

**UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO  
ESCUELA DE POSGRADO**



**MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE  
INFORMACIÓN PARA LA GENERACIÓN DE VALOR EN EL  
CONTROL DE LA CORRUPCIÓN DE FUNCIONARIOS Y  
SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES DE LA  
REGIÓN DE LAMBAYEQUE**

**TESIS PARA OPTAR EL GRADO ACADÉMICO DE  
MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN  
EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN**

**AUTOR**

**ROGER GUSTAVO ABANTO ORTIZ**

**ASESOR**

**RICARDO DAVID IMAN ESPINOZA**

**<https://orcid.org/0000-0003-0409-8773>**

**Chiclayo, 2021**

**MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE  
INFORMACIÓN PARA LA GENERACIÓN DE VALOR EN EL  
CONTROL DE LA CORRUPCIÓN DE FUNCIONARIOS Y  
SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES  
DE LA REGIÓN DE LAMBAYEQUE**

PRESENTADA POR:  
**ROGER GUSTAVO ABANTO ORTIZ**

A la Escuela de Posgrado de la  
Universidad Católica Santo Toribio de Mogrovejo  
para optar el grado académico de

**MAESTRO EN INGENIERÍA DE SISTEMAS Y  
COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN  
ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN**

APROBADA POR:

Gregorio Manuel León Tenorio  
PRESIDENTE

María Ysabel Arangurí García  
SECRETARIO

Ricardo David Iman Espinoza  
VOCAL

## **DEDICATORIA**

A mi padre Demetrio, quien en vida me encaminó por el sendero del bien; asimismo a mi madre Noema por su amor, apoyo y aliento incondicional.

A mis hermanas Bernardita y Rosana por saberme orientar y ser mis ejemplos de lucha a seguir.

Finalmente, con mucho amor a mi esposa Rubí y a mis hijos Lía y Gustavo, por ser mi fortaleza y fuente de mi energía.

## **EPIGRAFE**

“No hay vicio más execrable que la codicia, sobre todo entre los próceres y quienes gobiernan la nación, pues servirse de un cargo público para enriquecimiento personal resulta no ya inmoral, sino criminal y abominable.”

**Cicerón**

## **AGRADECIMIENTOS**

A mi asesor Mtro. Ricardo David Iman Espinoza por sus valiosas recomendaciones con la finalidad de culminar con éxito este trabajo de investigación.

Se agradece al Dr. Oscar Gilberto Zocón Alva, a la Mtro. Mónica Villavicencio Montoya, al Mtro. Paúl Martín Villacorta Chávez, a la Mtro. María Ysabel Arangurí García, así como al Mtro. Juan Ramón Dávila Ramírez por sus comentarios y aportes; así como a todos mis maestros y maestras que contribuyeron en mi formación.

## ÍNDICE

INTRODUCCIÓN .....	12
CAPÍTULO I MARCO TEÓRICO CONCEPTUAL .....	18
1.1. Antecedentes del problema.....	18
1.2. Base teórica conceptual .....	20
A. Corrupción .....	21
B. Riesgo .....	21
C. Gestión del riesgo .....	22
D. Estándares internacionales de riesgos.....	23
E. Marcos de referencia de gestión de riesgos. ....	25
F. Armonización: .....	35
G. Generación de valor:.....	35
CAPÍTULO II MATERIALES Y MÉTODOS .....	37
2.1. Tipo y nivel de investigación.....	37
2.2. Diseño de investigación.....	37
2.3. Población, muestra y muestreo .....	37
2.3.1. Población:.....	37
2.3.2. Muestra y muestreo .....	38
2.4. Criterios de selección.....	38
2.5. Técnicas e instrumentos de recopilación de datos .....	38
2.6. Procedimientos .....	39
2.7. Plan de procesamiento y análisis de datos .....	39
2.8. Consideraciones éticas .....	39
CAPÍTULO III RESULTADOS Y DISCUSIÓN .....	40
3.1. Diagnóstico del sector.....	40
3.2. Estudio comparativo .....	43

3.3. Propuesta de modelo.....	55
3.4. Discusión .....	62
CONCLUSIONES .....	64
REFERENCIAS BIBLIOGRÁFICAS.....	66
ANEXOS .....	71
Anexo n.º 1: Documentos de aceptación de las municipalidades.....	72
Anexo n.º 2: Información de las municipalidades provinciales.....	78
Anexo n.º 3: Documentos relacionados a los cuestionarios .....	86
Anexo n.º 4: Formatos del modelo .....	100
Anexo n.º 5: Repositorios del modelo .....	129
Anexo n.º 6: Validación del modelo por expertos .....	141

