Revisión del proceso de operaciones de TI para una empresa de servicios de salud

Review of the process of IT operations for a health services company

Recibido: febrero 04 de 2019 | Revisado: abril 26 de 2019 | Aceptado: junio 12 de 2019

Edward José Flores Masías
Claudia Araceli Marchand Góngora

ABSTRACT

The objective of this research is to perform the evaluation of the General IT Controls in Operations Management implemented by the systems management of a health services company, to determine if the established controls can reduce the potential risks to acceptable levels , based on good practices that exist in the framework of COBIT 5 work and aimed at measuring the degree of confidence of controls in systems that affect financial statements within a company. In the detailed description of the review structure, the corresponding processes were evaluated and opportunities for improvement were identified. Finally, based on the analysis performed and the results obtained, necessary recommendations will be provided, so that the company can solve the problems encountered in order to improve profitability, in the audit carried out on information security and the efficiency of the systems analyzed.

Keywords: COBIT 5, IT Audit, Operations Management

RESUMEN

El objetivo de la presente investigación consiste en realizar la evaluación de los Controles Generales de TI en la Gestión de Operaciones implementados por la gerencia de sistemas de una empresa de servicios de salud, para determinar si los controles establecidos pueden reducir los riesgos potenciales a niveles aceptables, basándose en las buenas prácticas que existen en el marco de trabajo de COBIT 5 y orientadas a medir el grado de confianza de los controles en los sistemas que afectan a los estados financieros dentro de una compañía. En la descripción detallada de la estructura de revisión se evaluaron los procesos correspondientes y se identificaron las oportunidades de mejora. Finalmente, en base al análisis realizado y a los resultados obtenidos, se brindarán recomendaciones necesarias, para que la compañía pueda solucionar los problemas encontrados con el fin de mejorar la rentabilidad, en la auditoría realizada de seguridad de la información y la eficiencia de los sistemas analizados.

Palabras clave: COBIT 5, Auditoría de TI, Gestión de Operaciones

[1] Universidad Nacional Federico Villarreal
email: eflores@unfv.edu.pe
[2] Universidad Nacional Federico Villarreal
email: marchandgongora@gmail.com

INTRODUCCIÓN

Actualmente, un elevado porcentaje de entidades utilizan los Sistemas de Tecnologías de Información de complejidad creciente como pilares clave para obtener, procesar y transformar la información dentro de sus procesos de negocio, incluyendo su información financiera.

Debido a esta dependencia en las TI, y para que la Entidad refleje y proporcione una imagen fiel de sus estados financieros, es necesario definir y evaluar el entorno de control de sus Sistemas.

La problemática radica, en que muchas entidades al momento de ser evaluadas, presentan incumplimientos o falta de implementación de controles, dentro de su entorno de control de TI, derivando una serie de riesgos de seguridad de la información. "En este escenario la revisión de los denominados controles generales de TI (CGTI), es un procedimiento indispensable para reducir los riesgos a un nivel aceptable". (Minguillón, 2010, p.125)

Según un informe realizado por Deloitte, en el año 2014, el Perú es el segundo país de Latinoamérica con mayor número de fraudes, equivalente a un 67%, originado por las brechas de seguridad interna. (García & Enero, 2018)

Puntos Destacados	Argentina	Chile	Colombia	Ecuador	Guatemala	México	Perú
1. Los encuestados creen que hay un incremento en el presupuesto de seguridad de la información.	69%	100%	100%	100%	100%	50%	67%
2. Los encuestados creen que los gastos en seguridad de la información están alineados o por encima del plan estimado.	69%	67%	0%	82%	50%	50%	100%
3a. Las iniciativas de seguridad más importantes son: Cumplimiento regulatorio y legislativo de seguridad de la información.	31%	0%	0%	45%	50%	38%	100%
3b. Las iniciativas de seguridad más importante es: Protección de datos.	15%	67%	0%	18%	50%	38%	100%
4. Los encuestados han implementado o comprado servicios en la nube.	31%	71%	100%	27%	0%	70%	33%
5. Los encuestados han experimentado incidentes de seguridad privada durante el último año.	23%	33%	100%	36%	0%	13%	67%

