Vol.7 No.4 (2023): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.7.4.2023.500-514

Risk analysis and strengthening of information technology at the Profesional Training an Updating center of the Universidad Católica de Cuenca.

Análisis de riesgos y fortalecimiento de la seguridad de la información en el Centro de Capacitación y Actualización Profesional de la Universidad Católica de Cuenca

Autores:

Chitacapa-Espinoza, Johanna Patricia
UNIVERSIDAD CATÓLICA DE CUENCA
Egresada de la Maestría de Ciberseguridad
Cuenca – Ecuador
jchitacapa@ucacue.edu.ec
https://orcid.org/0000-0001-9168-7773

Torres-Soto, Carlos Andrés
UNIVERSIDAD CATÓLICA DE CUENCA
Docente Tutor de la Maestría de Ciberseguridad
Cuenca – Ecuador
atorres@ucacue.edu.ec
https://orcid.org/0000-0003-3335-4158

Lugo-Gracia, Jorge
UNIVERSIDAD CENTRAL DEL ECUADOR
Docente de la Maestría de Ciberseguridad
Cuenca – Ecuador
jorge.lugo.82@ucacue.edu.ec
https://orcid.org/0000-0002-1314-7621

Fechas de recepción: 02-SEP-2023 aceptación: 02-OCT-2023 publicación: 15-DIC-2023

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Las Instituciones de Educación Superior obtienen, procesan y almacenan información delicada e importante para su gestión, siendo necesario proteger este activo de posibles amenazas que puedan ocasionar interrupciones en la continuidad de los servicios. El objetivo del estudio fue determinar los riesgos de la información en el subproceso oferta académica de las carreras del Centro de capacitación y actualización profesional de la Universidad Católica de Cuenca. Se adaptaron las fases de la Metodología MAGERIT en donde se identificaron los activos, las amenazas y vulnerabilidades, para luego estimar el riesgo de cada activo y finalmente se identificó las salvaguardas seleccionando los controles de la norma ISO 27002:2013 que aporten a la seguridad de los activos. En base al análisis realizado se encontraron los valores de riesgo actual y riesgo residual y como conclusión se aprecia un resultado favorable de la probable implementación de las salvaguardas identificadas, que podrían disminuir los factores de riesgo en el contexto estudiado.

Palabras clave: análisis de riesgos, MAGERIT, ISO 27002, activos de información, vulnerabilidades.

Abstract

Higher Education Institutions obtain, process and store sensitive and essential information for their management to protect this asset from possible threats that may cause interruptions in the continuity of services. The study aimed to determine the risk of information of the academic offer sub-process of the Center for Training and Professional Development of the Catholic University of Cuenca. The MAGERIT Methodology phases were adapted, where assets, threats and vulnerabilities were identified to estimate each asset's risk and finally identify the safeguards by selecting ISO 27002:2013 controls that contribute to the security of the assets. Based on the analysis, the current risk and residual risk values were found. In conclusion, a favorable result of the probable implementation of the identified safeguards is appreciated, which could reduce the risk factors in the context studied

Keywords: risk analysis, MAGERIT, ISO 27002, information assets, vulnerabilities.

Introducción

En la actualidad, la mayoría de las organizaciones dependen de la tecnología para garantizar el funcionamiento de sus procesos, dado el volumen, la importancia y la necesidad de la disponibilidad inmediata de la información, se considera trascendental que esta se encuentre protegida, pues al encontrarse en la red se convierte en blanco de diversos tipos de ciberataques, por lo que es necesaria la implementación de procesos que protejan los activos involucrados en la seguridad de la información.

Las Instituciones de Educación Superior - IES, dentro de sus procesos manejan información delicada, personal e importante, que de ser vulnerada puede poner en riesgo el normal funcionamiento de la institución y la confiabilidad de todos los involucrados en estos procesos, como lo corrobora Castro-Maldonado & Villar-Vega (2021), "…las instituciones de educación superior deben manejar de forma responsable la información de los actores que en ella se interrelacionan, como son los estudiantes, docentes y personal administrativo" (p. 46).

Para Zevallos (2019), todo tipo de organización que tenga procesos digitalizados está expuesta a riesgos informáticos, su investigación ofrece una visión completa sobre la gestión de riesgos, el autor menciona la importancia de utilizar las normas o metodologías de manera eficiente adaptándola a las situación que presenta cada organización con el fin de analizar y tratar los riesgos que están presente.

