UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

GESTIÓN DEL RIESGOS DEL ÁREA INFORMÁTICA DEL CENTRO DE EDUCACIÓN CONTINUA DE LA UNIVERSIDAD TÉCNICA DE MACHALA

RIOS YANZA MARIELA ESTEFANIA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

GESTIÓN DEL RIESGOS DEL ÁREA INFORMÁTICA DEL CENTRO DE EDUCACIÓN CONTINUA DE LA UNIVERSIDAD TÉCNICA DE MACHALA

RIOS YANZA MARIELA ESTEFANIA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

GESTIÓN DEL RIESGOS DEL ÁREA INFORMÁTICA DEL CENTRO DE EDUCACIÓN CONTINUA DE LA UNIVERSIDAD TÉCNICA DE MACHALA

RIOS YANZA MARIELA ESTEFANIA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 23 DE AGOSTO DE 2019

MACHALA
23 de agosto de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Gestión del riesgos del área informática del centro de educación continua de la Universidad Técnica de Machala, 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

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

ILLESCAS ESPINOZA WILMER HENRY
0704128776
ESPECIALISTA 3

Fecha de impresión: viernes 23 de agosto de 2019 - 09:22

URKUND

Urkund Analysis Result

Analysed Document:	MARIELA RIOS.docx (D54788273)
Submitted:	8/12/2019 7:21:00 PM
Submitted By:	jgonzalez@utmachala.edu.ec
Significance:	0 %

Sources included in the report:

Instances where selected sources appear:

0

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

La que suscribe, RIOS YANZA MARIELA ESTEFANIA, en calidad de autora del siguiente trabajo escrito titulado Gestión del riesgos del área informática del centro de educación continua de la Universidad Técnica de Machala, 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, 23 de agosto de 2019

RIOS YANZA MARIELA ESTEFANIA
0705756633

RESUMEN

El avance tecnológico tiene cabida en el mundo entero, en las diferentes organizaciones y en los diferentes departamentos que a ellas las componen, cada nueva tecnología integrada a esta era de avances tecnológicos ayuda de manera significativa al desempeño en el trabajo del ser humano, reduce el tiempo de ejecución y perfecciona cada actividad que se realiza.

En el ámbito académico tienen un aporte valioso, puesto que desde su integración a las planificaciones de estas instituciones innegablemente se ha mostrado una mejora en su desempeño y un mejor rendimiento a nivel académico. Pero, así como hay ciertos beneficios, existen riesgos que vienen ligados al crecimiento tecnológico, pues gracias a que la información se digitaliza existe mayor posibilidad de que esta sea vulnerada por piratas informáticos. En este caso se examinará la gestión de riesgos que tiene el Centro de Educación Continua de la UTMACH para hacer frente a este problema informático, dando así, lugar a la presentación de posibles medidas que podrían a favor de contrarrestar los riesgos que potencialmente afectarían el sistema en cuestión.

PALABRAS CLAVES: Seguridad, riesgos informáticos, gestión, centro de cómputo.

ABSTRACT

The technological advance has a place in the whole world, in the different organizations and in the different departments that comprise them, each new technology integrated to this era of technological advances significantly helps the performance in the work of the human being, reduces the execution time and perfects every activity that is carried out.

In the academic field they have a valuable contribution, since their integration into the planning of these institutions has undeniably shown an improvement in their performance and a better performance at the academic level. But, just as there are certain benefits, there are risks that are linked to technological growth, because thanks to the fact that information is digitized, there is a greater possibility that it will be harmed by hackers. In this case, the risk management of the Continuing Education Center of the UTMACH will be examined to deal with this computer problem, thus giving rise to the presentation of possible measures that could be in favor of counteracting the risks that could potentially affect the system. in question.

KEYWRDS: Security, computer risks, management, computer center.