Valores más Altos
Valores más Bajos

Figura 01: Los países con mayor índice de fraude
Fuente: Deloitte (2014). Principales países con mayor fraude

En el Perú, el factor oportunidad es el que explica, en mayor medida, la ocurrencia de fraude. Tanto la alta gerencia como la gerencia intermedia (en las empresas) coinciden en que éste factor explica el 80% de casos de fraude. (Lira, 2015)

La empresa de servicios de salud del presente estudio soporta sus procesos de gestión de la información interna y la de sus clientes de manera automatizada; es decir que existe dependencia de los sistemas informáticos para realizar, controlar y registrar sus operaciones y transacciones, implicando ello, que la empresa puede ser vulnerable ante amenazas que atenten contra la seguridad de su información; generando posibles riesgos e inseguridades procedentes de una amplia variedad de fuentes como: fraudes basados en informática, espionaje, vandalismo, sabotaje, daños por virus informáticos, ataques de intrusión o denegación de servicios, mal desarrollo de sistemas, caídas de los equipos tecnológicos críticos, etc.; que puedan estar impidiendo asegurar la continuidad del negocio o maximizando los daños a la organización o minimizando el retorno de las inversiones y las oportunidades de negocio.

Objetivo general:

Evaluar la efectividad y el cumplimiento de los controles generales de TI diseñados por una empresa de servicios de salud en Perú, en las categorías de Gestión de Accesos, Gestión de Cambios y Gestión de Operaciones de TI, para ayudar a minimizar los posibles riesgos de fraude.

Objetivos específicos:

- Evaluar la seguridad de la información y el cumplimiento de los controles generales de TI diseñados por la empresa de servicios de salud, en Gestión de Operaciones de TI, para evaluar el funcionamiento adecuado y el grado de confianza de los mismos.
- Analizar y Evaluar el funcionamiento adecuado de los controles de Gestión de Operaciones de TI, además de su grado de confianza.
- Proponer alternativas de solución y acciones de mejora que mitiguen los riesgos encontrados, basándose en las buenas prácticas que existen en el mercado actual.

Como justificación al presente trabajo realizado podemos mencionar:

Los desarrollos de auditorías se realizan en grandes, medianas y pequeñas empresas de todo el mundo, ya que permiten conocer los problemas que puedan tener las mismas, ya que tener deficiencias en sus procesos les pueden significar grandes pérdidas de dinero o ser alcanzados o superados por la competencia, este tema está en pleno auge en nuestro país. (Pulgarín, 2016, p.18)

Las organizaciones solicitan las auditorías externas cuando se detectan señales de debilidad, amenazas, desorganización, insatisfacción de los usuarios, falta evaluación de los niveles de riesgo, seguridad física y lógica, centro de proceso de datos fuera de control y falta de planes de contingencias. (Salinas, 2014)

Los procesos de evaluación de Controles Generales de TI (CGTI) considerados dentro del alcance es el Proceso de Gestión de Operaciones de TI.

Proceso de Operaciones de TI:

Realiza respaldos y restauraciones de información, programa y monitorea posibles desviaciones de las tareas automáticas de las aplicaciones y finalmente realiza el monitoreo de los problemas e incidentes reportados.

La información necesaria para realizar los procedimientos de prueba se solicitará al área de Tecnologías de la Información de la empresa.

MATERIALES Y MÉTODOS

Para el presente estudio se llevará a cabo el uso del estándar COBIT 5 en cuanto a los procesos indicados a continuación se refiere:

Revisión del proceso de operaciones de TI

En la revisión del proceso de gestión de operaciones de TI se revisarán los siguientes aspectos:

Gestión de respaldos y restauraciones, gestión de tareas programadas, gestión de incidentes.

A. Revisión de la Gestión de Respaldos y Restauraciones

Respaldos

Objetivo:

Revisar de manera oportuna los respaldos de información que realiza la empresa.

Proceso de Revisión:

1. Se identifican los controles y riesgos asociados en el proceso.
2. Se selecciona el universo de las copias de respaldo ejecutadas, en base a la periodicidad de la realización de las copias de respaldo.
3. Se realiza el recorrido y la muestra para validar que los respaldos hechos en el año hayan sido satisfactorios.
4. Recopilación de Hallazgos y recomendaciones

Restauraciones

Objetivo:

Identificar si se han realizado pruebas sobre los procedimientos de restauración de respaldos.

