UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

GESTIÓN DE RIESGOS INFORMÁTICOS A LOS QUE SE EXPONEN LOS EQUIPOS Y PROGRAMAS DEL DEPARTAMENTO INFORMATICO DE LA UTMACH

MAXI CABRERA MAYRA IVONNE
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

GESTIÓN DE RIESGOS INFORMÁTICOS A LOS QUE SE EXPONEN LOS EQUIPOS Y PROGRAMAS DEL DEPARTAMENTO INFORMATICO DE LA UTMACH

MAXI CABRERA MAYRA IVONNE
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

GESTIÓN DE RIESGOS INFORMÁTICOS A LOS QUE SE EXPONEN LOS EQUIPOS Y PROGRAMAS DEL DEPARTAMENTO INFORMATICO DE LA UTMACH

MAXI CABRERA MAYRA IVONNE
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 21 DE FEBRERO DE 2020

MACHALA
21 de febrero de 2020

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado GESTIÓN DE RIESGOS INFORMÁTICOS A LOS QUE SE EXPONEN LOS EQUIPOS Y PROGRAMAS DEL DEPARTAMENTO INFORMATICO DE LA UTMACH, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

GONZALEZ SANCHEZ JORGE LUIS
0703333898
TUTOR - ESPECIALISTA 1

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 2

OCHOA CAICEDO HECKLER ROTHWELL
0702681917
ESPECIALISTA 3

Fecha de impresión: viernes 21 de febrero de 2020 - 11:35

GESTIÓN DE RIESGOS INFORMÁTICOS A LOS QUE SE EXPONEN LOS EQUIPOS Y PROGRAMAS DEL DEPARTAMENTO INFORMÁTICO DE LA UTMACH

por Mayra Ivonne Maxi Cabrera

Fecha de entrega: 09-feb-2020 11:09p.m. (UTC-0500)
Identificador de la entrega: 1254452996
Nombre del archivo: MAYRA_IVONNE_MAXI_CABRERA.pdf (317.19K)
Total de palabras: 2470
Total de caracteres: 14574

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, MAXI CABRERA MAYRA IVONNE, en calidad de autora del siguiente trabajo escrito titulado GESTIÓN DE RIESGOS INFORMÁTICOS A LOS QUE SE EXPONEN LOS EQUIPOS Y PROGRAMAS DEL DEPARTAMENTO INFORMATICO DE LA UTMACH, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 21 de febrero de 2020

MAXI CABRERA MAYRA IVONNE
0107313520

RESUMEN

La era del conocimiento se solventa mediante sistemas informáticos, servicios virtuales y potencialidades ofimáticas, capaces de mejorar en todo sentido las actividades diarias, laborales, profesionales e integrarlas sutilmente a la sociedad. Aunque dichas bondades han revolucionado la educación, medicina, ciencias e ingeniería conllevan riesgos o condiciones adversas que son eclipsadas por sus ventajas.

Como responsabilidad social de la carrera de contabilidad y auditoría se analiza la gestión de riesgos informáticos en el departamento de informática de la Universidad Técnica de Machala, aplicando una metodología explicativa de carácter analítica para dirimir criterios al secuenciar un procedimiento adecuado a las vulnerabilidades detectadas en el estudio.

En los resultados se da una valoración cualitativa de los riesgos, analizando sus afectaciones en las distintas dependencias del sistema institucional; sin embargo, el mayor problema es el tiempo que degrada todas las prestaciones tecnológicas sin que el recurso humano tome las medidas pertinentes.

Palabras clave: gestión, riesgo informático, hardware, software, sistemas.

ABSTRACT

The age of knowledge is solved through computer systems, virtual services and office potential, capable of improving in every way the daily, work, professional activities and subtly integrate them into society. Although these benefits have revolutionized education, medicine, science and engineering, they carry risks or adverse conditions that are eclipsed by their advantages.

As a social responsibility of the accounting and auditing career, the management of computer risks in the IT department of the Technical University of Machala is analyzed, applying an explanatory methodology of analytical character to settle criteria when sequencing a procedure appropriate to the vulnerabilities detected in the study.