ÍNDICE DE CONTENIDOS

ÍNDICE DE IMÁGENES

ÍNDICE DE CUADROS

INTRODUCCIÓN

En los últimos años el mundo ha sido testigo del sinnúmero de cambios que han ocurrido frente a sus ojos, los avances tecnológicos son en gran parte uno de los iconos que marcan este cambio de era, pues no solamente se evidencian por la forma en que ahora funcionan las fabricas o los nuevos inventos que han surgido en los últimos años, sino por la importante incidencia que tienen dentro de los distintos sectores económicos de un país, sin importar el nivel en el que se encuentre.

Una de las grandes características de este crecimiento tecnológico que se desarrolla mundialmente, es la facilidad de subir información a internet para manejarla virtualmente, lo que permite el acceso rápido a ella desde cualquier ordenador en cualquier parte del mundo, algo que a primera vista influye ventajosamente en el desempeño del trabajo de cualquier persona, pero que si es visto desde el lado opuesto puede llegar a perjudicar significativamente a quien lo realice, pues al estar esta información en la red se vuelve vulnerable y entra en riesgo de que cualquier persona se adueñe de ella, pudiendo utilizarla a su conveniencia.

Ilustración 1. Ejes de seguridad.

Fuente: (Romero Castro, y otros, 2018)

Entonces, la seguridad informática se vuelve un tema imprescindible de tratar, pues ante los riesgos informáticos latentes en el medio es importante poder contar con herramientas que ayuden a contrarrestar estos peligros y con ello prevenir posibles daños a la información. Los expertos en el tema generalizan sobre la acción de la seguridad informática pero lo cierto es que en el área que sea, el objetivo que persigue es el mismo. La gestión de riesgos informáticos está determinada por un grupo de medidas que buscan poder proteger la

integridad de la información y del sistema informático, cuidando el buen estado del hardware y software utilizados por la entidad (Figueroa Suárez, Rodríguez Andrade, Bone Obando, & Saltos Gómez, 2017).

En este informe se desarrolla el estudio realizado a la gestión de riesgos informáticos en el departamento de cómputo del Centro de Educación Continua perteneciente a la Universidad Técnica de Machala, con lo que se busca conocer cuáles son las medidas de intervención utilizadas en el control de la información.

Además, se busca explicar definiciones para facilitar la comprensión del tema, al mismo tiempo que se determinará medidas que podrían considerarse en la mitigación de peligros informáticos, pues se considera que al momento no hay información en la red que esté exenta de ser vulnerada por intrusos.

