que integran la continuidad de seguridad de la información complementen el negocio con claves y procesos de gestión de riesgos. Se debe proporcionar consultorías de alto nivel		Estrategia de Seguridad de la información
Ofertar calidad y valor a los usuarios de los sistemas de información.	Garantizar que la seguridad de la información ofrezca valor	Las partes interesadas deben estar comprometidas a sostener una comunicación periódica de modo que se cumplan los requerimientos cambiantes de seguridad de la información.		Estrategia de Seguridad de la información
Cumplir los requerimientos legales y regulatorios relevantes.	Garantizar que se cumpla las obligaciones legales, que se gestionen las expectativas de las partes interesadas, y que se eviten sanciones	Se deben identificar las obligaciones de cumplimiento, se las debe traducir en requerimientos específicos de seguridad de la información y comunicar a las autoridades. Las sanciones asociadas al incumplimiento deben ser claramente comprendidas		Estado de cumplimiento de ISO 27001
Proporcionar datos exactos y oportunos sobre el ejercicio de la seguridad de la información	Apoyar los requerimientos de la organización.	Los requerimientos para la entrega de datos sobre el desempeño de la seguridad de la información deben estar claramente definidos y sustentados con las métricas más relevantes y adecuadas.		Informe mensual de gestión de la seguridad de la información
Evaluar las amenazas actuales y futuras hacia la información	Analizar y evaluar las amenazas emergentes de seguridad de la información	En la actualidad las tendencias más importantes y las amenazas específicas a la seguridad de la información se deben categorizar en un marco integral estándar que abraque un amplio espectro de temas como son los aspectos políticos, legales, económicos, socioculturales y técnicos.		Revisión y pruebas periódicas a la seguridad de la información
Promover la mejora continua en seguridad de la información	Reducir los costos, mejorar la eficacia y la eficiencia	Los modelos deben estar en constante cambio dentro de la organización		Indicador clave del desempeño, informes presentados mensualmente y anualmente de acuerdo a la gestión.
Defensa de la Organización				
Adoptar un enfoque basado en el riesgo	Garantizar que el riesgo sea tratado de una manera consistente y eficaz	Se debe examinar las opciones para abordar el riesgo vinculado con la información de modo que se puedan tomar decisiones fundamentales y documentadas sobre el tratamiento del riesgo.		Sistema de gestión de seguridad de la Información SGSI y la evaluación de riesgos
Proteger información	Evitar la divulgación de la	La información se debe identificar y luego clasificar de acuerdo a su nivel		Políticas y estándares de

clasificada	información clasificada.	de confidencialidad: secreta, restringida, interna y pública		seguridad de la información
Concentrase en aplicaciones críticas.	Priorizar la escasez de recursos de seguridad de la información protegiendo las aplicaciones	Comprender el impacto que puede tener en la organización, que ocasionaría una falta de integridad o disponibilidad de información importante, manipulada por las aplicaciones de la institución, mismas que pueden ser procesadas, almacenadas o transmitidas.		Políticas y estándares de seguridad de la información
Desarrollar sistemas seguros	Desarrollar sistemas de calidad y económicos en los cuales se pueda confiar.	La seguridad de la información debe ser integral para las fases de alcance, diseño, desarrollo y prueba del ciclo de vida de desarrollo de sistemas.		Estándares de seguridad de la información
Promover un comportamiento responsable respecto de la seguridad de la información**.**				
Actuar de una manera profesional y ética	Asegurar que las actividades relacionadas con la seguridad de la información sean confiables y eficientes	La seguridad de la información se basa en la capacidad de los profesionales que tenga una institución ya que de ellos depende del éxito o fracaso de precautelar la información.		Verificación de antecedentes
Promover una cultura positiva respecto de la seguridad de la información	Ejercer una influencia positiva respecto de la seguridad de la información sobre los usuarios	Se debe hacer énfasis en lograr que la seguridad de la información sea una pieza clave de la organización y que los usuarios se concienticen cada vez más sobre la seguridad.		Reuniones del comité de seguridad de gestión de la seguridad de la información SGSI, propuesto en el proyecto.