The results give a qualitative assessment of the risks, analyzing their effects on the different dependencies of the institutional system; However, the biggest problem is the time that degrades all technological benefits without the human resources taking the appropriate measures.

Keywords: management, computer risk, hardware, software, systems.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

1. INTRODUCCIÓN

Hoy en día las prestaciones informáticas solventan la mayoría de requerimientos sociales y optimizan las labores cotidianas, son imprecisables en organizaciones e instituciones que manejan gran cantidad de datos. El desarrollo tecnológico ha fusionado los sistemas digitales con las labores profesionales haciendo inseparable al *software* como herramienta tanto personal como académica o de cualquier índole.

La Universidad Técnica de Machala como entidad formadora de profesionales y constructora del conocimiento, hace uso de plataformas digitales, aplicaciones web, servicios vía internet, entre otros medios para desempeñar sus actividades al explotar las potencialidades del hardware y software en las diferentes disciplinas que ostenta.

Paralelamente a las clases, existen otras dependencias importantes que se encargan de tareas como matriculación, contabilidad, bienestar estudiantil, centro de educación continua, departamento de investigación, DNA, y departamento informático trabajando en sincronía para demostrar la integridad que caracteriza a nuestra alma mater.

No obstante, las bondades computacionales tienen su contra parte adversa debido a las amenazas/vulnerabilidades propias de los sistemas informáticos; por tal razón es relevante conocerlas tomando las medidas pertinentes al garantizar su seguridad y calidad.

La contabilidad y auditoría es una rama interdisciplinaria de la ingeniería, con la misión de ser un agente externo e interno de evaluación, asegurando el correcto funcionamiento de los sistemas contables, declaraciones tributarias y seguridad organizacional; donde la informaciòn es un activo vital para toda operación financiera. La auditoría informática es el área del conocimiento encomendada de velar por los medios computacionales, detectado debilidades, analizando controles tanto físicos como lógicos e inferir procedimientos al retroalimentar la calidad de la informaciòn con la finalidad de garantizar un desempeño óptimo al reducir al mínimo los riesgos del entorno empresarial.

El objetivo del escrito es Analizar la gestión del riesgo informático en los equipos y programas del departamento informático de la Utmach; se aplica una metodología abductiva al dirimir criterios a través de una revisión literaria para argumentar los resultados.

En la parte final se destacan las conclusiones, evidenciado el estado en seguridad informática de la dependencia analizada, objetando cuáles medidas son factibles y frente a qué amenazas se debe reaccionar en forma oportuna.

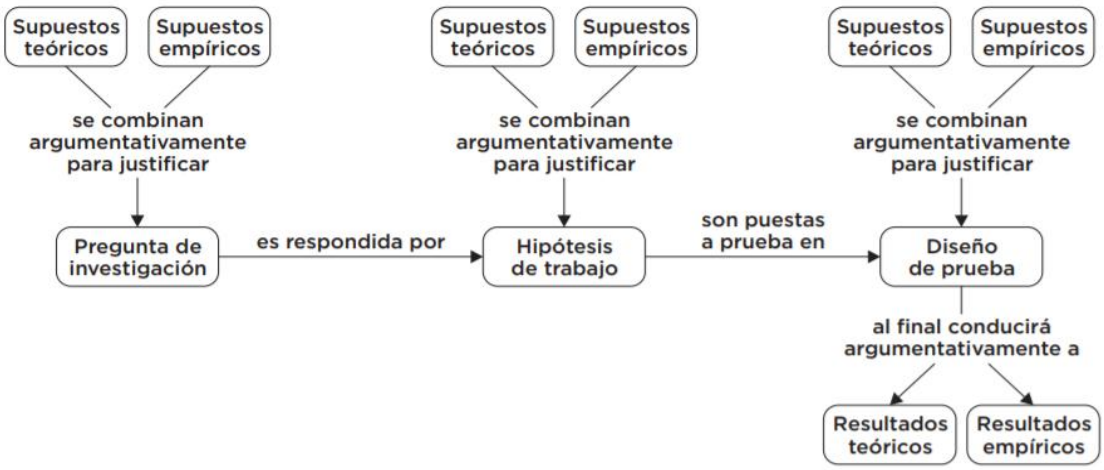
2. DESARROLLO

Consiste en describir el proceso para solventar el caso práctico, parte de la base epistemológica hasta la enunciación de resultados infiriendo el grado de seguridad computacional que ostenta el departamento de informática.

