Polo del Conocimiento

Pol. Con. (Edición núm. 63) Vol. 6, No 11
Noviembre 2021, pp. 1168-1185
ISSN: 2550 - 682X
DOI: 10.23857/pc.v6i11.3320

Análisis de riesgos del departamento de Tecnologías de la Información y Comunicación del Registro de la Propiedad de la ciudad de Cuenca, Ecuador

Risk analysis of the Information and Communication Technologies Department of the Property Registry of the city of Cuenca, Ecuador

Análise de risco do Departamento de Tecnologias de Informação e Comunicação do Registro de Imóveis da cidade de Cuenca, Equador

Cristian Polivio Llanos-Marín [I]
cpllanos@regprocue.gob.ec
https://orcid.org/0000-0002-5536-4552

Milton Campoverde-Molina [II]
mcampoverde@ucacue.edu.ec
https://orcid.org/0000-0001-5647-5150

Correspondencia: cpllanos@regprocue.gob.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

*Recibido: 30 de Septiembre de 2021 *Aceptado: 30 de Octubre de 2021 * Publicado: 20 de Noviembre de 2021

I. Ingeniero de Sistemas, Analista 4 de Tecnologías de la Información, Registro de la Propiedad del cantón Cuenca, Cuenca, Ecuador.
II. Ingeniero de Sistemas, Docente de la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica, Grupo de Investigación Simulación, Modelado, Análisis y Accesibilidad (SMA²), Unidad Académica de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

La evolución de la tecnología y la transformación digital de múltiples procesos y sistemas hace necesario un análisis de riesgos en las empresas. Por lo tanto, el presente artículo tiene como objetivo investigar la situación en la que se encuentra la Jefatura de Tecnologías de la Información y Comunicación del Registro de la Propiedad de la ciudad de Cuenca, Ecuador mediante el análisis de riesgos utilizando el marco de referencia COSO ERM. En los resultados se identificaron 21 riesgos inherentes, de los cuales 12 tienen alta criticidad, 8 media criticidad y 1 baja criticidad. Para mitigar estos riesgos se definieron controles y recomendaciones de auditoría que ayudarán a disminuir su impacto en los procesos de la empresa. Al aplicar estos controles el nivel de los riesgos disminuyó notablemente, de los 21 riesgos detectados 14 tendrán una criticidad media y 7 una criticidad baja. En conclusión, la implementación de los controles mejorará la rentabilidad de los procesos de la institución. Sin embargo, es un proceso continuo que se debe llevar a cabo para evitar problemas de integridad, confidencialidad y disponibilidad de la información de la institución.

Palabras Claves: Análisis de riesgos; COSO ERM; Riesgo inherente; Riesgo residual; Tecnologías de la Información.

Abstract

The evolution of technology and the digital transformation of multiple processes and systems makes necessary a risk analysis in companies. Therefore, the objective of this article is to investigate the situation of the Information and Communication Technologies Department of the Property Registry of the city of Cuenca, Ecuador by means of a risk analysis using the COSO ERM framework. The results identified 21 inherent risks, of which 12 are of high criticality, 8 are of medium criticality and 1 is of low criticality. To mitigate these risks, controls and audit recommendations were defined to help reduce their impact on the company's processes. By applying these controls, the level of risks decreased significantly; of the 21 risks detected, 14 will be of medium criticality and 7 of low criticality. In conclusion, the implementation of the controls will improve the profitability of the institution's processes. However, it is a continuous process that must be carried out to avoid problems of integrity, confidentiality and availability of the institution's information.

Keywords: Risk analysis; COSO ERM; Inherent Risk; Residual Risk; Information Technology.

Resumo

A evolução da tecnologia e a transformação digital de múltiplos processos e sistemas requerem uma análise de risco nas empresas. Portanto, este artigo tem como objetivo investigar a situação em que se encontra a Sede de Tecnologias da Informação e Comunicação do Registro Predial da cidade de Cuenca, Equador, por meio da análise de risco utilizando o referencial COSO ERM. Nos resultados, foram identificados 21 riscos inerentes, sendo 12 de criticidade alta, 8 de criticidade média e 1 de baixa criticidade. Para mitigar esses riscos, foram definidos controles e recomendações de auditoria para ajudar a reduzir seu impacto nos processos da empresa. Com a aplicação desses controles, o nível de riscos diminuiu notavelmente, dos 21 riscos detectados, 14 terão criticidade média e 7, baixa criticidade. Em conclusão, a implantação de controles proporcionará maior rentabilidade aos processos da instituição. No entanto, é um processo contínuo que deve ser realizado para evitar problemas de integridade, confidencialidade e disponibilidade das informações da instituição.

Palavras-chave: Análise de risco; COSO ERM; Risco inerente; Risco residual; Tecnologias da informação.

Introducción

La gestión de la información en los departamentos de Tecnologías de la Información (TI) dentro de cada una de las instituciones públicas o privadas generan una gran cantidad de datos. Sin embargo, existe preocupación ante las vulnerabilidades que pueden presentarse en el acceso a los datos a través de sus sistemas de TI. Considerando lo antes expuesto es necesario tomar acciones específicas y especializadas para poder brindar mayor seguridad, mantener la integridad, confidencialidad y disponibilidad de la información en las instituciones (Vaca & Casanova, 2014).

