UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"
ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE

"Herramienta de evaluación, identificación y priorización para la gestión de riesgos de T.I. Caso: Universidad Privada"

TESIS

Presentada para optar el Grado Académico de Maestro en Ingeniería de Sistemas con mención en Gerencia de Tecnologías de la Información y Gestión del Software

AUTOR:

Mgtr. Ing. Torres Benavides, Juan Antonio

ASESOR:

Mgtr. Ing. Zocón Alva, Oscar Gilberto

LAMBAYEQUE - PERÚ
2019

Herramienta de evaluación, identificación y priorización para la gestión de riesgos de T.I. Caso: Universidad Privada

Mgtr. Ing. Juan Antonio Torres Benavides
Autor

Mgtr. Ing. Oscar Gilberto Zocón Alva
Asesor

Tesis presentada a la Escuela de Postgrado de la Universidad Nacional Pedro Ruiz Gallo para optar el Grado Académico de MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE

Aprobado por:

Dr. Ernesto Karlo Celi Arévalo
Presidente

Dr. Luis Alberto Dávila Hurtado
Secretario

Dra. Jessie Bravo Jaico
Vocal

Lambayeque, 2019

Declaración jurada de originalidad

Yo, Juan Antonio Torres Benavides como investigador principal y Mgtr. Ing. Oscar Zocón Alva asesor del trabajo de investigación titulado ***Herramienta de evaluación, identificación y priorización para la gestión de riesgos de T.I. Caso: Universidad Privada***, declaramos bajo juramento que este trabajo no ha sido plagiado, ni contiene datos falsos. En caso se demostrara lo contrario, asumo responsablemente la anulación de este informe y por ende el proceso administrativo, a que hubiera lugar. Que puede conducir a la anulación del título o grado emitido como consecuencia de este informe.

Lambayeque, Noviembre del 2019.

_____

Juan Antonio Torres Benavides
Investigador principal

_____

Oscar Gilberto Zocón Alva
Asesor

Dedicatoria

A Dios Trino y Uno, por ser grande y generoso con nosotros y por eso estamos alegres (Sal.125, 1 – 6) y a Santa María Virgen por su acción intercesora.

A mi madre y abuela madre, por sus bendiciones desde el cielo.

A mi padre, hermanos y sobrinos por ser la energía renovadora e impulsora a conquistar las metas profesionales.

Agradecimiento

Al Mgtr. Ing. Oscar Gilberto Zocón Alva por sus conocimientos, experticia y perseverancia en la asesoría de mi tesis.

A mis profesores porque con sus conocimientos y experiencia me han permitido aprender más sobre gerencia de tecnologías de información y gestión del software.

A todos aquellos que han contribuido en la elaboración de este trabajo.

Índice General

Tabla de contenido

Índice de Tablas

Índice de Figuras

Índice de Anexos

Resumen

El objetivo del trabajo fue reducir la incertidumbre generada por la carencia de una herramienta que permita identificar, evaluar y priorizar los riesgos de Tecnologías de Información en una Universidad Particular de la Región Lambayeque, con la finalidad de mejorar la Gestión de Riesgos de TI, que actualmente se sustenta en la experticia del CIO.

El estudio se encuadra en enfoque cuantitativo con diseño pre experimental. La población y muestra a la vez estuvo conformada por 10 trabajadores del Área de TI y 07 expertos de la Región Lambayeque.

El trabajo se desarrolló en cinco etapas. La primera consistió en diagnosticar la realidad, es decir describir la actual Gestión de Riesgos de TI de la Universidad, para lo cual se aplicó una encuesta que se elaboró considerando componentes de Metodologías de Gestión de Riesgos. Los resultados obtenidos muestran una ineficiente Gestión de Riesgos de T.I. En una segunda etapa se identificó los tipos de riesgo que afronta la Universidad mediante fichas de observación. Luego se continuó con la fase de construcción de la herramienta y su posterior validación por los expertos; resultados que evidenciaron la aceptación de dicho instrumento y como consecuencia el éxito de la gestión de riesgos en la organización.

Finalmente se comprueba que el instrumento y su estructura propuesta reducen la incertidumbre en la identificación, evaluación y priorización de riesgos, elementos importantes en la gestión de riesgos en la Universidad.

Palabras clave: Riesgos, Gestión de Riesgos, Tecnologías de información

Abstract

The objective of the work was to reduce the uncertainty generated by the lack of an instrument that allows identifying, evaluating and prioritizing the risks of Information Technologies in a Private University of the Lambayeque Region, in order to improve IT Risk Management, which it is currently based on the expertise of the CIO.

The study is framed in a quantitative approach with a pre-experimental design. The population and sample at the same time consisted of 10 IT Area workers and 07 experts from the Lambayeque Region.

The work was developed in five stages. The first consisted in diagnosing the reality that is, describing the current IT Risk Management of the University, for which a survey was applied, which was prepared considering components of Risk Management Methodologies. The results obtained show an inefficient Risk Management of T.I. In a second stage, the types of risk faced by the University were identified through observation cards. Then, the construction phase of the instrument and its subsequent validation by experts continued; results that evidenced the acceptance of said instrument and as a consequence the success of risk management in the organization.

Finally, it is verified that the instrument and its proposed structure reduce the uncertainty in the identification, evaluation and prioritization of risks, important elements in the risk management in the University.

Keywords: Risks, Risk Management, Information Technologies

Introducción

McManus (2012) conceptualiza que el riesgo es un problema que podría causar alguna pérdida o amenazar el éxito de nuestro proyecto. Estos problemas potenciales podrían tener un impacto adverso en la rentabilidad del negocio o en el cronograma o éxito técnico del proyecto, así como en la calidad de nuestros productos de software o servicios de T.I. La universidad, no está exenta de esto.

Esta problemática no es ajena a las empresas de la región Lambayeque ni al sector de la educación superior, siendo así que las universidades particulares de la región han realizado inversiones para mejorar su infraestructura y servicios de TI con el objetivo de mantener su vigencia y mejorar su posicionamiento. (Reyes et al, 2016)

Por lo tanto, se hace necesario conocer e implementar la gestión de riesgos de información, entendiéndose por gestión de riesgo, según lo citado por (McManus, Ibidem): "… al proceso de identificar, abordar y eliminar este potencial problema antes de que puedan dañar nuestro proyecto."

En este sentido, la Entidad Prestadora de Servicios de Educación Superior, que de ahora en adelante se le llamará La Universidad y constituye el caso de estudio de este trabajo, no está exenta de los problemas descritos. Así mismo se conocen marcos de referencia (Aven, T. & Krohn, B. S, 2014) y buenas prácticas (ISACA, 2016) para hacer una gestión de riesgos eficiente (Aven, 2011), así como modelos y herramientas que materializan un Plan de Seguridad de Información (Ascanio, J. et al, 2015), como respuesta evidenciable de la gestión de riesgos que se está implementando. Expresan que todo este marco de buenas prácticas, modelos y herramientas debe adaptarse a la realidad que tienen para implementar la Gestión de Riesgos. Esta adaptación constituye uno de los principales problemas que afronta, dado que no existe una herramienta, que de manera objetiva permita identificar, evaluar y priorizar dichos riesgos. La evaluación de los activos y su posterior clasificación según las metodologías adoptadas han sugerido hacerlo tomando en cuenta la experiencia del personal del área, lo que perciben es haber realizado esta fase importante de manera subjetiva. Consideran que las metodologías empleadas deben establecer apriori, la validación y eficiencia de sus instrumentos. Por lo tanto este trabajo con el diseño de un instrumento de identificación, evaluación y priorización de riesgos pretende aportar al éxito de la Gestión de Riesgos de TI.

Capítulo I. Diseño Teórico

1.1 Antecedentes de la Investigación

1.1.1 Antecedente 1:

Project risk management: a deterministic quantitative technique for assessment and mitigation (Muriana et al, 2017)

Proyecto de gestión del riesgo: una técnica cuantitativa determinista para evaluación y mitigación

Este artículo de investigación, desarrollado en Palermo (Italia) explica una técnica determinista para evaluar y prevenir los riesgos de un proyecto (Muriana et al, 2017), en el que se pudo aplicar CPM y determinar la ruta crítica. Así mismo, enmarcado dentro del esquema de PMBOK, determina el estado del progreso de la actividad crítica y por consiguiente mide el riesgo que amenace y pueda hacer que el proyecto se vea afectado en tiempo y costo. Este trabajo consistió primero, en detectar el rendimiento de los factores de entrada, es decir, los costos, la calidad y el tiempo, de cada una de las actividades del proyecto. A medida que finaliza cada fase, los valores reales de los factores de entrada se detectan y se comparan con los planeados, y las acciones correctivas son tomadas para considerar el impacto de las actuaciones reales en el proyecto en general. Por lo tanto, el grado de riesgo actual del proyecto se determina a través del método de la suma ponderada entre el riesgo de la actividad real y lo planeado. Si es mayor de lo planeado, se toman medidas preventivas para mitigar el riesgo de todo el proyecto. Por último, de manera práctica las aplicaciones de la técnica se relacionan con proyectos en los que el cronograma, costos y requisitos deben definirse en la fase de planificación. También las amenazas o riesgos (desviaciones) se detectan en la fase de progreso de las actividades.

Este antecedente aporta a mi investigación, en la forma de cómo ha podido adaptar el marco conceptual de CPM y PMBOK, para proponer una forma sencilla y práctica de cuantificar el riesgo y poder mitigarlo.

1.1.2 Antecedente 2:

Guía para apoyar la priorización de riesgos en la gestión de proyectos de tecnologías de la información (Mosquera et al, 2013)

Este artículo de investigación, desarrollado en Colombia, propone una guía que hace uso de algunas buenas prácticas propuestas por el PMI -Project Management Institute, para apoyar la priorización de riesgos en proyectos de TI. La guía hace una descripción detallada de la forma

de aplicar cada técnica para disminuir los niveles de subjetividad con los que se realiza el proceso de priorización de riesgos. Así mismo concluye que actualmente es muy difícil encontrar en la literatura explicaciones de cómo utilizarlas. (Mosquera et al, pag 2)

Para el desarrollo de la guía; primero, elabora una revisión de la literatura, la cual permitió definir claramente el problema que presenta actualmente la priorización de riesgos en proyectos de TI, con lo cual se trabajó un marco conceptual con los procesos involucrados en la priorización de riesgos). Segundo, con base en el marco conceptual, se construyó la guía para la priorización de riesgos en proyectos de TI, la cual contiene una descripción de pasos que conlleva a la priorización de los mismos; en el desarrollo de la guía se efectuaron cinco experiencias con el fin de verificar su utilidad para priorizar riesgos y con los resultados y sugerencias obtenidas por parte de los participantes se hizo retroalimentación de la misma. (Mosquera et al, págs 2 - 4)

Finaliza la investigación desarrollando un prototipo de software que permite aplicar cada paso propuesto en la guía de manera automática, obteniendo resultados precisos y ordenados. Además, el prototipo software fue sometido a una evaluación de utilidad a través del juicio de expertos, teniendo en cuenta criterios de adecuación, precisión y cumplimiento.

Este antecedente es relevante para mi investigación porque describe claramente un problema similar al que estoy abordando, también hace un análisis de las metodologías vigentes concluyendo que la forma de hacer priorización de riesgos es subjetiva. Así mismo, me permite conocer un método de evaluación de la utilidad, a través del juicio de experto.

1.1.3 Antecedente 3:

Knowledge-based risk management framework for information technology project (Samer et al, 2012)

Marco de administración de riesgos basado en la gestión del conocimiento para proyectos de tecnología de información

El propósito de esta investigación, dirigida por un equipo de investigadores de EE.UU y Arabia Saudita, es explorar el campo de la Gestión de riesgos (RM) (Samer et al, pag.2) en relación con la Gestión del Conocimiento (KM) (Samer et al, pag.4). Intenta presentar un marco conceptual, llamado Gestión del Riesgo Basado en el Conocimiento (KBRM) que emplea procesos de KM para mejorar su efectividad y aumentar la probabilidad de éxito en proyectos innovadores de Tecnología de la información (TI). Aborda iniciativas para emplear Procesos de KM en procesos de RM revisando, interpretando la literatura relacionada y relevante en la integración con RM en proyectos de TI. (Samer et al, pag.5)

El documento expone algunos elementos pertinentes necesarios para construir el marco KBRM para proyectos de TI y también sugiere algún instrumento sobre la integración del proceso de KM y RM para mejorar el RRP (Riesgo Planificación de respuesta) eficiencia del proceso.

Concluye contribuyendo a la literatura y la práctica proporcionando un método claro para emplear KBRM como un marco para mantener a las organizaciones competitivas dentro del entorno empresarial.

Este antecedente es relevante para mi investigación porque contribuye con un modelo conceptual que me permite abordar el problema que deseo investigar, porque permite introducir conocimiento previo de los riesgos que se deben gestionar y cómo la organización debe incrementar ese conocimiento para aprender a responder de manera acertada.

1.1.4 Antecedente 4:

Real options in information technology risk management: an empirical validation of risk-option relationships (Benaroch et al, 2006)

Opciones reales en la gestión del riesgo de la tecnología de la información: una validación empírica de las relaciones de riesgo

Esta investigación desarrollada en Irlanda, propone un marco de gestión de riesgos basado en opciones (OBRIM), con el propósito de controlar el riesgo y maximizar el valor en las decisiones de inversión en tecnología de la información. La lógica central se basa en un conjunto de asignaciones o estrategias normadas para las diferentes opciones de riesgo, con ello se deben elegir opciones reales particulares para ser incorporadas en decisiones de inversión con el fin de controlar riesgos específicos. Este estudio prueba empíricamente si estas asignaciones se observan en la práctica. El sitio de investigación es una gran organización de servicios financieros irlandesa con prácticas establecidas de gestión de riesgos de TI no vinculadas a ningún marco de opciones. El análisis efectuado de la gestión de planes de riesgo

desarrollados para una amplia cartera de 50 inversiones en TI, encuentra un amplio respaldo empírico para la opción de mapeos de riesgo de OBRIM. Esto muestra que los administradores de TI siguen la lógica de gestión de riesgos basada en opciones, aunque puramente basadas en intuición. Desafortunadamente, confiar en esta lógica basada en intuición solo podría llevar a un riesgo sub óptimo o contraproducente. Para finalmente, argumentar que la gestión de la intuición debe ser complementada con el uso real de modelos formales de opciones, que permiten mejores percepciones cuantitativas que permitan determinar qué riesgos mitigar y combinar para abordar de manera efectiva los riesgos que más vale la pena controlar.

El aporte importante para mi investigación radica en la argumentación de los factores problemáticos similares a los que describo en la realidad problemática de la universidad particular a estudiar, pues la valoración, clasificación y priorización de riesgos se hacen de manera intuitiva lo que muchas veces no garantiza una gestión de riesgos eficiente, por lo que busco mediante una herramienta, dar mayor consistencia a ese proceso importante.

1.1.5 Antecedente 5:

Risk management guide for information technology systems (Stoneburner et al, 2002)
Guía para la gestión de riesgos

Este reporte técnico del Instituto Nacional de Estándares y Tecnología de EE.UU. propone una guía para la gestión de riesgos, empezando a definirlo como el proceso de identificación de riesgos, evaluación de riesgos y adopción de medidas para reducir el riesgo a un nivel aceptable. Describe que las organizaciones utilizan la evaluación de riesgos como primer paso en la metodología de gestión de riesgos, para determinar el alcance de la amenaza potencial, las vulnerabilidades y el riesgo asociado con un sistema de tecnología de la información (TI). El resultado de este proceso ayuda a identificar controles apropiados para reducir o eliminar el riesgo durante el proceso de mitigación de riesgos, el segundo paso de la gestión de riesgos implica priorizar, evaluar e implementar los controles apropiados de reducción de riesgos recomendados en el proceso de evaluación de riesgos. (Stoneburner et al, pag. 3)

Esta guía proporciona una base para el desarrollo de un programa eficaz de gestión de riesgos, que contiene tanto las definiciones como la orientación práctica necesaria para evaluar y mitigar los riesgos identificados en los sistemas de TI a lo largo de su ciclo de vida de desarrollo del sistema (SDLC). El objetivo final es ayudar a las organizaciones a gestionar mejor los riesgos relacionados con TI. El tercer paso en el proceso es la evaluación continua. En la mayoría de las organizaciones, los sistemas de TI se expandirán y actualizarán continuamente, sus componentes cambiarán y sus aplicaciones de software serán

reemplazadas o actualizadas con versiones más nuevas. Además, se producirán cambios de personal y es probable que las políticas de seguridad cambien con el tiempo. Estos cambios significan que aparecerán nuevos riesgos y que los riesgos previamente mitigados pueden volver a ser una preocupación. Por lo tanto, el proceso de gestión de riesgos está en curso y evolucionando. (Stoneburner et al, pag. 5)

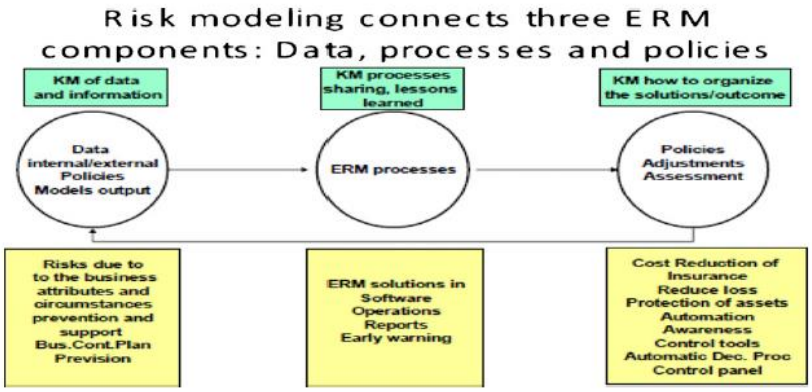
El aporte para mi investigación radica en que esta guía establece una clara secuencia de la gestión de riesgos, considerando que las organizaciones por su dinamismo generan nuevos riesgos, por lo que la concepción de gestión de riesgos y la metodología debe actualizarse, adaptarse a la realidad que la desea aplicar. Con sus argumentos puedo referenciar que el proceso de adaptación de toda metodología a la realidad que se desea gestionar es el proceso importante para su éxito.

1.2 Base Teórica

1.2.1 Teorías y Modelos Innovadores sobre Gestión de Riesgos de T.I.

1.2.1.1 Modelo de gestión de riesgo basado en el conocimiento

Figura N° 1: Metodología basada en la gestión del conocimiento para proyectos de tecnología de información



Knowledge Management Acts through Risk Modeling in Different Components of Enterprise Risk Management Processes in Rodriguez and Edwards (2008).

Fuente: El modelado de riesgos conecta tres componentes: datos, procesos y políticas - ERM (Administración del Riesgo Empresarial) (Samer et al, 2012) [1]

Los autores introdujeron una nueva metodología que contribuye a proporcionar orientación para desarrollar conocimiento sobre modelización de riesgos para mejorar la calidad y cantidad de procesos de RM (Gestión de riesgos). Como se muestra en la Figura

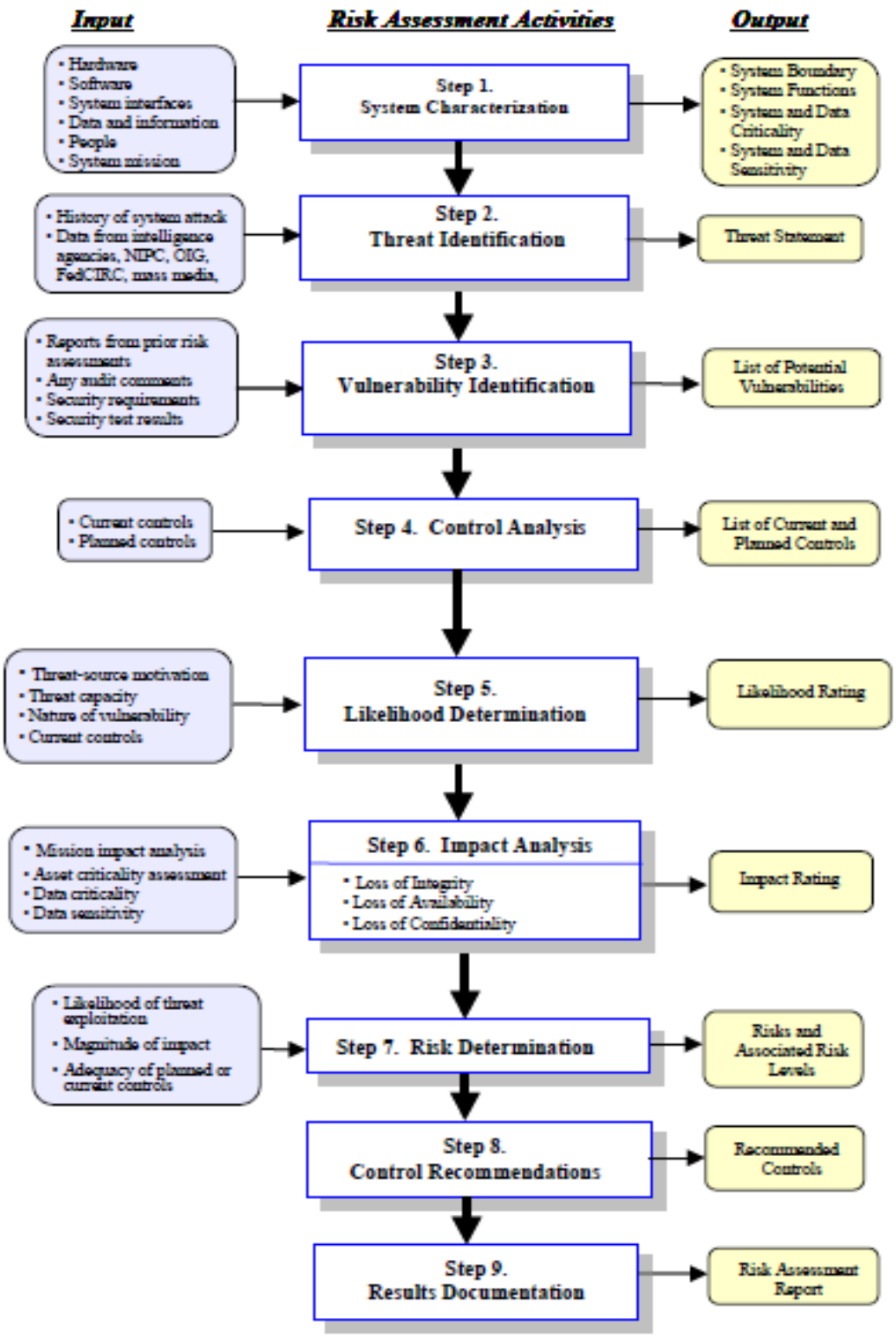
[1] **MARCO DE ADMINISTRACIÓN DE RIESGOS BASADO EN LA GESTIÓN DEL CONOCIMIENTO PARA PROYECTOS DE TECNOLOGÍA DE INFORMACIÓN (Samer et al, 2012)**

1, los autores afirmaron que existen tres componentes claves de ERM (Enterprise Risk Management); esto es: hay relaciones entre los datos, la búsqueda del problema, soluciones, políticas y organización de resultados como el riesgo.