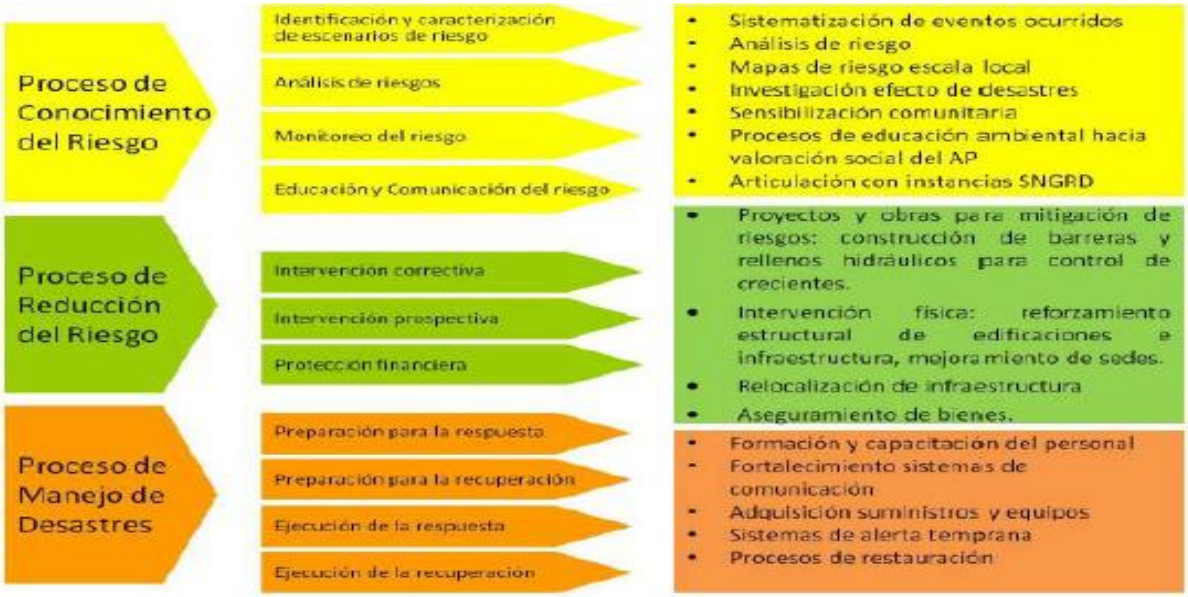

Ilustración 2. Esquema del proceso para gestión de riesgos.

Fuente: (Pérez Fernández,, Sáenz Gómez, & Gómez Vega, 2016)

FUNDAMENTACIÓN TEÓRICA

El entorno tecnológico que se vive actualmente la información digitalizada es vulnerable a ataques cibernéticos por lo que es importante crear planes o gestar la neutralización de riesgos informáticos, para el desarrollo del tema propuesto se ha investigado en fuentes confiables con el propósito de adquirir la información necesaria para explicar lo que se desea, a continuación, se describe la terminología relacionada al tema:

Sistemas informáticos del Centro de Educación Continua

En la Universidad Técnica de Machala existen varias áreas que se encargan de coordinar, administrar y manejar el funcionamiento de la institución, uno de ellos es el Centro de Educación Continua cuyo departamento informático tiene a su cargo el desarrollo de varias actividades de interés académico, entre ellas la elaboración de un Plan Anual de Educación Continua mediante el cual ofrece cursos de capacitación, seminarios y similares de forma presencial o a distancia, al personal administrativo, personal docente, estudiantes o público en general. Además es quien dirige el Instituto de Idiomas de la UTMACH y lleva un registro de todos aquellos programas que se dan, de quienes los facilitan y de todos aquellos que se desarrollen de acuerdo a la Ley Orgánica de Educación Superior (LOES) y Reglamentos actualizados (UTMACH, 2017).

Para la ejecución de todas estas actividades cuentan con un departamento informático que maneja el CEC, este sistema está conformado por equipos de cómputo y software especializados y personal capacitado que trabajen en conjunto para el cumplimiento de los objetivos.

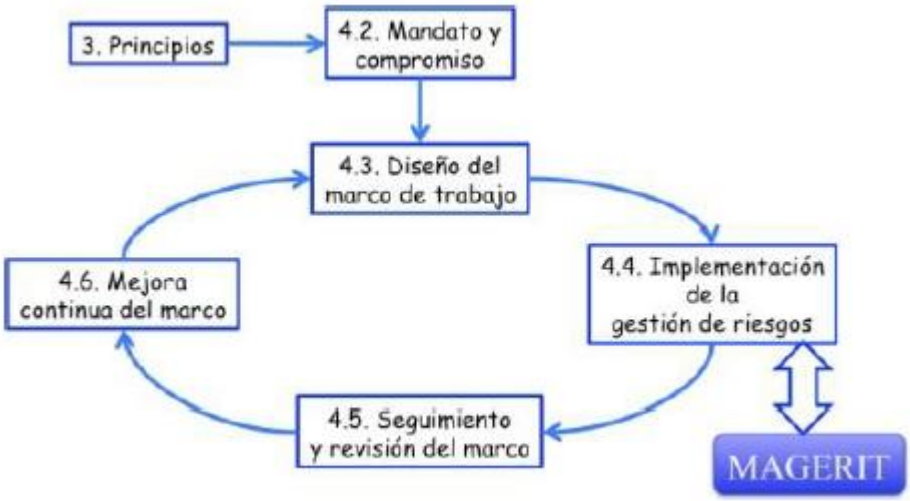

Ilustración 3. Proceso del trabajo de la gestión de riesgos.