En la actualidad las instituciones públicas son cada vez más dependientes de los departamentos de sistemas para el desarrollo de sus actividades propias de su negocio. La disponibilidad, integridad y confidencialidad de la información es el objetivo que tiene el departamento de sistemas dentro la empresa. El Registro de la Propiedad del cantón Cuenca (RPCC) depende

completamente de los sistemas con los que cuenta para su operatividad, los mismos que están a cargo de la Jefatura de Tecnologías de la Información y Comunicación (TIC's).

En el año 2021, se plantea desarrollar un Plan de Contingencia a través de un análisis de riesgos de la Jefatura de TIC's. Teniendo en cuenta que, este departamento ha implementado algunos controles de seguridad y de recuperación de ciertos recursos en la institución. Sin embargo, estos controles se han implementado sin un análisis de riesgos, que permita determinar el estado de mitigación de los riesgos. Además, estos riesgos podrían causar la interrupción prolongada de los servicios que brinda el RPCC. Por lo tanto, los sistemas de información del RPCC están expuestos ante desastres.

Según Curtis y Carey (2012) la metodología COSO ERM es un marco de referencia que ayuda a las empresas a identificar los riesgos potenciales existentes y a evaluar la eficacia y eficiencia de los controles. Para lograr esto, las instituciones deben tener un proceso de evaluación de riesgos que sea práctico, sostenible y fácil de entender, este proceso debe desarrollarse de forma estructurada y disciplinada.

Considerando la problemática, se tiene como objetivo de esta investigación realizar un análisis de riesgos del inventario de los activos informáticos del RPCC utilizando COSO ERM. Además, se establecerán controles que mitiguen los riesgos encontrados. Para el desarrollo de esta investigación se utilizará un análisis analítico-descriptivo a través de técnicas de indagación y análisis. Además, esta investigación servirá para el diseño de un Sistema de Gestión de Seguridad de la Información y Plan de Contingencia que requiere la institución a futuro.

En el presente artículo se tienen las siguientes secciones: en la sección 2 se presentan los conceptos relacionados que permite un mejor entendimiento al lector de los resultados, en la sección 3 se presentan las investigaciones relacionadas con el análisis de riesgos, resumida en sus objetivos, resultados y conclusiones, en la sección 4 se presenta la metodología que guiará a el proceso de obtención de los resultados, en la sección 5 se presentan los resultados del análisis de riesgos inherentes, residuales y controles, finalmente en la sección 6 se presentan las conclusiones en base a los resultados que se han obtenido en esta investigación.

Conceptos relacionados

Gestión de Riesgo Empresarial (ERM)

La Gestión de Riesgo Empresarial (ERM, Enterprise Risk Management**)** es una estrategia de arriba hacia abajo que tiene como finalidad identificar, evaluar y mitigar los posibles riesgos como ataques externos e internos, perédidas de información y otros posibles daños que pueden interferir con las operaciones y objetivos de la empresa (Hayes, 2021). Los lineamientos de la metodología ERM, indica cómo deben ser identificados y gestionados los riesgos empresariales, los mismos que están conformados por 5 componentes relacionados entre cada uno de ellos como se puede ver en la Figura 1.

Figura 1: Componentes de la Metodología ERM.

Fuente: (Committee of Sponsoring Organizations, 2017).

La ERM ha surgido como una tendencia comercial importante y relativa para el análisis de riesgos en las instituciones. Esta metodología ERM a diferencia con otras es que es más estructurada y con un enfoque disciplinado que alinea la estrategia, procesos, personas, tecnologías y conocimiento con el propósito de evaluar y gestionar los riesgos que enfrentan las empresas a medida que va creciendo (Shahzeb, Barry, & Freeman, 2013).

Mapa de calor

Un mapa de calor es una representación bidimensional de datos en la que los valores suelen estar representados por colores (a menudo rojo, verde y amarillo) y pueden variar dependiendo de la complejidad (Instituut van Internal Auditors, 2018). El mapa de calor ubica los riesgos en

un cuadrante, dependiendo de la probabilidad de ocurrencia del riesgo y del impacto que produce en caso de que el riesgo ocurra (Londoño, 2020).

Riesgo inherente

El riesgo inherente es el que se encuentra en los procesos y aparece del despliegue que se haga a cada proceso en particular y de la probabilidad de una afectación negativa a la rentabilidad o el funcionamiento de la institución (Benítez Rincón, 2020). En otras palabras, es aquel riesgo que se genera antes de que la institución implemente controles para su mitigación (Phoebe, 2021).

Riesgo residual

Un riesgo residual es el resultado obtenido después de la implementación de los controles (Phoebe, 2021). Sin embargo, algunos riesgos se pueden mitigar y otros solo minimizar por su complejidad, los cuales requieren tener un monitoreo permanente, estos riesgos son los que no permiten que la organización tenga un 100% de seguridad en sus procesos (Audittool, 2014).