Como resultado, su metodología propuesta utilizó el contexto y experiencia para mejorar el proceso de modelización de riesgos y su composición en los siguientes pasos: (1) responder preguntas relacionadas con la estrategia y planificación estratégica; (2) determinar los habilitadores para transferir conocimiento de riesgo de conocimiento tácito a explícito y viceversa; (3) producir conocimiento al entender los flujos de información; (4) entender la organización del conocimiento de riesgo; (5) descubrir las Claves para la gestión del riesgo tecnologías y técnicas (KM); (6) diseño del riesgo empresarial - Sistema para soportar modelos de riesgo; (7) finalmente, conectar organizaciones métricas de rendimiento y modelado de riesgos.

1.2.1.2 Modelo de evaluación de riesgos

Figura N°2: Metodología de evaluación de riesgos y los nueve pasos principales para llevar a cabo una evaluación de riesgos de un sistema de TI.



Fuente: Risk Assessment Methodology Flowchart (Stoneburner et al, 2002)[2]

[2] **GUÍA PARA LA GESTIÓN DE RIESGOS (Stoneburner, 2002)**

La evaluación de riesgos es el primer proceso en la metodología de gestión de riesgos. Las organizaciones utilizan la evaluación de riesgos para determinar el alcance de la amenaza potencial y el riesgo asociado con un sistema de TI a lo largo de su ciclo de vida de desarrollo de sistemas (SDLC). El resultado de este proceso ayuda a identificar controles apropiados para reducir o eliminar el riesgo durante el proceso de mitigación de riesgos. (Stoneburner et al, pag. 2)

El riesgo es una función de la probabilidad de una amenaza dada: la fuente ejerce una vulnerabilidad potencial particular y el impacto resultante de ese evento adverso en la organización. (Stoneburner et al, pag. 3)

Para determinar la probabilidad de un evento adverso futuro, las amenazas a un sistema de TI deben analizarse junto con las posibles vulnerabilidades y los controles establecidos para el sistema de TI. El impacto se refiere a la magnitud del daño que podría ser causado por el ejercicio de una vulnerabilidad por una amenaza. El nivel de impacto se rige por los impactos potenciales en las actividades de la organización y, a su vez, produce un impacto en los recursos de TI afectados (por ejemplo, la criticidad y la sensibilidad de los componentes y datos del sistema de TI). La metodología de evaluación de riesgos abarca nueve pasos principales: Caracterización del sistema, identificación de la amenaza, identificación de vulnerabilidad, análisis de control, determinación de la probabilidad, análisis de impacto, determinación de riesgo, recomendaciones de control y documentación de los resultados.

1.2.2 Descripción resumida de los Modelos de Gestión de Riesgos más conocidos en T.I.

1.2.2.1 Modelo Magerit

Figura N°3: Las cinco fases de la Metodología Magerit

Fuente: Risk analysis review (Bergvall et al, 2015)[3]

Es necesario contextualizar el origen y objetivos que Magerit alcanza. Primero, fue preparado y promovido por el Consejo Superior de Administración Electrónica, en respuesta a la percepción de que el gobierno (y en términos más amplios, la sociedad) depende cada vez más de la información y la tecnología para alcanzar sus objetivos de servicio. Pero hoy en día el método se usa en organizaciones de todo el mundo. Tomado de *Bergvall (2015).*

Los objetivos de Magerit son:

- Los encargados de los sistemas de información estén al tanto de la existencia de los riesgos y de la necesidad de tratarlos a tiempo.
- Analizar estos riesgos mediante su método sistemático.
- Ayudar a describir y planificar las medidas apropiadas que permitan mantener los riesgos bajo control.
- Ayudar en el proceso de evaluación, auditoría y certificación o acreditación, según corresponda en cada caso.

Según *Bergvall (2015)* las fases, que a continuación se describen, permiten comprender la secuencia de su metodología:

Identificación de activos.

[3] **REVISIÓN DEL ANÁLISIS DE RIESGOS (Bergvall et al, 2015)**

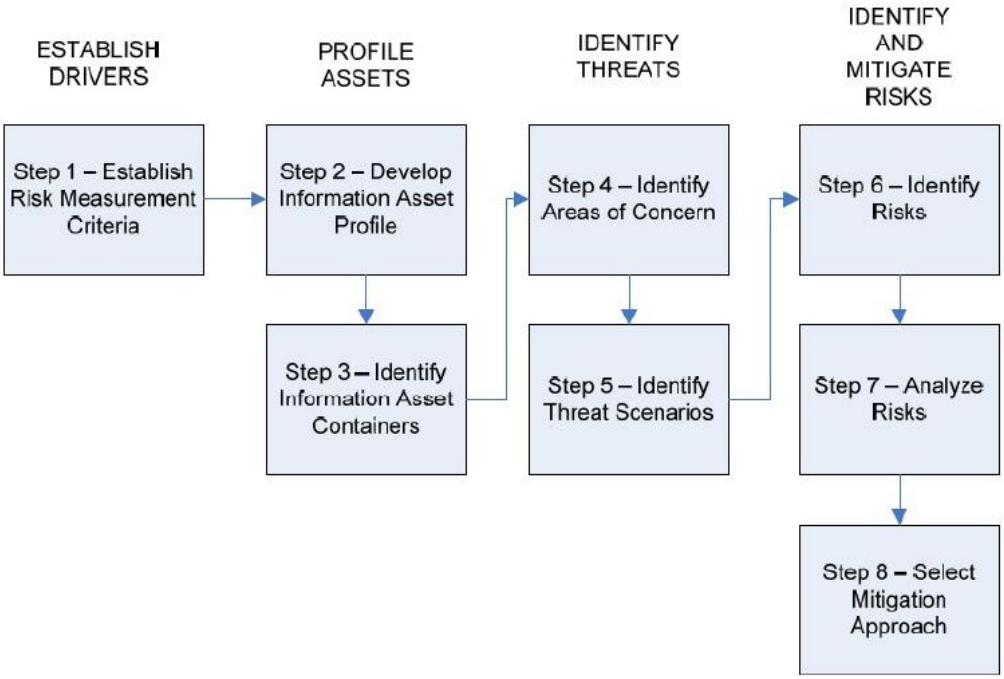
Determinación de amenazas y activos expuestos.
Análisis de qué y cómo prevenir riesgos disponibles en el sistema.
Definición de los impactos y amenazas contra los activos.
Estimación del riesgo.

1.2.2.2 Modelo Octave

OCTAVE significa “Evaluación de la amenaza, activo y vulnerabilidad operacionalmente crítica". Los métodos OCTAVE son flexibles y auto dirigido. Con el uso de OCTAVE, los equipos pequeños en las unidades de negocio y TI pueden trabajar juntos para abordar las necesidades de seguridad de su organización. El método se puede adaptar al ambiente de riesgo, seguridad y nivel de habilidad únicos de una organización. OCTAVE mueve a una organización hacia una visión de seguridad operacional basada en el riesgo y aborda la tecnología en un contexto comercial. OCTAVE Allegro es el más recientemente método desarrollado y apoyado activamente. Este método se basa en dos versiones anteriores llamadas OCTAVE Original y OCTAVE-S. El OCTAVE original método fue creado en 1999 por el Software Engineering Institute ubicado en Universidad Carnegie Mellon en Pittsburgh, Pennsylvania. *(Bergvall, 2015. Pag.13)*

El foco principal de OCTAVE Allegro son los activos de información. Los activos importantes en una organización se identifican y evalúan según el contexto de cómo se usan, donde se almacenan, transportan, procesan y cómo están expuestos a amenazas, vulnerabilidades e interrupciones como resultado. Este proceso ayuda a reducir la posibilidad de que la recopilación de datos importantes y el análisis se realizan para activos que no están bien definidos. El método es también apropiado para ser utilizado por personas que desean realizar análisis de riesgo sin amplia participación organizacional, experiencia o aporte. OCTAVE consta de ocho pasos organizados en cuatro fases y son:

Figura N°4: Las ocho fases de Metodología Octave Allegro.



Fuente: Risk analysis review (Bergvall, 2015. Pags. 12-13) [4]

1. La organización desarrolla criterios de medición de riesgos basados en la organización de la información.
2. Los activos de información que se determinan críticos son documentados. Este proceso de elaboración establece límites claros para el activo, identifica sus requisitos de seguridad e identifica todas las ubicaciones donde se encuentra el activo almacenado, transportado o procesado.
3. Las amenazas a los activos de información se identifican por las ubicaciones donde se almacenan, transportan o procesan los activos.
4. Los riesgos a los activos de información se identifican y analizan y el desarrollo de los enfoques de mitigación se inicia.

1.2.2.3 Metodología de gestión de riesgo de TI según ISO 27001

Una metodología de gestión de riesgos consiste en cómo debe llevarse a cabo para cumplir con lo establecido por la Norma ISO 27001. En un contexto general debe estimar el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización y posteriormente implementar el o los

[4] Ibídem, p. 13

controles adecuados para su tratamiento. Según ISACA (2009), las etapas mínimas que debe contemplar una metodología de gestión de riesgos de TI son:

1.2.2.3.1 Estimación de Riesgos

La estimación de riesgos describe cómo estudiar los riesgos dentro de la planeación general del entorno informático y se divide en los siguientes pasos:

– La identificación de riesgos, genera una lista de riesgos capaces de afectar el funcionamiento normal del entorno informático.

– El análisis de riesgos, mide su probabilidad de ocurrencia y su impacto en la organización.

– La asignación de prioridades a los riesgos.

1.2.2.3.2 Identificación de Riesgos

En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático. Los principales factores que se ven afectados son:

– Creación de la planificación: Incluye la planificación excesivamente optimista, planificación con tareas innecesarias y organización de un entorno informático sin tener en cuenta áreas desconocidas y la envergadura del mismo.

– La organización y gestión, presupuestos bajos, el ciclo de revisión/decisión de las directivas es más lento de lo esperado.

– El entorno de trabajo; mal funcionamiento de las herramientas de desarrollo, espacios de trabajo inadecuados y la curva de aprendizaje de las nuevas tecnologías son más largas de lo esperado.

– Las decisiones de los usuarios finales: Falta de participación de los usuarios finales y la falta de comunicación entre los usuarios y el Departamento de Informática o similar.

– El personal contratado: Falta de motivación, falta de trabajo en equipo y trabajos de poca calidad.

– Los procesos que incluyen: La burocracia, falta de control de calidad y la falta de entusiasmo.

Se puede considerar como los orígenes de la Administración de los Riesgos de TI a los siguientes aspectos:

– Requerimientos legales, regulatorios, contractuales.

– Acelerados avances tecnológicos.

– Incidentes de seguridad (comunicaciones divulgadas)

– Preocupación de los usuarios

– Pérdidas económicas

– Crecimiento generalizado de procesos de negocio soportados en tecnología de información.

1.2.2.3.3 Análisis de Riesgos

Una vez hayan identificado los riesgos desde lo planificado, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución. Esta fase implica valorar los riesgos y su real dimensión de ocurrencia.

1.2.2.3.4 Exposición a Riesgos

Una actividad útil y necesaria en el análisis de riesgos es determinar su nivel de exposición en cada uno de los procesos en que se hayan identificado.

1.2.2.3.5 Estimación de la Probabilidad de Pérdida

Las principales formas de estimar la probabilidad de pérdida son las siguientes:

– Disponer de la persona que está más familiarizada con el entorno informático para que estime la probabilidad de ocurrencia de eventos perjudiciales.

– Usar técnicas Delphi o de consenso en grupo. El método Delphi consiste en reunir a un grupo de expertos para solucionar determinados problemas. Dicho grupo realiza la categorización individual de las amenazas y de los objetos del riesgo.

– Utilizar la calibración mediante adjetivos, en la cual las personas involucradas eligen un nivel de riesgo entre (probable, muy probable) y después se convierten a estimaciones cuantitativas.

1.2.2.3.6 Priorización de Riesgos

En este paso de la estimación de riesgos, se estiman su prioridad de manera que se tenga forma de centrar el esfuerzo para desarrollar la gestión de riesgos. Cuando se realiza la priorización (elementos de alto riesgo y pequeños riesgos), estos últimos no deben ser de gran preocupación, pues lo verdaderamente crítico no se puede dejar en un segundo plano.

1.2.2.3.7 Control o tratamiento de Riesgos

Una vez que se hayan identificado los riesgos del entorno informático y analizado su probabilidad de ocurrencia, existen bases para controlarlos que son:

– Planificación.

– Resolución de riesgos.

– Monitorización de riesgos.

1.2.2.3.8 Planificación de Riesgos

Su objetivo, es desarrollar un plan que controle cada uno de los eventos perjudiciales a que se encuentran expuestas las actividades informáticas.

1.2.2.3.9 Resolución de Riesgos (Incluye mitigación y transferencia de riesgos)

La resolución de los riesgos está conformada por los métodos que controlan el problema de un diseño de controles inadecuado, los principales son:

– Evitar el Riesgo: No realizar actividades arriesgadas.

– Conseguir información acerca del riesgo.

– Planificar el entorno informático de forma que si ocurre un riesgo, las actividades informáticas sean cumplidas.

– Eliminar el origen del riesgo, si es posible desde su inicio.

– Asumir y comunicar el riesgo.

1.2.2.3.10 Monitorización de Riesgos

La vida en el mundo informático sería más fácil si los riesgos apareciesen después de que hayamos desarrollado planes para tratarlos. Pero los riesgos aparecen y desaparecen dentro del entorno informático, por lo que se necesita una monitorización para comprobar cómo protegerse del descontrol de un riesgo e identificar como aparecen nuevos eventos perjudiciales en las actividades informáticas.

1.2.3 Definiciones teóricas sobre la Gestión de Riesgos de T.I.

1.2.3.1 Riesgo

(McManus, 2012) define riesgo "…al problema que podría causar alguna pérdida o amenazar el éxito de nuestro proyecto, pero que no ha sucedido todavía. Estos problemas potenciales podrían tener un impacto adverso en la rentabilidad del negocio o en el cronograma o éxito técnico del proyecto, así como en la calidad de nuestros productos de

software o servicios de T.I. También pueden impactar en la moral del equipo del proyecto."

De acuerdo a (ISACA, 2009) en los Lineamientos para la Gestión de Seguridad de TI publicadas por la Organización Internacional de Estandarización (ISO) en su (ISO/IEC PDTR 13335−1), riesgo es el potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y, por consiguiente, ocasione pérdida o daño a la organización.

Según Alejandro Medina (2007) riesgo se define como la probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando la confidencialidad, la integridad y la disponibilidad de la información […]. Riesgo es: – La condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa. – La posibilidad de un impacto negativo sobre los objetivos de la empresa.

1.2.3.2 Activos de información

Para (Solarte, 2015), los sistemas de información, los datos contenidos en ellas y la información son los activos más valiosos para las organizaciones empresariales y se hace necesario brindarles una protección adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad.

1.2.3.3 Riesgo tecnológico

Según (Ramírez, 2011), el riesgo tecnológico es intrínseco al uso de tecnología. Puede incidir sobre las metas y objetivos organizacionales y ser causa de otro tipo de riesgos. Por ello el daño, interrupción, alteración o falla derivada del uso de TI puede implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico.

1.2.3.4 Gestión de riesgos

(Ramírez, et al), la define como el uso de metodologías integradas y ágiles para gestionar riesgos con el fin de minimizar el impacto que pueda causar la violación de alguna de las dimensiones de la seguridad (esto corresponde a la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad)

1.2.3.5 Proceso de gestión de riesgo

Costas Santos (2011) establece que la Gestión de los Riesgos permite tener control sobre el desarrollo, la implementación y funcionamiento de los procesos, lo cual llevará a lograr de manera eficiente el cumplimiento de sus objetivos estratégicos y estar preparados para enfrentar cualquier incidente que pueda presentarse. Sobre los procesos, se construyen controles con el objetivo de reducir la frecuencia de las amenazas o limitar el daño causado y llevar el nivel de riesgo a un nivel aceptable por la organización. Dependiendo del tipo de riesgo, se puede optar por:

– Evitar el riesgo: por ejemplo eliminando el activo.

– Mitigar el riesgo: implementando controles para reducir la probabilidad y el impacto.

– Transferir el riesgo: por ejemplo contratando un seguro con cobertura para ese riesgo.

– Aceptar el riesgo: reconociendo que el riesgo existe y monitorizarlo. Una vez que los controles han sido aplicados, el nivel de riesgo que queda es el riesgo residual. Como se establece en los Requerimientos de los Sistemas de Gestión de Seguridad de la Información en la norma ISO 27001; la Dirección debe establecer el nivel de riesgo aceptable para la organización. Los riesgos que excedan de ese nivel deben ser reducidos.

1.2.3.6 Nivel de riesgo aceptable

De acuerdo a Costas Santos (2011), riesgo aceptable es el que conlleva un potencial de pérdida menor y que de producirse fallas operacionales no afectan significativamente las condiciones de la operación. […] los activos con riesgo extremo e intolerable deben ser llevados al menos al nivel tolerable. Y en el caso de activos críticos deben ser llevados al nivel aceptable. Para la aceptación definitiva de los riesgos se debe tener en cuenta: – La Política organizacional. – Sensibilidad y criticidad de los activos involucrados. – Niveles aceptables de los posibles impactos. – Rentabilidad de la implementación.

1.3 Definiciones conceptuales

1.3.1 Alcance y arquitectura

Para Brown, S. (2016), la arquitectura mide el suministro de TI de infraestructura empleada por las Universidades, así como la evaluación y aplicación de tecnologías emergentes.

1.3.2 Gestión de procesos de negocio soportados por TI

Habilidad para posibilitar o dirigir los cambios en los procesos de negocio y su entrega de valiosas soluciones personalizadas para las unidades de negocio internas y los clientes

externos o socios. Los sistemas de TI son principalmente habilitadores de procesos de negocio y los estándares de TI son definidos y aplicados a nivel de unidad funcional en coordinación emergente en todas las unidades funcionales del negocio.

1.3.3 Evaluación subjetiva del riesgo

Proceso que permite la ponderación que se adjudica al riesgo, basada en la experiencia del evaluador. No emplea herramienta o técnica validada que pueda refrendar su ponderación.

1.3.4 Evaluación objetiva del riesgo

Proceso cuantitativo, verificado que pondera el riesgo en base a escalas, haciendo más objetiva la asignación que le otorga el evaluador al riesgo analizado.

1.4 Operacionalización de Variables

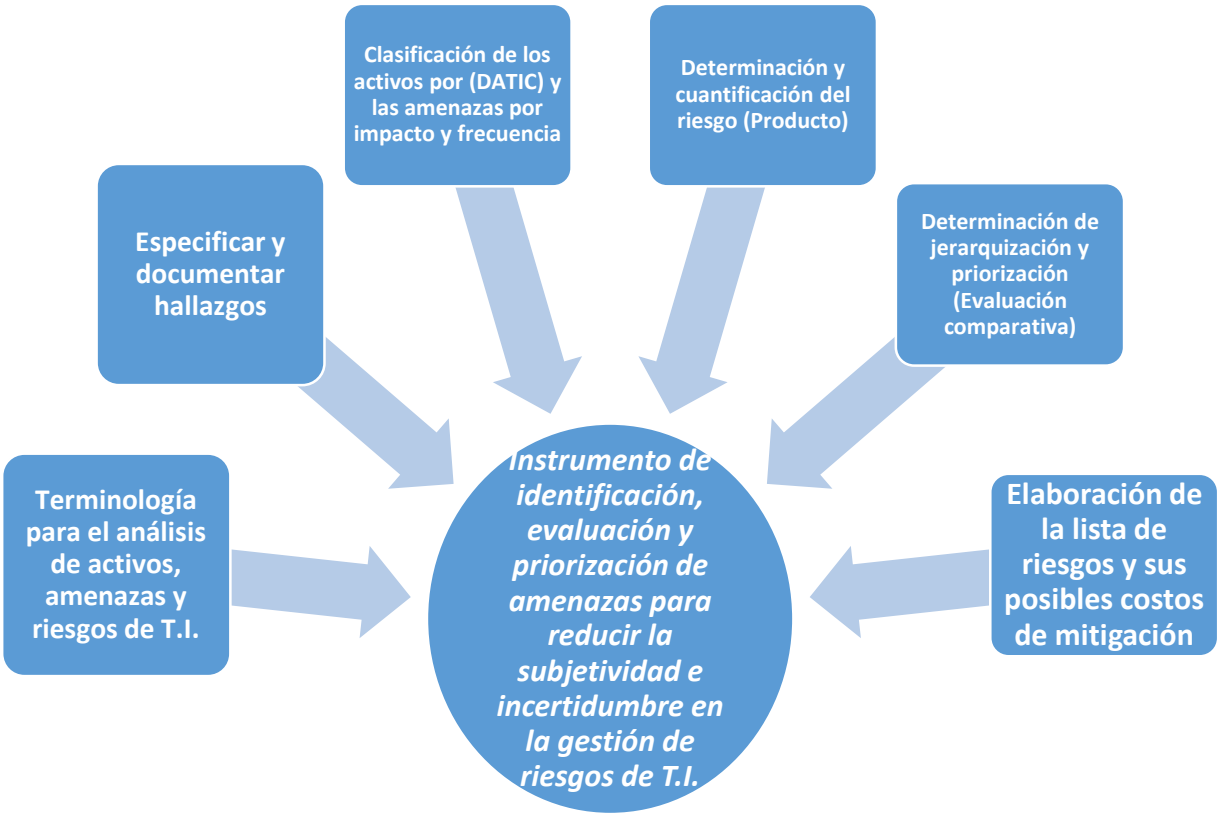
Tabla 01: Operacionalización de la Variable Dependiente

Variable Dependiente	**Definición de la Variable**	**Dimensión**	**Indicadores**	**Instrumento**
Reducción de la incertidumbre en la gestión de riesgos de T.I.	Reducir la falta de seguridad, de confianza o de certeza sobre el control de los riesgos de TI, especialmente cuando crea inquietud la aparición de la amenaza o riesgo de la información en la Universidad, objeto de análisis del presente trabajo.	Identificar riesgos	* # de riesgos de TI * # de amenazas de TI * # de catástrofes de TI	Guía de observación
		Evaluar riesgos	Nivel de probabilidad de ocurrencia del riesgo (%). Nivel de impacto del riesgo (%).	Matriz de evaluación
		Priorizar riesgos a tratar	# de riesgos priorizados	Lista de riesgos priorizados
		Planificar respuesta o tratamiento a los riesgos	- Tiempos de respuesta para amenazas categoría 1. - Tiempos de respuesta para amenazas categoría 2.	Lista de actividades planificadas para mitigar riesgos

Fuente: Elaboración propia

Variable Independiente (Esquema de la propuesta de solución)

Figura N°5: Estructura del Instrumento a crear.