Fuente: (Cruz Ojeda, 2018)

Gestión de riesgos informáticos

Son un conjunto de técnicas que pueden aplicarse en diversos entornos, dependiendo las necesidades que se tenga y considerando que es donde se necesita cuidar la seguridad.

La gestión de riesgos informáticos debe analizar los riesgos y vulnerabilidades tomando en cuentas los parámetros y normativas vigentes, para poder intervenirlos y mitigarlos con el fin

de evitar los posibles problemas que podrían causarle a la institución (Corda, Viñas, & Coria, 2017).

En vista del rápido avance de la tecnología en los últimos años y la implementación de las TIC's (Tecnologías de Información y Comunicación) en el medio, es evidente el aumento de información que circula en la red, lo cual genera ventajas en su utilización pero por otro lado provoca que surjan nuevos y mayores riesgos informáticos. Por lo que, en este ambiente tecnológico todo aquel que se encargue de la gestión de riesgos informáticos debe ser alguien preparado y debidamente capacitado, alguien capaz precisar los riesgos inminentes y que pueda plantear soluciones ante ello.

Para conseguir una correcta protección de datos informáticos es necesaria la participación no solo de los técnicos informáticos, sino de todos los integrantes de la institución; con el fin de involucrar a todos y que todos sepan del proceso llevado a cabo como medida de protección de la información interna, logrando así que perdure la gestión de riesgos efectuada (Solarte Solarte, Enriquez Rosero, & Benavides Ruano, 2015).

Cuadro 1. Ciclo de Deming aplicado a la gestión de riesgos.

Ciclo	Procedimientos
Planear	Definir el contexto
	Establecer el rumbo de la gestión de riesgos
	Análisis de riesgos informáticos
	Identificar alternativas de mitigación de riesgos.
Hacer	Efectuar planificación de atenuación de riesgos
	Utilizar recursos
	Integrar procesos que manejen la gestión de riesgos
	Implementar programación que ayude a la formación
Verificar	Realizar seguimientos y revisar eficiencia de controles realizados
	Calificar la eficacia de las medidas llevadas a cabo
	Revisar el análisis de riesgos habitualmente
Actuar	Efectuar auditorías internas
	Instaurar correcciones que ayuden a prevenir daños
	Comunicar al personal sobre las acciones tomadas al respecto
	Asegurarse de la eficacia de las correcciones efectuadas

Fuente: (Solarte Solarte, Enriquez Rosero, & Benavides Ruano, 2015)

Amenazas y Vulnerabilidades

Teóricamente estos son conceptos que tienen similitud, es decir que hacen referencia a lo mismo; ambos están dentro del ámbito de seguridad informática.

Las vulnerabilidades informáticas conforman las posibles respuestas de la organización frente a las amenazas potenciales a las que puede estar propensa la información; cualquier

suceso sin importar su origen o procedencia puede perturbar el bienestar de los datos informáticos dañando los sistemas.

Cuadro 2. Clasificación de las Vulnerabilidades informáticas.

CLASIFICACIÓN DE LAS VULNERABILIDADES INFORMÁTICAS	
Vulnerabilidad física	Afectan a la infraestructura de la organización, lugar de almacenamiento de la información
Vulnerabilidad natural	Todo lo relacionado con la naturaleza y que ponen en riesgo la información
Vulnerabilidad del hardware	Posibles fallas de fabrica o mala configuración de computadoras
Vulnerabilidad del software	Accesos ilícitos a sistemas informáticos, sin conocimiento del usuario
Vulnerabilidad de medios o dispositivos	Soportes físicos utilizados para grabar información
Vulnerabilidad de las comunicaciones	Recorrido de la información, hacia donde va a llegar.
Vulnerabilidad humana	Daños por parte de las personas a los equipos de cómputo o a la información.