Tabla 2: Principios de seguridad de la Información según COBIT 5

Como se puede observar los componentes están basados en seguridad de la aplicación, la criptografía, monitoreo, gestión de incidentes, seguridad en línea, gestión de software malicioso(malware). (Fúster, de la Guía, Hernandez, Montoya, & Muñoz, 2001), protección de los datos, ciclo de vida del desarrollo del software, gestión de proveedores, planificación de continuidad del negocio, privacidad, gestión de identidades y acceso, gestión de riesgos, seguridad física, concientización, gobierno, política, gestión del ciclo de vida de los activos, rendición de cuentas y propiedad configuración del sistema, seguridad de la red que son los ejes fundamentales en donde deben cimentar las IES todas sus estrategias de seguridad ya que existen personas que buscan dañar la información o simplemente eliminarla por conveniencia, pero también se tienen los casos de estudiantes o docentes que en busca de investigación alteran información o consultan cosas que por su perfil no deben tener acceso. Azán, Bravo, Rosales, Trujillo, García & Pimentel, 2014).

4. Pruebas

El objetivo, de la investigación es planificar, organizar dirigir, evaluar y retroalimentar las actividades estratégicas para la implementación de los servicios de TIC's e implementar las acciones de seguridad preventivas, disuasivas y reactivas que permitan proteger la información dentro de las IES, y particularmente en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga.

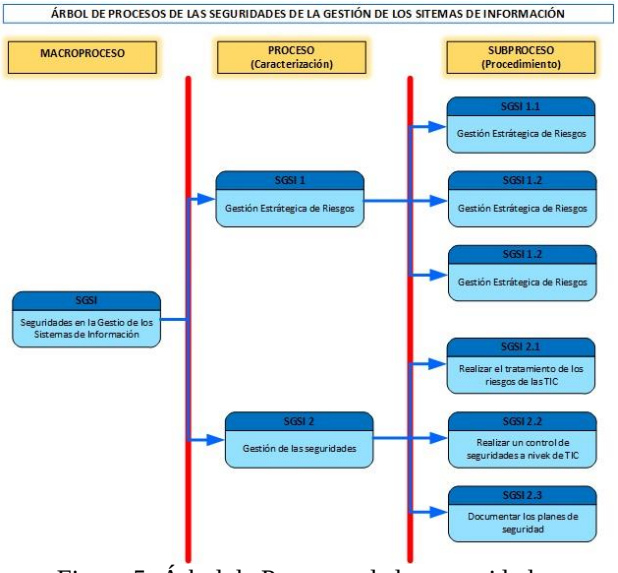

Figura 5: Árbol de Procesos de las seguridades

Con la aplicación del árbol de procesos se garantiza la disponibilidad y la integridad de los datos en los sistemas de información de la organización, esto arrojo como resultado de las buenas prácticas empleadas en la aplicación de normas y estándares de COBIT y estándares. (Núñez, 2013, pp.111-117).

Dentro del proceso se debe asegurar con los requisitos legales que estén según la norma actual vigente y de entes que regulen el tratamiento de la información.

SUBPROCESO	VOLUMEN		TIEMPO
	CANTIDAD	UNIDAD	PROMEDIO(minutos)
Gestión de Proyectos y requerimientos de TIC	1	Proyecto	259200
	1	Adquisición	27000
Gestión de Riesgos de TIC	6	Solicitud	129600
Seguridad de la Información	1	Monitoreo ejectutado por BD	1440

Tabla 3. Información Cuantitativa

5. Procesos Estadísticos

En la investigación se realiza un análisis a las aplicaciones que fueron desarrolladas de acuerdo a las necesidades de la Universidad de las Fuerzas

Armadas ESPE extensión Latacunga y al momento tecnológico por lo que en ocasiones no representan un aspecto relevante dentro de las seguridades de la información.