Fuente: Elaboración propia – producción inédita

1.5 Hipótesis

El diseño de una herramienta que desarrolle una base común para la terminología de análisis de riesgos, especifique y documente los hallazgos en la etapa diagnóstica, clasifique las evidencias por su impacto y frecuencia, cuantifique las amenazas por impacto y frecuencia, determine la priorización de riesgos de T.I. reduce la incertidumbre en la gestión de riesgos de T.I. en una Universidad Privada.

Capítulo II. Métodos y Materiales

2.1 Tipo de Investigación

La presente investigación se encuadra en enfoque cuantitativo con diseño pre experimental.

2.2 Método de Investigación

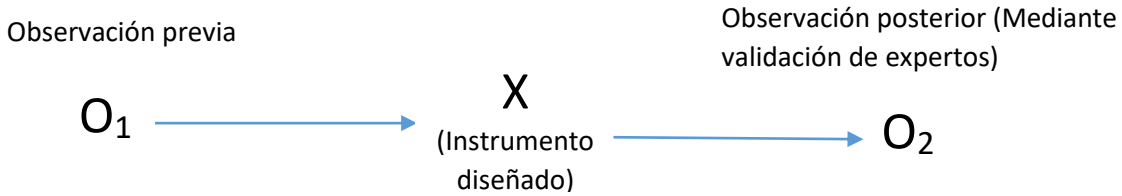
La presente investigación se realizó en 5 fases tal como se muestra en la siguiente tabla:

Tabla N° 2: Fases del método de investigación

FASES	ACTIVIDAD
FASE 1	*Descripción de la realidad actual de la Universidad.
	*Diagnóstico de los procesos o actividades relacionadas a identificación de riesgos. Método: Observación. Técnica: Observación directa. Instrumento: Guías de observación.
FASE 2	*Evaluación, medición y descripción de las actividades de gestión de riesgos que asume la Universidad. Método: Reporte. Técnica: Reporte. Instrumento: Registros físicos o virtuales.
	* Identificación de riesgos y valoración de los activos. Método: Observación. Técnica: Observación directa Instrumento: Matriz de riesgos.
FASE 3	*Elaboración de herramienta metodológica para la tipificación, evaluación y priorización de riesgos.
	*Fundamentación del instrumento propuesto.
FASE 4	*Pruebas de aceptación con los expertos.
FASE 5	*Redacción de informe.

Fuente: Elaboración propia

2.3 Diseño de Contrastación



Donde:

O_1: Es la observación previa con evidencias y mediciones de la realidad antes de aplicar el instrumento que se propone como solución al problema.

O_2: Es la observación posterior a la aplicación del instrumento solución del problema. Pero como no se va a aplicar dicha solución en la Universidad por carencia de tiempo, se reemplaza por la validación de juicio de expertos.

X: Instrumento solución al problema.

2.4 Población, Muestra y Muestreo

En la Fase 1 y fase 2 del desarrollo de la presente investigación se aplicó una encuesta de diagnóstico aplicada a los trabajadores del Área de T.I.

Por lo tanto, la ***población*** es finita y está conformada por el total de 10 trabajadores que realizan actividades relacionadas a los sistemas de información, su mantenimiento, prevención y funcionamiento.

Para esta investigación la ***muestra*** es la misma de la población por ser finita y de fácil acceso a ella. Además porque los 10 trabajadores tienen las mismas características o idoneidad para responder a la encuesta formulada. Por ello, no hay necesidad de ***muestreo.***

2.5 Técnicas, Instrumentos, Equipos y Materiales de Recolección de Datos

Tabla 03: Métodos, técnicas e instrumentos

Método	Técnica	Instrumento
Cuestionarios	Cuestionarios	Encuesta
Reportes	Reportes	Registros físicos, virtuales.
Entrevista individual	Entrevista	Entrevista
Observación	Observación Directa	Guías de observación

Fuente: Elaboración propia

Encuesta: Dirigida a la muestra, conformada por los 10 trabajadores del área de T.I. y a 07 expertos para la validación de la propuesta de solución.

Instrumento:

Se aplicó dos cuestionarios:

1.- Cuestionario diagnóstico

Permitirá diagnosticar y describir los procesos y actividades que la organización realiza considerando las Metodologías o Estrategias de Gestión de Riesgos.

2.- Cuestionario dirigido a los Expertos

Permitirá la validación de la propuesta solución mediante la recolección de indicadores de aceptación o rechazo de la propuesta y su estructura. Así como sus sugerencias de mejora. La intención es verificar si el instrumento solución preparado realmente soluciona el problema. (Adaptado de Hernández, et al (2010)). Así mismo, indica que existen tres tipos de evidencia para la validez: 1) evidencia relacionada con el contenido, 2) evidencia relacionada con el criterio y 3) evidencia relacionada con el constructo:

1. Evidencia relacionada con el contenido.

La validez de contenido se refiere al grado en que un instrumento refleja un dominio específico de contenido de lo que se mide.

2. Evidencia relacionada con el criterio.

La validez de criterio, establece que un instrumento de medición al comparar sus resultados con los de algún criterio externo, debe medir lo mismo.

3. Evidencia relacionada con el constructo.

La validez de constructo, se refiere a qué tan exitosamente un instrumento representa y mide un concepto teórico. A esta validez le concierne en particular el significado del instrumento, esto es, qué está midiendo y cómo opera para medirlo.

Por lo tanto, la propuesta de solución (Instrumento) fue validada mediante la *evidencia de contenido* obteniendo la *Validez de Contenido* de mi propuesta. Validada por los expertos seleccionados de acuerdo a los criterios que se consideraron en su momento.

Tabla 04: Materiales

Materiales de recolección de datos
Pc’ (01)
Laptop (01)
Impresora (01)
02 millares de papel bond
Lapiceros (10)
Memoria USB (02)

Fuente: Elaboración propia

2.6 Procesamiento y Análisis de Datos

Después de haber realizado la recolección de los datos a través de las técnicas de recolección aplicadas (encuesta y observación), se realizó la prueba de validez de cada instrumento. Luego de validar los datos tabulados haciendo uso del SPSS se procedió a analizarlos e interpretarlos. A continuación se explica la secuencia de procesamiento y análisis de datos que se seguirá en la presente investigación:

Validación y edición: Aquí se realizó la validez de los instrumentos. También se verificó si las preguntas hechas para la identificación de los factores problemáticos, causas y efectos fueron correctas. Así mismo, se validará si las preguntas de los cuestionarios dirigidos a expertos para la validación del instrumento fueron correctas. Con ello debemos obtener datos suficientes y correctos. También observar si hay errores o incoherencias por parte de las respuestas de los encuestados.

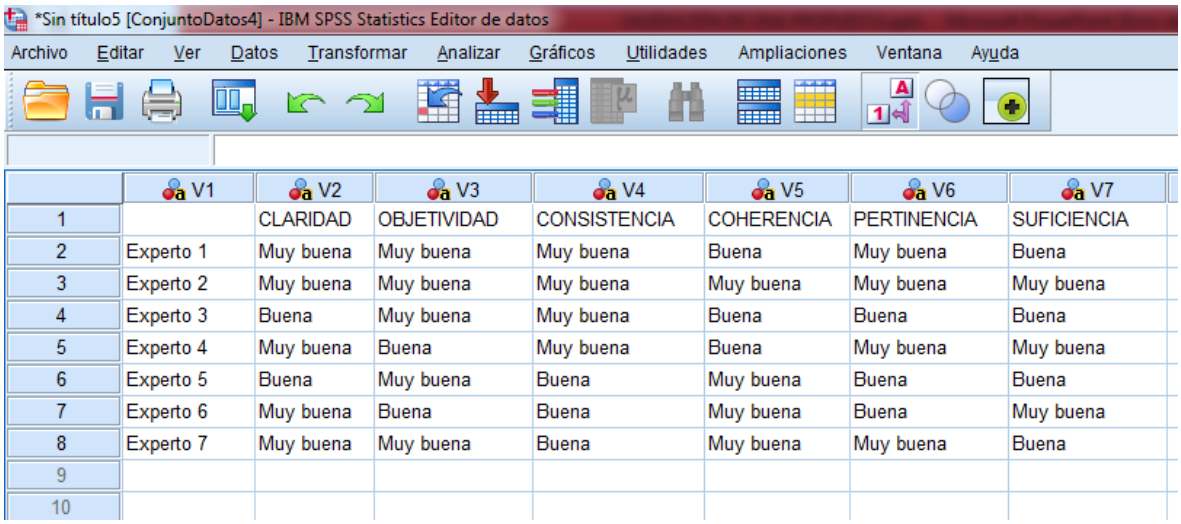
Codificación: Proceso por el cual se le asignará códigos a las respuestas obtenidas de las preguntas hechas para trabajarlas en el SPSS y EXCEL.

Introducción de los datos: Fase donde se transcribieron los datos a un medio electrónico. Para así obtener resultados de la data recogida anteriormente. Se utilizó el SPSS por ser un software que permite ejecutar técnicas de análisis estadístico, como también exploración grafica de datos, líneas de tiempo y tablas multidimensionales. También se utilizó el Excel.

Tabulación y análisis estadístico: Aquí se pasan los datos a tablas cruzadas para luego analizar gráficamente.

A continuación algunas evidencias del procesamiento de datos.

Figura N°6: Evidencia procesamiento de datos en SPSS.



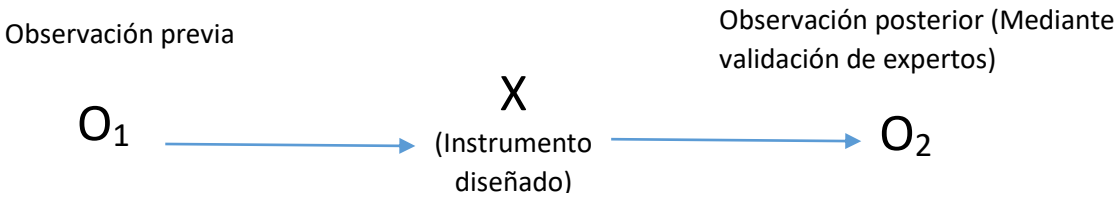
	V1	V2	V3	V4	V5	V6	V7
1		CLARIDAD	OBJETIVIDAD	CONSISTENCIA	COHERENCIA	PERTINENCIA	SUFICIENCIA
2	Experto 1	Muy buena	Muy buena	Muy buena	Buena	Muy buena	Buena
3	Experto 2	Muy buena	Muy buena	Muy buena	Muy buena	Muy buena	Muy buena
4	Experto 3	Buena	Muy buena	Muy buena	Buena	Buena	Buena
5	Experto 4	Muy buena	Buena	Muy buena	Buena	Muy buena	Muy buena
6	Experto 5	Buena	Muy buena	Buena	Muy buena	Buena	Buena
7	Experto 6	Muy buena	Buena	Buena	Muy buena	Buena	Muy buena
8	Experto 7	Muy buena	Muy buena	Buena	Muy buena	Muy buena	Buena
9							
10							

Fuente: Elaboración propia

Capítulo III. Resultados

Los resultados se explicarán teniendo en cuenta el diseño de investigación indicado, que ayudó a determinar el Método que la Investigación ha desarrollado y que a continuación se detalla.

Figura N°7: Diseño de la investigación.



Fuente: Elaboración propia

3.1.- O_1: Observación previa a la aplicación de la herramienta - Evidencias del problema

3.1.1.- Descripción de la realidad actual de la Universidad objeto de estudio.

La universidad tiene más de 18 años de fundada. Actualmente tiene un aproximado de 7,500 estudiantes distribuidos entre las carreras profesionales ofrecidas a la sociedad lambayecana. El área de TI está conformada por un equipo de 10 personas, entre responsables de proyectos de infraestructura tecnológica y desarrollo de sistemas.

La universidad cuenta con una infraestructura tecnológica conformada por un data center con 5 servidores, 2 sistemas de prevención de intrusos (IPS), 35 switchs administrables, 1 routers de salida, 6 switchs core, 4 firewalls, cableado estructurado certificado. El personal técnico cuenta con certificaciones en cableado estructurado, gestión de servicios de TI y servidores GNU/Linux.

Además, la universidad cuenta con 10 sistemas informáticos para el soporte de sus actividades administrativas y académicas, los cuales son de desarrollo propio.[5]

[5] Información resumida y obtenida del ITEM 1 del *Instrumento diagnóstico – Ficha de Observación para describir los procesos o actividades de la Universidad considerando lo expuesto por la Metodología de Evaluación de Riesgos de un Sistema de TI. (Stoneburner, 2002).(VER ANEXO 4)*

3.1.2.- Descripción de los procesos o actividades relacionadas a identificar riesgos.

Tomando en consideración las observaciones recogidas en el Item 2 y 3 del *Instrumento diagnóstico – Ficha de Observación para describir los procesos o actividades de la Universidad considerando lo expuesto por la Metodología de Evaluación de Riesgos de un Sistema de TI. (Stoneburner, 2002)* se obtiene los siguientes resultados:

En cuanto a la declaración de amenazas

1.- En ocasiones utilizan formatos para el registro y declaración de amenazas.

2.- Se observaron 18 documentos que han registrado incidencia de posibles amenazas a los sistemas informáticos, servidores y/o activos de T.I. de la Universidad, de lo que se concluye que el 60% de documentos contiene datos incorrectos puesto que no hay evidencia alguna que pueda corroborar lo descrito. Así mismo el 100% tiene una descripción empírica al no evidenciar lenguaje o formato de alguna M.G.R. de T.I. Además se han registrado posibles amenazas (Así lo dice el texto), sin evidenciar magnitud y frecuencia.

En cuanto a la declaración de vulnerabilidades

1. No se evidenció la existencia de reportes de identificación de riesgos de T.I.
2. Sí existen requerimientos de seguridad de servidores, ejecutados tanto por los gestores de BD y software. Así mismo, el identificador de usuarios para los puntos de acceso tiene un protocolo de seguridad.
3. No se realizan auditorías de seguridad de información.

3.1.3.- Evaluación, medición y descripción de las actividades de gestión de riesgos que asume la universidad.

Para evidenciar esta realidad problemática y poder evaluar, medir y ahora describir las actividades de gestión de riesgos de T.I. que la Universidad asume, se aplicó el *Instrumento diagnóstico aplicado al Personal de T.I. basada en la Metodología basada en la gestión del conocimiento para proyectos de tecnología de información (Samer, 2012)* a los 10 trabajadores del Área de Tecnologías de Información de la Universidad cuyos resultados se describen:

TABLA 05: Resultados encuesta diagnóstica aplicada a los trabajadores de T.I.

Trabajador T.I.	ITEM 1				ITEM 2					ITEM 3
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**
1	1	2	2	2	1	5	5	5	2	1
2	1	1	1	1	3	5	5	5	2	2
3	1	1	1	1	4	5	5	5	2	2
4	1	2	2	2	1	5	5	5	2	1
5	1	2	1	2	1	5	5	5	2	3
6	1	1	2	1	1	5	5	5	1	1
7	1	2	2	2	1	5	5	5	2	2
8	1	2	2	2	1	5	5	5	2	2
9	1	2	2	2	1	5	5	5	1	2
10	1	1	1	1	1	5	5	5	2	1

Fuente: Elaboración propia

La presente tabla resume las respuestas a cada pregunta proporcionada por cada uno de los trabajadores del Área de T.I.

ESTADISTICAS DESCRIPTIVAS

```
GET DATA
/TYPE=XLSX
/FILE='C:\MAESTRIA UNPRG\EL INFORME DE TESIS\TESIS RECOLECCION DE DATOS DE PERSONAL DE TI2.xlsx'
/SHEET=name 'Hoja1'
/CELLRANGE=FULL
/READNAMES=ON
/DATATYPEMIN PERCENTAGE=95.0
EXECUTE.
DATASET NAME ConjuntoDatos3 WINDOW=FRONT.
FREQUENCIES VARIABLES=P1 P2 P3 P4 P5 P6 P7 P8 P9 P10
/ORDER=ANALYSIS.
```

Tabla 06: Validación de datos de encuesta a Trabajadores de T.I.

Frecuencias

Notas

Salida creada		24-APR-2019 12:53:42
Comentarios		
Entrada	Conjunto de datos activo	ConjuntoDatos3
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	10
Manejo de valores perdidos	Definición de perdidos	Los valores perdidos definidos por el usuario se tratan como perdidos.
	Casos utilizados	Las estadísticas se basan en todos los casos con datos válidos.
Sintaxis		FREQUENCIES VARIABLES=P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 /ORDER=ANALYSIS.
Recursos	Tiempo de procesador	00:00:00.02
	Tiempo transcurrido	00:00:00.01

Estadísticos

		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
N	Válido	10	10	10	10	10	10	10	10	10	10
	Perdidos	0	0	0	0	0	0	0	0	0	0

Fuente: Elaboración propia

El SPSS reporta que todos los datos recogidos son válidos y con esto podemos valorar lo recogido para su posterior discusión.

Tablas de frecuencias

Tabla 07: Resultados Pregunta 1.

P1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	1	10	100,0	100,0	100,0

Fuente: Elaboración propia

Interpretación: La pregunta 1, reporta que todos los trabajadores manifiestan conocer al menos una Metodología de Gestión de Riesgos de T.I.

Tabla 08: Resultados Pregunta 2.

P2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	1	4	40,0	40,0	40,0
	2	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia

Interpretación: La pregunta 2, reporta que el 60% de trabajadores no ha aplicado una Metodología de Gestión de Riesgos de T.I.

Tabla 09: Resultados Pregunta 3.

P3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	1	4	40,0	40,0	40,0
	2	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia

Interpretación: La pregunta 3, reporta que el 60% de trabajadores no conoce de herramienta, instrumento, formato alguno que le haya permitido la materialización una Metodología de Gestión de Riesgos de T.I.

Tabla 10: Resultados Pregunta 4.

P4

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	1	4	40,0	40,0	40,0
	2	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia

Interpretación: La pregunta 4, reporta que el 60% de trabajadores no conoce de alguna estrategia o plan para abordar las amenazas de T.I. que puede sufrir la organización

Tabla 11: Resultados Pregunta 5.

P5

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	1	8	80,0	80,0	80,0
	3	1	10,0	10,0	90,0
	4	1	10,0	10,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia

Interpretación: La pregunta 5, reporta que el 80% de trabajadores nunca ha aplicado algún protocolo o formato para la materialización de la Metodología de Gestión de Riesgos de T.I. Así mismo, sólo el 10% de trabajadores manifiesta que en ocasiones, aplicó algún protocolo o formato para los fines descritos. También el último 10%, casi siempre.

Tabla 12: Resultados Pregunta 6.

P6

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	5	10	100,0	100,0	100,0

Fuente: Elaboración propia

Interpretación: La pregunta 6, reporta que el 100% de trabajadores manifiesta que la identificación de riesgos se realiza considerando sólo la experiencia del CIO

Tabla 13: Resultados Pregunta 7.

P7

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	5	10	100,0	100,0	100,0

Fuente: Elaboración propia

Interpretación: La pregunta 7, reporta que el 100% de trabajadores manifiesta que la evaluación de riesgos se realiza considerando sólo la experiencia del CIO

Tabla 14: Resultados Pregunta 8

P8

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	5	10	100,0	100,0	100,0

Fuente: Elaboración propia

Interpretación: La pregunta 8, reporta que el 100% de trabajadores manifiesta que la priorización de riesgos se realiza considerando sólo la experiencia del CIO

Tabla 15: Resultados Pregunta 9

P9

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	1	2	20,0	20,0	20,0
	2	8	80,0	80,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia

Interpretación: La pregunta 9, reporta que el 80% de trabajadores manifiesta que no existe la identificación de riesgos de T.I. validados por el CEO de la Organización. Mientras que un 20% expresa que sí

Tabla 16: Resultados Pregunta 10

P10

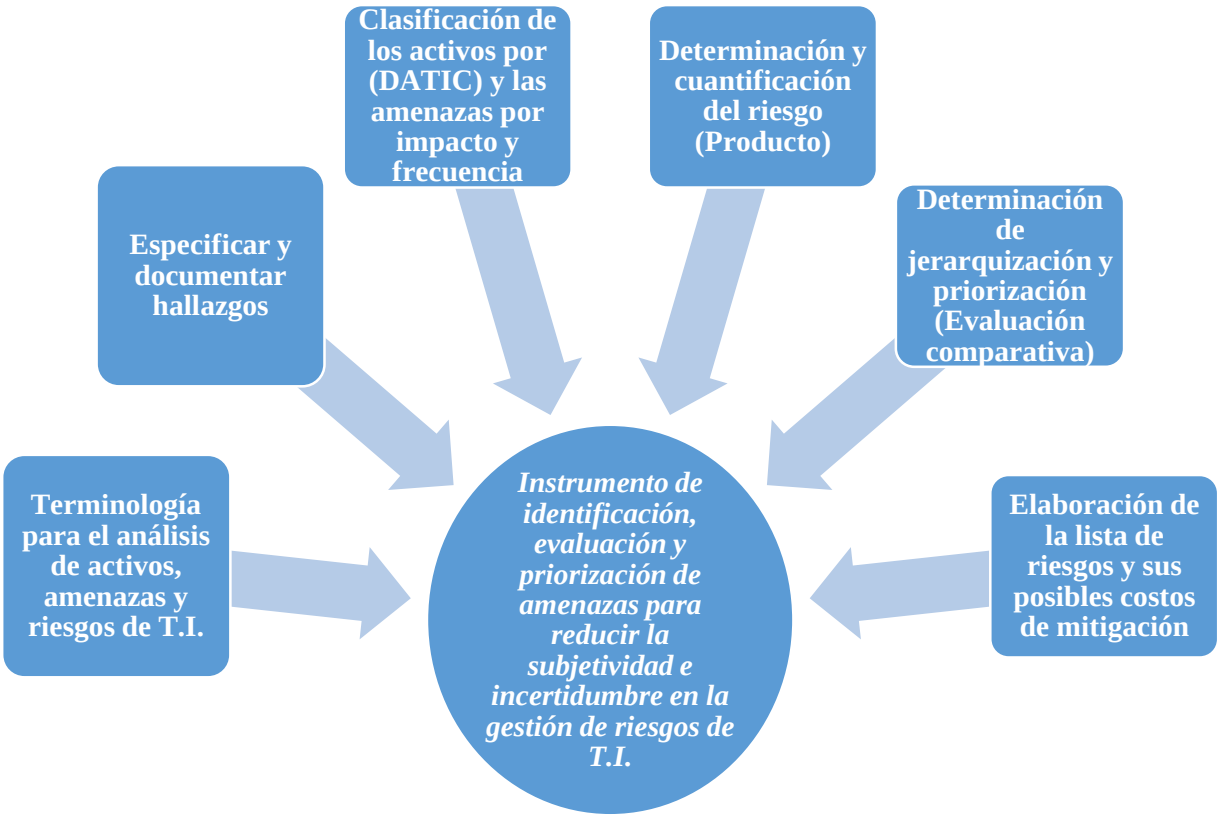
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	1	4	40,0	40,0	40,0
	2	5	50,0	50,0	90,0
	3	1	10,0	10,0	100,0
	Total	10	100,0	100,0	

Fuente: Elaboración propia

Interpretación: La pregunta 10, reporta que el 50% de trabajadores manifiesta ser ineficiente las actuales iniciativas o políticas de Gestión de Riesgos de T.I. que aplica la organización. Mientras que el 40% la valora como muy ineficiente y un 10% ni eficiente ni ineficiente.