El análisis de riesgos es una forma de disminuir las consecuencias de los ataques, conocer las amenazas, puede ayudar a mitigar el impacto que estas puedan tener al momento que se materialicen, este es un proceso metódico en donde se realiza la identificación y valoración de los activos y amenazas, así como la determinación de las salvaguardas para cada riesgo. Así lo asiente Moncayo (2014) al decir "el análisis de riesgos tiene como propósito, determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo. En el análisis de riesgos se analiza el impacto que puede ser ocasionado a consecuencia de que ocurran amenazas" (p.75).

Para esto existen algunas metodologías y estándares ISO – International Organization for Standarization, que detallan los pasos a seguir para un análisis y gestión de riesgos, para su implementación, se debe considerar que dichas herramientas se adaptan a las necesidades de cada organización, pudiendo ser aplicadas de forma individual o en combinación de varias, conforme sea de utilidad y beneficio para la organización.

En este sentido Bravo Ramos & Yoo (2020), crearon una nueva propuesta de metodología de gestión de riesgos para un sistema de biblioteca universitaria basado en 6 pasos que se establecieron luego de haber analizado Magerit, Octave y Nist 800-30, la cual les permitió realizar un análisis de riesgos con precisión en los activos, riesgo y amenazas para este ámbito en particular e incluso con las mejoras implementadas dejaron sentado un precedente para una certificación futura en la norma ISO 27001.

En el mismo criterio del punto anterior Imbaquingo et al. (2019), realizaron una evaluación de seguridad del Sistema de evaluación docente en la Universidad Técnica del Norte – UTN, Ecuador, utilizando la metodología Magerit, para el análisis de riesgos y poder identificar el estado de la seguridad de la información; en cambio utilizaron los controles de la ISO 27002:2013 para verificar el cumplimiento de la seguridad de la información del sistema de evaluación docente en la UTN, logrando al final de su investigación determinar el cumplimento del 51% de la política de seguridad en la Institución de Educación Superior – IES, antes mencionada.

En la provincia de Tungurahua – Ecuador, se realizó un estudio de ciberseguridad en las plataformas educativas de los Institutos Tecnológicos Superiores Públicos – ITSP, para esto los autores utilizaron la metodología Magerit y la norma ISO 27032, que les permitió respectivamente realizar la selección de las áreas de afectación, la identificación de las amenazas y vulnerabilidades, la selección de controles y la generación de salvaguardas necesarias. Si bien el estudio constituye una guía, también se menciona que cada ITSP debe implementar su propio análisis de riesgos basado en su realidad ((Morales-Paredes & Medina, 2021).

La presente investigación se inicia con una revisión bibliográfica sobre el análisis de riesgos de la información apoyada en la metodología Magerit y a su vez considera una revisión de los controles de la ISO 27002, que puedan reforzar la seguridad de la información en el subproceso oferta académica de las carreras del Centro de capacitación y actualización profesional, con esto busca sentar una línea base de investigación y proporcionar un instrumento de guía para una posible implementación en otros departamentos de la Universidad Católica de Cuenca.

Como objetivo principal de la investigación se planteó el determinar los riesgos de la información en el subproceso oferta académica de las carreras del Centro de capacitación y actualización profesional de la Universidad Católica de Cuenca, específicamente también se enuncian los siguientes objetivos: fundamentar teórica y científicamente sobre el análisis de riesgos de la información, desarrollar un análisis de riesgos en el subproceso oferta académica de las carreras y por ultimo establecer los controles asociados a los riesgos encontrados en el subproceso seleccionado.