Fuente: Elaboración propia

METODOLOGÍA

En esta sección se hace referencia a la metodología empleada en la investigación y elaboración del informe en donde se desarrolla el tema propuesto, las técnicas o métodos empleados se detallan a continuación:

Investigación Bibliográfica

Este es un proceso que se basa en la búsqueda de información a través de libros, artículos de revistas científicas, tesis o sitios web, todos autorizados académicamente por ser albergue de información confiable. Estos documentos utilizados deben tener una antigüedad no mayor a 5 años de la fecha a la que se los utiliza (Gómez Luna, Fernando Navas, Aponte Mayor, & Betancourt Buitrago, 2014).

Método Analítico-Sintético

Es la conjugación de dos métodos bastante útiles para procesar información, este método disgrega la información (un todo) en partes para poder examinarla por separado, logrando así una revisión ordenada, completa y dando lugar a un mejor análisis de los datos recopilados pudiendo así formar ideas. Es muy útil en las investigaciones donde se tiene información por separado, se la estudia, analiza y sintetiza hasta obtener el material necesario (Maya, 2014).

Método Inductivo

Responde al razonamiento de pequeñas partes, que son analizadas para llegar a una conclusión o una idea general, es un método muy parecido al método analítico. En este método se estudia ejemplos simples o mas pequeños que luego de ser lo suficientemente analizados dan paso a un razonamiento general (Maya, 2014).

Método Deductivo

Este es un método en donde se parte del análisis de una idea universal o un todo para llegar a una conclusión. Se hace la descomposición de la información generalizada que se tiene respecto a un determinado tema, pudiendo tener partes mas pequeñas que permitan realizar un mejor y más profundo análisis (Maya, 2014).

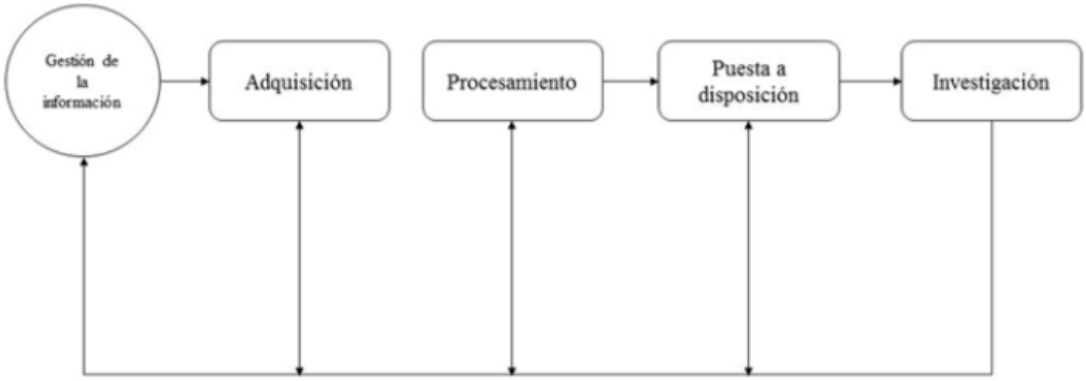

Ilustración 4. Procesamiento de la información en el proceso de investigación.

Fuente: (Prieto Castellanos, 2017)

DESARROLLO

Análisis de riesgos y vulnerabilidades informáticas

En la era tecnológica que se vive actualmente, el desarrollo y perfeccionamiento del manejo de información es un hecho, la información que años anteriores se apilaba en documentos escritos ahora esta a disposición del usuario con solo un clic, dispuesta en cualquier ordenador desde cualquier ubicación.

La digitalización de la información aporta ventajosamente a la optimización en el trabajo de cualquier entidad, pero tiene la desventaja de que, al estar dispuesta en la red, no solo puede tener acceso a ella su propietario sino cualquier intruso que quiera hacer uso de ella para su beneficio.

Por ello para cada entidad es muy importante realizar una serie de estudios preventivos con los que busca analizar los posibles riesgos a los que esta propensa su información. Dicha evaluación debe hacerse tomando en cuenta las características de la información pues no toda tiene el mismo rigor, así se podrá identificar los riegos a los que está expuesta y que medidas podría tomarse como medida de control (Calderón Ramos, 2015).