3.2.- (X) Instrumento diseñado: Propuesta de solución

Figura N°8: Estructura de la propuesta de solución.



Fuente: Elaboración propia – producción inédita

DESCRIPCIÓN DE CADA UNA DE LAS FASES DE LA HERRAMIENTA QUE SE PROPONE PARA REDUCIR LA INCERTIDUMBRE EN LA IDENTIFICACIÓN, EVALUACIÓN Y PRIORIZACIÓN DE LOS RIESGOS DE TI

1.- Desarrollo de una base común para la terminología de análisis de riesgos

La herramienta propone una base conceptual y definición de términos para efectuar el análisis requerido. Esta etapa consiste en que el CIO de TI (Quien hará el análisis de riesgos) pueda equiparar sus conocimientos, definiciones terminológicas a los términos estándares que la herramienta maneja. Así mismo, cada jefe de área de la Dirección de TI y la Gerencia General de la organización también conocerá los siguientes términos:

AMENAZA DE TECNOLOGÍA DE INFORMACIÓN

Posible problema que podría causar alguna pérdida o amenazar el éxito del producto de software, servicio o proyecto de T.I.

RIESGO DE TECNOLOGÍA DE INFORMACIÓN

Es la amenaza que constituye un problema potencial y podrían tener un impacto adverso en la rentabilidad del negocio o en el cronograma o éxito técnico del producto, servicio o proyecto, así como en la calidad de ellos. La amenaza se dimensiona como riesgo cuando se mide por su impacto y frecuencia.

ESTIMACIÓN DEL RIESGO DE TECNOLOGÍA DE INFORMACIÓN

La estimación de riesgos de TI describe cómo estudiar los riesgos dentro de la planeación general del entorno informático y se divide en los siguientes pasos: i) La identificación de riesgos, genera una lista de riesgos capaces de afectar el funcionamiento normal del entorno informático. ii) El análisis de riesgos, mide su probabilidad de ocurrencia y su impacto en la organización y iii) La asignación de prioridades a los riesgos.

RIESGO = PROBABILIDAD X IMPACTO

IDENTIFICACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN

En este paso se identifican los factores que introducen una amenaza en el éxito del producto de software, servicio o proyecto de T.I. Los principales factores de riesgo se clasifican en: para los activos de la Capa Cliente y para los activos de la Capa Servidor.

ACTIVO DE TECNOLOGÍA DE INFORMACIÓN

Los sistemas de información, los datos contenidos en ellas y la información son los activos más valiosos para las organizaciones empresariales y se hace necesario brindarles una protección

adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad y otros aspectos técnicos.

IMPACTO DEL RIESGO

Son las consecuencias o resultado del riesgo sufrido. Estas siempre son negativas en aspectos de seguridad de información y de servicios de tecnología de información.

FRECUENCIA DEL RIESGO

Es el número de veces en que un riesgo se repite durante un horizonte de tiempo determinado o referencial.

ACTIVOS DE LA CAPA CLIENTE

Son aquellos que generan, procesan y almacenan la información necesaria para la operación y el cumplimiento de los objetivos de la compañía. Así mismo, esta clasificación también se otorga a todos los activos que tienen interacción con los clientes o usuarios de los sistemas informáticos, datos o información de la organización.

ACTIVOS DE LA CAPA SERVIDOR

Es la clasificación que se otorga a todos los activos, de aplicaciones o datos de la organización que se almacenan, procesan o ubican en los servidores o contenedores de información.

AMENAZAS DE LA CAPA CLIENTE

Es la clasificación que se otorga a todas las amenazas que se podrían en los activos de la capa cliente.

AMENAZAS DE LA CAPA SERVIDOR

Es la clasificación que se otorga a todas las amenazas que se podrían suscitar en los activos de la capa servidor.

ACTIVO: INFORMACIÓN DATOS VITALES DE LA ORGANIZACIÓN

Es el activo relacionado a información core del negocio que permite a la organización prestar sus servicios que pueden ser almacenados o trasladados de un lugar a otro por medios digitales que son importantes también para la organización. Pertenece a este activo los indicadores del Plan Estratégico, información de recursos humanos, finanzas, bancos, curriculum vitae, remuneraciones, sanciones, penalidades, reconocimientos, información particular y planes operativos de recursos humanos, etc.

ACTIVO: INFORMACIÓN PERSONAL

Activo relacionado a usuarios internos y externos, operadores, administradores del sistema, de BBDD, comunicaciones, programadores, etc.

ACTIVO: INFORMACIÓN CLASIFICADA

Es el activo de información que contiene información exclusiva para la Alta Dirección de la Universidad.

ACTIVO: COPIAS DE SEGURIDAD

Es la copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. También se le lama respaldo, copia de reserva, backup.

ACTIVO: CONFIGURACIONES

Es el activo que contiene las funciones destinadas a soportar directamente o indirectamente los servicios de la infraestructura de hardware y software que satisface las necesidades de los usuarios.

VALORACIÓN DE LOS ACTIVOS

[D] DISPONIBILIDAD.

Es vital para el negocio tener la información core a todo momento las 24 horas del día por los 7 días de la semana.[6]

[A] AUTENTICIDAD DE QUIÉN ACCEDE AL SERVICIO.

Importante determinar quién es el que manipula o genera la información. Si alguien manipula la información vital sin autorización puede generar problemas de autenticidad[7]

[T] TRAZABILIDAD DE QUIÉN ACCEDE AL SERVICIO, CUÁNDO Y QUÉ HACE.

Es importante tener registro de los accesos y sus actividades. A esto le llamamos traza y es necesario generarlo en una bitácora.[8]

[6] Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

[7] Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

[8] Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

[I] INTEGRIDAD.

Es importante tener claro la coherencia y validación de la información que se almacena y procesa en el sistema.[9]

[C] CONFIDENCIALIDAD.

Es muy importante la confidencialidad para el negocio, por lo tanto se debe tener claro quién tiene los permisos de usuario validados.[10]

CLASIFICACIÓN DE RIESGOS

Los riesgos se clasifican en:

AMENAZAS: ACTIVO INFORMACIÓN DATOS VITALES DE LA ORGANIZACIÓN

AMENAZA 1: FUGAS DE LA INFORMACIÓN

Se denomina fuga de información al incidente que pone en poder de una persona ajena la organización, información confidencial que sólo debería estar disponible para integrantes de la misma.

AMENAZA 2: SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO

Expresión informática que describe los actos ilícitos de personas inescrupulosas para estafar, obtener información personal, contraseñas para fines ilícitos.

AMENAZA 3: ERRORES DE LOS USUARIOS

Referido a los errores que los usuarios cometen con los activos de información. Pueden ser errores de permisos de usuario, configuraciones, etc.

AMENAZA 4: REVELACIÓN DE LA INFORMACIÓN

Por lo general compartir contraseñas, información exclusiva de la organización, etc con personas que le pueden dar mal uso a dicho activo.

AMENAZAS: ACTIVO INFORMACIÓN PERSONAL

AMENAZA 1: MODIFICACIÓN DE LA INFORMACIÓN

Cambio de las características, la esencia de la información alterando la fiabilidad de su contenido.

[9] Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]

[10] Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]

AMENAZA 2: ABUSO DE PRIVILEGIOS DE ACCESO

Referido a la entrega de privilegios de los activos de información que exceden los requerimientos de su perfil de usuario o puesto de trabajo.

AMENAZA 3: FUGAS DE LA INFORMACIÓN

Se denomina fuga de información al incidente que pone en poder de una persona ajena la organización, información confidencial que sólo debería estar disponible para integrantes de la misma.

AMENAZA 4: SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO

Expresión informática que describe los actos ilícitos de personas inescrupulosas para estafar, obtener información personal, contraseñas para fines ilícitos.

AMENAZA 5: ERRORES DEL ADMINISTRADOR DEL SISTEMA

Relacionados a la inexactitud, integridad y protección de todos los procesos y recursos de información

AMENAZAS: ACTIVO INFORMACIÓN CLASIFICADA

AMENAZA 1: REVELACIÓN DE LA INFORMACIÓN

Por lo general compartir contraseñas, información exclusiva de la organización, etc con personas que le pueden dar mal uso a dicho activo.

AMENAZA 2: MODIFICACIÓN DE LA INFORMACIÓN

Cambio de las características, la esencia de la información alterando la fiabilidad de su contenido.

AMENAZA 3: ABUSO DE PRIVILEGIOS DE ACCESO

Referido a la entrega de privilegios de los activos de información que exceden los requerimientos de su perfil de usuario o puesto de trabajo.

AMENAZA 4: SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO

Expresión informática que describe los actos ilícitos de personas inescrupulosas para estafar, obtener información personal, contraseñas para fines ilícitos.

AMENAZA 5: ACCESO NO AUTORIZADO

Consiste en acceder de manera indebida, sin autorización o contra derecho a la información clasificada, con la finalidad de obtener una satisfacción ilícita con el activo tomado.

AMENAZAS: ACTIVO CONFIGURACIONES

AMENAZA 1: CONTAMINACIÓN ELECTROMECÁNICA

Vibraciones, polvo, suciedad, rayaduras a discos duros, etc.

AMENAZA 2: FUEGO

Posibilidad de que el fuego acabe con recursos del sistema.

AMENAZA 3: INUNDACIONES

Posibilidad de que el agua acabe con recursos del sistema. Por ejemplo: escapes, fugas, inundaciones, etc.

AMENAZA 4: CORTE DE SUMINISTRO ELÉCTRICO

Cese de la alimentación de potencia eléctrica.

AMENAZA 5: AVERÍA DE ORIGEN FÍSICO Y LÓGICO

Fallos en los equipos o en los programas. Puede ser debida a un defecto de origen o durante el funcionamiento del sistema.

AMENAZA 6: ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE EQUIPOS (HARDWARE)

Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

AMENAZA 7: ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)

Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

AMENAZAS: ACTIVO COPIAS DE SEGURIDAD DE INFORMACIÓN

AMENAZA 1: DESASTRES NATURALES

Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.

AMENAZA 2: FENÓMENO DEL NIÑO

Es un desastre natural que tiene especial relevancia por sus efectos colaterales tanto a estructuras físicas como a coberturas digitales.

AMENAZA 3: FUEGO

Posibilidad de que el fuego acabe con recursos del sistema.

AMENAZA 4: INUNDACIONES

Posibilidad de que el agua acabe con recursos del sistema. Por ejemplo: escapes, fugas, inundaciones, etc.

AMENAZA 5: AVERÍA DE ORIGEN FÍSICO Y LÓGICO

Fallos en los equipos o en los programas. Puede ser debida a un defecto de origen o durante el funcionamiento del sistema.

AMENAZA 6: CONTAMINACIÓN ELECTROMAGNÉTICA

Vibraciones, polvo, suciedad, rayaduras a discos duros, etc.

AMENAZA 7: CORTE DEL SUMINISTRO ELÉCTRICO

Cese de la alimentación de potencia eléctrica.

AMENAZA 8: PÉRDIDA DE EQUIPOS

La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Por lo general se pierden con frecuencia equipos y soportes de información. Acompañado a esto, si son equipos que hospedan datos, se sufre fuga de información.

VALORACIÓN DE LAS AMENAZAS

La valoración de una amenaza es la estimación de la frecuencia (Probabilidad de ocurrencia) e impacto (Consecuencia) de un riesgo. Se resume en el siguiente cuadro:

Tabla N° 17: Impacto y frecuencia de una amenaza

IMPACTO (CONSECUENCIA)	
5	MUY ALTO
4	ALTO
3	MEDIO
2	BAJO
1	MUY BAJO

PROBABILIDAD DE OCURRENCIA		
FRECUENTE	80% - 100%	5
PROBABLE	61% - 80%	4
OCASIONAL	41% - 60%	3
RARO	21% - 40%	2
IMPROBABLE	1% - 20%	1

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Así mismo, al efectuar la cuantificación del riesgo, al multiplicar las valorizaciones asignadas en las tablas anteriores, obtendremos el tipo de riesgo y su jerarquización. De esta manera podemos identificar en la tabla siguiente que las celdas de color rojo (frecuente, muy alto), (frecuente, alto), (probable, muy alto) y (probable, alto) son las que identifican los mayores riesgos y a quienes se les debe tener mayor consideración. De la misma forma, las celdas de color dorado representan riesgos de consideración intermedia, las celdas de color verde caña, riesgos de menor preocupación y los de color turquesa son los riesgos aceptables o tolerables que no deben ser descuidados porque se pueden convertir en catastróficos si es que no se tratan o mitigan.

Tabla N° 18: Matriz d clasificación de riesgos

		5	4	3	2	1
		FRECUENTE	PROBABLE	OCASIONAL	RARO	IMPROBABLE
5	MUY ALTO					
4	ALTO		R3 / R2	R1		
3	MEDIO					
2	BAJO					
1	MUY BAJO					

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Leyenda de colores

- Riesgo muy alto
- Riesgo alto
- Riesgo medio
- Riesgo bajo
- Riesgo muy bajo

2.- Especificar y documentar los hallazgos en la etapa del análisis

Se han empleado diferentes herramientas para la recolección de evidencias en cuanto a los posibles riesgos (amenazas) que enfrenta la Universidad en estudio, con la finalidad de validar la información recopilada. Los instrumentos han aportado información valiosa.

Tabla 19: Ficha de observación y registro de incidencias de T.I.

1. DATOS INFORMATIVOS

1.1. Descripción del Data Center:	
1.2. Descripción de los servicios que ofrece:	
1.3. Descripción del activo(s) a registrar:	

1.4. Responsable:
1.5. Cargo:
1.6. Título:_____ Especialidad:
1.7. Celular: _____ e-mail:
1.8. Fecha: ____/____/2019 al _____/_____/2019

1.9. Turnos:

	Mañana:	**Hora**	**Inicio:** **Término:**
	Tarde:	**Hora**	**Inicio:** **Término:**
	Noche:	**Hora**	**Inicio:** **Término:**

ACTIVOS DE LA CAPA CLIENTE										
1	**INFORMACIÓN DATOS VITALES DE LA ORGANIZACIÓN**	**L**	**M**	**M**	**J**	**V**	**S**	**D**	**Frecuencia**	**Observaciones**
	Amenaza 1: Fugas de la información									
	Amenaza 2: Suplantación de la identidad del usuario									
	Amenaza 3: Errores de los usuarios									
	Amenaza 4: Revelación de la información									
2	**INFORMACIÓN PERSONAL**	**L**	**M**	**M**	**J**	**V**	**S**	**D**	**Frecuencia**	**Observaciones**
	Amenaza 1: Fugas de la información									
	Amenaza 2: Alteraciones de la información									
	Amenaza 3: Errores del administrador del sistema									
	Amenaza 4: Abusos de privilegios de acceso									
	Amenaza 5: Suplantación de la identidad del usuario									
	Amenaza 6: Modificación de la información									
3	**INFORMACIÓN CLASIFICADA**	**L**	**M**	**M**	**J**	**V**	**S**	**D**	**Frecuencia**	**Observaciones**
	Amenaza 1: Fugas de la información									
	Amenaza 2: Alteraciones de la información									
	Amenaza 3: Acceso no autorizado									
	Amenaza 4: Abusos de privilegios de acceso									
	Amenaza 5: Suplantación de la identidad del usuario									
	Amenaza 6: Modificación de la información									
ACTIVOS DE LA CAPA SERVIDOR										
1	**COPIAS DE SEGURIDAD**	**L**	**M**	**M**	**J**	**V**	**S**	**D**	**Frecuencia**	**Observaciones**

	Amenaza 1: Desastres naturales									
	Amenaza 2: Fenómeno del Niño									
	Amenaza 3: Fuego									
	Amenaza 4: Inundaciones									
	Amenaza 5: Avería de origen físico y lógico									
	Amenaza 6: Contaminación electromagnética									
	Amenaza 7: Corte del suministro eléctrico									
2	**CONFIGURACIONES**	**L**	**M**	**M**	**J**	**V**	**S**	**D**	**Frecuencia**	**Observaciones**
	Amenaza 1: Contaminación electromagnética									
	Amenaza 2: Fuego									
	Amenaza 3: Inundaciones									
	Amenaza 4: Corte del suministro eléctrico									
	Amenaza 5: Avería de origen físico y lógico									

Fuente: Elaboración propia

Tabla 20: Para la evaluación de procesos involucrados – impactos sufridos

Procesos involucrados	Indique el activo afectado	Indique la amenaza sufrida	Describa las herramientas utilizadas para su identificación,	Describa el tipo de evidencia que ha recogido y su custodia (archivado o guardado en…)	Describa los impactos
Administración de red					
Administración de servidores					

Control de puntos de accesos					

Fuente: Elaboración propia

Tabla 21: Información del personal involucrado en el registro

PERSONAL INVOLUCRADO EN EL REGISTRO DE INCIDENCIAS DE T.I.

1. DATOS INFORMATIVOS

1.1. Nombres y apellidos del responsable del registro	
1.2. Descripción del cargo que desempeña:	
1.3. Descripción del activo(s) a registrar:	

1.4. Título: _____ Especialidad: _____

1.5. Celular: _____ e-mail: _____

1.6. Jefe responsable: _____

Fuente: Elaboración propia

3.- Clasificación de las evidencias por impacto y frecuencia

Teniendo en cuenta que el alcance de la presente investigación es ayudar a disminuir la subjetividad e incertidumbre en la identificación, evaluación y priorización de riesgos de T.I. se procede a evaluar las evidencias y a cuantificar el impacto y frecuencia de ocurrencia. A continuación se describe en resumen, los valores para medir la frecuencia e impacto y se proponen los siguientes formatos más importantes:

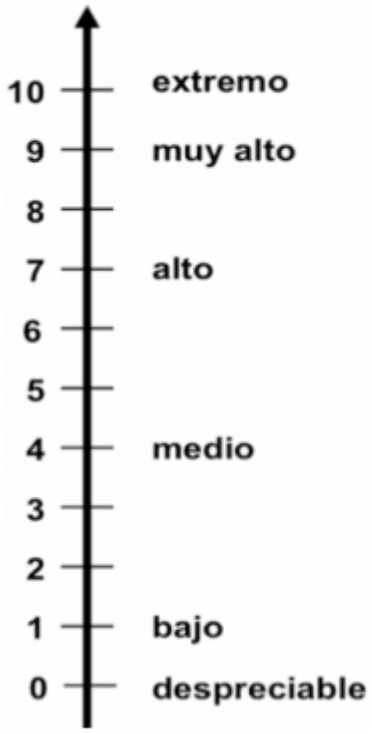
Tabla 22: Matriz de riesgos y ubicación de cada amenaza

PROBABILIDAD DE OCURRENCIA		
FRECUENTE	80% - 100%	5
PROBABLE	61% - 80%	4
OCASIONAL	41% - 60%	3
RARO	21% - 40%	2
IMPROBABLE	1% - 20%	1

Impacto - Medida Cualitativo		
MA	**MUY ALTA**	5
A	**ALTA**	4
M	**MEDIA**	3
B	**BAJA**	2
MB	**MUY BAJA**	1

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Figura N°9: Escala de valoración de los activos



valor	
10	extremo
9	muy alto
6-8	alto
3-5	medio
1-2	bajo
0	despreciable

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Tabla 23: Ficha de observación y clasificación de los activos de T.I. para la identificación, evaluación y priorización de riesgos de T.I.

1. DATOS INFORMATIVOS

1.1. Descripción del Data Center:	
1.2. Descripción de los servicios que ofrece:	
1.3. Descripción del activo a registrar:	

1.4. Responsable:

1.5. Cargo:
1.6. Título:_____ Especialidad:
1.7. Celular: _____ e-mail:
1.8. Fecha: ____ /____ _/2019

INDICACIONES	VALORACIÓN	DESCRIPCIÓN
Marque con una (X) en cada indicador la valoración que considere pertinente para cada uno de los activos que se describen a continuación. El mayor rango que asigne denota que el activo es más importante.	0	Despreciable
	1 – 2	Bajo
	3 – 5	Medio
	6 – 8	Alto

	9	Muy alto
	10	Extremo
Son los criterios que debe valorar en cada uno de los activos, pues ellos están describiendo la importancia y priorización de acuerdo a la escala que se describe líneas arriba y ud debe elegir.	D	Disponibilidad
	A	Autenticidad
	T	Trazabilidad
	I	Integridad
	C	Confidencialidad

N°	Indicadores	Valoración						Observaciones
		0	1-2	3-5	6-8	9	10	
ACTIVOS DE LA CAPA CLIENTE								
1	**INFORMACIÓN DATOS VITALES DE LA ORGANIZACIÓN**							
	1.1 Disponibilidad (D)							
	1.2 Autenticidad (A)							
	1.3 Trazabilidad (T)							
	1.4 Integridad (I)							
	1.5 Confidencialidad (C)							
2	**INFORMACIÓN PERSONAL**							
	2.1 Disponibilidad (D)							
	2.2 Autenticidad (A)							
	2.3 Trazabilidad (T)							

	2.4 Integridad (I)							
	2.5 Confidencialidad (C)							
3	**INFORMACIÓN CLASIFICADA**							
	3.1 Disponibilidad (D)							
	3.2 Autenticidad (A)							
	3.3 Trazabilidad (T)							
	3.4 Integridad (I)							
	3.5 Confidencialidad (C)							
ACTIVOS DE LA CAPA SERVIDOR								
1	**COPIAS DE SEGURIDAD**							
	1.1 Disponibilidad (D)							
	1.2 Autenticidad (A)							
	1.3 Trazabilidad (T)							
	1.4 Integridad (I)							
	1.5 Confidencialidad (C)							
2	**CONFIGURACIONES**							
	2.1 Disponibilidad (D)							
	2.2 Autenticidad (A)							
	2.3 Trazabilidad (T)							
	2.4 Integridad (I)							

	2.5 Confidencialidad (C)							

Fuente: Elaboración propia

Tabla 24: Ficha de registro de amenazas de TI por su frecuencia e impacto para su posterior identificación, evaluación y priorización de riesgos de T.I.