## LISTA DE CUADROS

Cuadro n.º 1: Técnicas e instrumentos de recopilación de datos .....	38
Cuadro n.º 2: Diagnóstico en las municipalidades provinciales de Lambayeque.....	41
Cuadro n.º 3: Comparación a nivel macro .....	44
Cuadro n.º 4: Análisis comparativo - fase de comunicación y consulta.....	46
Cuadro n.º 5: Análisis comparativo - fase de alcance, contexto y criterios.....	47
Cuadro n.º 6: Análisis comparativo - fase de identificación del riesgo .....	49
Cuadro n.º 7: Análisis comparativo - fase de análisis del riesgo .....	50
Cuadro n.º 8: Análisis comparativo - fase de valoración del riesgo .....	51
Cuadro n.º 9: Análisis comparativo - fase de tratamiento del riesgo.....	52
Cuadro n.º 10: Análisis comparativo - fase de seguimiento y revisión .....	54
Cuadro n.º 11: Análisis comparativo - fase de registro e informe .....	55
Cuadro n.º 12: Cuadro presentación de los pasos del modelo propuesto .....	57
Cuadro n.º 13: Fase 1: Actividades preliminares.....	57
Cuadro n.º 14: Fase 2: Contexto, alcance y criterios .....	58
Cuadro n.º 15: Fase 3: Evaluación del riesgo - Identificación del riesgo .....	59
Cuadro n.º 16: Fase 3: Evaluación del riesgo - Análisis y valoración del riesgo .....	60
Cuadro n.º 17: Fase 4: Tratamiento del riesgo.....	61
Cuadro n.º 18: Componente transversal: Seguimiento o revisión .....	62
Cuadro n.º 19: Resultados del estadístico de W de Kendall.....	63
Cuadro n.º 20: Resultados del estadístico de V de Aiken.....	63

## LISTA DE GRÁFICOS

Gráfico n.º 1: Componentes de la ISO 31000:2018-02 .....	23
Gráfico n.º 2: Fases de la NTP-ISO/IEC 27005:2018-02 .....	25
Gráfico n.º 3: Componentes de Cobit 2019 .....	26
Gráfico n.º 4: Objetivos y dominios del Modelo Cobit 2019 .....	26
Gráfico n.º 5: Prácticas claves del objetivo de gobierno del riesgo.....	27
Gráfico n.º 6: Prácticas claves del objetivo de gestión del riesgo .....	28
Gráfico n.º 7: Octave – S – Fase 1 .....	31
Gráfico n.º 8: Octave – S – Fase 2 .....	31
Gráfico n.º 9: Octave – S – Fase 3 .....	32
Gráfico n.º 10: Evaluación de riesgos según NIST .....	33
Gráfico n.º 11: Procesos de la gestión de riesgos según NIST .....	34
Gráfico n.º 12: Familias de riesgos propuestos por NIST .....	35
Gráfico n.º 13: Resultados de la creación de valor .....	36
Gráfico n.º 14: Macroprocesos de las municipalidades .....	43
Gráfico n.º 15: Fases del modelo propuesto .....	56

## RESUMEN

El objetivo esta investigación fue generar valor en el control de la corrupción al proponer un modelo de gestión de riesgos de tecnologías de información (MGR - TI) para las municipalidades provinciales de la región de Lambayeque.

Se ha realizado una investigación de tipo cuantitativa empleando un diseño de investigación experimental - preprueba/posprueba; para ello se procedió a observar y analizar la realidad de las municipalidades provinciales de la región de Lambayeque, lo cual permitió recabar información sobre la realidad de las citadas municipalidades, determinándose que existen problemas en su gestión de riesgos de tecnologías de información (GR-TI) los cuales pueden provocar un acto de corrupción.

En tal sentido, se realizó un estudio comparativo de estándares y normas relacionados con la GR - TI, y tomando en cuenta su problemática se generó un modelo apropiado para los gobiernos provinciales de la región de Lambayeque, orientado a generar valor en el control de la corrupción de funcionarios o servidores; modelo práctico, ágil y dinámico según la validación de profesionales expertos.