La Universidad Técnica de Machala es una institución de carácter institucional, por lo tanto las medidas que debe tomar incluyen a la información de toda una Universidad, por lo tanto las auditorias informáticas que deben realizarse, deben ser periódicamente porque debido a la gran cantidad de información que manejan en la red y del grado de importancia que es, puede verse afectada si es que llega a caer en manos equivocadas.

Gestión de Riesgos informáticos en Instituciones Educativas

La gestión de riesgos constituye a un grupo de metodologías que son llevadas a cabo con el fin de identificar las posibles amenazas que existen en un sistema informático y las fallas que estas podrían causar a este sistema.

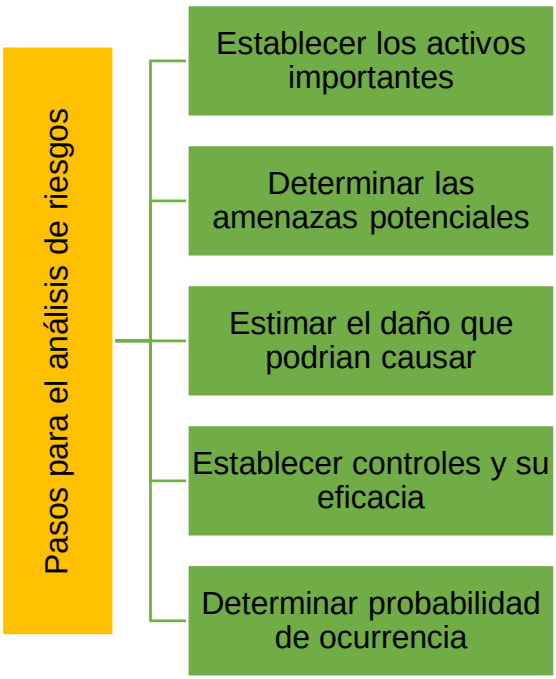

Ilustración 5. Esquema con los pasos para realizar un análisis de riesgos informáticos.

Fuente: Elaboración propia

En las instituciones educativas, en universidades principalmente, hoy en día el manejo de la información digitalizada es una necesidad porque debido al volumen de información que deben manejar y procesar diariamente es simplemente imposible que se haga manualmente, lo que lleva al problema de los cyber ataques o robo de información por parte

de usuarios ajenos a la institución, por lo tanto, es necesario que habitualmente se realice una gestión de riesgos informáticos; lo cual lleva no solo a la identificación de riesgos sino también a su eliminación y custodia de la información.

En universidades principalmente existen ciertos estándares de seguridad de la información, debido a la importancia que ella tiene; por esto es fundamental que se creen ciertos patrones para la gestión de riesgos o también conocidos como frameworks, en este grupo hay una metodología muy utilizada por diversas empresas de diferentes categorías, llamada OCTAVE que garantiza un correcto desempeño en la evaluación de riesgos y de fácil realización. (Calderón Ramos, 2015)

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

Para cada organización, del tipo que sea, es muy importante que se evalúe su sistema informático, pues al ser quien maneja la información de la institución es quien mas propenso esta a sufrir atentados con el fin de robar los datos informáticos que contiene.

Para el análisis o evaluación de riesgos informáticos se ha creado una herramienta que propone realizar el trabajo auditor de manera precisa y eficaz, esta herramienta tiene por nombre Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), pues ha sido creada con el fin de realizar estimación de peligros organizacionales que se vinculen a la acción diaria de las instituciones. Inicialmente identifica la información mas importante de la entidad (considerando los demás aspectos de importancia para la organización como: softwares, documentación física, empleados).

Así OCTAVE se encarga de estudiar toda la infraestructura de información e investiga el uso que se le da a ella, para ello es muy necesario que cada integrante de equipo que maneja dicha información este capacitado y tenga la capacidad de entender cuál es la información de primordial importancia y cuales son las medidas de protección deben tomar (Enríquez Carmona, 2013).

Cuadro 3. Fases para la implementación de la metodología OCTAVE.