1. DATOS INFORMATIVOS

1.1. Descripción del Data Center:	
1.2. Descripción de los servicios que ofrece:	
1.3. Descripción del activo a registrar:	

1.4. Responsable:

1.5. Cargo:
1.6. Título:_____ Especialidad:
1.7. Celular: _____ e-mail:
1.8. Fecha: ____ /____ _/2019

1.9. Turnos:

Mañana: Hora: Inicio:
Término:

Tarde: **Hora:** **Inicio:**
Término:

Noche: **Hora:** **Inicio:**
Término:

INDICACIONES	VALORACIÓN	DESCRIPCIÓN DEL IMPACTO
Marque con una (X) en cada indicador de IMPACTO que a continuación se describe para valorar a cada una de las amenazas de cada activo de TI, que se pueden convertir en riesgos serios para la organización. Asigne la valoración que considere pertinente. El mayor rango que asigne denota el mayor impacto que puede generar dicha amenaza.	**5**	**Muy alto**
	4	**Alto**
	3	**Medio**
	2	**Bajo**
	1	**Muy bajo**
INDICACIONES	**VALORACIÓN**	**DESCRIPCIÓN DE LA FRECUENCIA**
Marque con una (X) en cada indicador de FRECUENCIA que a continuación se describe para valorar las veces de ocurrencia de cada una de las amenazas de cada activo de TI. Asigne la valoración que considere pertinente. El mayor rango que asigne denota la mayor frecuencia de ocurrencia de dicha amenaza.	**5**	**Frecuente (80% - 100%)**
	4	**Probable (61% - 80%)**
	3	**Ocasional (41% - 60%)**
	2	**Raro (21% - 40%)**
	1	**Improbable (1% - 20%)**

N°	Indicadores	IMPACTO					FRECUENCIA					Observaciones
		5	4	3	2	1	5	4	3	2	1	
ACTIVOS DE LA CAPA CLIENTE												
1	**INFORMACIÓN DATOS VITALES DE LA ORGANIZACIÓN**											
	Amenaza 1: Fugas de la información											
	Amenaza 2: Suplantación de la identidad del usuario											
	Amenaza 3: Errores de los usuarios											
	Amenaza 4: Revelación de la información											
2	**INFORMACIÓN PERSONAL**											
	Amenaza 1: Fugas de la información											
	Amenaza 2: Alteraciones de la información											
	Amenaza 3: Errores del administrador del sistema											
	Amenaza 4: Abusos de privilegios de acceso											
	Amenaza 5: Suplantación de la identidad del usuario											
	Amenaza 6: Modificación de la información											
3	**INFORMACIÓN CLASIFICADA**											
	Amenaza 1: Fugas de la información											
	Amenaza 2: Alteraciones de la información											
	Amenaza 3: Acceso no autorizado											

	Amenaza 4: Abusos de privilegios de acceso											
	Amenaza 5: Suplantación de la identidad del usuario											
	Amenaza 6: Modificación de la información											
ACTIVOS DE LA CAPA SERVIDOR												
1	**COPIAS DE SEGURIDAD**											
	Amenaza 1: Desastres naturales											
	Amenaza 2: Fenómeno del Niño											
	Amenaza 3: Fuego											
	Amenaza 4: Inundaciones											
	Amenaza 5: Avería de origen físico y lógico											
	Amenaza 6: Contaminación electromagnética											
	Amenaza 7: Corte del suministro eléctrico											
2	**CONFIGURACIONES**											
	Amenaza 1: Contaminación electromagnética											
	Amenaza 2: Fuego											
	Amenaza 3: Inundaciones											
	Amenaza 4: Corte del suministro eléctrico											
	Amenaza 5: Avería de origen físico y lógico											

Fuente: Elaboración propia

4.- Determinación y cuantificación del riesgo

En esta fase se define qué amenazas son riesgos para la organización, al asumir la cuantificación del impacto y frecuencia de cada una de ellas (generada en la Fase 3) para determinar su real dimensión. Se sigue la siguiente expresión matemática:

RIESGO = PROBABILIDAD X IMPACTO

Así mismo se toma en cuenta la valoración de cada activo de TI, también dado en la fase anterior, para determinar cómo la amenaza pone en riesgo el activo más importante para el negocio. Esta valoración de importancia fue dada no sólo por el CIO, sino que en conjunto con el CEO y demás subgerentes involucrados en determinar esta importancia y valoración.

Por otro lado, se asigna un valor monetario (Monto económico asumido por la organización) al proceso que se invierte en la realización del activo y el posible costo por mitigar la amenaza, esto permite tener una primera aproximación a la inversión que tendría que asumir la organización si es que no mitiga o toma medidas preventivas para los riesgos prioritarios.

5.- Determinación de jerarquización y priorización (evaluación comparativa)

Teniendo en cuenta los resultados obtenidos en la fase anterior (Fase 4) y tomando como referencia las Metodologías Magerit y Octave sobre la Gestión de riesgos (considerando los catálogos y procedimientos que se manejan en ellas), se procede a realizar una comparación y jerarquización de aquellos riesgos que han sido cuantificados, ordenándolos de mayor a menor de acuerdo al producto obtenido.

6.- Elaboración de la lista de riesgos y sus posibles costos de mitigación

Finalmente se muestra la lista de riesgos, encabezando aquellos que necesitan mayor atención porque generan mayor impacto en la organización. Acompañado de los posibles costos por las acciones a tomar para su mitigación.

Con estas fases se puede proceder a una nueva evaluación más detallada y objetiva de los riesgos que afronta la organización, con la finalidad de determinar las mejores formas de cuantificarlo y mitigarlo. Así mismo, ayuda a tener una lista de prioridades presupuestadas para esta mitigación.

Herramienta Informática

A continuación se describe la herramienta informática que se ha construido para agilizar la identificación, evaluación y priorización

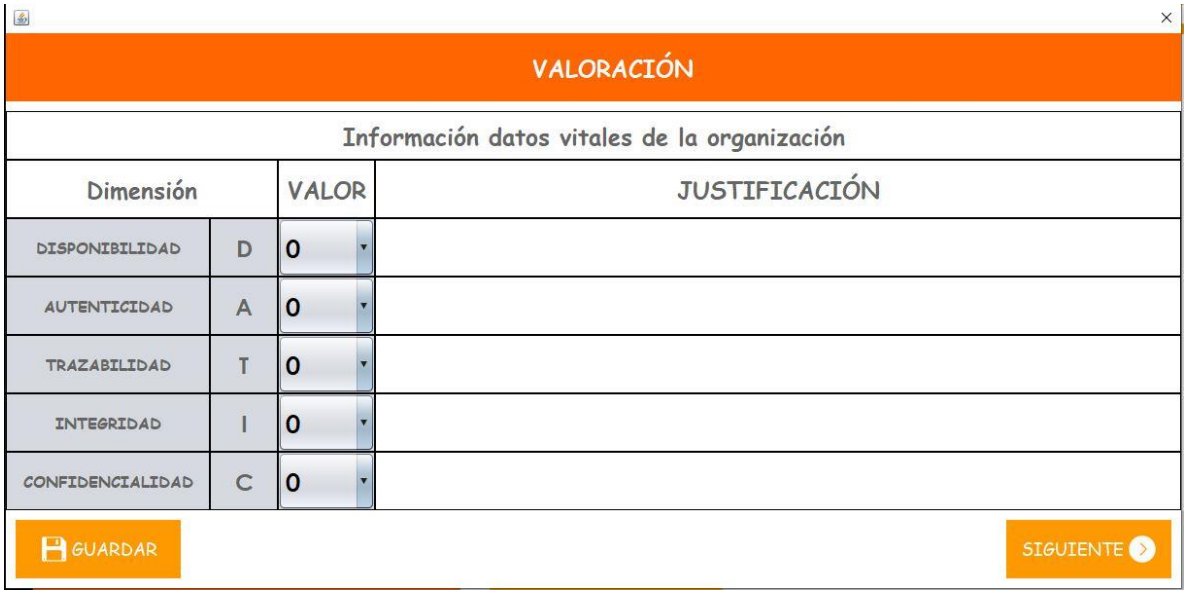
Figura N° 10: Menú Principal – Capa Cliente

Fuente: Elaboración propia

En esta ventana se puede apreciar el menú principal de los activos de la capa cliente, con la finalidad de poder editar la valoración que el CIO y CEO u otra área o instancia han considerado otorgar.

Figura N° 11: Menú Principal – Capa Servidor

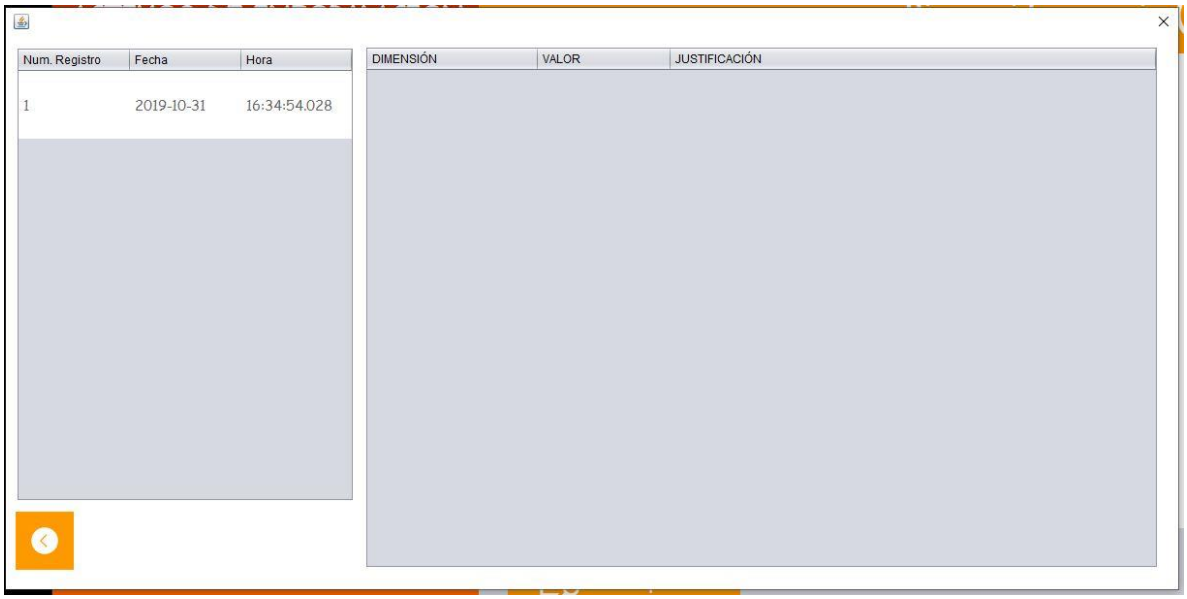
Figura N° 12: Valoración de los activos – capa cliente



Fuente: Elaboración propia

Esta interfaz permite ingresar los valores (del 0 al 10) y con los criterios de D, A, T, I, C. de los Activos de la Capa Cliente. Todos los valores están inicializados en cero. En el ejemplo, se puede ingresar los valores para el Activo Información datos vitales de la organización.

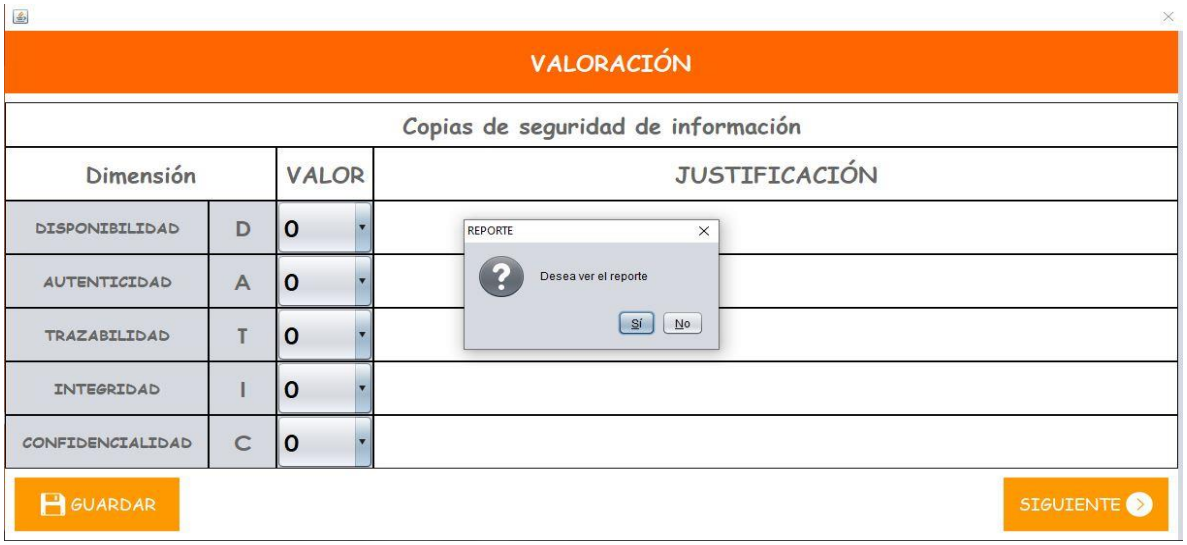
Figura N° 13: Interfaz del reporte general de activos



Fuente: Elaboración propia

Esta interfaz permite mirar el reporte detallado del registro de activos de TI, indicando la dimensión, su valoración y la justificación de dicha valoración.

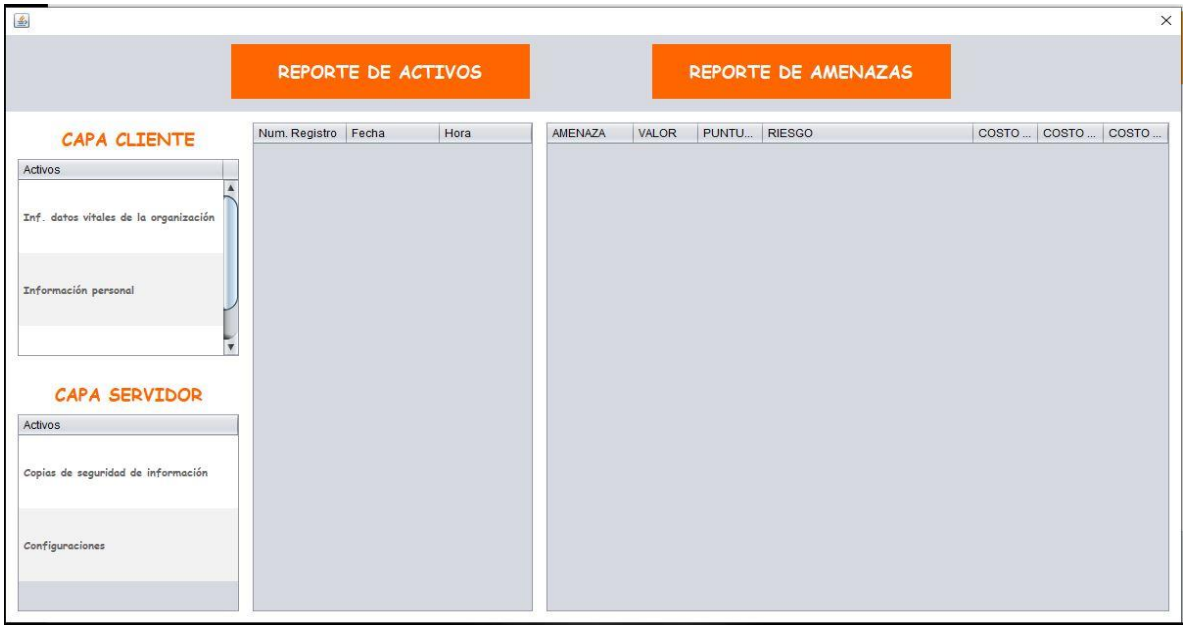
Figura N° 14: Valoración de los activos – capa servidor



Fuente: Elaboración propia

Esta interfaz permite ingresar los valores (del 0 al 10) y con los criterios de D, A, T, I, C. de los Activos de la Capa Servidor. Todos los valores están inicializados en cero. En el ejemplo, se puede ingresar los valores para el Activo Copias de seguridad de información. Así mismo, cuando se ha guardado la información ingresada en este formulario, el sistema genera una alerta, preguntando si desea mirar el reporte de los activos y sus valoraciones.

Figura N° 15: Interfaz: reportes de activos y amenazas

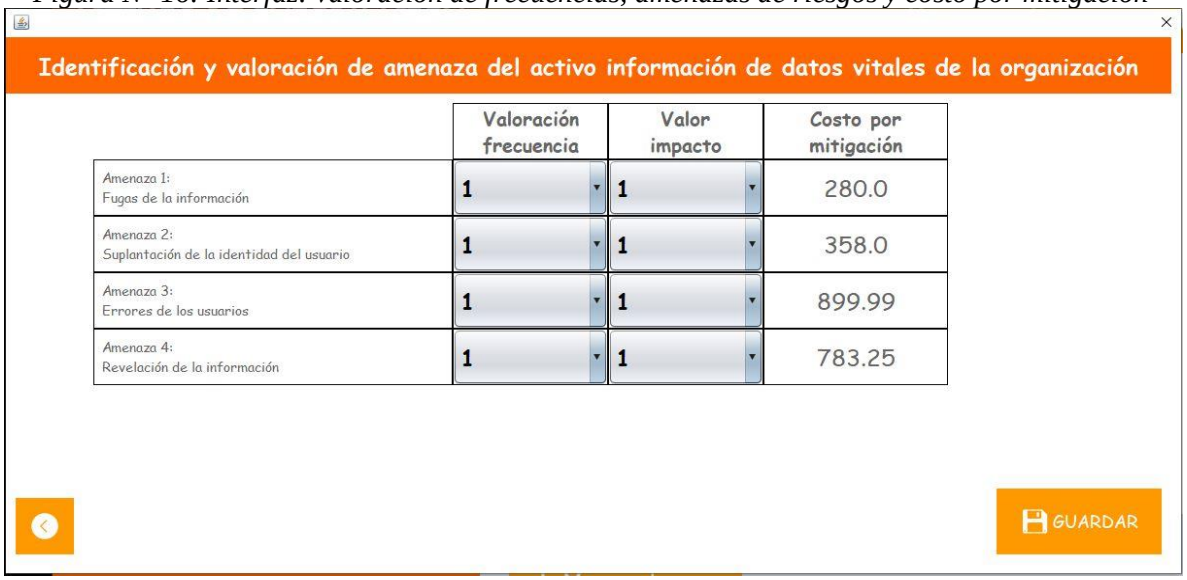


Fuente: Elaboración propia

Esta interfaz permite mirar los reportes por cada una de las capas. En el reporte de activos se puede verificar en el encabezado el número de registro, fecha y hora de su registro. En el de amenazas se

identifica la amenaza, valores totales producto de la frecuencia e impacto, riesgo y tipo (Color), costo real del activo, costo por mitigar y lo que se estaría ahorrando por tener una buena política de gestión de riesgos. Este reporte es importante porque resume la clasificación y valoración de los activos y sus amenazas.

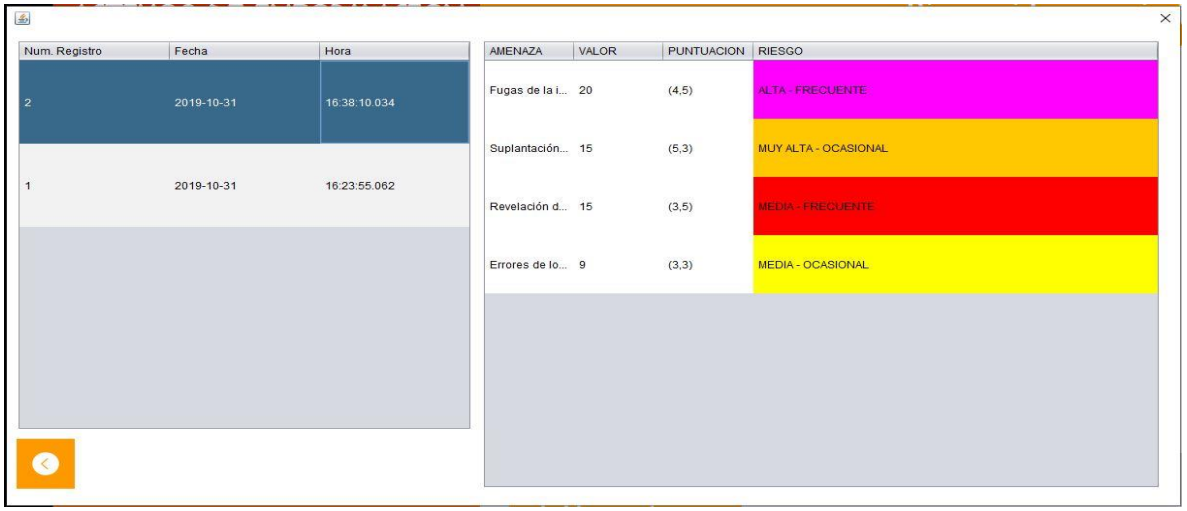
Figura N° 16: Interfaz: valoración de frecuencias, amenazas de riesgos y costo por mitigación



Fuente: Elaboración propia

Con esta interfaz se puede registrar la frecuencia e impacto que se han registrado en las fichas de observación, debidamente verificadas. Así mismo, se visualiza el costo por mitigación que ya se ha estudiado y calculado de manera objetiva. Esto con la finalidad de hacer los cálculos respectivos sobre costos de mitigación, etc.