2.1 Marco teórico:

Es la contextualización del objeto de estudio, donde se definen los aspectos claves del proyecto desde su propia perspectiva induciendo al lector a comprender la temática bajo la guía del autor al documentarse adecuadamente.

Figura 1. Estructura cotidiana de un proyecto investigativo



Fuente: (RAMOS, 2018)

2.1.1 Contabilidad y auditoría.

Es una carrera profesional de amplio espectro, con la difícil tarea de cohesionar los estados contables con las normativas competentes, dar integridad y confiabilidad a los valores presentados; además es una labor que exige ética e inclusive se eleva a una caldiad moral como supervisor monetario.

De acuerdo con Pizarro, Ormaza y Ruiz (2018) sus funciones son:

- Auditoria de estados financieros
- Análisis de estados contables, políticas y procesos monetarios
- Asesoría, planificación y capacitación al incrementar la productividad
- Mejorar la eficiencia y desarrollo de la organización

2.1.2 Auditoria Informàtica.

Es la inspección cuidadosa de los sistemas digitales, con el objeto de encontrar fortalezas y debilidades al medir la funcionalidad de los mismos en beneficio de la organización, realizando las acciones pertinentes (Arcentales Fernández & Caycedo Casas, 2017).

En el campo de las instituciones de educación superior la auditoria de sistemas, es la retroalimentación de su seguridad al preservar datos e informaciòn, permite determinar controles aplicables a su contexto empresarial a un costo factible para ser ejecutado.

2.1.3 Investigaciòn Bibliográfica.

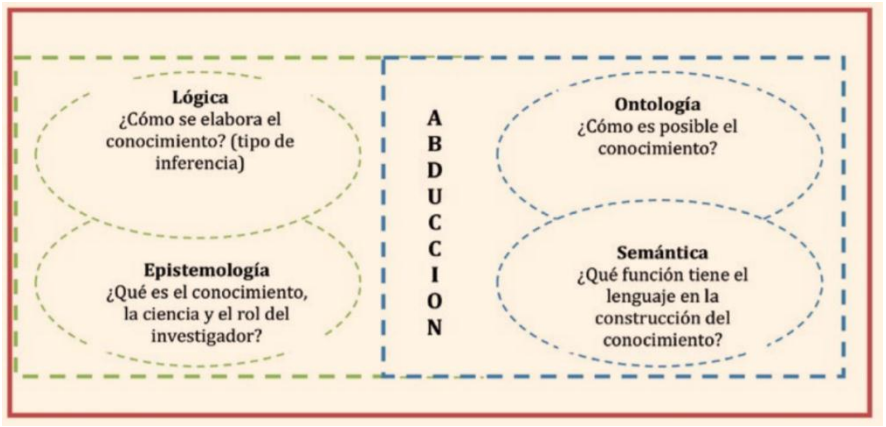
Es la búsqueda sistematizada de informaciòn documentada sobre una temática, con la idea de sustentar las opiniones del autor en contraste con publicaciones en el mismo ámbito, construyendo el marco teórico heurísticamente (Martín & Lafuente, 2017).

Está técnica es prácticamente aplicable en todo proceso y más al argumentar una auditoría basada en reglamentos, estatutos o leyes vigentes que dan objetividad a los procesos.

2.1.4 Análisis abductiva.

Es un proceso lógico en el cual se suma conocimientos dentro de un mismo contexto, facilita explicar las hipótesis e inducir conjeturas en forma concisa analizando sus relaciones hasta verificar lo planteado.