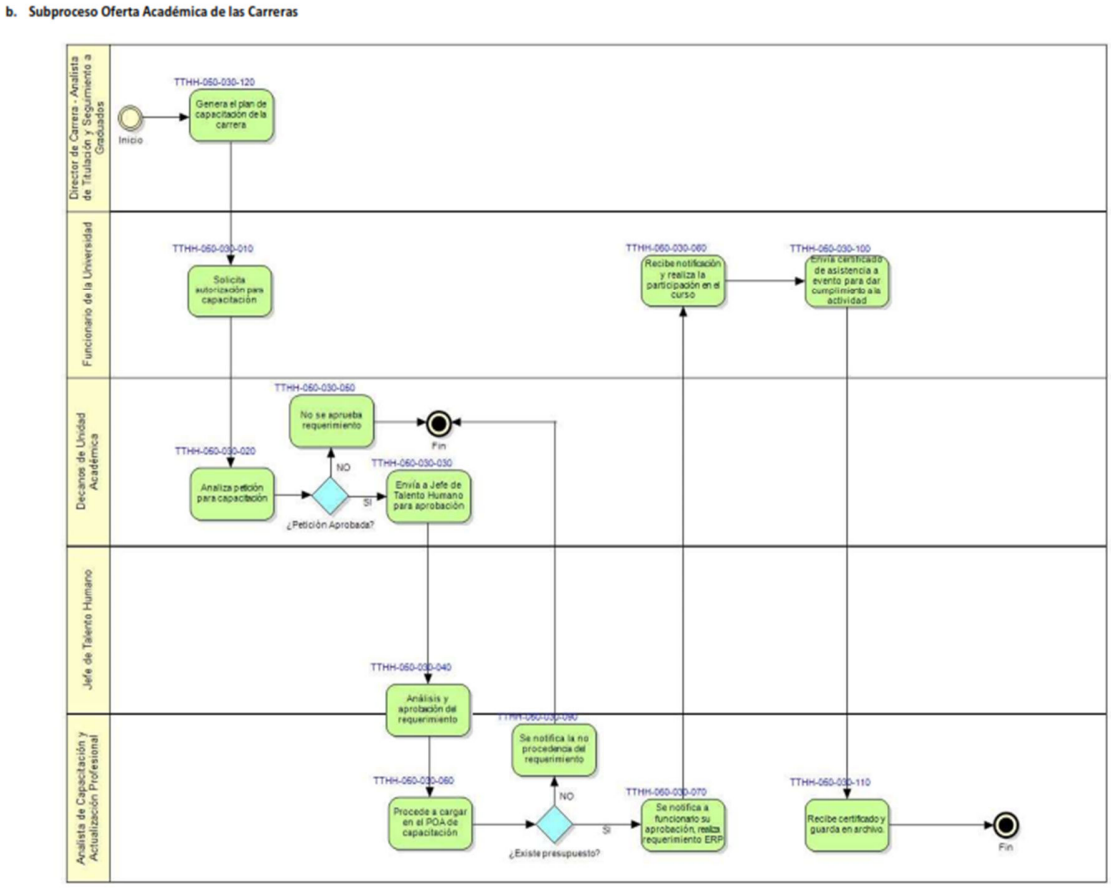
Material y métodos

El presente trabajo de investigación inició con la identificación de fuentes confiables de información, como: proyectos de investigación, artículos originales, tesis de grado y posgrado, documentos, páginas web, entre otras, con información relevante sobre los riesgos de la información, metodologías usadas y normas ISO, seleccionando tanto artículos nacionales como internacionales que tengan un aporte significativo a esta investigación.

Para el análisis de los riesgos en el subproceso de oferta académica de las carreras del Centro de capacitación y actualización profesional de la Universidad Católica de Cuenca, se inició con una revisión del subproceso que identifica las necesidades específicas de capacitación de los docentes universitarios, considerando los dominios, las líneas de investigación y los programas de vinculación con la sociedad en los ámbitos declarados por cada carrera, información que fue proporcionada luego una revisión conjunta con el personal encargado de este procedimiento.
Específicamente este subproceso detalla el camino a seguir de una solicitud de capacitación, partiendo desde la concepción de la misma, seguida por la autorización de la máxima autoridad de la unidad académica(decano), petición que luego es enviada al Centro de capacitación y actualización profesional para analizar su viabilidad, de ser favorable se aprueba su realización por la Jefatura de Talento Humano, esta ejecución queda evidenciada en proyectos aprobados, registrados en el sistema de gestión de recursos (ERP) y en algunas ocasiones constará también en la plataforma entorno virtual de enseñanza aprendizaje (EVEA), finalmente el cierre del mismo está atado a la entrega de certificados luego de terminado el curso, como se muestra en la figura 1.

Figura 1

Subproceso Oferta Académica de las Carreras



Fuente: Tomado de Manual de Procesos y Procedimientos de Talento Humano (Universidad Católica de Cuenca, 2020)

Es importante indicar que para realizar un análisis de riesgos existen varias metodologías y estándares, sin embargo es necesario considerar que la selección y utilización de estas herramientas se adaptan a las necesidades propias de cada institución o proceso a analizar, en consecuencia a lo expresado, el análisis de riesgos de este subproceso se orientó en las fases de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT adaptándola a la realidad de este subproceso, como se muestra en la figura 2.