Procedimiento de Revisión:

1. Se identifican los controles y riesgos asociados en el proceso.
2. Se selecciona un recorrido y una muestra de las restauraciones efectuadas en el periodo de revisión y se valida que las restauraciones se hayan realizado.
3. Fnalmente se recopilan los hallazgos y las recomendaciones.

B. Revisión de la Gestión de Tareas Programadas

Objetivo:

Consiste en verificar que la compañía posee un adecuado control sobre sus tareas programadas y que los problemas con procedimientos programados pueden ser detectados y resueltos oportunamente.

Proceso de Revisión:

1. Se identifican los controles y riesgos asociados en el proceso.
2. Se solicita el detalle de las tareas ejecutadas en los servidores del alcance.
3. Se valida quienes son los usuarios con acceso a la gestión de las tareas programadas y si se encuentran autorizadas.
4. Recopilación de Hallazgos y recomendaciones.

C. Revisión de Gestión de Incidentes

Objetivo:

Validar si la empresa identifica incidencias en la gestión de operaciones, si estas han sido evaluadas y atendidas oportunamente por personal calificado.

Procedimiento de revisión:

1. Se identifican los controles y riesgos asociados en el proceso.
2. Se solicita el listado de todos los incidentes relacionados al proceso operativo de la empresa.
3. Se realiza el recorrido y la muestra de incidentes para verificar que todos fueron revisados, analizados y resueltos de manera oportuna.
4. Recopilación de Hallazgos y recomendaciones.

RESULTADOS

A. Revisión de Respaldos y Restauración:

Entendimiento:
Respaldo

Los respaldos de información son realizados de forma automática por la herramienta de extracción de la empresa. Todos los respaldos que realiza la herramienta son de tipo Total para los sistemas SIS01 y SIS02.

A continuación, se coloca un resumen del cronograma de respaldo:

Nro	SERVIDOR	FRECUENCIA	SISTEMA	TIPO
1	Backup_SIS01	diario	SIS01	Total
2	Backup_SIS01	semanal	SIS01	Total
3	Backup_SIS01	mensual	SIS01	Total
4	Backup_SIS02	diario	SIS02	Total
5	Backup_SIS02	semanal	SIS02	Total
6	Backup_SIS02	mensual	SIS02	Total

Figura 02: Categorías de revisión del proceso de operaciones
Fuente: Elaboración propia.

Control identificado:

Los datos de las aplicaciones se copian en medios de backups al menos semanalmente, y los mismos son resguardados físicamente en una locación diferente al equipo de producción.

Riesgo asociado:

Pérdida de datos o pérdida de capacidad de procesar con precisión los datos, debido a problemas de hardware o software.

Control a probar:

La herramienta de Backups realiza las copias de respaldo (Full) de forma diaria, semanal o mensual.

Universo de respaldos (Periodo: abril-octubre)

De acuerdo al cronograma respaldos mostrado, se identificaron 486 respaldos realizados para los Sistemas Oracle SIS02 y SIS01, los cuales fueron realizados en el periodo indicado del año 2018.

Tabla 01: *Universo de respaldos*

Nombre JOB	Abril Octubre
Bkp_SIS01 - Diario	201
Bkp_SIS01 - Semanal	34
Bkp_SIS01 - Mensual	8
Bkp_SIS02 - Diario	201
Bkp_SIS02 - Semanal	34
Bkp_SIS02 - Mensual	8
TOTAL	486

Fuente: Elaboración propia

Tabla 02: *Recorrido de respaldos*

Nro	Descripción	Día	Fecha	Sistema	Responsable
129	JOB 1 - SIS01 Diario	Martes	22/07/2018	SIS01	Jose Moore, Administrador de Base de Datos

Fuente: Elaboración propia

Recorrido de respaldos (Periodo: abril-octubre)

Se utilizó la aplicación "Generador de números aleatorios", para seleccionar el recorrido en función del universo de casos identificados.