Figura 2. Explicación filosófica de la abducción



Fuente: (Nunez Moscoso, 2019)

2.1.5 Seguridad Informàtica.

Es un proceso continuo, consiste en mantener al mínimo la probabilidad de darse un evento adverso para los sistemas computacionales, su meta secundaria es preservar la calidad e integridad de la informaciòn (Quiroz-Zambrano & Macías-Valencia, 2017).

2.1.6 Debilidades y amenazas.

Las debilidades en sistemas operativos son toda vulnerabilidad explotable, es decir los caminos por donde se concreta un ataque; por ejemplo, contraseñas débiles, falta de controles físicos, falta de auditoria, carencia de certificados web o personal especializado son algunos puntos flacos en la seguridad.

Las amenazas son cualquier agente que puede materializar un daño sobre el sistema, generalmente los elementos desatendidos e ignorados son las mayores amenazas (Castillo Fiallos, Cisneros Barahona, Méndez Naranjo, & Jácome Segovia, 2017).

Las más comunes se destacan a continuación:

- Hackers
- Virus, malware, bob net
- Softwares piratas
- Sistema operativo desactualizado
- Espionaje e infiltración de datos

2.1.7 Riesgos en sistemas informáticos.

El riesgo es la posibilidad de efectuarse un ataque, según Niño y Sigila (2018) son:

- Inyección SQL
- Pérdida de autentificación
- Exposición de datos sensibles
- Entidades externas XML
- Configuración de seguridad incorrecta
- Ataques XSS (Cross-site-scripting)
- Explotar vulnerabilidades conocidas

2.1.8 Controles y medidas de protección de datos.

Son las formas de supervisar la calidad de la informaciòn, prevenir y responder ante posibles ataques o cubrir debilidades detonantes en violaciones de seguridad; existen dos principalmente los físicos aplicados al personal y en segundo lugar los lógicos aplicados a los activos intangibles mediante software o archivos digitales.

Cuadro 1. Controles de seguridad informáticos aplicables a un entorno institucional

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).

Fuente: (Martelo, Luis, & Maza, 2018)

2.1.9 Departamento de Informàtica Utmach.

Es una dependencia transversal que gestiona todas las acciones referentes a la infraestructura tecnológica; la Dirección de TIC`s tiene su propio reglamento en políticas de seguridad e imparte responsabilidades a todos los implicados, para sistematizar la seguridad informática en todos los procesos tanto académicos como administrativos.

Se resalta que hoy en día los datos son comparables al petróleo, gracias a su valor comercial y tratamiento asociado con otros fines en estudios de mercado o conductas en consumidores (Mendoza Enríquez, 2018).

2.2 Caso Práctico:

Las nociones prácticas son las competencias de mayor valor en la vida profesional, por ende, las universidades optan por dar autonomía al estudiante al momento de resolver casos prácticos, vinculando por cuenta propia los conocimientos adquiridos en la carrera (Morga, Cusó, & Juárez, 2018). El complexivo es una abstracción discreta de las labores encontradas en el campo de acción con el objeto de incentivar juicio crítico al ejercer la carrera.

2.2.1 Riesgos Informáticos en la Utmach.

En primera instancia se deben identificar las debilidades y vulnerabilidades, describiendo sus afectaciones en las diversas áreas operativas, derivadas del departamento de informática.

Cuadro 2. Vulnerabilidades en las áreas del departamento informático

CONCEPTO	**VULNERABILIDADES**	**EFECTOS**
Sistemas operativos	Desactualizados, falta de licencias y errores en su instalación Antivirus caducados, sin licencia	Fallos continuos en el sistema Pérdidas de datos y registros por virus o intromisiones
Hardware	No actualizados, falta de mantenimiento y corrección de averías	Poca versatilidad, daños parciales o totales a los equipos
Rede e internet	Saturación de la red Estudiante y Docente Poca accesibilidad a los servicios online dentro del campus Posibles pérdidas de datos e	Pérdida de activos digitales, no disponibilidad de plataformas o servicios online Demoras en proyectos y no ejecución de tareas

	informaciòn	
Administrativo	No se ejecuta auditoria externa ni designa fondos para renovación tecnología	Deterioro en la calidad e integridad de los servicios, daños en la infraestructura
Personal	No se dan controles físicos a gran escala, poca socialización de políticas y no se cuenta con personal especializado	Pérdida de datos e informaciòn sensible

Fuente: Elaboración Propia

Los efectos aún no se han presentado en la institución, pero ya se notan malestares como la lentitud del internet, falta de dinamismo en los servicios online, computadoras sin las prestaciones requeridas, ni un plan de mejora que remedio tales adversos.