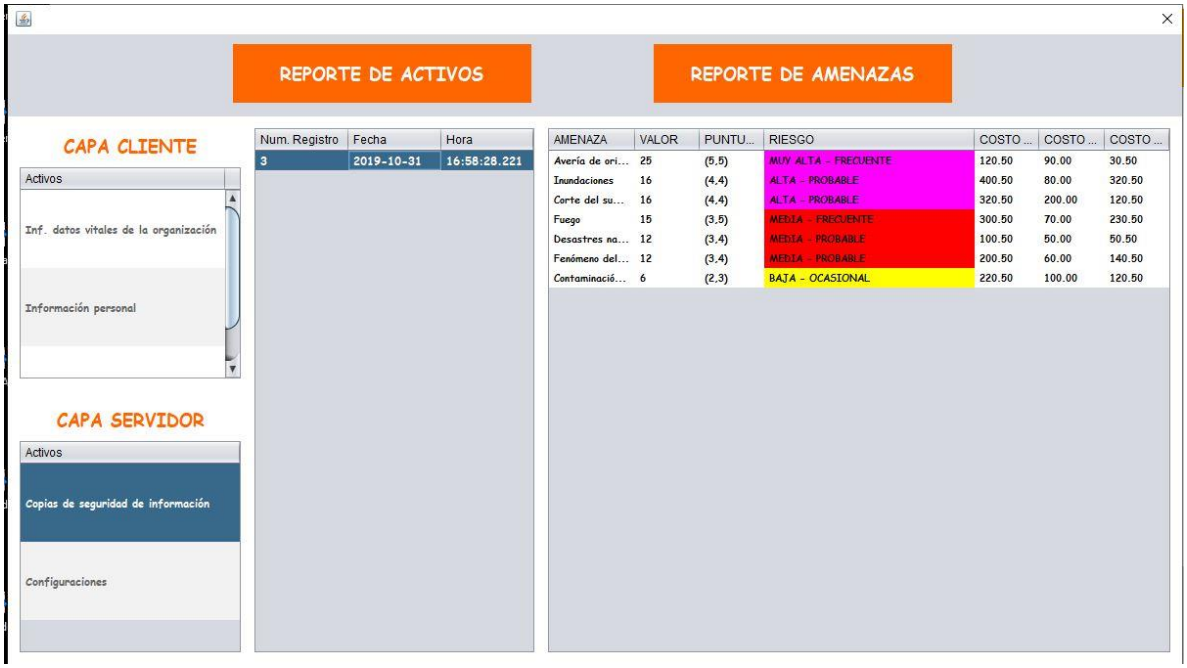
Figura N° 17: Interfaz reporte priorización de amenazas por impacto y frecuencia



Fuente: Elaboración propia

Se muestra la lista de los riesgos por cada uno de los activos, priorizados por su impacto y frecuencia. Empezando a listar los de mayor cuantificación por el producto impacto y frecuencia.

Figura N° 18: Interfaz priorización de riesgos por activos de TI – Costos



Fuente: Elaboración propia

Se muestra el Menú principal para generar las listas de los riesgos por cada uno de los activos, priorizados por su impacto y frecuencia. Empezando a listar los de mayor cuantificación por el producto impacto y frecuencia. Así mismo, se muestra el costo real del activo, costo por mitigar y lo que se estaría ahorrando por tener una buena política de gestión de riesgos.

Caso de Aplicación

Fase 1: Desarrollo de una base común para la terminología de análisis de riesgos

Verificar páginas 38 al 40

Fase 2: Especificar y documentar los hallazgos en la etapa del análisis

En esta etapa se observa y registran los hallazgos en las fichas de observación que se encuentran en las páginas 45 - 48

Fase 3: Clasificación de los activos por las dimensiones (D, A, T, I, C) y las amenazas por impacto y frecuencia

Tabla N° 25: Identificación de Activos de TI (Capa cliente y servidor)

CAPA CLIENTE

CÓDIGO: INFO – VR	**NOMBRE: Información datos vitales de la organización**
DESCRIPCIÓN: Información importante para la organización.	
TIPO: Esencial	
UNIDAD RESPONSABLE: Gerencia General	
PERSONA RESPONSABLE: Gerente General	
UBICACIÓN (TÉCNICA O GEOGRÁFICA): Oficina de Gerencia General	
CANTIDAD: 4 GB. Aprox.	

CÓDIGO: INFO – PER	**NOMBRE: Información personal**
DESCRIPCIÓN: Información importante de cada trabajador que requiere confidencialidad y custodia. Se extiende a la información de cada trabajador contenidas en las planillas de remuneraciones.	
TIPO: Esencial - Datos de carácter Personal de Nivel Alto	
UNIDAD RESPONSABLE: Recursos Humanos	
PERSONA RESPONSABLE: Gerente de Recursos Humanos	
UBICACIÓN (TÉCNICA O GEOGRÁFICA): Oficina de Recursos Humanos	
CANTIDAD: 16 GB. Aprox.	

CÓDIGO: INFO – CLASSIFIED	**NOMBRE: Información clasificada**
DESCRIPCIÓN: Información clasificada como balances, rentabilidad, deudores, bonos, auditorías, etc que requiere confidencialidad y custodia.	
TIPO: Esencial - Datos Clasificados. Nivel Alto de confidencialidad	
UNIDAD RESPONSABLE: Gerencia General.	
PERSONA RESPONSABLE: Gerente General.	
UBICACIÓN (TÉCNICA O GEOGRÁFICA): Oficina de Gerencia General	
CANTIDAD: 8 GB. Aprox.	

CAPA SERVIDOR

CÓDIGO: BACKUP	**NOMBRE: Copias de seguridad de información**
DESCRIPCIÓN: Copias de seguridad de información importante para la organización, así como información clasificada.	
TIPO: Datos / Información	
UNIDAD RESPONSABLE: Dirección de Soporte Técnico.	
PERSONA RESPONSABLE: Director de Soporte Técnico.	
UBICACIÓN (TÉCNICA O GEOGRÁFICA): Oficina de Soporte Técnico.	
CANTIDAD: 2 servidores.	

CÓDIGO: CONF	**NOMBRE: Configuraciones**
DESCRIPCIÓN: Procedimiento crítico para guardar la Información crítica de la organización que tiene influencia con otras áreas de la organización.	
TIPO: Datos / Información	
UNIDAD RESPONSABLE: Dirección de Soporte Técnico.	
PERSONA RESPONSABLE: Director de Soporte Técnico.	
UBICACIÓN (TÉCNICA O GEOGRÁFICA): Oficina de Soporte Técnico.	

Tabla N° 26: Valoración de los Activos de TI (Capa cliente y servidor)

[D] Disponibilidad.
[A] Autenticidad de quién accede al servicio.
[T] Trazabilidad de quién accede al servicio, cuándo y qué hace.
[I] Integridad.
[C] Confidencialidad.

CÓDIGO: INFO – VR	**NOMBRE: Información datos vitales de la organización**	
DESCRIPCIÓN: Información importante para la organización		
VALORACIÓN		
Dimensión	Valor	Justificación
[D]	10 (Extremo)	Es vital para el negocio tener la información core a todo momento
[I]	9 (Muy alto)	Si alguien manipula la información vital sin autorización
[C]	10 (Extremo)	Es muy importante la confidencialidad para el negocio
[T]	6 (Daño grave)	Es necesario tener un registro de los accesos a la información vital

CÓDIGO: INFO – PER	**NOMBRE: Información personal**	
DESCRIPCIÓN: Información importante de cada trabajador que requiere confidencialidad y custodia		
VALORACIÓN		
Dimensión	Valor	Justificación
[D]	10 (Extremo)	Es vital para el negocio tener la información core a todo momento
[A]	5 (Daño importante)	Es indispensable identificar a ciencia cierta a quien accede a la información
[I]	9 (Muy alto)	Si alguien manipula la información vital sin autorización
[C]	10 (Extremo)	Es muy importante la confidencialidad para el negocio
[T]	6 (Daño grave)	Es necesario tener un registro de los accesos a la información vital

CÓDIGO: CONF	**NOMBRE: Configuraciones**	
DESCRIPCIÓN: Procedimiento crítico para guardar la Información crítica de la organización que tiene influencia con otras áreas de la organización.		
VALORACIÓN		
Dimensión	Valor	Justificación
[D]	10 (Extremo)	Es vital para el negocio tener a disponibilidad los protocolos de configuraciones de la información core
[A]	8 (Daño alto)	No tener la autenticidad de los que accedan a las configuraciones de los sistemas es grave.
[I]	9 (Muy alto)	Si alguien manipula la configuración de los sistemas sin autorización
[C]	10 (Extremo)	Es muy importante la confidencialidad de los protocolos de configuración del para el negocio
[T]	6 (Daño grave)	Es necesario tener un registro de los accesos a las consolas de configuración

CÓDIGO: INFO – CLASSIFIED	**NOMBRE: Información clasificada**
DESCRIPCIÓN: Información clasificada como balances, rentabilidad, deudores, bonos, auditorías, etc que requiere confidencialidad y custodia	
VALORACIÓN	

Dimensión	Valor	Justificación
[D]	10 (Extremo)	Es vital para el negocio tener la información core a todo momento
[A]	9 (Muy alto)	Se debe identificar a ciencia cierta al usuario que accede a esta información
[C]	10 (Extremo)	Es muy importante la confidencialidad para el negocio
[T]	6 (Daño grave)	Es necesario tener un registro de los accesos a la información vital

CÓDIGO: BACKUP	**NOMBRE: Copias de seguridad de información**	
DESCRIPCIÓN: Copias de seguridad de información importante para la organización, así como información clasificada.		
VALORACIÓN		
Dimensión	Valor	Justificación
[D]	10 (Extremo)	Es vital para el negocio tener la información core a todo momento
[A]	8 (Daño alto)	Debe identificarse adecuadamente a quien hace las copias de seguridad para efectos de responsabilidad
[T]	6 (Daño grave)	Es necesario tener un registro de lo accesos a la información vital

Fuente: Elaboración propia

Tabla N° 26: Valoración de las Amenazas de TI (Capa cliente y servidor)

CAPA DE NEGOCIO

ACTIVO	**Información datos vitales de la organización**
Amenaza 1	Fugas de la información
Amenaza 2	Suplantación de la identidad del usuario
Amenaza 3	Errores de los usuarios
Amenaza 4	Revelación de la información

ACTIVO	**Información personal**
Amenaza 1	Alteraciones de la información
Amenaza 2	Abuso de privilegios de acceso
Amenaza 3	Fugas de la información
Amenaza 4	Suplantación de la identidad del usuario
Amenaza 5	Modificación de la información
Amenaza 6	Errores del administrador del sistema

ACTIVO	**Información clasificada**
Amenaza 1	Revelación de la información
Amenaza 2	Alteraciones de la información
Amenaza 3	Abuso de privilegios de acceso
Amenaza 4	Suplantación de la identidad del usuario

Amenaza 5	Modificación de la información
Amenaza 6	Acceso no autorizado

CAPA SERVIDOR

ACTIVO	**Copias de seguridad de información**
Amenaza 1	Desastres naturales
Amenaza 2	Fenómeno del Niño
Amenaza 3	Fuego
Amenaza 4	Inundaciones
Amenaza 5	Avería de origen físico y lógico
Amenaza 6	Contaminación electromagnética
Amenaza 7	Corte del suministro eléctrico

ACTIVO	**Configuraciones**
Amenaza 1	Contaminación electromecánica
Amenaza 2	Fuego
Amenaza 3	Inundaciones
Amenaza 4	Corte de suministro eléctrico
Amenaza 5	Avería de origen físico y lógico

Fuente: Elaboración propia

Tabla N° 27: Valoración de los Activos de TI considerando D,A,T,I,C y las Amenazas (Capa cliente y servidor)

CAPA CLIENTE

		NIVEL	**D**	**I**	**C**	**A**
ACTIVO	**Información datos vitales de la organización**					
Amenaza 1	Fugas de la información	**MA**	**100%**	**100%**		
Amenaza 2	Suplantación de la identidad del usuario	**A**				
Amenaza 3	Errores de los usuarios	**B**				80%
Amenaza 4	Revelación de la información	**MA**			100%	

		NIVEL	**D**	**I**	**C**	**A**
ACTIVO	**Información personal**					
Amenaza 1	Alteraciones de la información	**MA**		**100%**		**100%**
Amenaza 2	Abuso de privilegios de acceso	**MA**	**80%**			
Amenaza 3	Fugas de la información	**MA**			**100%**	
Amenaza 4	Suplantación de la identidad del usuario	**A**				**100%**
Amenaza 5	Modificación de la información	**MA**		**80%**		
Amenaza 6	Errores del administrador del sistema	**B**	**50%**		**50%**	

		NIVEL	D	I	C	A
ACTIVO	**Información clasificada**					
Amenaza 1	Revelación de la información	**MA**			**100%**	**80%**
Amenaza 2	Alteraciones de la información	**MA**		**80%**	**100%**	
Amenaza 3	Abuso de privilegios de acceso	**A**				**100%**
Amenaza 4	Suplantación de la identidad del usuario	**MA**				**100%**
Amenaza 5	Modificación de la información	**MA**		**80%**		
Amenaza 6	Acceso no autorizado	**MA**	**70%**			**80%**

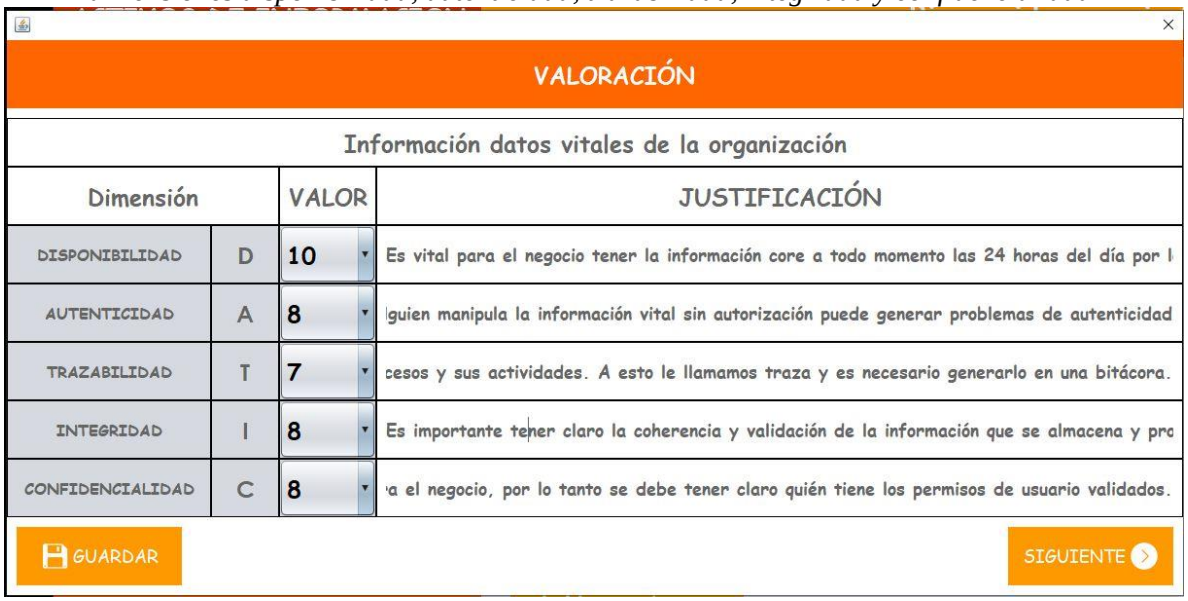
CAPA SERVIDOR

		NIVEL	D	I	C	A
ACTIVO	**Copias de seguridad de información**					
Amenaza 1	Desastres naturales	**MA**	**100%**			
Amenaza 2	Fenómeno del Niño	**MA**	100%			
Amenaza 3	Fuego	**A**	100%			
Amenaza 4	Inundaciones	**A**	100%			
Amenaza 5	Avería de origen físico y lógico	**MA**		80%		
Amenaza 6	Contaminación electromagnética	**B**	80%	40%		
Amenaza 7	Corte del suministro eléctrico	**A**	100%			

		NIVEL	D	I	C	A
ACTIVO	**Configuraciones**					
Amenaza 1	Contaminación electromecánica	**MA**	**100%**			
Amenaza 2	Fuego	**A**	100%			
Amenaza 3	Inundaciones	**A**	100%			
Amenaza 4	Corte de suministro eléctrico	**MA**	100%			
Amenaza 5	Avería de origen físico y lógico	**MA**	80%	100%		

Fuente: Elaboración propia

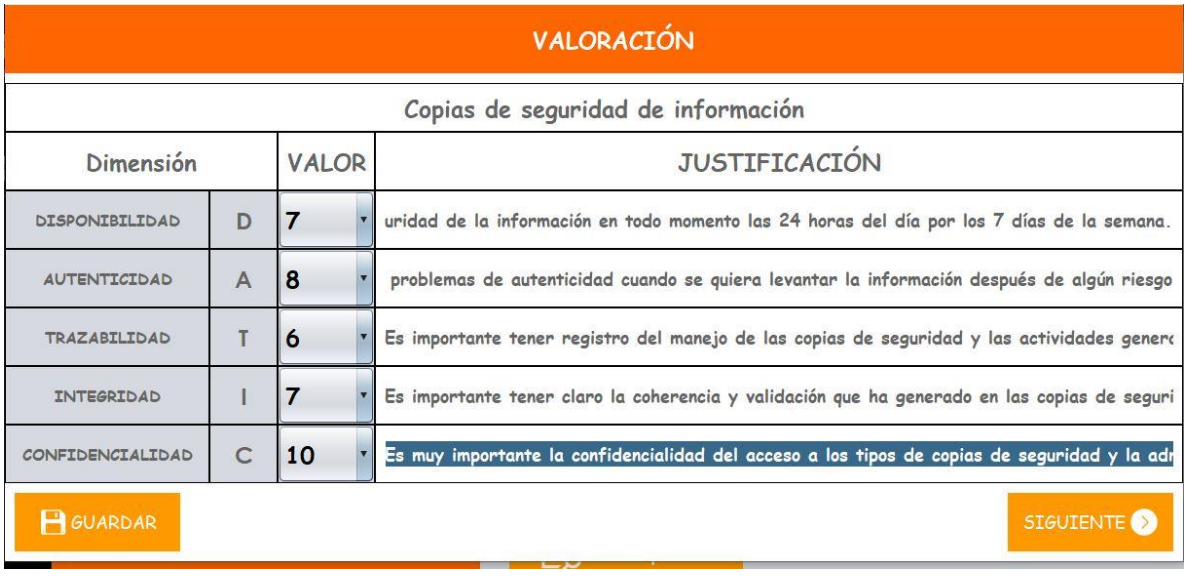
Figura N°18: Valorización de los activos (información datos vitales de la organización) por las dimensiones disponibilidad, autenticidad, trazabilidad, integridad y confidencialidad



Fuente: Elaboración propia

En esta interfaz se muestra la valoración del activo Información datos vitales de la organización en mérito a las dimensiones de Disponibilidad, Autenticidad, Trazabilidad, Integridad y Confidencialidad valorizados desde el 0 al 10 recogida en los instrumentos de la fase anterior. Además se incluye una pequeña justificación de dicha valoración. Cabe indicar que esta valoración se asume en consenso el CIO, CEO y personas involucradas en estas decisiones.

Figura N°19: Valorización de los activos (copias de seguridad de información) por las dimensiones disponibilidad, autenticidad, trazabilidad, integridad y confidencialidad



Fuente: Elaboración propia

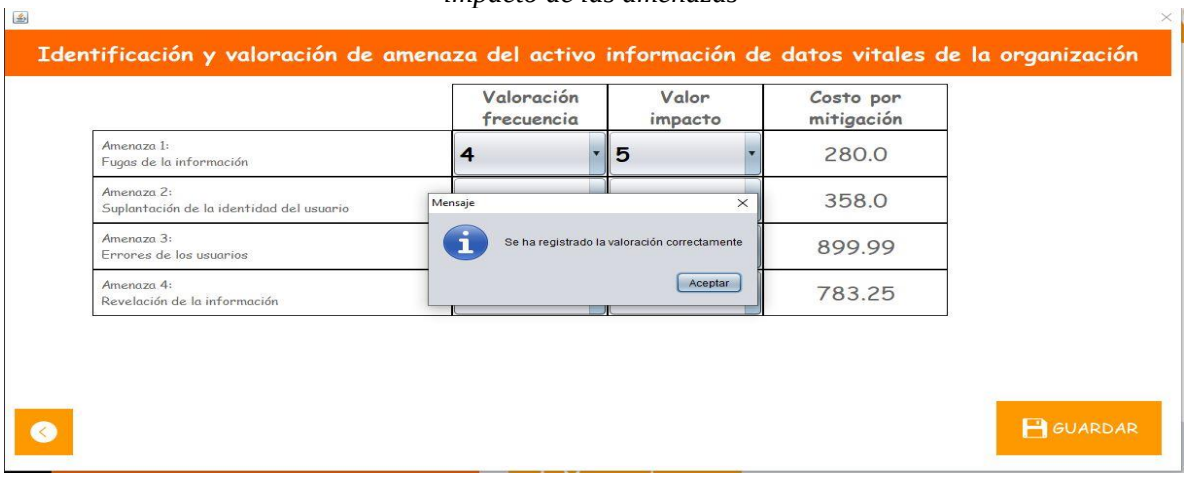
En esta interfaz se muestra la valoración del activo Copias de seguridad de información en mérito a las dimensiones de Disponibilidad, Autenticidad, Trazabilidad, Integridad y Confidencialidad valorizados desde el 0 al 10. Además se incluye una pequeña justificación de dicha valoración. Cabe indicar que esta valoración se asume en consenso el CIO, CEO y personas involucradas en estas decisiones. Esta información es recogida en los instrumentos de la fase anterior.

Figura N°20: Identificación y valorización de amenazas del activo información de datos vitales de la organización

Fuente: Elaboración propia

Se da la valorización de acuerdo a los informes recogidos en la fase anterior tomando en cuenta la frecuencia de ocurrencia y su impacto. Así mismo se muestra el costo por mitigar la amenaza. Esta valoración no es subjetiva sino recogida con evidencias.