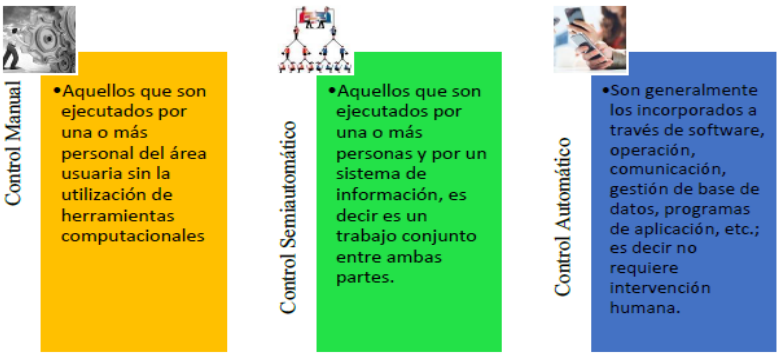
Activos informáticos

Según Wiki (2021), los activos informáticos de una empresa generalmente son considerados: el hardware, software, base de datos, aplicaciones, componentes que conforman los sistemas y la infraestructura de red dentro de la organización. Los sistemas de TI son el conjunto de estos activos que comúnmente son la base para la operatividad de la empresa (Wang, Shi, Nevo, & Chen, 2015).

Tipos de control

Los tipos de control que el modelo ERM propone para la mitigación de riesgos identificados en el riesgo inherente se realiza a través de los siguientes criterios (Sulca Córdova & Becerra Paguay, 2017):

Figura 2: Tipos de control.



Fuente: (Sulca Córdova & Becerra Paguay, 2017).

Pol. Con. (Edición núm. 63) Vol. 6, No 11, Noviembre 2021, pp. 1168-1185, ISSN: 2550 - 682X

Trabajos relacionados

En el año 2014, se realizó un análisis de riesgos de los activos informáticos del Departamento de Tecnologías de la Información de la empresa Tecniseguros S.A. utilizando dos marcos de referencia, COSO ERM y Magerit 3.0. En los resultados del análisis se identificaron 28 riesgos, que en algunos de los casos fueron agrupados. La medición de la probabilidad e impacto de ocurrencia se realizó a través de la experiencia de los auditores y expertos del negocio. Los autores concluyeron que con la metodología COSO ERM pudieron identificar y determinar los controles necesarios para poder minimizar o mitigar los riesgos. Una vez aplicado los controles ciertos procesos tuvieron una madurez, menos el proceso de mantenimiento de aplicaciones teniendo que ser revisado y reevaluado (Calderón Carrasco & Ocaña Aldaz, 2014).

En el año 2014, se realizó un análisis de riesgos que tuvo como objetivo revelar y entender los procesos tecnológicos, identificar los riesgos más significativos por medio de una valoración aplicando como marco de referencia las metodologías COSO ERM y COBIT 4.1 de los procesos de admisión y nivelación de la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación. En los resultados se determinó que el riesgo total es de 3,90 sobre 5,00. Los autores concluyeron recomendando procesos y controles que garanticen una gobernanza ordenada. Además, emitieron un informe de auditoría donde se encuentran los riesgos y recomendaciones, asimismo sugirieron diseñar e implementar un Plan de Continuidad del Negocio (Vaca & Casanova, 2014).

En el año 2017, se realizó una investigación que tuvo como objetivo un análisis de riesgos para la toma de decisiones operativas relacionas con la tecnología de computación de un proveedor de servicios en la nube de la Compañía PT. Media Andalan Bersana utilizando COSO ERM como marco de control de seguridad. En los resultados de la investigación se encontraron los siguientes tipos de riesgos: legal, financiero, tecnológico, operacional, seguridad y ambiental. En total se encontraron 39 riesgos, los con más alto nivel de impacto fueron en tecnología y seguridad. Al final concluyeron que la compañía debe determinar estrategias para la mitigación de los riesgos a través de la definición de modelos procesos de implementación y servicios cloud. Además, se determinó que la empresa tiene una calificación de "sólido" en términos de política de seguridad, seguridad física, técnicas de salvaguardias y una calificación de nivel

"pobre" en términos de análisis de impacto empresarial y plan de recuperación de desastres (Suroso, Harisno, & Noerdianto, 2017).

En el año 2017, se realizó un análisis de riesgos de los procesos: compras y gestión de recaudación y cobranza utilizando el marco COSO ERM. En los resultados se detectaron 6 riesgos en cobranza y 6 riesgos en compras. Siendo los riesgos con más alta criticidad el de recaudación y cobranza. Los autores concluyeron que mediante la aplicación de COSO ERM se evaluó y midió el impacto que ocasionarían en las actividades de la empresa los riesgos si llegarán a ocurrir. Además, recalcan que la metodología ERM se adapta fácilmente a las empresas públicas y privadas para el análisis de riesgos (Sulca Córdova & Becerra Paguay, 2017).