2.2.2 Evaluación de riesgos informáticos.

Es necesario valorar los riesgos para designar acciones al grado de peligrosidad, se han clasificado de acuerdo a una escala cualitativa, sencilla y práctica; aquellos riesgos que causan estragos totales son catalogados como *ALTO*, los que causan daño parcial o controlable nivel *MEDIO*, la ausencia de daños al tener un buen funcionamiento es riesgo *BAJO*.

Cuadro 3. Valoración cualitativa de los riesgos identificados

IMPACTO	ALTO	MEDIO	BAJO
Sistema operativo	Pérdida total de datos e informaciòn Incapacidad total de los ordenadores	Pérdida parcial de datos Falla temporal del sistema	No existen probabilidades factibles de pérdidas o ataques
Hardware	Daños irreparables y pérdida total de activos tangibles Alto costo de renovación	Daños parciales a los equipos y costo promedio en su reparación	No se presentan fallos en el hardware
Rede e internet	Inhabilitación total de servicios y no accesibilidad a la red Destrucción de los activos lógicos e infraestructura digital	Pérdida de datos e inconsistencias en las funciones gestadas online Daño parcial a la infraestructura lógica	Todos los sistemas lógicos vía online operan al 100%
Administrativo	Desconfianza hacia las autoridades Irresponsabilidad e incompetencia al no evitar tales supuestos	Pérdida de la aceptación institucional y problemas asociados al bajo rendimiento organizacional	Control e integridad en sus responsabilidad, alta aceptación política
Personal	Abandonar la	Falencias en cuidar	Empoderamiento

	institución Desistir de sus cargos Corromper, hurtar o exponer datos sensibles	los activos, filtración de datos o conflictos con la competencia	del recurso humano y mayor desarrollo organizacional

Fuente: Elaboración Propia

Se observa que los riesgos en su mayoría son viabilizados, por dos descuidos generales el primero la falta de auditoria y retroalimentación de su seguridad; el segundo la carencia de fondos monetarios para efectuar las acciones necesarias.

Es relevante denotar, que la gestión de riesgo pese a ser una disciplina profesional, es también una cuestión cultural debiendo inculcarse, educar y ser socializada constantemente al menos mediante juntas internas, para analizar el estado actual evitando deterioros progresivos en los sistemas.

2.2.3 Metodologías para gestión de riesgos.

Es imperioso implementar una gestión propia para responder ante los riesgos, no solo informáticos sino en general, contar con un plan de acción hace la diferencia entre recuperarse o no de un desastre; en estos últimos años se han desarrollado metodologías a nivel internacional ampliamente aceptadas por entidades públicas, por ello se analizan las dos más comunes en el área computacional.

COBIT 5.

Objetivos de Control para las Tecnologías de la Información y Relacionada, es un proceso sistemático para supervisar el riesgo, es caracterizado por diferenciar control de gobierno en TIC`s al ser adaptable se puede acoplar a los requerimientos de la Utmach.