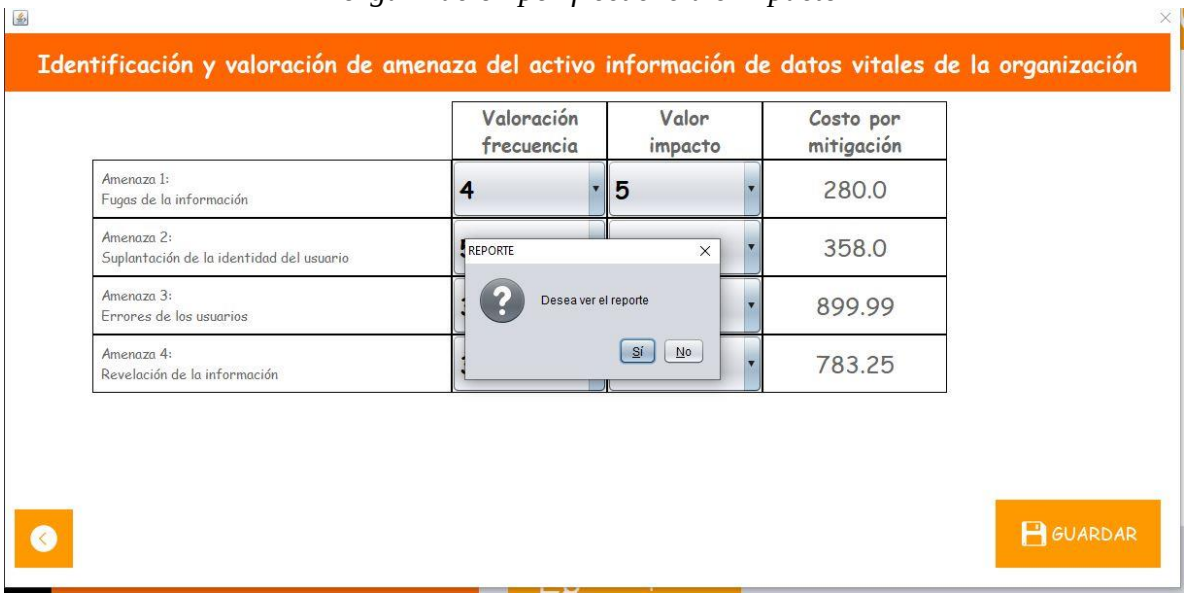
Figura N°21: Interfaz confirmación del registro correcto de la valoración de la frecuencia e impacto de las amenazas



Fuente: Elaboración propia

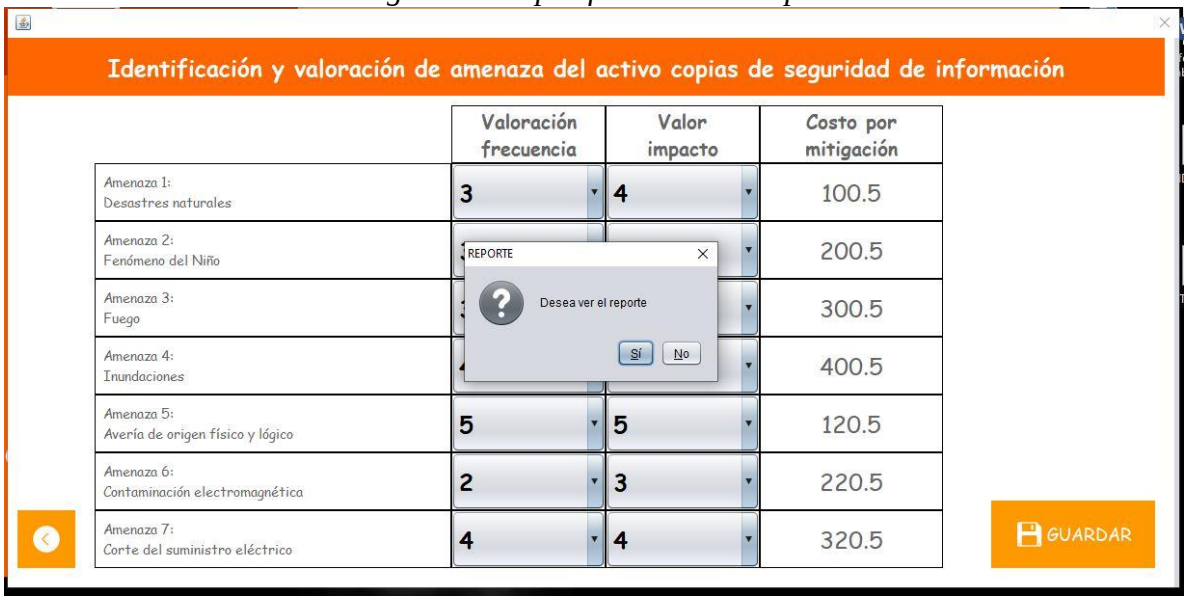
Sistema muestra mensaje de confirmación de registro correcto de amenazas por su frecuencia e impacto del activo información datos vitales de información.

Figura N°22: Valoración de las amenazas del activo de información de datos vitales de la organización por frecuencia e impacto



Fuente: Elaboración propia

Figura N°23: Valoración de las amenazas del activo copias de seguridad de información de la organización por frecuencia e impacto



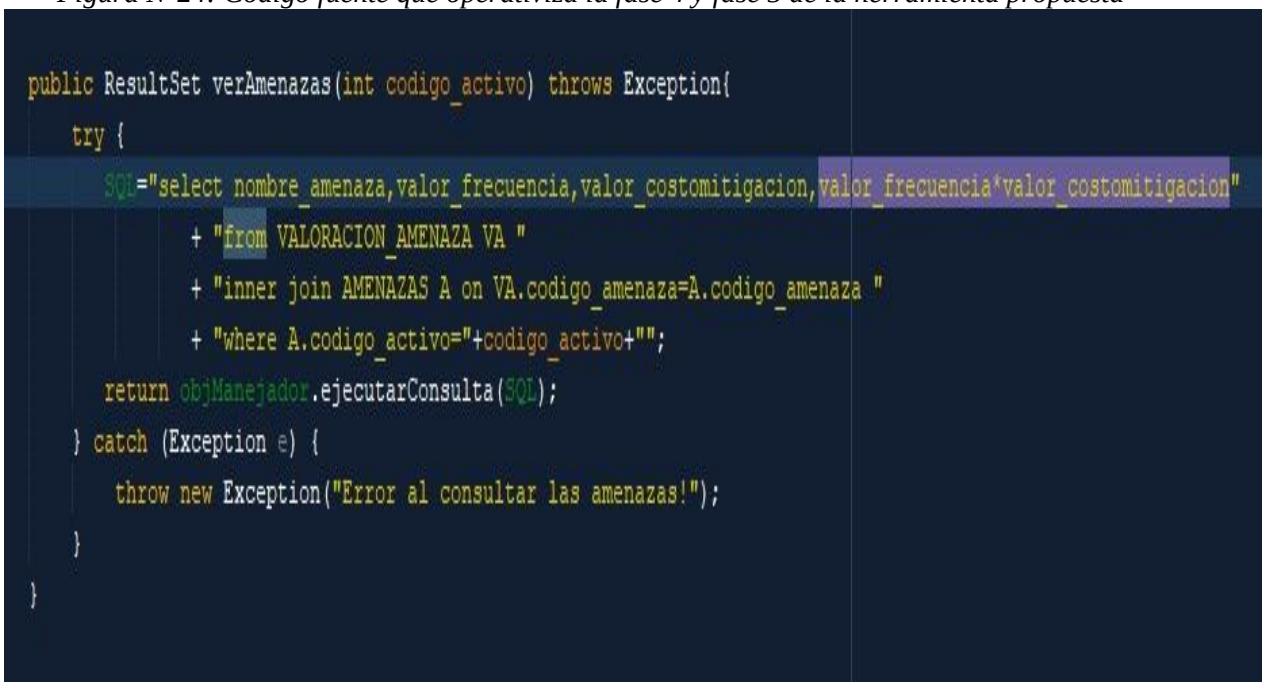
Fuente: Elaboración propia

En estas dos interfaces se muestra el mensaje en el que se pregunta si el usuario desea observar el reporte de las valorizaciones ingresadas y por orden descendente

Fase 4: Determinación y cuantificación del riesgo (Producto) y Fase 5: Determinación de jerarquización y priorización (evaluación comparativa)

Se toma en cuenta la siguiente información en el código fuente:

Figura N°24: Código fuente que operativiza la fase 4 y fase 5 de la herramienta propuesta



```
public ResultSet verAmenazas(int codigo_activo) throws Exception{
    try {
        SQL="select nombre_amenaza,valor_frecuencia,valor_costomitigacion,valor_frecuencia*valor_costomitigacion"
                + "from VALORACION_AMENAZA VA "
                + "inner join AMENAZAS A on VA.codigo_amenaza=A.codigo_amenaza "
                + "where A.codigo_activo="+codigo_activo+"";
        return objManejador.ejecutarConsulta(SQL);
    } catch (Exception e) {
        throw new Exception("Error al consultar las amenazas!");
    }
}
```

Fuente: Elaboración propia

Aquí se muestra el código fuente que ejecuta la fase 4 y fase 5. Esto es, se halla el producto al considerar el impacto y frecuencia de cada amenaza por cada activo con la finalidad de dimensionar el riesgo. Posteriormente se hará la jerarquización.

Así mismo para la jerarquización de riesgos se considera la matriz de identificación de tipos de riesgos, por su impacto y frecuencia.

		5	4	3	2	1
		FRECUENTE	PROBABLE	OCASIONAL	RARO	IMPROBABLE
5	**MUY ALTA**					
4	**ALTA**					
3	**MEDIA**					
2	**BAJA**					
1	**MUY BAJA**					

Tabla N° 28: Identificación de riesgos de TI considerando su ocurrencia e impacto

		NIVEL	PROBABILIDAD	TIPO DE RIESGO
ACTIVO	**Información datos vitales de la organización**			
Amenaza 1	Fugas de la información	**MA**	4	(5,4)
Amenaza 2	Suplantación de la identidad del usuario	**A**	4	(4,4)
Amenaza 3	Errores de los usuarios	**B**	3	(2,3)
Amenaza 4	Revelación de la información	**MA**	4	(5,4)

		NIVEL	PROBABILIDAD	TIPO DE RIESGO
ACTIVO	**Información personal**			
Amenaza 1	Alteraciones de la información	**MA**	4	(5,4)
Amenaza 2	Abuso de privilegios de acceso	**MA**	4	(5,4)
Amenaza 3	Fugas de la información	**MA**	4	(5,4)
Amenaza 4	Suplantación de la identidad del usuario	**A**	4	(4,4)
Amenaza 5	Modificación de la información	**MA**	3	(5,3)
Amenaza 6	Errores del administrador del sistema	**B**	2	(2,2)

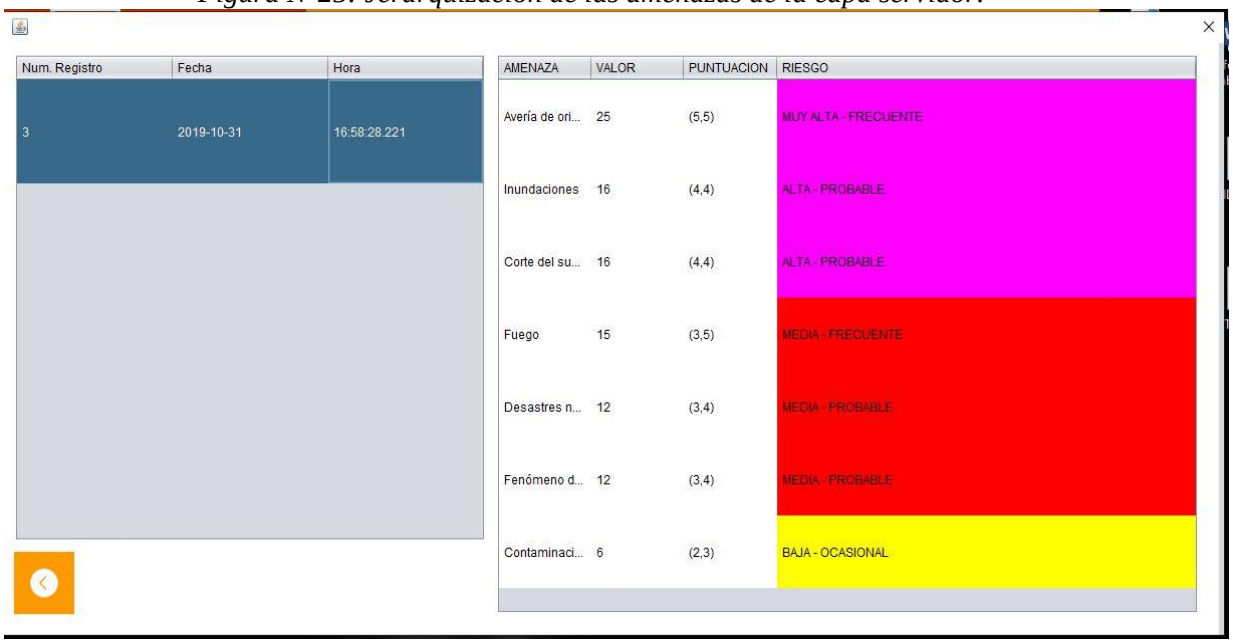
		NIVEL	PROBABILIDAD	TIPO DE RIESGO
ACTIVO	**Información clasificada**			
Amenaza 1	Revelación de la información	**MA**	5	(5,5)
Amenaza 2	Alteraciones de la información	**MA**	4	(5,4)
Amenaza 3	Abuso de privilegios de acceso	**A**	3	(4,3)
Amenaza 4	Suplantación de la identidad del usuario	**MA**	2	(5,2)
Amenaza 5	Modificación de la información	**MA**	3	(5,3)
Amenaza 6	Acceso no autorizado	**MA**	4	(5,4)

		NIVEL	PROBABILIDAD	TIPO DE RIESGO
ACTIVO	**Copias de seguridad de información**			
Amenaza 1	Desastres naturales	**MA**	2	(5,2)
Amenaza 2	Fenómeno del Niño	**MA**	2	(5,2)
Amenaza 3	Fuego	**A**	1	(4,1)
Amenaza 4	Inundaciones	**A**	1	(4,1)
Amenaza 5	Avería de origen físico y lógico	**MA**	4	(5,4)
Amenaza 6	Contaminación electromagnética	**B**	4	(2,4)
Amenaza 7	Corte del suministro eléctrico	**A**	4	(4,4)

		NIVEL	PROBABILIDAD	TIPO DE RIESGO
ACTIVO	**Configuraciones**			
Amenaza 1	Contaminación electromecánica	**MA**	4	(5,4)
Amenaza 2	Fuego	**A**	1	(4,1)
Amenaza 3	Inundaciones	**A**	1	(4,1)
Amenaza 4	Corte de suministro eléctrico	**MA**	4	(5,4)
Amenaza 5	Avería de origen físico y lógico	**MA**	4	(5,4)

Fuente: Elaboración propia

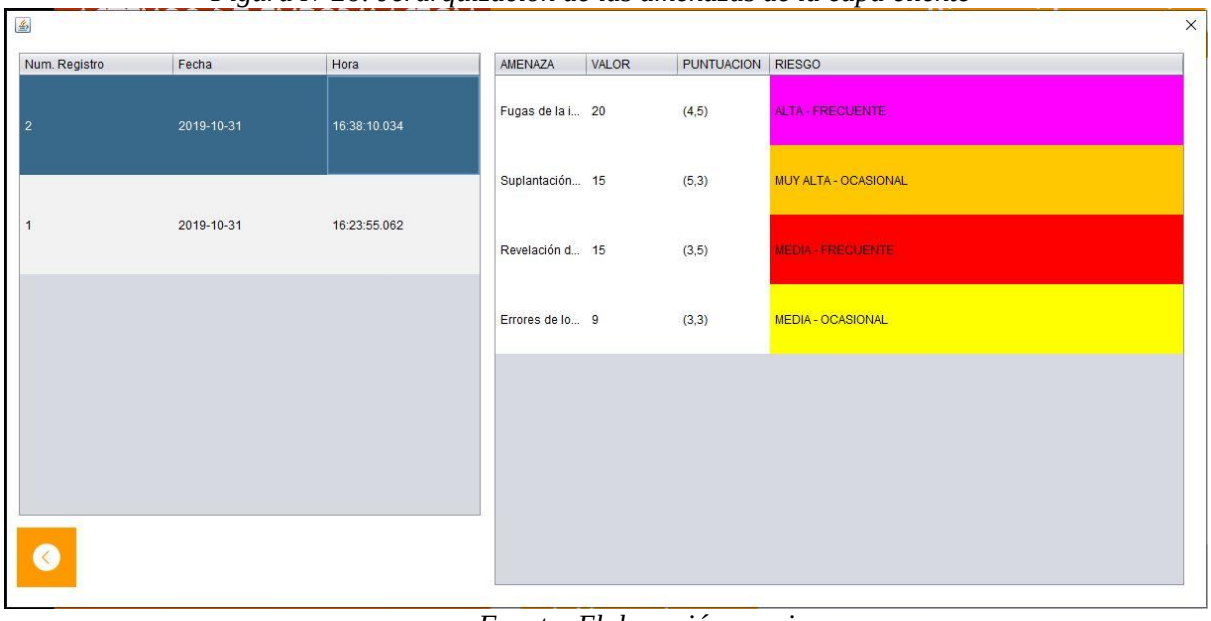
Figura N°25: Jerarquización de las amenazas de la capa servidor.



Fuente: Elaboración propia

En la presente figura se muestra la amenaza avería de origen como el riesgo mayor, por tener el valor 25 e indica que su impacto es muy alta y su ocurrencia es frecuente y la denota de color rojo intenso para señalarla como tal.

Figura N°26: Jerarquización de las amenazas de la capa cliente



Fuente: Elaboración propia

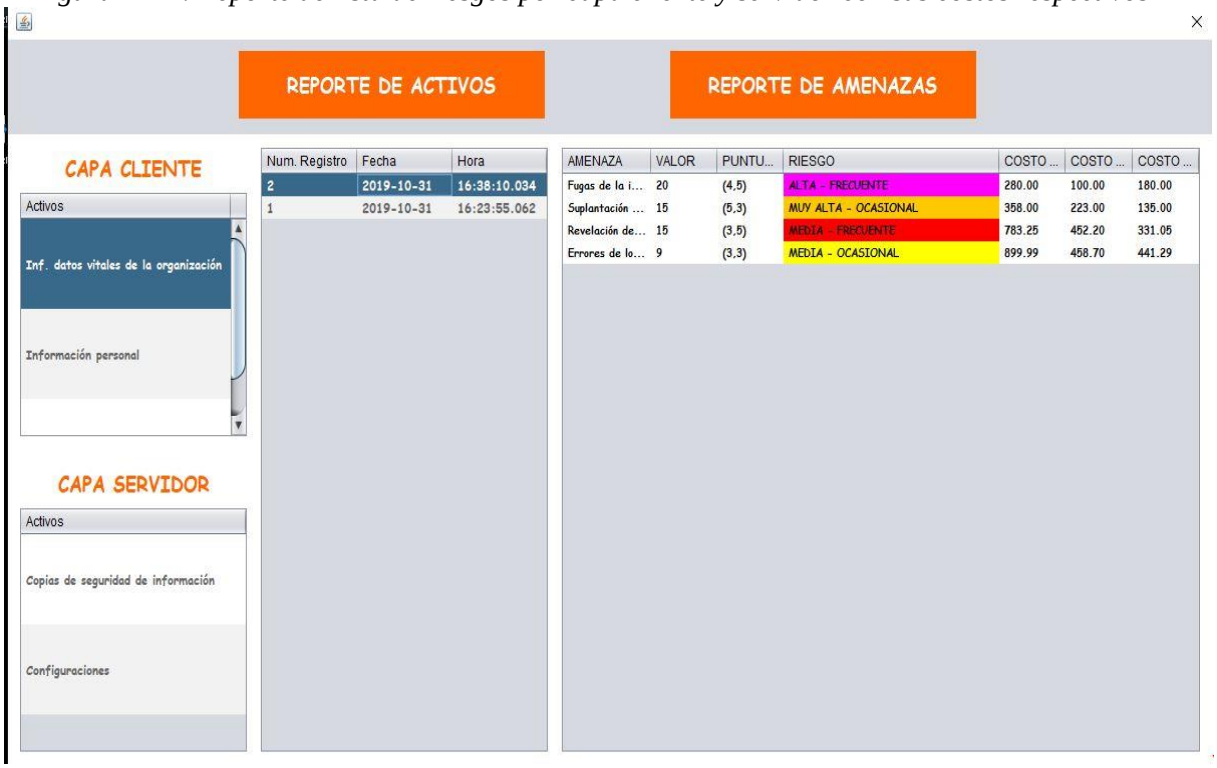
En ambas interfaces se aprecia el producto de la frecuencia e impacto y como consecuencia de ello su jerarquización en orden descendiente en mérito al referido producto. Los colores dan a entender

esa priorización que complementa la visibilidad a dicha jerarquización. En el ejemplo la jerarquización de las amenazas de la Capa Servidor y de la Capa Cliente.

En la figura se muestra la amenaza fuga de la información como el riesgo mayor, por tener el valor 20 y la denota de color rojo intenso para señalarla como tal.

Fase 6: Elaboración de la lista de riesgos y sus posibles costos de mitigación

Figura N°27: Reporte de lista de riesgos por capa cliente y servidor con sus costos respectivos



Fuente: Elaboración propia

En esta interfaz se evidencia las amenazas del activo información datos vitales de la organización, con su debida valoración y producto teniendo en consideración entre impacto y frecuencia de ocurrencia, así como los costos reales del activo, costo por mitigarlos y lo que se estaría ahorrando por tener una buena política de gestión de riesgos. Esto permitirá tener una objetiva identificación, evaluación y priorización de los riesgos para mejorar su gestión y tratamiento.

3.3.- O_2: Observación posterior a la aplicación de la herramienta

Los resultados para el DESPUÉS, se describen considerando la Evaluación por Juicio de 07 expertos, con la finalidad de medir el grado de aceptación y validación de la propuesta de solución (Instrumento para identificar, evaluar y priorizar amenazas de T.I. para la gestión de riesgos de TI en una Universidad Particular)

TABLA 29: Resultados de Instrumento Validación de Propuesta por Juicio de Expertos

	CLARIDAD	OBJETIVIDAD	CONSISTENCIA	COHERENCIA	PERTINENCIA	SUFICIENCIA
Experto 1	5	5	5	4	5	4
Experto 2	5	5	5	5	5	5
Experto 3	4	5	5	4	4	4
Experto 4	5	4	5	4	5	5
Experto 5	4	5	4	5	4	4
Experto 6	5	4	4	5	4	5
Experto 7	5	5	4	5	5	4

Fuente: Elaboración propia

Aquí se evidencia la aprobación, aceptación de los contenidos de mi propuesta, considerando los criterios de claridad, objetividad, consistencia, coherencia, pertinencia y suficiencia de mi propuesta.

Capítulo IV. Discusión

Seguimos considerando el diseño de investigación y de acuerdo a ello hacemos la discusión de resultados. La lógica consiste en verificar el ANTES y el DESPUÉS de la propuesta de mejora.