Figura 2

Fases para el análisis de riesgos de la metodología MAGERIT

Fuente: Elaboración propia.

Identificación y valoración de activos

Para la identificación de los activos fue necesario analizar todos los recursos de información que forman parte del proceso seleccionado y que contienen, gestionan o transmiten datos importantes que requieren ser evaluados y protegidos, para esto se procedió con un levantamiento de un inventario de activos de información, luego se procedió a la identificación, clasificación, valoración y determinación de la importancia de cada uno de ellos.

En esta primera etapa se consideró importante tipificar los activos, para esto se utilizó la clasificación que Magerit presenta en su libro 2, como son activos de tipo: Datos, servicios, aplicaciones informáticas (SW), equipos informáticos (HW), soporte de la información, equipamiento auxiliar, redes de comunicaciones, instalaciones y personas. La valoración de los activos se ejecutó basado en tres dimensiones: confidencialidad, integridad y disponibilidad, para esto los criterios de valoración fueron: bajo=1, medio = 2; alto=3, valoraciones que al ser promediadas determinaron la importancia que tiene el activo dentro del proceso, clasificándolos en prescindible=1, importante=2, grave=3.

Identificación y valoración de amenazas

En esta sección se identificaron las vulnerabilidades que presenta cada activo y las amenazas a las que podría estar expuesto, la valoración de las mismas se realizó en base a la probabilidad y al impacto de la ocurrencia de la amenaza según las tablas 1 y 2.

Tabla 1.

Valoración de la probabilidad de la ocurrencia

Probabilidad de ocurrencia	**Valor Numérico**	**Descripción**
Probable	4	El evento puede ocurrir tres veces o más al año
Ocasional	3	El evento puede ocurrir dos veces al año
Remota	2	El evento puede ocurrir una vez al año
Improbable	1	El evento puede ocurrir alguna vez o casi nunca

Fuente: Elaboración propia

Tabla 2.

Valoración del impacto de la ocurrencia

Impacto de la ocurrencia	Valor Numérico	Descripción
Alto	4	Interrupción total de los procesos con efectos graves a la institución.
Moderado	3	Interrupción parcial de los procesos con efectos para la institución.
Medio	2	Interrupción mínima de los procesos con bajo efecto para la institución.
Bajo	1	Casi sin interrupción de los procesos, sin efectos para la institución.

Fuente: Elaboración propia

Estimación del riesgo

La valoración del riesgo se presenta en una escala de 4 niveles, en donde se mide la probabilidad de ocurrencia del evento y el impacto que este llegaría a tener sobre el activo, dicho esto con las valoraciones anteriores se define el tipo de riesgo, que para este caso se tipificó como riesgo bajo, moderado y alto. Ver figura 3.

Figura 3.

Valoración del Riesgo

PROBABILIDAD						
	PROBABLE	4	Riesgo Moderado 4	Riesgo Moderado 8	Riesgo Alto 12	Riesgo Alto 16
	OCASIONAL	3	Riesgo Bajo 3	Riesgo Moderado 6	Riesgo Alto 9	Riesgo Alto 12
	REMOTA	2	Riesgo Bajo 2	Riesgo Moderado 4	Riesgo Moderado 6	Riesgo Moderado 8
	IMPROBABLE	1	Riesgo Bajo 1	Riesgo Bajo 2	Riesgo Bajo 3	Riesgo Moderado 4
			1	2	3	4
			BAJO	MEDIO	MODERADO	ALTO
			IMPACTO			

Fuente: Elaboración Propia.