Figura 3. Habilidades de COBIT 5

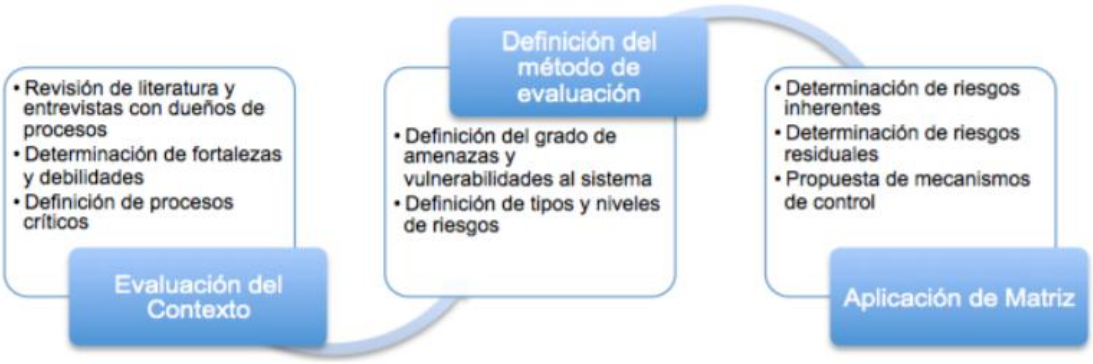
Fuente: (Yrigoyen-Quintanilla, 2016)

Normativa ISO 31000.

La organización internacional de estandarización siempre busca la eficiencia, se sustenta en apreciaciones estratégicas y procesos operativos factibles en todo ámbito sin importar su finalidad o razón social. La familia ISO esquematiza la gestión en evaluar, definir y aplicar una serie de acciones al mitigar los peligros en forma eficiente; sin embargo, su meta es armonizar el desarrollo organizacional no lograr certificación.

Figura 4. Modelo de gestión normativas ISO 31000:2012

Fuente: (GUTIERREZ & SANCHEZ-ORTIZ, 2018)



Política de seguridad informática Utmach.

Se basa en establecer obligaciones a estudiantes, docentes y empleados, pero no es socializada ni actualizada, su aplicación es cuestionable debido a su desconocimiento general; aunque aplica los siguientes controles:

- Aplicaciones informáticas
- Control de software malicioso
- Acceso a internet
- Correo electrónico
- Equipos informáticos
- Gestiòn de contraseñas de usuarios
- Copias de respaldo
- Acuerdos de confidencialidad

Las políticas pueden ser reforzadas, potenciadas u optimizadas concatenando la metodología ISO/COBIT en la dirección de TIC`s, haciendo de la seguridad un proceso dinámico y no una reglamentación archivada.

No obstante, no se han presentado casos que ameriten un alto riesgo, pero es mejor prevenir antes que lamentar daños o pérdidas irreparables.

2.2.4 Gestiòn riesgos en el departamento de TIC`s.

La gestión es un proceso, un conjunto de interacciones y conductas tanto técnicas como cotidianas al mantener óptimas condiciones operativas, al no contar con una planificación formal se propone la siguiente:

- Auditar anualmente los sistemas informáticos
- Evaluar los riesgos acordes a las prioridades institucionales
- Socializar y verificar acatamiento de las políticas de seguridad
- Actualizar hardware/software en forma paulatina, renovar normativas e inventariar equipos
- Revisar cada dependencia, solicitar informes a las autoridades y sintetizar informaciòn
- Analizar los informes de cada dependencia para trazar acciones holísticas
- Coordinar la implementación de controles, mejores a implementos tecnológicos
- Potenciar la infraestructura virtual, comprar dominios propios y mejorar el servicio de internet
- Presupuestar las acciones preventivas, predictivas y correctivas anualmente, en caso de no suceder connatos ahorrar fondos para responder a posibles desastres
- Dinamizar la gestión de riesgos, medir avances, identificar errores y culturizar la seguridad en toda la universidad

El plan expuesto es de carácter holístico, basado en conjeturas teóricas, prácticas e inclusive técnicas al proponer una solución objetiva al caso práctico, con el trasfondo de mejorar el desempeño de la Utmach, reforzando sus prestaciones entorno a las TIC`s.

3. CONCLUSIONES:

El análisis de la gestión en las áreas de influencia del departamento informático, demostró que existen riesgos de valoración *MEDIA* a nivel general, las políticas de seguridad y controles paralelos mantienen al margen las debilidades más superficiales, pero la pasividad e inacción de la gestión es la que inevitablemente dañara los sistemas por falta de mantenimiento, vetustez e implementación casi nula de medidas correctivas en hardware, software, redes e internet, personal o gerencia que no son elemento separables sino una sola entidad social.