4.1.- Antes de la propuesta de mejora

El Diagnóstico de la situación actual, se realizó con la aplicación de dos instrumentos de recolección de información: Ficha de observación diagnóstica y Encuesta diagnóstica aplicada a los trabajadores de T.I. Con ello se obtienen las siguientes interpretaciones:

4.1.1.- En cuanto a la ficha de observación diagnóstica

En cuanto a la declaración de amenazas

Al utilizar en ocasiones formatos para el registro y declaración de amenazas, existe evidencia de una mala Gestión de Riesgos de T.I. y los actuales registros existentes al tener información no evidenciable se descalifica cualquier iniciativa que desee implementarse puesto que existen datos incorrectos y subjetivos. Así mismo, no hay desconocimiento de las Metodologías de Gestión de Riesgos, sino que no existe un formato o plantilla que les permita clasificar la amenaza y registrarla adecuadamente.

En cuanto a la declaración de vulnerabilidades

Al no existir reporte alguno de identificación de riesgos de T.I. como consecuencia reafirma la interpretación de existir una Gestión de Riesgos de T.I. inexistente y las iniciativas no la hacen eficiente. La organización está resistiendo a los ataques y amenazas por su buena política de seguridad a través de hardware y software, pero será motivo de indagación del alto costo que afronta por esta decisión.

Fiabilidad de la Ficha de Observación

Para verificar la confiabilidad del instrumento, es decir la Ficha de Observación Diagnóstica de la presente investigación, se utilizó el coeficiente de Alfa de Cronbach, el cual estima la fiabilidad a través de un conjunto de ítems que miden una misma dimensión. George y Mallery (2003) sugiere como criterio general para evaluar el coeficiente de Alfa de Cronbach:

> 0.9 es excelente

> 0.8 es bueno

> 0.7 es aceptable

> 0.6 es cuestionable

> 0.5 es pobre

< 0.5 es inaceptable

En relación a la confiabilidad de la dimensión de declaración de amenazas, se obtiene:

Tabla 30: Estadísticas de fiabilidad Ficha de Observación – Dimensión Amenazas

Alfa de Cronbach	N de elementos
,814	4

Fuente: Resultados obtenidos en IBM SPSS

En relación a la confiabilidad de la dimensión de declaración de vulnerabilidades, se obtiene:

Tabla 31: Estadísticas de fiabilidad Ficha de Observación- Dimensión Vulnerabilidad

Alfa de Cronbach	N de elementos
,851	3

Fuente: Resultados obtenidos en IBM SPSS

Por lo que los resultados obtenidos con este instrumento son confiables para la presente investigación.

4.1.2.- En cuanto a la encuesta diagnóstica aplicada a los trabajadores de T.I.

En relación a la confiabilidad del presente instrumento, se obtiene:

Tabla 32: Fiabilidad de encuesta diagnóstica aplicada a trabajadores de T.I.

Fiabilidad

Notas

Salida creada		24-APR-2019 13:00:45
Comentarios		
Entrada	Conjunto de datos activo	ConjuntoDatos3
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	10
	Entrada de matriz	
Manejo de valores perdidos	Definición de perdidos	Los valores perdidos definidos por el usuario se tratan como perdidos.

	Casos utilizados	Las estadísticas se basan en todos los casos con datos válidos para todas las variables en el procedimiento.
Sintaxis		RELIABILITY /VARIABLES=P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA.
Recursos	Tiempo de procesador	00:00:00.00
	Tiempo transcurrido	00:00:00.01

Resumen de procesamiento de casos

		N	%
Casos	Válido	10	100,0
	Excluido[a]	0	,0
	Total	10	100,0

Estadísticas de fiabilidad

Alfa de Cronbach[a]	N de elementos
0,931	10

Se demuestra que el presente instrumento ha obtenido un 93.1% de confiabilidad que según la clasificación de George y Mallery (2003) es excelente", es decir mi instrumento tiene un alto grado de confiablidad, siendo relevante la información que proporciona y que a continuación se describe:

En cuanto a los resultados obtenidos en la Pregunta 1 hasta la Pregunta 10 (Ver tabla 07 a tabla 16) permiten concluir que la Gestión de Riesgos de T.I en la Universidad es deficiente, no por desconocimiento del personal sino por sustentarse sólo en la experiencia y subjetividad del CIO (Ver Tabla 12, 13 y 14). Además es muy grave que el CEO de la organización no haya formalizado e identificado los riesgos organizacionales y por lo que la Gerencia está dispuesta a invertir para mitigarlos (Ver Tabla 15).

Por otro lado, no existe en la organización formato, instrumento o protocolo que ayude a identificar, evaluar y priorizar los riesgos de T.I. pues su trabajo es muy informal (Ver Tabla 11). También constituye una debilidad, que el personal no tenga experiencia en la implementación de Metodologías de Riesgos de T.I. (Ver Tabla 08)

No tener un plan o estrategia de tratamiento de riesgos de TI la hace vulnerable (Ver tabla 14) Finalmente, los trabajadores evidencian que el actual trabajo o iniciativas para la gestión de riesgos es muy ineficiente (Ver Tabla 16)

4.2.- Después de la propuesta de mejora

Los resultados para el DESPUÉS, se describen considerando la Evaluación por Juicio de Expertos, que muestra los siguientes resultados en términos de Fiabilidad del Instrumento y Validez de Contenido:

4.2.1.- También se obtuvieron resultados para la ***fiabilidad del instrumento*** que a continuación se describen.

Tabla 33: Fiabilidad del Instrumento (Propuesta de Solución) a construir

		Notas
Salida creada		24-APR-2019 14:25:55
Comentarios		
Entrada	Datos	C:\MAESTRIA UNPRG\EL INFORME DE TESIS\TESIS JUAN TORRES FIABILIDAD 2.sav
	Conjunto de datos activo	ConjuntoDatos13
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	7
	Entrada de matriz	
Manejo de valores perdidos	Definición de perdidos	Los valores perdidos definidos por el usuario se tratan como perdidos.
	Casos utilizados	Las estadísticas se basan en todos los casos con datos válidos para todas las variables en el procedimiento.

Sintaxis		RELIABILITY /VARIABLES=OBJETIVIDAD CONSISTENCIA COHERENCIA PERTINENCIA SUFICIENCIA CLARIDAD /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA.
Recursos	Tiempo de procesador	00:00:00.00
	Tiempo transcurrido	00:00:00.10

[ConjuntoDatos13] C:\MAESTRIA UNPRG\EL INFORME DE TESIS\TESIS JUAN TORRES FIABILIDAD 2.sav

Resumen de procesamiento de casos

		N	%
Casos	Válido	7	100,0
	Excluido[a]	0	,0
	Total	7	100,0

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,901	6

Fuente: Elaboración propia

Se demuestra que el presente instrumento para la validación de expertos ha obtenido un 90.1% de confiabilidad que según la clasificación de George y Mallery (2003) es excelente", es decir mi instrumento tiene un alto grado de confiablidad, siendo relevante la información que proporcione para esta investigación.

4.2.2.- Así mismo, se obtuvo información sobre la ***validez de la propuesta de solución***, tal como se describe a continuación:

Tabla Nro. 34: Validez de Contenido del Instrumento

	Experto 1	Experto 2	Experto 3	Experto 4	Experto 5	Experto 6	Experto 7	∑ri	Pri
Ítem 1	5	5	4	5	4	5	5	33	4.714285714
ítem 2	5	5	5	4	5	4	5	33	4.714285714
ítem 3	5	5	5	5	4	4	4	32	4.571428571
Ítem 4	4	5	4	4	5	5	5	32	4.571428571
ítem 5	5	5	4	5	4	4	5	32	4.571428571
ítem 6	4	5	4	5	4	5	4	31	4.428571429
∑Pri									27.57
∑Pri/J									4.60
CPR									0.875873016
Pe									0.00000121
CVc = (CPR - Pe)=									0.86587180

Fuente: Elaboración propia

Coeficiente de Validez del Contenido (CVc)

Para el cálculo del CVc se tiene:

CVC = CPR – Pe

$$CPR = \frac{\sum_{i=1}^{N} PRi}{\frac{J}{N}}$$

$$Pe = \left(\frac{1}{J}\right)^{J}$$

Donde

PRi = Promedio de rango

∑Pri = Sumatoria del promedio de rango

CPR = Coeficiente de proporción de rango

J = Número de Expertos: 7

N = Número de Ítems: 6

Pe = Probabilidad de error

Por lo tanto, la Validez del Contenido, de mi instrumento obtuvo el 87% de aceptación, cuya interpretación es que la Validez y Concordancia del contenido del instrumento es "Alta". Con lo que se demuestra que mi instrumento es claro, objetivo, consistente, coherente, pertinente y suficiente para los expertos y como consecuencia se infiere que ayudará en la gestión de riesgo de T.I.

4.3.- Discusión en cuanto a la hipótesis

Habiendo concluido la verificación de Juicio de Expertos, puedo afirmar que mi propuesta de solución comprueba la hipótesis: "El diseño de un instrumento que desarrolle una base común para la terminología de análisis de riesgos, especifique y documente los hallazgos en la etapa del análisis, clasifique las evidencias por su impacto y frecuencia, realice la prueba de evaluación comparativa, determine la priorización de riesgos de T.I. reduce la incertidumbre en la gestión de riesgos de T.I. en una Universidad Privada en Chiclayo" evidenciada en los resultados que los 07 expertos me han proporcionado sobre la validez de contenido de mi instrumento.

Conclusiones

1.- El diseño de una herramienta que desarrolle una base común para la terminología de análisis de riesgos, especifique y documente los hallazgos en la etapa del análisis, clasifique las evidencias por su impacto y frecuencia, realice la prueba de evaluación comparativa, determine la priorización de riesgos de T.I. reduce la incertidumbre en la gestión de riesgos de T.I. en una Universidad Privada en Chiclayo porque le permitirá implementar una gestión de riesgos de TI sustentada en evidencias y prioridades para cualquier Metodología de Gestión de Riesgos.

2.- El instrumento propuesto mejora la confiabilidad en la identificación, evaluación y priorización de riesgos porque no sólo se sustenta en la experticia del CIO sino que exige el cumplimiento de matrices que cuantifican la amenaza o riesgo, así como el impacto que generan.

3.- Se reduce el impacto negativo y nefasto en la Universidad en la que se aplica el Instrumento de Gestión de Riesgos porque se genera un plan de tratamiento y contingencia de los referidos riesgos de T.I.

4.- El instrumento diseñado ha alcanzado el 87% de aceptación por parte de los expertos, lo que implica que la gestión de riesgos de TI para la Universidad tendrá éxito.

5.- El instrumento propuesta de solución, ha alcanzado el 90.1% de confiabilidad por lo tanto es relevante la información que proporcione para la Gestión de Riesgos de T.I.

Recomendaciones

1.- Realizar una encuesta piloto para determinar los factores problemáticos con mayor eficiencia y no volver a replantear los instrumentos por falta de confiabilidad.

2.- Conciliar el Plan de mitigación de riesgos con la Alta Dirección de la Universidad para su efectiva ejecución presupuestal.

3.- Evaluar los resultados del plan de mitigación a efectos de realizar una mejora continua al mismo proceso.

Referencias Bibliográficas

Alhawari, S., Karadsheh, L., Talet, A. N., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management*, *32*(1), 50-65.

Bergvall, J. & Svensson, L. (2015). *Risk analysis review*

Benaroch, M., Lichtenstein, Y., & Robinson, K. (2006). Real options in information technology risk management: An empirical validation of risk-option relationships. *MIS quarterly*, 827-864.

Escobar-Pérez, J., & Cuervo-Martínez, A. (2008). Validez de contenido y juicio de expertos: una aproximación a su utilización. Avances en medición, 6, 27-36.

Flage, R., & Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis. *Reliability: Theory & Applications*, *4*(2-1 (13)).

García, J. (2013). Infoexplosión Nuevas estrategias de gestión de la información. *Big Data*, *95*, 51.

Larson, E. W., & Gray, C. F. (2015). A Guide to the Project Management Body of Knowledge: PMBOK (®) Guide. Project Management Institute.

M Tascón - Big Data, 2013 - telos.fundaciontelefonica.com

McCarty, A., & Skibniewski, M. (2017). The Impact of PMIS Training: Patterns of Benefit Realization in Project Management Information Systems Training. *Journal of Engineering, Project & Production Management*, *7*(1).

McManus, J. (2012). *Risk management in software development projects*. Routledge.

Solarte, F. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*

Muriana, C., & Vizzini, G. (2017). Project risk management: A deterministic quantitative technique for assessment and mitigation. *International Journal of Project Management*, *35*(3), 320-340.

Ramírez, L. F. M., Alegría, D. J. A., & Martínez, L. M. S. (2013). Guía para apoyar la priorización de riesgos en la gestión de proyectos de tecnologías de la información. *Revista GTI*, *12*(33), 15-32.

Ramírez, A., Ortiz, Z. (2011). *Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios.* En: Ingeniería, Vol. 16, No. 2, pág. 56-66.

Tascón, M. (2013). Pasado, presente y futuro. *Big Data*, *95*, 47.

Silberfich, P. A., & Cruz, A. (2009). Análisis y Gestión de riesgos en TI ISO 27005–Aplicación Práctica. *Buenos Aires, Argentina: Segurinfo*.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

Tristán-López, A. (2008). Modificación al modelo de Lawshe para el dictamen cuantitativo de la validez de contenido de un instrumento objetivo. Avances en Medición, 6, 37-48

Anexos

Anexo 1: Matriz de Congruencia

Tabla N° 35: Matriz de congruencia

Título	Problema	Objetivo General	Objetivos específicos
Herramienta de evaluación, identificación y priorización para la gestión de riesgos de T.I. Caso: Universidad Privada.	¿De qué manera una herramienta que identifique, evalúe y priorice riesgos de TI disminuye la incertidumbre en la gestión de riesgos de TI en una Universidad Privada?	Diseñar una herramienta que permita identificar, evaluar y priorizar los riesgos de TI para la gestión de riesgos en una Universidad Particular.	Reducir el impacto que generan los riesgos de TI en la Universidad.
			Mejorar la confiabilidad del análisis, evaluación y priorización de riesgos de TI.
			Aplicar el juicio de expertos para la medición de la validez de contenido de la herramienta propuesta.

Fuente: Elaboración propia

ANEXO 2: Instrumento para validación de expertos

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
ESCUELA DE POSGRADO

Ingeniero(a): _____
PRESENTE

Reciba un cordial saludo.

Motivado por su reconocida trayectoria profesional en Tecnologías de la Información, Ingeniería de Sistemas, Computación o Informática, me complace dirigirme a Usted para solicitar su valiosa colaboración como EXPERTO en la validación de un instrumento que permita la identificación, evaluación y priorización de riesgos de T.I. mediante un test que a continuación se anexa, cuyos resultados serán considerados en la investigación titulada *Herramienta de evaluación, identificación y priorización para la gestión de riesgos de T.I. Caso: Universidad Privada.*.

Después de analizada la propuesta sírvase contestar marcando con un aspa en la casilla que usted considera conveniente, además de hacerme llegar alguna observación al respecto, en cada ítem propuesto.

Agradezco su valiosa colaboración.

Atentamente.

_____

Juan Antonio Torres Benavides
Email: torrebenj@yahoo.es
Celular: 978729108

Lambayeque, marzo del 2019.

INSTRUMENTO VALIDACIÓN DE EXPERTO DEL INSTRUMENTO EVALUACIÓN, IDENTIFICACIÓN Y PRIORIZACIÓN DE RIESGOS DE T.I.

I. DATOS GENERALES.

1.1. Apellidos y nombres del Experto ……..

1.2. Grado Académico……...

1.3. Área de experiencia profesional……

1.4. Institución donde labora……

1.5. Cargo actual……

Objetivo de la investigación	Diseñar un instrumento que permita evaluar, identificar y priorizar los riesgos de TI para la gestión de riesgos en una Universidad Particular de la Región Lambayeque.
Objetivo de la valoración del experto	Establecer la validez de contenido al incorporar el juicio de expertos en la estructura del instrumento considerando su claridad, objetividad, consistencia, coherencia, pertinencia y suficiencia.

II. VALIDACIÓN CUANTITATIVA DE LA PROPUESTA.

FIABILIDAD Y VALIDEZ DE CONTENIDO DEL INSTRUMENTO PROPUESTO PARA LA GESTIÓN DE RIESGOS DE T.I.						
CRITERIOS DE EVALUACION PARA LA PROPUESTA	**INDICADORES DE EVALUACIÓN PARA LA PROPUESTA**	**MUY MALA**	**MALA**	**NI MALA NI BUENA**	**BUENA**	**MUY BUENA**
		1	**2**	**3**	**4**	**5**
1. CLARIDAD	La estructura del instrumento es de fácil comprensión, su sintaxis y semántica se comprende fácilmente.					
2. OBJETIVIDAD	La estructura del instrumento está planteada con procesos o					

	actividades concretos, y observables.					
3. CONSISTENCIA	Existe organización lógica entre las actividades y procesos del instrumento para identificar, evaluar y priorizar los riesgos de T.I.					
4. COHERENCIA	Los procesos o actividades del instrumento tiene relación lógica con la gestión de riesgos de T.I.					
5. PERTINENCIA	Los resultados esperados coadyuvan a identificar, evaluar y priorizar los riesgos de T.I. de manera objetiva.					
6. SUFICIENCIA	Los elementos de la estructura del instrumento son suficientes para identificar, evaluar y priorizar los riesgos de T.I.					

Adaptado de: Escobar y Cuervo (2008)

III. VALIDACIÓN CUALITATIVA DE LA PROPUESTA.

3.1. ¿La propuesta cumple su objetivo? Favor explicar su argumento

……...…
……...

3.2. ¿La propuesta debe mejorarse en los siguientes aspectos? Favor explicar su argumento

……
…….

3.3. ¿Definitivamente, la propuesta no cumple con el objetivo propuesto? Favor explicar su argumento

……
……...

Lambayeque, …… de …….. de 2019

……..

FIRMA DEL EXPERTO

ANEXO 3: Instrumento diagnóstico aplicado al Personal de T.I. basada en la Metodología basada en la gestión del conocimiento para proyectos de tecnología de información (Samer, 2012)

ENCUESTA REALIZADA AL PERSONAL DE TI DE LA UNIVERSIDAD OBJETO DE ESTUDIO

Fecha: _____ Nro.

Responsable: _____

Objetivo: Conocer el nivel de conocimiento de Metodología de gestión de riesgos por parte del personal de T.I. así como la implementación de estándares o normas de gestión de riesgos en dicha institución. Encuesta elaborada según Metodología basada en la gestión del conocimiento para proyectos de tecnología de información (Samer et al, 2012)

Datos Relevantes del Área de T.I.

Encuestado : _____

Cargo : _____

Años en el área : _____

Item 1: Conocimiento sobre gestión de riesgos

1.1.- ¿Tiene conocimiento de alguna Metodología de Gestión de Riesgos de T.I.? Si es SI especifique.

1	Sí
2	No

Especifique: _____

1.2.- ¿Han aplicado alguna Metodología de Gestión de Riesgos de T.I. para salvaguardarse de amenazas o desastres? Si es SI especifique.

1	Sí
2	No

Especifique: _____

1.3.- ¿Conoce de alguna herramienta, instrumento, formato, que le haya permitido la materialización de la Metodología de Gestión de Riesgos de T.I.? Si es SI especifique.

1	Sí
2	No

Especifique: _____

1.4.- ¿Conoce de alguna estrategia o plan para abordar las amenazas de T.I. que puede sufrir la organización? Si es SI especifique.

1	Sí
2	No

Especifique: _____

Item 2: Transferencia del Conocimiento tácito a explícito sobre gestión de riesgos (Materialización de la(s) Metodología(s))

2.1.- Aplican algún protocolo o formato para la materialización de la MGR

	1. Nunca
	2. Casi nunca
	3. En ocasiones
	4. Casi siempre
	5. Siempre

2.2.- ¿La identificación de riesgos se realiza considerando sólo la experiencia del CIO?

	1. Nunca
	2. Casi nunca
	3. En ocasiones
	4. Casi siempre
	5. Siempre

2.3.- ¿La evaluación de riesgos se realiza considerando sólo la experiencia del CIO?

	1. Nunca
	2. Casi nunca
	3. En ocasiones
	4. Casi siempre
	5. Siempre

2.4.- ¿La priorización de riesgos se realiza considerando sólo la experiencia del CIO?

	1. Nunca
	2. Casi nunca

	3. En ocasiones
	4. Casi siempre
	5. Siempre

2.5.- ¿Existe identificación de riesgos de T.I. validados por el CEO de la Organización?

1	Sí
2	No

Item 3: Evaluación de la eficiencia de las iniciativas de G.R. de T.I.

3.1.- Se le pide dar su valoración de la actual eficiencia de las iniciativas o políticas de Gestión de Riesgos de T.I. que aplica la organización

	1 Muy ineficiente
	2 Ineficiente
	3 Ni eficiente ni ineficiente
	4 Eficiente
	5 Muy eficiente

ANEXO 4: Instrumento diagnóstico – Ficha de Observación para describir los procesos o actividades de la Universidad considerando lo expuesto por la Metodología de Evaluación de Riesgos de un Sistema de TI. (Stoneburner, 2002).

FICHA DE OBSERVACIÓN

Fecha: | Nro.

Responsable: _____

Objetivo: Observar la organización para recoger información sobre sus políticas de gestión de riesgos de T.I. implementadas. El presente instrumento se sustenta en la Metodología de evaluación de riesgos de un sistema de TI. (Stoneburner, 2002).

Datos Relevantes del Área de T.I.

Años de funcionamiento : _____

Nombre del Director : _____

Nro. De trabajadores : _____

Item 1: Caracterización de los sistemas

Nro. De Sistemas Informáticos en funcionamiento

Sistemas Informáticos Principales

Nro. De Datas Center's

Sistemas y Datos Criticos

Sistemas y Datos expuestos a internet

Item 2: Declaraciones de amenazas

2.1.- Utilizan formatos para el registro y declaración de amenazas

	1. Nunca
	2. Casi nunca

	3. En ocasiones
	4. Casi siempre
	5. Siempre

2.2.- Los documentos evaluados contienen datos :

1	Incorrectos
2	Ni incorrectos / Ni correctos
3	Correctos

2.3.- ¿Los documentos observados se estructuran con alguna metodología de riesgo?

1	Sí
2	No

2.4.- ¿Existen registros de amenazas o ataques a los sitemas informáticos?

1	Sí
2	No

Item 3: Identificación de vulnerabilidades

2.5.- ¿Existen reportes sobre identificación de riesgos de T.I.?

1	Sí
2	No

2.6.- ¿Existen criterios de requerimientos de seguridad?

1	Sí
2	No

2.7.- ¿Realizan auditorías de seguridad información?

1	Sí
2	No