Metodología

La metodología de esta investigación se divide en las siguientes fases:

1. **Análisis de los activos informáticos**. En esta fase se identifican todos los activos con los que cuenta la Jefatura de TIC's. Los activos son todos los recursos relacionados con las TI como software, hardware, comunicación, archivo digital, manuales, etc. (Rodríguez, 2020).
2. **Identificación y valoración de los riesgos**. En esta fase se identifican los riesgos a los que está expuesto la institución utilizando COSO ERM. Luego se realiza una valoración de cada uno de los riesgos, de acuerdo a su probabilidad e impacto (Rodríguez, 2020).
3. **Control y Monitoreo (Riesgo Residual).** En esta fase se establecen controles a los riesgos encontrados en la institución. Estos controles permitirán disminuir o mitigar la probabilidad de ocurrencia de los riesgos (Rodríguez, 2020).
4. **Recomendaciones de auditoría.** En esta fase se realizan las recomendaciones de auditoría para cada uno de los riesgos encontrados en el RPCC.

Resultados

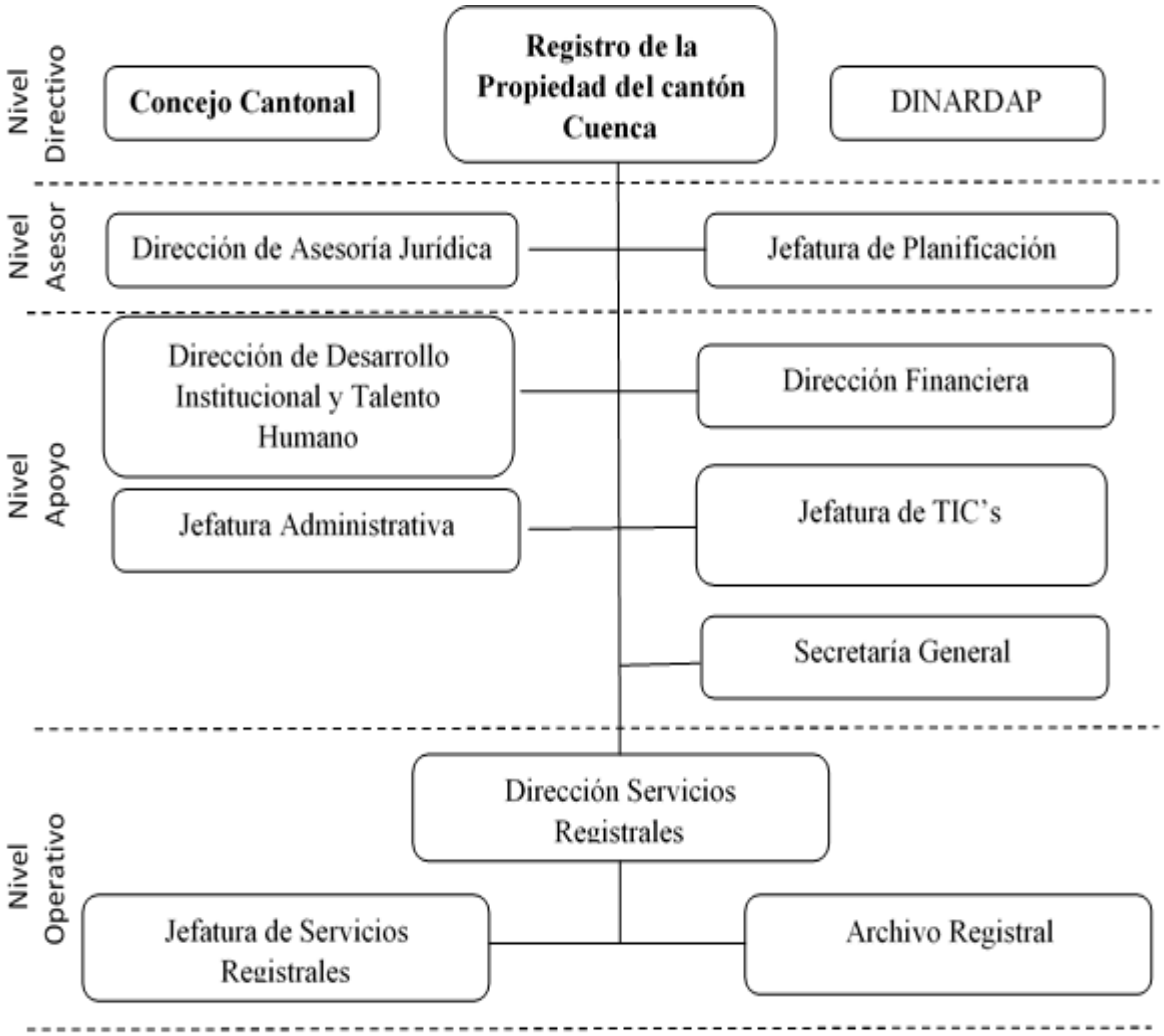
El Registro de la Propiedad del cantón Cuenca es una institución pública adscrita al Gobierno Autónomo Descentralizado (GAD) Municipal de Cuenca. El mismo que tiene como función inscribir físicamente y electrónicamente los bienes que estén en los sectores urbanos, suburbanos, rurales o de cualquier otro sector territorial que está determinada por la Ilustre Municipalidad de Cuenca dentro de las competencias que fueron concebidas por el Código

Orgánico de Organización Territorial (COOTAD). Esta tiene un historial de cada uno de los predios de los cuales se podrá emitir certificados o inscripciones que requiere la ciudadanía (Registro de la Propiedad del cantón Cuenca, 2011).