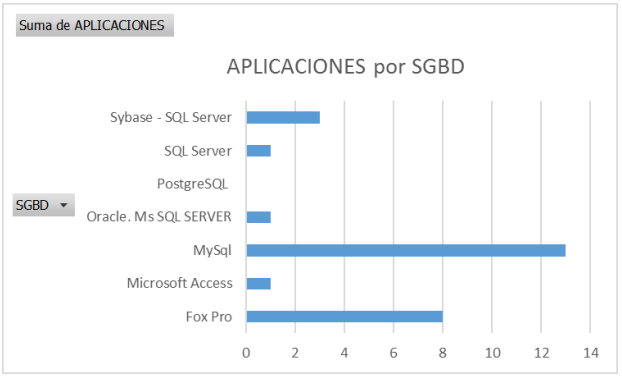

Figura 6. Aplicativos en producción

En la fig. 6. Se muestra todos los aplicativos que tiene la Universidad y en los SGBD en los que fueron desarrollados o adquiridos para cubrir las necesidades de automatización de la información.

Se puede observar que se tiene en la mayoría de SGBD que se tiene en la actualidad, así como en algunos que ya salieron del mercado, pero que todavía por intereses institucionales no han sido actualizados o cambiados hacia otros motores de Bases de Datos.

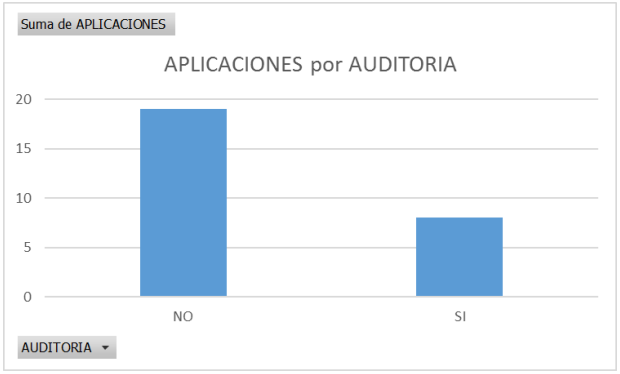

Figura 7: Aplicaciones que cuentan con Auditoria

De las aplicativos que se tienen en la Universidad 19 de ellas no cuentan con una auditoria a nivel de ingreso y operaciones entre registros en las bases de datos lo que supone un alto grado de exposición a un potencial robo de información, mientras que 8 de las mismas si tienen este tipo de aporte a la seguridad.

6. Evaluación de Resultados

Para la aplicación de la investigación se plantea en la Universidad de las Fuerzas Armadas ESPE extensión Latacunga, donde se tiene aplicativos en distintos SGBD y que se pudo observar que en algunos casos se tienen falencias que fueron detectadas a lo largo del presente trabajo

	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
	Inicial	En desarrollo	Definido	Gestionado	Optimizado
Política	Ausencia de política	Política limitada	N/A	Tramites	Limitado
Roles y responsabilidades	No definida	No definida	No definida	En tramites	N/A
Automatización	Manual	Regular	Baja	Ninguna	N/A
Alcance	No implementado	Limitado	Normal		
Eficacia	N/A	Poca	Poca	Avanzado	Mínima
Gestión de incidentes	Sin seguimiento	Ninguna			Avanzada
Medición	Sin medición	Bajo control	Poca	Media	Ninguna
Informes	Sin informes	Controlado	N/A	Avanzada	Bajo
Nomenclatura: **N/A:** No Aplica					

Tabla 4: Tabla de los modelos de madures

La tabla muestra el resultado de la investigación realizado en los SGBD de las aplicaciones de la Universidad de las Fuerzas Armadas ESPE, y en los cuales se tiene como resultado unos bajos estándares de acuerdo a las normas aplicadas por COBIT 5, a todos los parámetros que se pueden medir.