**Palabras clave:** Corrupción, riesgo de tecnología de información, gestión de riesgos, generación de valor.

## ABSTRACT

The objective of this research was to generate value in the control of corruption by proposing an information technology risk management model (MGR - TI) for the provincial municipalities of the Lambayeque region.

Quantitative research has been carried out using an experimental research design - pretest / posttest; for this, the reality of the provincial municipalities of the Lambayeque region was observed and analyzed, which allowed gathering information on the reality of the aforementioned municipalities, determining that there are problems in their information technology risk management (GR-TI ) which can provoke an act of corruption.

In this sense, a comparative study of standards and norms related to GR-TI was carried out, and taking into account its problems, an appropriate model was generated for the provincial governments of the Lambayeque region, aimed at generating value in the control of the corruption of officials or servers; practical, agile and dynamic model according to the validation of expert professionals.

**Keywords:** Corruption, information technology risk, risk management, value generation.

## INTRODUCCIÓN

Casi a diario se es testigo de cómo la corrupción viene ganando terreno en diferentes países; tales como Yemen, Siria, Sudán del Sur y Somalia; los cuales figuran, según [1, p. 3], como los primeros cuatro países más corruptos en el sector público a nivel global.

En el 2018 António Manuel de Oliveira Guterres, en [2], dijo que se estima que la corrupción representa para el mundo un forado de aproximadamente \$ 2,6 billones de dólares. De otro lado, Cybersecurity Ventures en [3, p. 3] predijo que el cibercrimen le costará al mundo \$ 6 billones de dólares anuales para 2021, en comparación con \$ 3 billones de dólares en 2015.

Según [4] la Policía Italiana realizó una investigación, que duró 6 meses, revelando un fraude por de 224 mil euros, lo que llevó a investigar a un total de 135 personas (incluidas 20 beneficiarias). El fraude consistía en que personas extranjeras (en su mayoría egipcios, paquistaníes, marroquíes y chinos) pagaron hasta 4 mil euros por licencias de conducir, a malos empleados; los que se ocupaban de la emisión, renovación y revisión de los permisos de conducir. La Policía Italiana incautó cuentas corrientes, 5 inmuebles, 2 motos y 5 coches entre ellos un Ferrari y un Mercedes, además, se incautó 90 licencias de conducir de diversas categorías.

El panorama internacional es sombrío; sin embargo, para tener alguna posibilidad de frenar la corrupción, los gobiernos deberán fortalecer los controles [1, p. 4], opinión que también comparte El Fondo Monetario Internacional en [5, p. 4], en la cual insta a los gobiernos a empeñarse a lidiar contra las vulnerabilidades

para hacer frente a la amalgama de retos que implica la corrupción; en este proceso el rol de las TI es fundamental para lograr apuntalar las labores de control en tres puntos básicos: la parte presupuestal, la recaudación y la implementación de controles. Es decir, los gobiernos deberán ser más eficientes al identificar los riesgos que conllevan a la corrupción y de esta manera tener la posibilidad de gestionar los citados riesgos.

La situación no es diferente en América Latina; tal es así que Transparencia Venezuela, en [6] informó que la emergencia humanitaria que vive Venezuela ha provocado que se hayan abierto más de 20 investigaciones por desfalcos en diferentes países<sup>1</sup> por casi \$ 25 mil millones de dólares, hechos como este ubican a Venezuela como el país de América Latina con más percepción de corrupción y el quinto a nivel internacional.

Según [7] la Fiscalía General de la Nación del gobierno colombiano evidenció el robo de aproximadamente \$ 2 091 893,70 de dólares del Municipio de Valledupar y logró que en agosto de 2018 un ex empleado fuera condenado por el delito de acceso deliberado al sistema informático; el fraude ocurrido entre el 2004 y 2011 consistió en el uso indebido del software con la finalidad de alterar los pagos de 10 300 predios del citado municipio.

Así mismo Juan Manuel Harán, editor del portal WeLiveSecurity de ESET, informó en [8] que el Banco de Chile sufrió un robo sistemático realizado por uno de sus trabajadores, por importe aproximado \$ 700 000,00 dólares, este realizó una serie de transferencias de manera indebida entre el 2017 y el 2018.