Determinar las salvaguardas

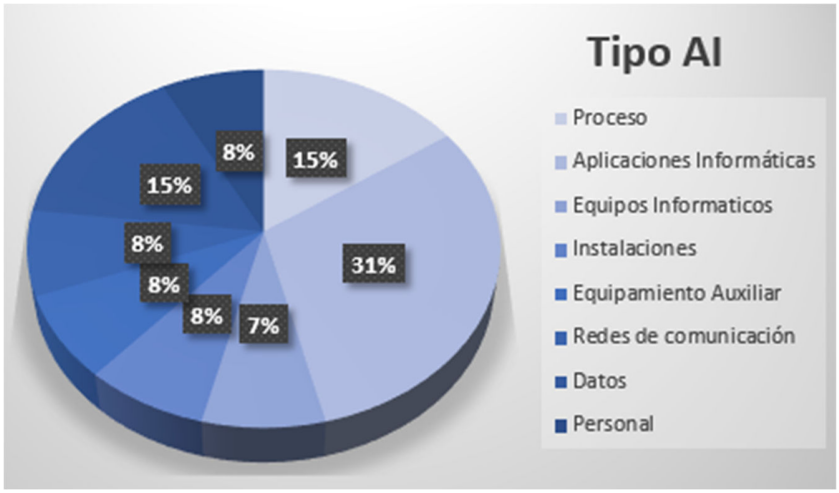
Una vez determinados los riesgos, se precisó importante primero realizar una revisión de las medidas de seguridad para las deficiencias encontradas, concluyendo que si existen algunas políticas o procesos propios de la Universidad que han están creados y pueden aportar a la seguridad de la información, pero que su socialización e integración en todos los procesos ha sido casi nula. Con este precedente se procedió al análisis y selección de los controles del estándar ISO 27002:2013 que aportan a mejorar la seguridad de la información en el subproceso estudiado.

Resultados

Del análisis de riesgo desarrollado al subproceso de oferta académica de las carreras del Centro de capacitación y actualización profesional de la Universidad Católica de Cuenca, se identificó un total de 13 activos que si bien es cierto se clasificaron según la importancia en: prescindible, importante y grave; pero se vio la necesidad de analizar todos los activos encontrados en este proceso, aquí se identificó al 31% de los activos tipo-aplicación y el 15% tipo-proceso por nombrar, en los valores más altos. Ver figura 4.

Figura 4.

Tipos de Activos



Fuente: Elaboración Propia

Del proceso de identificación de amenazas, se encontró un total de 28 vulnerabilidades asociadas a 19 amenazas, que para efectos de identificación se codificaron con la denominación de ACT más las iniciales del nombre de activo y del tipo de activo como lo muestra en la primera columna en la tabla 3.

A continuación, en las siguientes columnas consta la estimación asignada tanto a la probabilidad como al impacto de la ocurrencia lo que dará como resultado el nivel de riesgo acreditado a cada vulnerabilidad, obteniendo los siguientes resultados 6 vulnerabilidades de riesgo alto,10 de riesgo moderado y 12 de riesgo bajo.

Tabla 3.
Estimación del riesgo

Código	Probabilidad Ocurrencia	Impacto Ocurrencia	Promedio	Nivel de Riesgo
ACT1_PRO_PC_V1	2	1	2	Riesgo bajo
ACT2_PRO_SPA_V1	3	3	9	Riesgo alto
ACT3_API_CI_V1	2	1	2	Riesgo bajo
ACT3_API_CI_V2	2	1	2	Riesgo bajo
ACT3_API_CI_V3	3	1	3	Riesgo bajo
ACT4_API_ERP_V1	4	3	12	Riesgo alto
ACT4_API_ERP_V2	4	2	8	Riesgo moderado
ACT4_API_ERP_V3	2	1	2	Riesgo bajo
ACT4_API_ERP_V4	2	2	4	Riesgo moderado
ACT5_API_EVEA_V1	2	2	4	Riesgo moderado
ACT6_API_ZOOM_V1	2	2	4	Riesgo moderado
ACT7_EQI_PC_V1	1	1	1	Riesgo bajo
ACT7_EQI_PC_V2	3	2	6	Riesgo moderado
ACT7_EQI_PC_V3	2	3	6	Riesgo moderado
ACT7_EQI_PC_V4	2	2	4	Riesgo moderado
ACT7_EQI_PC_V5	4	3	12	Riesgo alto
ACT8_INS_OCD_V1	1	2	2	Riesgo bajo
ACT8_INS_OCD_V2	1	1	1	Riesgo bajo
ACT8_INS_OCD_V3	3	1	3	Riesgo bajo
ACT8_INS_OCD_V4	3	2	6	Riesgo moderado
ACT9_EA_UPS_V1	4	3	12	Riesgo alto
ACT9_EA_UPS_V2	1	3	3	Riesgo bajo
ACT9_EA_UPS_V3	4	3	12	Riesgo alto
ACT10_RC_SI	4	3	12	Riesgo alto
ACT11_DAT_DD_V1	2	3	6	Riesgo moderado
ACT11_DAT_DD_V2	2	3	6	Riesgo moderado
ACT12_DAT_DF	1	1	1	Riesgo bajo
ACT13_PER_PC	1	1	1	Riesgo bajo

Fuente: Elaboración propia

Con los riesgos definidos se procedió a la selección de las salvaguardas, que son los controles ISO27002:2013, para esto solo se consideró vulnerabilidades que se encuentren en riesgo moderado y alto. Para una mejor descripción de los resultados, las salvaguardas seleccionadas se describen en el orden en el que se presentan los dominios de la norma ISO 27002:2013 agrupando en cada uno los controles seleccionados para cada vulnerabilidad.