Estructura orgánica del Registro de la Propiedad del cantón Cuenca

La estructura orgánica de la empresa juega un papel muy importante en el proceso de análisis de riesgos debido a que permite determinar que departamentos deben disponer la información para el análisis. La estructura orgánica del RPCC se puede ver en la Figura 3.

Figura 3: Estructura Orgánica del RPCC.



Fuente: (Registro de la Propiedad del cantón Cuenca, 2011).

Análisis de los activos informáticos

Esta fase inicia con la selección del hardware, software y sistemas que serán parte del análisis de riesgos. La selección se realizó a los equipos de hardware y software del Data Center como por ejemplo dispositivos de almacenamiento de datos, de conectividad, comunicación, etc. Además, se seleccionaron todos los sistemas con los que trabaja la institución incluido su repositorio digital, bases de datos, sistemas web (ventanilla virtual, sistema de turnos, página web) y correo electrónico. También, se consideraron los equipos de digitalización, impresión, computadores y herramientas ofimáticas que son propias de la institución. Los cuales tienen licencias bajo arrendamiento con una empresa externa. Todos los activos que se encontraron fueron corroborados con el departamento de activos fijos de la institución. Para revisar los activos informáticos seleccionados podemos acceder a nuestro conjunto de datos en Mendeley (https://doi.org/10.17632/4h67m9wcvp.1).

Identificación de los riesgos

En esta fase se aplica la metodología COSO ERM para identificar los riesgos y su impacto de ocurrencia en los recursos informáticos. La identificación de los riesgos se realiza con el personal de la Jefatura de TIC's y se construye una base de datos de riesgos. Los riesgos fueron determinados luego de varias reuniones (ver Tabla 1) con la Jefa(e) de la Jefatura de TIC's, los analistas de TI que son parte del departamento y los usuarios dueños de los procesos. Además, se realizó entrevistas con usuarios internos para identificar otros riesgos que pueden interrumpir los procesos.

Tabla 1. Reuniones Programadas.

Fecha	Hora	Participantes	Temas
20-04-2021	10h00	Jefa (e) y analistas de TI	Análisis de riesgos Data Center
23-04-2021	10h00	Jefa (e) y analistas de TI	Análisis de riesgos sistemas
26-04-2021	14h30	Jefa (e) y analistas de TI	Análisis de riesgos equipos informáticos
28-04-2021	08h00	Jefa (e) y analistas de TI	Análisis de riesgos sistemas web
30-04-2021	15:30	Jefa (e) y analistas de TI	Análisis de riesgo equipos

La lista de riesgos que se encontraron se pueden ver en la Tabla 2. Estos riesgos proceden de diferentes fuentes tanto externas como internas.

Tabla 2. Riesgos Inherentes Identificados.

Tipificación	Riesgo evaluado
R1	Ingreso de Spam o phishing a través de correo electrónico.
R2	Renovación de los equipos de Checkpoint.
R3	Fallas en la conexión de red.
R4	No existe un control en la implementación de software de base.
R5	Procesos inexistentes de control de cambio.
R6	Vulnerabilidad en el acceso a las bases de datos.
R7	Falta de seguridad lógica a nivel de servidores.
R8	No existe manual de procesos sobre el desarrollo y cambios del software propietario.
R9	Desastres naturales fuego, agua, sismos.
R10	Fallos en la infraestructura del edificio.
R11	Degradación de los soportes de almacenamiento.
R12	Errores y fallos no intencionados por parte de usuarios, administrador, y/o configuración.
R13	Vulnerabilidad de software.
R14	Suplantación de la identidad de usuarios.
R15	Abuso de privilegios de accesos.
R16	Alteración de la información.
R17	Robo de equipos y archivos.
R18	Ausencia del personal técnico de TI.
R19	Inoperatividad del Data Center.
R20	Difusión de software dañino (virus).
R21	No cumplir con el principio de oportuno, ya que la información no se tiene en el momento que se requiere.

Riesgo inherente

El riesgo inherente son cada uno de los riesgos encontrados, valorados de acuerdo a la matriz de evaluación de riesgos. Esta valoración se clasifica en: bajo, medio y alto como se puede ver en la Tabla 3.

Tabla 3. Valoración del riesgo inherente.

Escala	Valor	Identificación
Bajo	**1.00 a 1.99**	**Verde**
Medio	**2,00 a 3,99**	**Amarillo**
Alto	**4,00 a 5,00**	**Rojo**

Valoración del riesgo

Una vez identificado los riesgos en la etapa anterior, es necesario que se analice el impacto y la vulnerabilidad de cada riesgo en el negocio. Para lo cual se debe asignar una valoración de acuerdo a la matriz de evaluación de riesgos en donde estarán las siguientes variables:

- *Tipificación del Riesgo:* Es una pequeña identificación de los riesgos en forma abreviada de manera secuencial.
- *Riesgo Evaluado:* Es la identificación del riesgo encontrado tras la etapa que lleva su nombre.
- *Criticidad:* Indica el estado de gravedad del riesgo dependiendo de la valoración de vulnerabilidad e impacto que haya puesto el funcionario consultado.
- *Vulnerabilidad:* Hace referencia a la posible concurrencia que se pueda dar al riesgo que se está evaluando, para esta investigación se calificará de 1 a 5.
- *Impacto:* Indica las consecuencias que podría originar el riesgo en caso de suscitarse al igual que la vulnerabilidad esta evaluada entre 1 a 5.
- *Calificación funcionario:* Calificación entre 1 a 5 que pone el funcionario consultado según su criterio en las variables de Vulnerabilidad e Impacto.