FASES DE LA METODOLOGIA OCTAVE	
Fase 1	Elaboración de perfiles de posibles amenazas informáticas
Fase 2	Reconocimiento de vulnerabilidades en el sistema informático
Fase 3	Puesta en marcha de medidas de seguridad

Fuente: Elaboración propia

Modelo PDCA (Plan, Do, Check, Act)

Existe un modelo especial que hace que el análisis y gestión de riesgos sean satisfactorios, este modelo o metodología es conocido como PDCA (Planificar, Hacer, Verificar y Actuar).

Este modelo se centra en la necesidad de dirigir el proceso de análisis de riesgos informáticos, al mismo tiempo que propone alternativas de mitigación de esos peligros, planeando acciones que podrían realizarse de acuerdo a la planificación de la entidad.

Este es un modelo que puede ser utilizado en la planificación de una gestión de riesgos informáticos en cualquier tipo de entidad, podría ser muy útil en Instituciones educativas, debido al proceso secuencial y la facilidad que tiene para efectuarse. Es una metodología que se podría emplear en la gestión de riesgos del Centro de Educación Continua de la UTMACH.

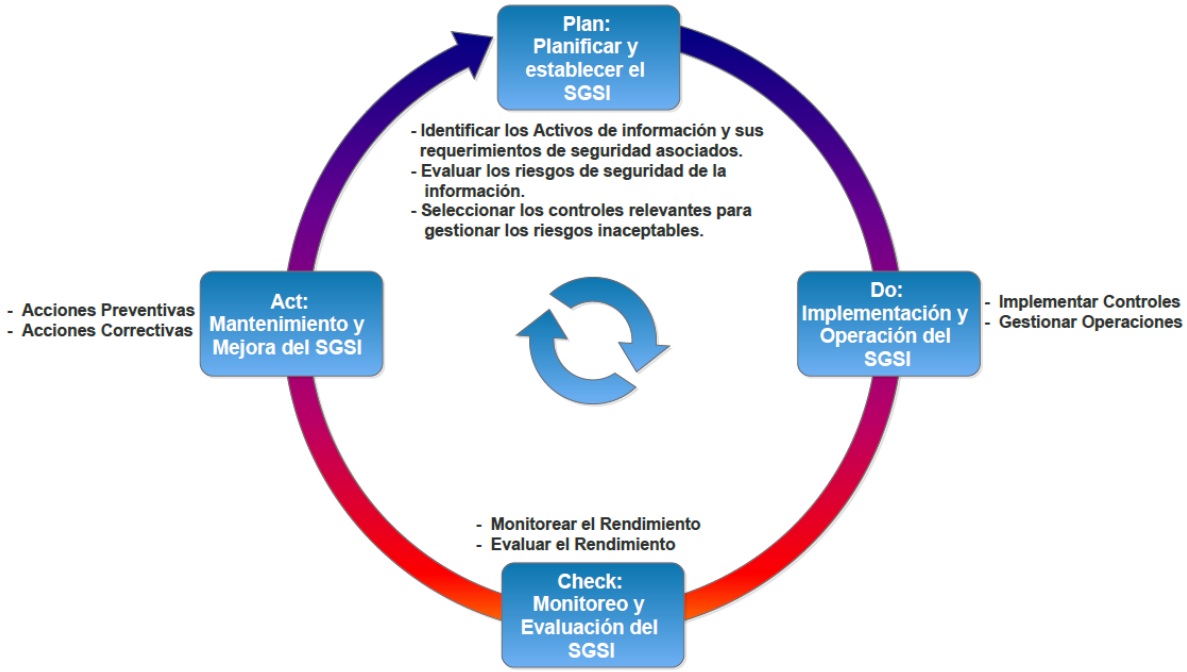

Ilustración 6. Método PDCA.