Dominio 7. Seguridad ligada a los recursos humanos
Dentro de este dominio se seleccionó el control 7.1.2 Términos y condiciones de contratación, orientado a generar una cultura organizacional en cuanto a las responsabilidades que deben asumir los empleados con la seguridad de la información, en este dominio recae la vulnerabilidad ACT2_PRO_SPA_V1, cuyo activo se refiere a procesos propios de capacitación docente.

Dominio 9. Control de accesos
Para este dominio los controles seleccionados fueron 9.1.1 Política de control de accesos, recae la vulnerabilidad ACT8_INS_OCD_V4, asignado al activo que soporta accesos físicos no autorizado; el control 9.4.2 Procedimiento de ingreso seguro y el control 9.4.3 Sistema de gestión de contraseñas de usuario, para los activos que soportan vulnerabilidades de acceso a la información no autorizada como ACT4_API_ERP_V4, ACT5_API_EVEA_V1, ACT6_API_ZOOM_V1, ACT7_EQI_PC_V4.

Dominio 11. Seguridad física y ambiental
Este dominio dentro de su descripción menciona que busca evitar accesos no autorizados, proteger a los activos de amenazas internas o externas y evitar la interrupción de servicios, dicho esto, los controles seleccionados fueron 11.2.8 Equipos de usuario desatendido y 11.2.9 Políticas de escritorio limpio y pantalla limpia, para las vulnerabilidades ACT4_API_ERP_V2 y ACT11_DAT_DD_V1; el control 11.2.2 Instalaciones de suministro para ACT9_EA_UPS_V1 y ACT9_EA_UPS_V3, y el control 11.2.4 Mantenimiento de los equipos para la vulnerabilidad ACT7_EQI_PC_V2.

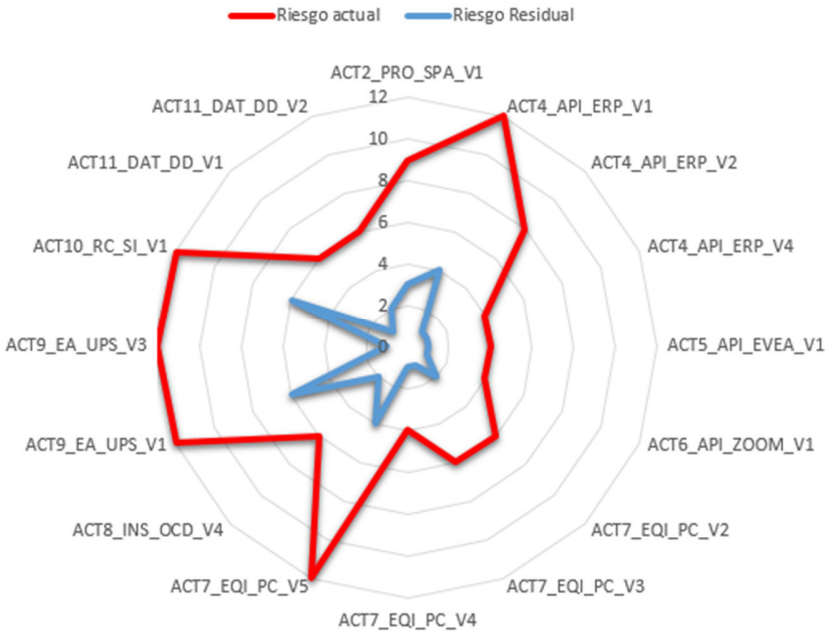
Dominio 12. Seguridad en la operativa
Se optó por los controles A.12.2.1 Protección contra códigos maliciosos y A.12.6.2 Restricciones sobre la instalación de software, para la vulnerabilidad ACT7_EQI_PC_V5; también se seleccionó el control 12.3.1 Respaldo de la información para las vulnerabilidades ACT7_EQI_PC_V3 y ACT11_DAT_DD_V2.