Tabla 4. Valoración Impacto/Vulnerabilidad.

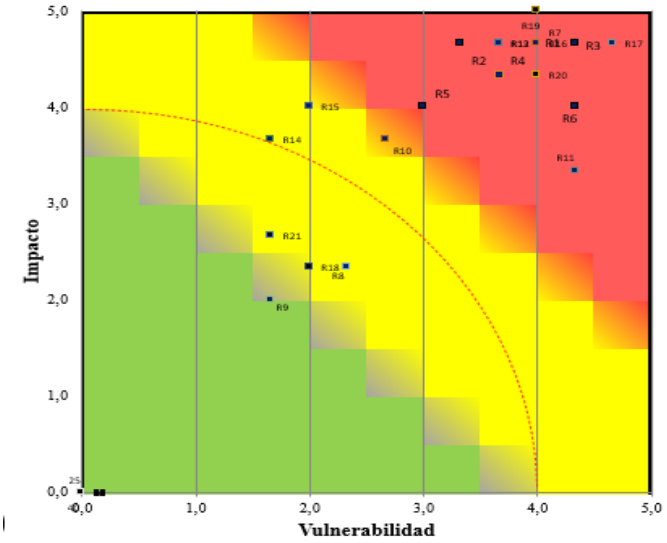
	Valoración		**1.00 a 1.99**	**2,00 a 3,99**	**4,00 a 5,00**
Impacto	Baja	**1.00 a 1.99**			
	Medio	**2,00 a 3,99**			
	Alta	**4,00 a 5,00**			
			Vulnerabilidad		

En esta etapa se valoran los riesgos encontrados de acuerdo a su impacto y vulnerabilidad utilizando el juicio de tres analistas de TI en la matriz de evaluación de riesgos. Teniendo como resultado que, de los 21 riesgos identificados 12 tienen alta criticidad, 8 media criticidad y 1 baja criticidad. La matriz del riesgo inherente según la valoración de 3 analistas de tecnologías de la información se encuentra disponible en nuestro conjunto de datos en Mendeley (https://doi.org/10.17632/4h67m9wcvp.1).

Mapa de Calor

En la Figura 4 se presenta el mapa de calor de los riesgos inherentes encontrados en los activos informáticos del RPCC. En este mapa se identifica que el 81% de los riesgos están por encima del cuadrante promedio indicando su criticidad. Los riesgos que están en el cuadrante de color rojo son a los que se les debe dar prioridad y supervisión para llegar a su mitigación o minimizar su impacto en caso de que ocurriera. A continuación, se muestra el mapa de calor que se genera en base a la calificación en base a la matriz de evaluación de riesgos dentro del RPCC.

Figura 4: Resultados de la matriz de evaluación de riesgos.



Fuente: Elaboración propia.

Control y Monitoreo (Riesgo residual)

En esta fase se determinan estrategias y procedimientos para mitigar o bajar el nivel del riesgo (riesgo inherente). Estas estrategias o procedimientos son definidos como controles que se aplican para corregir las vulnerabilidades en los activos informáticos. Este riesgo es el residuo luego que el RPCC ha realizado una acción para mitigar la vulnerabilidad o impacto que pueda tener este en la institución. Estos riesgos tendrán una calificación igual al riesgo inherente como bajo, medio y alto.

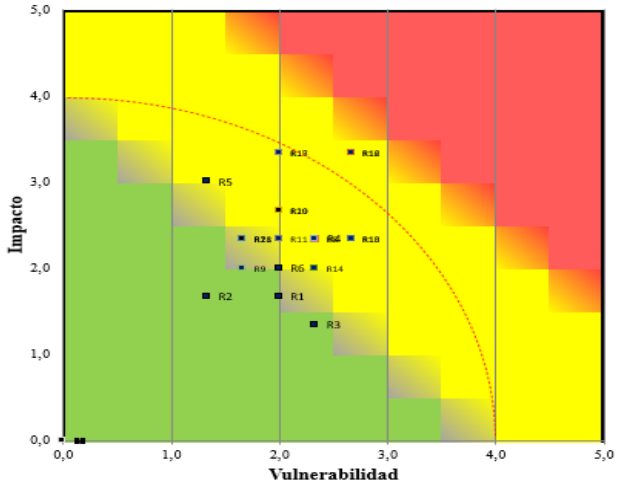
Con la aplicación de los controles a los riesgos inherentes encontrados se obtiene el riesgo residual. Teniendo como resultado que, de los 21 riesgos detectados 14 tienen una criticidad

media y 7 una criticidad baja. La matriz de los riesgo residual según la valoración de 3 analistas de tecnologías de la información se encuentra disponible en nuestro conjunto de datos en Mendeley (https://doi.org/10.17632/4h67m9wcvp.1).