Otro caso se expone en [9], cuando La Fiscalía General de la Nación de Colombia señala que investiga a un ex funcionario del municipio colombiano de Baraya, departamento de Huila; pues presume que se aprovechó de su cargo, durante los años 2017 y 2018, para desfalcar al municipio en una suma total de \$ 944 866 440,00 de pesos; se presume que utilizó el aplicativo contable denominado

---

<sup>1</sup> Investigaciones realizadas en Estados Unidos, España, Portugal, Brasil, Ecuador, Argentina, Perú, entre otros países.

HAS SQL en al menos 60 ocasiones, aprovechado para elaborar y modificar diversos tipos de comprobantes, con la finalidad encubrir su actos. Hecho que evidencia una vez más la falta de controles toda vez que se empleó un acceso autorizado al sistema informático; pero, se presume que hizo uso indebido del mismo, con la finalidad de delinquir.

En [10] se muestra el análisis de encuestas de más de 17 000 participantes de casi 20 países de América Latina y el Caribe; en cual puede apreciar dos aspectos importantes: el primero, más del 50% de los ciudadanos de 9 de estos países tienen la sensación que la corrupción en su país ha aumentado; y el otro aspecto es que más del 50% de los ciudadanos de 12 de estos países creen que sus gobernantes no realizan los esfuerzos necesarios para luchar contra la corrupción.

Por otro lado, de acuerdo a [1, p. 3] el Perú ha obtenido un índice de percepción de corrupción de 36, ocupando el puesto 101 de 180 países (sobrepasando en Latinoamérica a Colombia ubicado en el puesto 96, a Ecuador en el puesto 93, entre otros) es de precisar, que se aprecia una ligera mejora en relación al índice de 35 obtenido en el año 2018; sin embargo, en el sector público del país los peruanos seguimos percibiendo problemas de corrupción.

Tanto es así que, La Contraloría General de la República del Perú (CGR), manifestó en [11, p. 94], que en el último semestre del 2019, producto de las auditorías realizadas, la Procuraduría Pública inició 142 procesos judiciales, estos corresponden a 918 funcionarios o servidores denunciados, por un importe de S/ 263 570 998,49. Se hace hincapié que en comparación con el último semestre del 2018 [12, p. 53] el número de procesos judiciales así como de funcionarios y servidores denunciados ha aumentado en 30,98% y 16,99% respectivamente; esto quiere decir, que se han identificado más casos de corrupción lo cual tiene un impacto negativo en los ciudadanos, sobre todo en los más vulnerables.

Como resultado de un examen especial a una entidad limeña la CGR en [13], identificó un perjuicio de S/ 1 455 400,00 en contra del estado peruano; esto debido a que se presume que los imputados, de manera indebida, cambiaron los estados en el aplicativo informático de 1 (Válido) a 5 (No cumple con criterio del Reglamento

Nacional de Tránsito) o 6 (Placa de Provincia) impidiendo que se den trámite a las papeletas por infracción de tránsito correspondientes; hecho que evidencia la falta de controles informáticos.

Otro caso, se muestra en [14], donde la CGR identificó, que las personas implicadas permitieron la prescripción de deudas tributarias y no tributarias, con un perjuicio de S/ 27 416 972,49; debido a que el Sistema de Tributación Municipal no contaba con mecanismo de alerta para evitar la prescripción.

Además, en el Informe Ejecutivo Semestral de Gestión Julio – Diciembre 2019 [11, p. 27], La CGR, propone que el Sistema de Control Interno (SCI) de las entidades gubernamentales del país se fortalezcan; esto implica mejorar, entre otros aspectos, la gestión de riesgos; esto quiere decir, que las entidades gubernamentales, entre ellas las municipalidades, deberán disponer bajo responsabilidad la implementación y el fortalecimiento de la gestión de riesgos y de este modo generar valor en el control de la corrupción.

Sin embargo, el presidente del comité de control interno de una de las municipalidades, el 26 de junio de 2018, mediante [15, p. 1], informó a su Alcalde que: “A nivel general, el SCI de la Municipalidad (...) alcanza un nivel de desarrollo Insuficiente, con diferencias entre los componentes que la conforman; siendo Incipiente en el componente de Evaluación de Riesgos (...)”. Del mismo modo, según [16, p. 27], otra de las municipalidades señaló que no cuenta con planes o capacitaciones para mitigación de riesgos.