Desde la perspectiva de la auditoria informática se destaca que las vulnerabilidades y amenazas proceden del interior de la institución, no se registra atentados o acciones malintencionadas desde el exterior; enfatizando en que la gestión es un *verbo* no un concepto, puesto que es aplicada sin retroalimentar ni renovar esfuerzos.

El problema no son los riesgos, ni las vulnerabilidades; es la *gestión* no se toma acciones o decisiones en mitigar los peligros a los sistemas, la deficiencia en aplicación de normas, estado de los equipos, falta de fondos e indiferencia frente a la situaciòn de la infraestructura informática es el mayor percance a resolver, exigiendo una concientización a nivel general sobre todo en la gerencia.

El factor *tiempo* es clave en la gestión de riesgos, la desactualización de equipos, normativas e infraestructura lógica es inevitable, por ello se aconseja aplicar el plan de acción expuesto y periódicamente mejorar las prestaciones informáticas, mediante una gestión integra desde la parte económica hasta cultural en los estudiantes.

4. REFERENCIAS BIBLIOGRÁFICAS

Arcentales Fernández, D. A., & Caycedo Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las Ciencias, Vol. 3*, 157-173.

Castillo Fiallos, J., Cisneros Barahona, A., Méndez Naranjo, P., & Jácome Segovia, D. (2017). "Modelo para la reducción de riesgos de seguridad informática en servicios web. *Dominio de las Ciencias,Vol. 3, Nº. Extra 3*, 676-688.

GUTIERREZ, Y. E., & SANCHEZ-ORTIZ, A. (2018). Diseño de un Modelo de Gestión de Riesgos basado en ISO 31.000:2012 para los Procesos de Docencia de Pregrado en una Universidad Chilena. *Formación universitaria; vol.11, n.4*, 15-32.

Martelo, R. J., Luis, C. T., & Maza, D. A. (2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Información Tecnológica – Vol. 29 Nº 1*, 3-10.

Martín, S. G., & Lafuente, V. (2017). Referencias bibliográficas: indicadores para su evaluación en trabajos científicos. *Investigación bibliotecológica, Vol 31, No 71*, 151-180.

Mendoza Enríquez, O. A. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *REVISTA DEL INSTITUTO CIENCIAS JURÍDICAS DE PUEBLA; vol.12 no.41*, 267-291.

Morga, N. G., Cusó, J. P., & Juárez, M. M. (2018). Desarrollo de Competencias Transversales en la Universidad de Murcia: Fortalezas, Debilidades y Propuestas de Mejora. *Revista Digital de Investigación en Docencia Universitaria; Vol 12, No 2*, 88-113.

Niño Benitez, Y., & Silega Martínez, N. (2018). Requisitos de Seguridad para aplicaciones web. *Revista Cubana de Ciencias Informáticas; Vol 12, Supl 1*, 205-221.

Nunez Moscoso, J. (2019). RAZONAMIENTO ABDUCTIVO: UNA CONTRIBUCIÓN A LA CREACIÓN DEL CONOCIMIENTO EN EDUCACIÓN. *Cadernos de Pesquisa; Vol.49, No.171* , 308-328.

Pizarro Anchundia, S. E., Ormaza Cevallos, M. G., & Ruiz Malbarez, M. (2018). La auditoría y su control de calidad: visualización de los servicios que ofrecen las empresas auditoras de Manabí, Ecuador. *Cofin Habana; Vol 12, No 2*, 268-279.

Quiroz-Zambrano, S. M., & Macías-Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias,Vol. 3, Nº. Extra 3*, 676-688.

RAMOS, J. R. (2018). CÓMO SE CONSTRUYE EL MARCO TEÓRICO DE LA INVESTIGACIÓN. *Cadernos de Pesquisa; vol.48, n.16*, 830-854.

Yrigoyen-Quintanilla, M. (2016). Modelo de referencia de gobierno de las tecnologías de la información para instituciones universitarias. *Interfases, Nº. 9*, 87-115.