Fuente: (Arévalo Moscoso & Cedillo, 2017)

Las cuatro fases se definen a continuación:

- Planificar: Fijar objetivos y determinar los procedimientos a seguir para la gestión de riesgos informáticos. Lo que se busca es proporcionar resultados acordes a las políticas de la empresa u organización.
- Hacer: En este paso se realiza la operación y ejecución de procesos destinados a controlar los riesgos, considerando las políticas especificadas.

- Verificar: Se debe evaluar los procesos y el desempeño en el control de los riesgos identificados, además se debe presentar resultados.
- Actuar: Establecer políticas de gestión de riesgos informáticos e incluir las modificaciones establecidas con el fin de mejorar los procesos (Arévalo Moscoso & Cedillo, 2017).

CONCLUSIONES Y RECOMENDACIONES

Al finalizar el desarrollo del tema propuesto se ha logrado identificar los diferentes métodos que se toman en cuenta por parte de las organizaciones, con el fin de gestionar la mitigación de riesgos informáticos que vulneren la información interna y confidencial.

En el Centro de Educación Continua de la Universidad Técnica de Machala se maneja todo tipo de información que forma parte importante del desarrollo institucional, la gestión de riesgos informáticos consiste en una serie de procesos llevados a cabo con la finalidad de hacerle frente a las amenazas latentes en el medio, aquellas amenazas que atentan contra la seguridad de la información almacenada en la red.

En una institución no abastece solamente gestionar los riesgos a los que esta vulnerable la seguridad informática, se necesita tener planteados ciertos procesos que establezcan los riesgos, estimen su potencialidad, los evalúen y sepan tratarlos hasta disminuirlos al máximo y si es posible, hasta eliminarlos; para ello se debe tener la participación de todos los colaboradores de la entidad, pues solo así se lograra mantener el proceso en función y control constante.

REFERENCIAS BIBLIOGRÁFICAS

Arévalo Moscoso, F. M., & Cedillo, P. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica*, 31-42.

Calderón Ramos, V. P. (2015). *Análisis de Riesgos Informáticos y Desarrollo de un Plan de Seguridad de la Información para el Gobierno Autónomo Descentralizado Municipal Catamayo.* Loja: Universidad Nacional de Loja.

Corda, M. C., Viñas, M., & Coria, M. K. (2017). Gestión de riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave (La Plata)*, 1-18.

Cruz Ojeda, D. N. (2018). *Plan de riesgos y contingencias informáticas basado en un acuerdo de nivel de servicio aplicada a la empresa Plasticaucho Industrial.* Ambato: Universidad Técnica de Ambato.

Enríquez Carmona, E. J. (23 de Septiembre de 2013). *Universo, el periódico de los universitarios*. Obtenido de https://www.uv.mx/universo/535/infgral/infgral_08.html

Figueroa Suárez, J. A., Rodríguez Andrade, R. F., Bone Obando, C. C., & Saltos Gómez, J. A. (2017). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, 145-155.

Gómez Luna, E., Fernando Navas, D., Aponte Mayor, G., & Betancourt Buitrago, L. A. (2014). Metodología para la revisión bibliográfica y la gestión de información de temas científicos, a través de su estructuración y sistematización. *Dyna*, 158-163.

Maya, E. (2014). *Métodos y técnicas de investigación.* México: Universidad Nacional Autónoma de México.

Pérez Fernández,, B. J., Sáenz Gómez, P. A., & Gómez Vega, W. J. (2016). Gestión del riesgo en una institución educativa de la ciudad de San José de Cúcuta, Colombia. *Revista Virtual Universidad Católica del Norte*, 183-214.

Prieto Castellanos, B. J. (2017). El uso de los métodos deductivo e inductivo para aumentar la e□ciencia del procesamiento de adquisición de evidencias digitales. *Pontificia Universidad Javeriana*, 1-27.

Romero Castro, M. I., Figueroa Moràn, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Manabí: Área de Innovación y Desarrollo,S.L.

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL*, 492-507.

UTMACH. (2017). *Centro de Educación Continua*. Obtenido de http://cec.utmachala.edu.ec/index.php/quienes-somos/nosotros