Mapa de calor

En la Figura 5 se presenta el mapa de calor de los riesgos residuales encontrados en los activos informáticos del RPCC. En este mapa se identifica que el 95% de los riesgos están por debajo del cuadrante promedio indicando su criticidad y el 5% por encima. En base a los resultados obtenidos se puede concluir que se tiene que hacer una revisión exhaustiva de los controles para llegar a una mitigación total de los riesgos.

Figura 5: Resultados de la evaluación de los riesgos aplicado los controles.



Fuente: Elaboración propia.

Divulgación de Procedimientos

La divulgación de los procedimientos se realizará a con cada uno de los analistas de TI que forman parte de la Jefatura de TIC's. Además, se desarrollará un Plan de Contingencia para la implementación de los controles y mitigación de los riesgos. La divulgación de las estrategias y procedimientos a los funcionarios externos a la Jefatura de Tecnologías de la Información se lo hará a través de los siguientes medios:

- ✓ Charlas.
- ✓ Afiches.
- ✓ Fondos de pantalla a través del Active Directory.

- ✓ Correo Institucional.

Recomendación de auditoría de riesgos

Las recomendaciones de auditoría se fundamentan en el riesgo residual para poder tener un mejor control sobre los riesgos que aún persisten en la institución. Esto se lo realiza en base a un análisis de expertos utilizando los controles definidos para así tener menor probabilidad de que puedan ocurrir.

Tabla 5. Auditoria de riesgos.

Riesgo	Conclusión	Recomendación
R1	No existe un filtrado de correo para evitar los ataques de Spam o phishing.	Establecer un filtrado de correo a través de Cloud.
R2	Con las licencias caducadas de los equipos de checkpoint no se puede realizar un control correcto.	Migrar toda la configuración a una virtualización.
R3	No existe un plan de acciones para identificar las conexiones con problemas.	Establecer un mapeo y monitoreo permanente en la estructura de red.
R4	No existe un control en la implementación de software de base.	Instaurar políticas para la instalación de software por parte de los usuarios.
R5	No existen un control de cambios sobre los procesos que se realizan dentro de la Jefatura de TIC's.	Realizar manuales o bitácoras de cambios.
R6	Los accesos a los servidores no cumplen con los estándares.	Crear políticas de acceso a los servidores.
R7	Falta de seguridad lógica para el ingreso a los servidores de aplicación.	Crear políticas para el control de accesos no permitidos.
R8	No existen manuales de procesos para el desarrollo y cambios del software propio.	Elaborar manuales de procesos de desarrollo.
R9	Los desastres naturales tomando en cuenta que la institución ya tuvo que afrontar (inundación).	Crear manual de procesos ante desastres naturales.
R10	Fallos en la infraestructura del edificio (fugas de agua, fallo en los sistemas de ventilación, etc.).	Tener mecanismos para evaluar el impacto de la infraestructura sobre el funcionamiento del Data Center.
R11	Protección de los soportes de almacenamiento.	Elaborar políticas de protección y conservación de la información.
R12	Errores y fallos no intencionados por parte de usuarios.	Desarrollar procesos de revisión, y control.
R13	Al tener sistemas desarrollados vulnerables a diferentes tipos de ataques en el código fuente.	Desarrollar parches o a su vez planificar el desarrollo de nuevos sistemas.
R14	Suplantación de identidad de los usuarios internos o externos.	Elaborar políticas que permitan el registro y monitoreo de los usuarios.
R15	Dejan grabados credenciales y claves.	Elaborar procesos disciplinarios definidos en caso de que se presenten.
R16	Alteración de la información especialmente en el sistema registral.	Elaborar procedimientos para proteger y manejar la información crucial.
R17	El robo de equipos o archivos es un riesgo a tomar en cuenta.	Elaborar políticas de protección física en las instalaciones y mecanismos de monitoreo.
R18	Ausencia del personal de TI en el departamento.	Implementar políticas para que siempre este un técnico.

R19	Fallos de los equipos que se encuentran en el Data Center.	Actuar con proactividad en la creación de un plan sólido y ejecutable.
R20	Capacitación a los usuarios sobre amenazas de virus, correos infectados, etc.	Instalar antivirus con licencias actualizadas, firewall.
R21	Disponibilidad de la información que se encuentra en la base de datos de la institución.	Disminuir el tiempo de respuesta de recuperación de base de datos.

En resumen, es necesario la creación de un comité de riesgo de TI que dé seguimiento a los controles que se implementen para mitigar los riesgos identificados. Así mismo este comité estará encargado de identificar nuevos riesgos que puedan ir surgiendo. Este comité tendrá que reportar informes trimestrales de los avances y controles a la Máxima Autoridad del RPCC.

Otro aspecto importante es la instalación de software de seguridad y firewall tanto de hardware como software. Además, elaborar políticas de seguridad para la creación y cambios de contraseñas de los usuarios. También, es necesario revisar y segmentar los roles y los privilegios de los usuarios internos de la institución.

Finalmente es necesario la elaboración de políticas para el acceso a los servidores, Data Center, suplantación de identidad, instalación de software, procedimientos para proteger y manejar la información, protección física en las instalaciones, entre otros. Estas políticas deben ser difundidas a todos los usuarios internos de la institución para su cumplimiento.