Dominio 17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
17.2.1 Disponibilidad de instalaciones de procesamiento de información (Redundancia) este control fue seleccionado para las siguientes vulnerabilidades ACT4_API_ERP_V1 y ACT10_RC_SI_V1, activos que corresponden a garantizar la disponibilidad de los servicios.

Por último, se realizó una proyección del resultado de la implementación de las salvaguardas sobre las vulnerabilidades de riesgo alto y moderado, esto se lo puede apreciar en la figura 5, donde la línea de color rojo muestra el riesgo actual y la línea de color azul representa el

riesgo residual, aquí se puede apreciar la disminución de los riesgos al aplicar las salvaguardas.

Figura 5.
Riesgo Actual vs Riesgo Residual



Fuente: Elaboración propia

Conclusiones

La globalización tecnológica fuerza a todo tipo de organización a velar por la seguridad de sus activos de información, la presente investigación encuentra un amplio número de documentación que fundamenta teórica y científicamente el análisis y gestión de riesgos como un referente inicial en la seguridad de la información, además de proporcionar una visión sobre las diferentes herramientas, metodologías o estándares para su ejecución.

El análisis de riesgos evidenció que la Institución cuenta en ciertos aspectos con procesos ya establecidos, documentados y aprobados en temas relativos a la seguridad de la información, sin embargo, estos no son socializados, lo que genera el desconocimiento en el personal y por ende se traduce en probables amenazas que al ejecutarse pueden desencadenar en la ejecución de ataques informáticos.

Los resultados de este análisis identifican claramente los riesgos a los que están expuestos los activos del subproceso de oferta académica de las carreras y su manera de mitigarlos por medio de la aplicación de las salvaguardas, que para este caso fueron analizadas desde los controles de la ISO27002:2013, por otro lado, el análisis de una probable aplicación de las salvaguardas demostró una notable disminución del riesgo de los activos al establecer los controles asociados.

Al cumplir con los tres objetivos específicos se puede también concluir que se logró, por ende, determinar los riesgos de la información en el subproceso oferta académica de las carreras del Centro de capacitación y actualización profesional de la Universidad Católica de Cuenca, este estudio puede ser considerado como una guía para futuras implementaciones en otros departamentos de la institución u otras instituciones de educación superior.

Referencias bibliográficas

Bravo Ramos, M., & Yoo, S. G. (2020). *Developing an Information Security Management System for Libraries Based on an Improved Risk Analysis Methodology Compatible with ISO/IEC 2700, 1067,* 371-379. https://doi.org/10.1007/978-3-030-32033-1_34

Castro-Maldonado, J. J., & Villar-Vega, H. F. (2021). Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior. *Revista modum*, *3*. https://revistas.sena.edu.co/index.php/Re_Mo/article/view/4543

Imbaquingo, D., Herrera, E., Herrera, I., Arciniega, S., Guamán, V., & Ortega Bustamante, M. (2019). Evaluación de sistemas de seguridad informáticos universitarios Caso de Estudio: Sistema de Evaluación Docente. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *E22*, 349-362. https://www.proquest.com/openview/79375ff0d1508d97ed5cfb0aebd35669/1?pq-origsite=gscholar&cbl=1006393

Moncayo, D. (2014). *Modelo de evaluación de riesgos en activos de Tic's para pequeñas y medianas empresas del sector automotriz* [Tesis maestría, Escuela Politécnica Nacional]. Repositorio de la Escuela Politécnica Nacional https://bibdigital.epn.edu.ec/bitstream/15000/8499/3/CD-5741.pdf

Morales-Paredes, P., & Medina, P. (2021). Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua—Ecuador. *3C TIC: Cuadernos de desarrollo aplicados a las TIC*, *10*, 49-75. https://doi.org/10.17993/3ctic.2021.102.49-75

Universidad Católica de Cuenca. (2020). Manual de Procesos y Procedimientos de Talento Humano. Jefatura de Talento Humano. https://documentacion.ucacue.edu.ec/files/original/e4333b1fc1085ed5e5c3c1e906b4abf2.pdf

Zevallos, M. (2019) Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. Revista Peruana de Computación y Sistemas, 2(2):43-60. http://dx.doi.org/10.15381/rpcs.v2i2.17103

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.