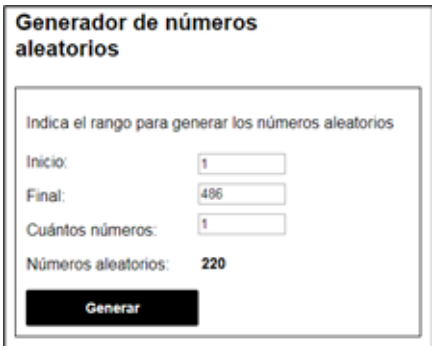

Figura 03: Generador de números aleatorios

Muestra de respaldos (Período: abril-octubre).

En base a los criterios de muestra, el número de casos seleccionados por Sistema será el siguiente:

Tabla 03: *Muestra Estratificada de respaldos*

Nombre JOB	Universo	Muestra
Bkp_SIS01 - Diario	201	7
Bkp_SIS01 - Semanal	34	1
Bkp_SIS01 - Mensual	8	1
Bkp_SIS02 - Diario	201	7
Bkp_SIS02 - Semanal	34	1
Bkp_SIS02 - Mensual	8	1
TOTAL	486	18

Elaboración propia

Se utilizó la aplicación "Generador de números aleatorios", para seleccionar las muestras por Sistema:

Muestra Backup_SIS01 – Diario

Utilizando el generador de números aleatorios, se obtuvo que los casos # 49, 56, 73, 101, 123, 149 y 183 son los seleccionados.

Muestra Backup_SIS01 – Semanal

Utilizando el generador de números aleatorios, se obtuvo que el caso # 27 fue el seleccionado.

Muestra Backup_SIS01 – Mensual

Utilizando el generador de números aleatorios, se obtuvo que el caso # 12 fue el seleccionado.

Muestra Backup_SIS02 – Diario

Utilizando el generador de números aleatorios, se obtuvo que los casos # 21, 43, 55, 80, 131, 155 y 178 son los seleccionados.

Se observa que las copias de respaldo de la muestra fueron ejecutadas de manera exitosa y cumplieron con el control identificado.

Restauración

Las pruebas de restauración de las copias de respaldo se efectúan trimestralmente de acuerdo a lo indicado por la empresa.

Control identificado:

Los backups se restauran a solicitud, y los mismos son resguardados físicamente en una locación diferente al equipo de producción.

Riesgo asociado:

Pérdida de datos o pérdida de capacidad de procesar con precisión los datos, debido a problemas de hardware o software.

Control a probar:

Esto se dará a través de la herramienta de restauraciones de las copias de respaldo de manera trimestral.

Universo de restauraciones (Periodo: abril-octubre).

En el Periodo de abril a octubre sólo se realizaron dos restauraciones.

Tabla 04: *Muestra de respaldos*

Nro.	Descripción	Día	Fecha	Sistema	Responsable	Control
49	JOB 1 - SIS01 Diario	sábado	12/05/2018	SIS01	Jose Moore	Ok
56	JOB 1 - SIS01 Diario	lunes	21/05/2018	SIS01	Jose Moore	Ok
73	JOB 1 - SIS01 Diario	jueves	31/05/2018	SIS01	Jose Moore	Ok
101	JOB 1 - SIS01 Diario	sábado	7/07/2018	SIS01	Jose Moore	Ok
123	JOB 1 - SIS01 Diario	jueves	9/08/2018	SIS01	Jose Moore	Ok
149	JOB 1 - SIS01 Diario	jueves	13/09/2018	SIS01	Jose Moore	Ok
183	JOB 1 - SIS01 Diario	lunes	17/09/2018	SIS01	Jose Moore	Ok
27	JOB 2 - SIS01 Semanal	domingo	23/09/2018	SIS01	Jose Moore	Ok
12	JOB 3 - SIS01 Mensual	sábado	12/05/2018	SIS01	Jose Moore	Ok
21	JOB 4 - SIS02 Diario	lunes	22/04/2018	SIS02	Jose Moore	Ok
43	JOB 4 - SIS02 Diario	lunes	7/05/2018	SIS02	Jose Moore	Ok
55	JOB 4 - SIS02 Diario	sábado	19/05/2018	SIS02	Jose Moore	Ok
80	JOB 4 - SIS02 Diario	miércoles	20/06/2018	SIS02	Jose Moore	Ok
131	JOB 4 - SIS02 Diario	viernes	10/08/2018	SIS02	Jose Moore	Ok
155	JOB 4 - SIS02 Diario	viernes	17/08/2018	SIS02	Jose Moore	Ok
178	JOB 4 - SIS02 Diario	viernes	24/08/2018	SIS02	Jose Moore	Ok
13	JOB 5 - SIS02 Semanal	domingo	17/06/2018	SIS02	Jose Moore	Ok
8	JOB 6 - SIS02 Mensual	martes	4/09/2018	SIS02	Jose Moore	Cumple