Conclusiones

El objetivo de esta investigación fue realizar un análisis de riesgos del inventario de los activos informáticos del RPCC utilizando COSO ERM y establecer controles para mitigarlos. Con esta finalidad se realizó una revisión de todos los activos informáticos con los que cuenta el RPCC, para analizar las vulnerabilidades de cada uno de los equipos y sistemas. Luego se categorizaron los riesgos a través de una valoración para determinar su impacto en la institución.

Teniendo en cuenta que el riesgo inherente es aquel que puede generarse por factores internos o externos y afectar la rentabilidad de los procesos de una empresa. Luego del análisis de riesgos utilizando COSO ERM se identificaron 21 riesgos inherentes, de los cuales 12 tienen alta criticidad, 8 media criticidad y 1 baja criticidad. Para mitigar los riesgos se han creado controles fundamentados en buenas prácticas. El riesgo resultante después de la implementación de los controles se llama riesgo residual. Con la implementación de los controles se logrará que de los 21 riesgos detectados 14 tengan una criticidad media y 7 una criticidad baja.

Es importante que el RPCC implemente los controles y recomendaciones de auditoría para reducir el nivel de los riesgos inherentes. Además, la creación del comité de riesgo de TI para que se monitoree la implementación de los controles y elabore informes de nuevos riesgos que deban ser mitigados. Teniendo en cuenta, la evolución de la tecnología y la transformación digital de múltiples procesos y sistemas, hace necesario la evaluación constante de riesgos que se puedan presentar en las instituciones como nuevos escenarios. La gestión de los riesgos empresariales es un proceso continuo de revisión, análisis e implementación de controles de manera consistente y fundamentada en las mejores prácticas. Además, es importante la difusión de los controles implementados a todos los usuarios de la institución.

Como trabajos futuros se realizará una investigación sobre la implementación de gobierno de TI y gestión de servicios para la administración de incidentes y portafolios de proyectos.

Agradecimiento

A la Máxima Autoridad del Registro de la Propiedad del cantón Cuenca., Dra. Andrea Brasales J. y a la Universidad Católica de Cuenca por su apoyo con el personal docente para la culminación de esta investigación.

Referencias

1. Audittool. (2014). Red Global de Conocimientos en Auditoría y Control Interno. Recuperado el 13 de 11 de 2021, de https://n9.cl/9yn2h
2. Benítez Rincón, S. (2020). Diseño de un Sistema de Control Interno basado en el Modelo COSO III, para la compañia Induasis S.A.S. (Monografía de Contador Público). Universidad de Cundinamarca, Cundinamarca.
3. Calderón Carrasco, J. C., & Ocaña Aldaz, D. A. (2014). Auditoria Informática Basado en el Análisis de Riesgos de la empresa Tecniseguros S.A. Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE.
4. Committee of Sponsoring Organizations, o. (2017). Enterprise Risk Management Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission. Recuperado el 02 de 10 de 2021, de https://n9.cl/sbyoy

5. Curtis, P., & Carey, M. (2012). Risk Assessment in Practice. Committee of Sponsoring Organizations of the Treaway Comission.
6. Hayes, A. (2021). Investopedia. Recuperado el 02 de 10 de 2021, de https://www.investopedia.com/terms/e/enterprise-risk-management.asp
7. Instituut van Internal Auditors. (2018). Instituut van Internal Auditors. Recuperado el 12 de 10 de 2021, de https://n9.cl/ejrgi
8. Londoño, I. (2020). Pirani. Recuperado el 11 de 11 de 2021, de https://n9.cl/63d4c
9. Phoebe, F. (2021). SecurityScorecard. Recuperado el 15 de 09 de 2021, de https://n9.cl/039qo
10. Registro de la Propiedad del cantón Cuenca. (2011). Registro de la Propiedad. Recuperado el 11 de 13 de 2021, de https://n9.cl/mkoo0
11. Rodríguez, P. (2020). Ambit Building Solutions Together. Recuperado el 11 de 11 de 2021, de https://n9.cl/2dlus
12. Shahzeb, A. M., Barry, H., & Freeman, J. (2013). Enterprise Risk Management (ERM): A New Way of Looking at Risk Management at an Organisational Level. ResearchGate.
13. Sulca Córdova, G. C., & Becerra Paguay, E. R. (2017). Control interno. Matriz de riesgo: Aplicación metodología COSO II. Revista Publicando, 106 - 125.
14. Suroso, J. S., Harisno, & Noerdianto, J. (2017). Implementation of COSO ERM as Security Control Framework in Cloud Service Provider. Journal of Advanced Management Science, 322-326.
15. Vaca, C., & Casanova, E. (2014). Auditoría de Sistemas Basada en riesgos al SNNA de la SENESCYT. Repositorio de la Universidad de las Fuerzas Armadas ESPE.
16. Wang, Y., Shi, S., Nevo, S., & Chen, Y. (2015). The interaction effect of assets and IT management on firm perfomance: A systems perpective. International Journal of Information Management, 580-593.
17. WiKi, C. (2021). Cio Wiki. Recuperado el 25 de 09 de 2021, de Cio Wiki: https://n9.cl/mmzsi