CONCLUSIONES

- La implementación de la guía técnica, mejoró la planificación de procesos de seguridad, pero en cambio desnudo otras facetas dentro de la administración de SGBD en los aplicativos.
- Los controles aplicados a las actualizaciones y cambios en los sistemas de información cubren las necesidades de seguridad de los datos en los departamentos de la institución, con procesos definidos para cada actividad para los administradores y personal técnico.

BIBLIOGRAFÍA

Bugosen Abi-Gosen, O. J., & Tejada Ruiz, C. D. (2015). Adaptación de modelo de gobierno y gestión de TI para la empresa virtual IT Expert basado en Cobit 5.

Carvajal, A. M. R., & León, H. A. N. (2011). Seguridad en bases de datos. Revista Cubana de Ciencias Informáticas, 5(1).

De la Paz, L. D., Mendoza, J. L. G., López-Porrero, B. E., González-González, L. M., & Lemahieu, W. (2015). Técnicas para capturar cambios en los datos y mantener actualizado un almacén de datos. Revista Cubana de Ciencias Informáticas, 9(4), 89-103.

Bleha, S., Slivinsky, C., & Hussien, B. (1990). Computer-access security systems using keystroke dynamics. IEEE Transactions on pattern analysis and machine intelligence, 12(12), 1217-1222.

Dorai, R., & Kannan, V. (2011). SQL injection-database attack revolution and prevention. J. Int'l Com. L. & Tech., 6, 224.

Disterer, G. (2013a). Iso/iec 27000, 27001 and 27002 for information security management.

Disterer, G. (2013b). Iso/iec 27000, 27001 and 27002 for information security management.

Al Omari, L., Barnes, P. H., & Pitman, G. (2012). Optimising COBIT 5 for IT governance: examples from the public sector. Paper presented at the Proceedings of the ATISR 2012: 2nd International Conference on Applied and Theoretical Information Systems Research (2nd. ATISR2012).

Beckers, K., Faßbender, S., Heisel, M., Heisel, J.-C., & Schmidt, H. (2012). Supporting the development and documentation of ISO 27001 information security management systems through security requirements engineering approaches. Paper presented at the International Symposium on Engineering Secure Software and Systems.

Preittigun, A., Chantatub, W., & Vatanasakdakul, S. (2012). A Comparison between IT Governance Research and Concepts in COBIT 5. International Journal of Research in Management & Technology, 2(6), 581-590.

Bartens, Y., De Haes, S., Eggert, L., Heilig, L., Maes, K., Schulte, F., & Voß, S. (2014). A visualization approach for reducing the perceived complexity of COBIT 5 Advancing the Impact of Design Science: Moving from Theory to Practice (pp. 403-407): Springer.

Mera Balseca, A. S. (2014). Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP Petroecuador de acuerdo a norma ISO/IEC 27002 y COBIT 5. Universidad de las Fuerzas Armadas ESPE. Maestría en Gerencia de Redes y Telecomunicaciones.

Moya, O. P., & Véliz, Y. Z. (2013). Proceso para gestionar riesgos en proyectos de desarrollo de software Process to manage risks in software development projects. Revista Cubana de Ciencias Informáticas, 7(2).

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1-13.

Fúster, A., de la Guía, D., Hernandez, L., Montoya, F., & Muñoz, J. (2001). Técnicas criptográficas de protección de datos. Alfaomega, Grupo Editor.

Amoore, L. a. The politics of possibility : risk and security beyond probability.

Azán-Basallo, Y., Bravo-García, L., Rosales-Romero, W., Trujillo-Márquez, D., García-Romero, E. A., & Pimentel-Rivero, A. (2014). Solución basada en el Razonamiento Basado en Casos para el apoyo a las auditorías informáticas a bases de datos Solution based on Case-Based Reasoning for supporting a computer auditing database. Revista Cubana de Ciencias Informáticas, 8(2).

Núñez, A. C. (2013). Conceptos de seguridad informática y su reflejo en la cámara de cuentas de Andalucía. Auditoría pública: revista de los Organos Autónomos de Control Externo (61), 111-117.