Fuente: Elaboración propia

Tabla 05: *Universo de restauraciones*

Sistema	Descripción	Fecha
SIS02	1° trimestre	Junio 2018
SIS02	2° trimestre	Julio 2018

Fuente: Elaboración propia

Muestra de restauración (Periodo: abril-octubre)

Tabla 06: *Muestra de Restauración*

Sistema	Descripción	Fecha	Control
SIS02	2° trimestre	Julio 2018	Cumple

Fuente: Elaboración propia

Se observa que la restauración de la copia de respaldo, fue ejecutada de manera exitosa y cumplió con el control identificado.

B. Revisión de Tareas Programadas:

Se realizó la revisión de los privilegios de acceso que tienen los usuarios sobre las tareas configuradas en los servidores que contienen los sistemas en alcance:

• SERVER02: Servidor de Aplicación SIS02.
• SERVER03: Servidor de Base de Datos SIS02.
• SERVER01: Servidor de Aplicación y Base de Datos de SIS01.

Control identificado:

Personal de TI monitorea la ejecución de las tareas programadas (Job Schedule) y efectúa acciones apropiadas ante los problemas que surgen.

Riego asociado:

Tratamiento inapropiado de problemas con programas (job schedule) que no se ejecutaron adecuadamente hasta su finalización.

Control a probar:

El personal autorizado tiene acceso de ejecución de tareas programadas.

Servidor SERVER02

Tabla 07: *Tareas ejecutadas en el servidor SERVER02*

Nº	Tarea Programada	Descripción	Programación
1	Task Alert	Verificación de alertas en Linux	Diario, c/20 min
2	Task FreeSpace	Verificación de espacio libre en file systems	Diario, c/05 min
3	Task copy_bkp	Proceso previo a la clonación	Diario, a las 23:00
4	resourcesSO.sh	Consumo de recursos de los sistemas operativos	Diario, a las 9:30 a.m

Fuente: Elaboración propia

Tabla 08: *Usuarios administradores del Servidor SERVER02*

Name	Password	User ID	Principle Group	Account Name	Home Directory	Shell
root	x	0	0	root	/root	/bin/bash

Fuente: Elaboración propia

Se observa que el perfil administrador del sistema lo tiene la cuenta root, cuyo propietario es el Sr. Jose Moore - Administrador de Base de Datos.

Tabla 09: *Usuarios administradores del Servidor SERVER03*

USER_ID	USER_NAME	DESCRIPTION	RESPONSIBILITY
225	J_MOORE	Jose Moore	Administrador de Sistema
1	SYSADMIN	System Administrator	Administrador de Sistema

Fuente: Elaboración propia

Los usuarios responsables de la administración y ejecución de los jobs son las cuentas J_MOORE y SYSADMIN, ambas administradas por el Sr. Jose Moore - Administrador de Base de Datos.

C. Revisión de Gestión de Incidentes:

Entendimiento

Como parte del entendimiento del proceso Gestión de Incidentes, se obtuvo una reunión con el Administrador de BD, a fin de tener un entendimiento del Proceso de Gestión de Cambios de Incidentes.

1. El Usuario Final reporta el incidente vía correo electrónico / teléfono.
2. El Administrador de Servicios de TI, el Administrador de Red o Administrador de Bases de Datos, identifica el incidente, lo registra y asocia al grupo de servicios que corresponda en la aplicación de Registro de incidentes.
3. El incidente es derivado al personal de Service Desk, quién analiza el incidente e identifica el problema.
4. Service Desk resuelve, registra el incidente y da por cerrado el ticket.

Control identificado:

Los incidentes o problemas relacionados a TI son identificados y resueltos de manera oportuna.

Riego asociado:

Demoras en la atención y resolución de problemas debido a la mala gestión de incidentes relacionados a TI.

Control a probar:

Atención y resolución oportuna del incidente reportado relacionado a las operaciones de TI.

Universo de incidentes (Periodo: octubre 2017- setiembre 2018)

El universo de incidentes se extrajo del Servidor de procesos programados, filtrándose los que se encontraban resueltos y que pertenecían a los sistemas dentro del alcance.

Recorrido de incidentes (Periodo: octubre 2017- setiembre 2018)

Se utilizó la aplicación "Generador de números aleatorios", para seleccionar el recorrido en función del universo de incidentes resueltos identificados.
El caso #178 fue elegido como recorrido.

Tabla 10: *Recorrido de incidentes*

Nro.	Origen	Sistema rubro	Sistema	Cod documento	Fecha creación	cod_asignacion analista
178	Aplicaciones	APL - Sistemas SIS02	Accounts Payable	REP-003669	23/11/2017	jperez

Fuente: Elaboración propia

Muestra de incidentes (Periodo: octubre 2017- setiembre 2018)

En base a los criterios de muestra, el número de incidentes seleccionados, registrados en el servidor de procesos programados será el siguiente:

Tabla 11: *Muestra seleccionada de incidentes*

Sistema	Universo	Muestra
Sistema Control de Tareas	134	11

Fuente: Elaboración propia

Se utilizó la aplicación "Generador de números aleatorios", para seleccionar las muestras:

Muestra Incidentes – Servidor de procesos programados

Los casos # 27, 34, 43, 50, 66, 75, 88, 101, 115, 123, 131 son los seleccionados.

En la revisión realizada de los casos de muestra, se observó que los incidentes no manejan criterio de severidad (alto impacto, medio impacto y bajo impacto) y tampoco tiempos de respuesta definidos, lo cual no permite dar una adecuada atención a los incidentes.

Como resultado del presente estudio se llegó a identificar las siguientes oportunidades de mejora para la gestión de operaciones de la empresa de servicios de salud:

Oportunidad de mejora 1: operaciones de ti – gestión de incidentes

Condición:

Durante la revisión del procedimiento de gestión de incidentes, se identificó que los incidentes no cuentan con un adecuado manejo y monitoreo, generándose colas en los requerimientos de los usuarios diariamente, además de disconformidad y desconfianza. En el actual flujo de atención, todas las incidencias son atendidas de acuerdo al orden de reporte o de acuerdo al criterio que toma el personal encargado de su diagnóstico, el diagnóstico de las incidencias se tratan en un solo nivel.

Impacto:

El no contar con un adecuado manejo de incidentes, podría conllevar a que exista el riesgo que se presente un incidente que afecte el desempeño o paralice las operaciones del negocio y no se puedan restablecer en el tiempo requerido.

Recomendación:

Se recomienda contar con procesos definidos para la mejora en la gestión de incidentes de manera óptima y que refleje la realidad. Así mismo se recomienda evaluar la implementación del Proceso ITIL de gestión de incidentes de TI, ya que sus prácticas permiten realizar mejor el trabajo, incrementar la calidad del servicio y reducir costes.

Oportunidad de mejora 2: entorno de control de ti – políticas y procedimientos

Condición:

Durante la revisión se observó que la Compañía carece de una Política de seguridad de la información y de un Plan de Continuidad de Negocios (BCP).

Impacto:

El no contar con una política de seguridad de la información clara y definida, conlleva a que existan riesgos que atenten contra los activos críticos de la Compañía, que no se estén gestionando de manera adecuada.

El no contar con políticas y procedimientos

actualizados relacionados a continuidad de negocios, podría conllevar a que exista el riesgo que se presente un incidente que afecte el desempeño o paralice las operaciones del negocio y no se pueden restablecer en el tiempo requerido.

Recomendación:

Elaborar una Política General de Seguridad de la Información que esté orientada a proteger la información (en la totalidad de su ciclo de vida: creación, difusión, modificación, almacenamiento, preservación y eliminación) así como los medios y las personas que acceden a la misma con la finalidad de garantizar su integridad, disponibilidad y confidencialidad.
Elaborar un plan de continuidad de negocios que tenga como objetivo proteger los procesos críticos de la Compañía contra desastres o fallas que atenten contra las operaciones del negocio.

Como resultado de la revisión efectuada, se han observado deficiencias en los controles identificados, las cuales representan un riesgo elevado para la integridad, confidencialidad, autenticidad, disponibilidad y trazabilidad de la información de la empresa de servicios de salud. Sobre las deficiencias se han propuesto oportunidades de mejora con el objetivo de que la Gerencia pueda tomar acciones en base a las recomendaciones indicadas con el objetivo de reducir los riesgos de fraude.

Los problemas de seguridad de la información y las dificultades operacionales pueden detectarse antes de que suceda por lo que le permite a la organización evitar mayores costos a causa de las deficiencias detectadas.

Una vez realizada la evaluación de controles generales de TI se recomienda lo siguiente:

- Evaluar la aplicación de los planes de acción recomendados como resultado de la revisión.
- Alinear los objetivos estratégicos con las políticas que se tienen planteadas en la compañía y a su vez monitorear el cumplimiento de los mismos.
- Establecer una gestión de Tics en base a estándares y buenas prácticas de la industria que garanticen la seguridad e integridad de los servicios de TI.
- Concientizar al personal y a la alta dirección de la compañía sobre la importancia y criticidad de la seguridad de la información en los procesos de negocio.
- Realizar la auditoría en el uso de tecnologías de información con una frecuencia de una vez al año

DISCUSIÓN

Después de haber realizado el presente estudio para abordar el tema de la validación de controles en el ámbito de la gestión de operaciones de TI en la empresa de servicios de salud, se revisaron e identificaron trabajos de auditorías de TI donde no solo se tiene en cuenta el marco de trabajo de COBIT 5, tal como se ha descrito en el presente trabajo, sino también que otros trabajos, como es el caso de Roberto, A. (2017) Evaluación de Controles Generales de TI, y su Impacto en los Estados Financieros, han utilizado el soporte adicional de otros estándares internacionales, tal es el caso de la norma ISO2000, así como también el ámbito de gestión de servicios de ITIL, de esta forma, completando el soporte adecuado para garantizar una mejor solución a los resultados obtenidos por la revisión realizada.

REFERENCIAS

Alfonso, Y., Blanco, B., & Loy, L. (2012). Auditoría con Informática a Sistemas Contables. Revista de Arquitectura e Ingeniería, 6(2).

Aviles, R. (2017). Evaluación de Controles Generales de TI y su impacto en los Estados Financieros (Trabajo final de Maestría). Universidad Abierta de Cataluña, Barcelona, España.

Espinoza, W. (2016). The information technology as constructionist tool for financial auditor. Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia, 11(11).

García, E., & Enero, R. Sistema de información para la prevención y control de fraude para colaboradores de red de tienda de una entidad financiera del Perú. (Tesis de Licenciatura). Universidad Tecnológica del Perú, Lima.

Martinez, D., Negrín, E., López, L., & Rodríguez, K. (Diciembrede 2017). Propuestadeunprogramade auditoría a los sistemas de información. Revista Especializada en Ciencias Administrativas, 8(2).

Minguillón, A. (Diciembre de 2010). La revisión de los controles generales en un. Auditoría Pública(52).

Montaño, V., Combita, H., & De la Hoz, E. (2017).

Alineación de Cobit 5 Y Coso IC–IF para definición de controles basados en Buenas Practicas de TI en cumplimiento de la Ley Sarbanes - Oxley. Revista Espacios, 38(23).

Pulgarín, A. Auditoría Informática a la empresa Ecuamails. (Tesis de licenciatura). Universidad Tecnológica Israel, Cuenca.

Salinas, J. E. (Noviembre de 2014). Control Interno y uso de TI en las organizaciones: elempresario. Obtenido de http://elempresario.mx/auditoria/control-interno-uso-ti-organizaciones

Soberanis, M. d., & Herrera, F. La auditoría interna en la detección y prevención de fraudes. (Trabajo Nacional). XXX Conferencia Interamericana de Contabilidad, Uruguay.

Vacio, V. (Diciembre de 2014). Principio 11 de COSO III: AUDITOOL. Obtenido de https://www.auditool.org/blog/control-interno/3128-principio-11-selecciona-y-desarrolla-controles-generales-sobre-tecnologia