Los hechos expuestos en el párrafo anterior coinciden con el resultado del diagnóstico realizado a los gobiernos provinciales de la Región de Lambayeque, en él se determinó que existen problemas en las tareas de GR - TI; esta situación obstaculiza las citadas labores y por ende no permite contrarrestar eficientemente acontecimientos potenciales asociados a la corrupción; hechos que podrían impactar negativamente la ejecución de los procesos de TI con la consecuente afectación en el resultado de los objetivos de las municipalidades.

Con relación a las causas de la corrupción, Quiroz en [17, p. 45] centra su enfoque en la ausencia de controles adecuados que limiten los comportamientos al margen de la ley, provocados por el desmesurado poder político, la burocracia ineficiente y las preferencias económicas; esto quiere decir que, si lográramos identificar y analizar la lógica de los citados comportamientos oportunistas, podríamos ir un paso adelante en este enfrentamiento frente la corrupción.

En [18] se señaló que la corrupción impacta directamente en los aspectos: social (pues incrementa la pobreza y la brecha de exclusión), económico (ocasiona ganancias al margen de ley y la desaceleración del crecimiento) y político (la población pierde su confianza en la clase política). En síntesis, las consecuencias mostradas convierten a la corrupción en un fenómeno complejo y de alto impacto; sin embargo, nos muestra también la necesidad de hacerle frente.

Por los hechos expuestos, se planteó el siguiente problema: ¿Cómo podríamos generar valor en el control de la corrupción de funcionarios o servidores en las municipalidades provinciales de la región de Lambayeque? En tal sentido se propuso el desarrollo de un MGR - TI para generar valor en el control de la corrupción de funcionarios o servidores en los gobiernos provinciales de la citada región.

Ante esta situación se formuló como objetivo general de la investigación, generar valor en el control de la corrupción al proponer un MGR - TI para los gobiernos provinciales de la región de Lambayeque; por lo que se planteó los siguientes objetivos específicos:

- Comparar los estándares y marcos de referencias internacionales relacionadas con la GR - TI.
- Proponer un MGR - TI para asegurar la generación de valor en el control de la corrupción de funcionarios o servidores en los gobiernos provinciales de la región de Lambayeque.
- Validar el MGR - TI para asegurar la generación de valor en el control de la corrupción de funcionarios o servidores en las municipalidades provinciales de la Lambayeque.

La importancia de esta investigación se basó fundamentalmente en la relevancia social pues pretende prevenir actos de corrupción y por ende mejorar la inversión social y la condición de vida de los pobladores de las citadas municipalidades. Respecto a la importancia económica, estuvo abocada a proteger los activos y procesos críticos de estos gobiernos provinciales. En cuanto a la justificación tecnológica, la implementación del proyecto permitirá generar valor en la lucha contra la corrupción haciendo uso un MGR - TI exclusivo para municipalidades de la región de Lambayeque. Finalmente, la importancia de índole científica radica en que se propuso un modelo validado por expertos que no existía en el mercado.

## **CAPÍTULO I MARCO TEÓRICO CONCEPTUAL**

### **1.1. Antecedentes del problema**

De la indagación relacionada a las investigaciones que guardan relación con la presente se pudo tener acceso a los siguientes trabajos:

En el 2017 Crespo en [19], señaló que frente a la falta de conocimiento sobre cómo proteger la información y lo complicado de implementar los procedimientos establecidos en las normas internacionales para lograr nivel de protección en las MYPES ecuatorianas, propuso Ecu@Risk, una MGR - TI para este tipo de empresas. Este estudio se basó en un análisis comparativo de varias metodologías y estándares internacionales correlacionados con la gestión de riesgos; sin embargo, no fue enfocado al tema de corrupción. La importancia de este antecedente reside en que nos presenta una manera de cómo abordar la armonización de estos estándares y metodologías.

Así mismo el 2017 Arellano en [20] señaló que la corrupción es un fenómeno social denso, además en parte de sus conclusiones mencionó que la corrupción se puede acotar, para la cual se requiere comprender cómo las relaciones en una organización pueden estar generando justamente el fenómeno de la corrupción. La utilidad de este artículo en el desarrollo de esta investigación radicó en la desnormalización del citado fenómeno, hecho que

permite tener conocimiento sobre los componentes que sostienen la corrupción.

Otra contribución es la presentada por Cuesta el 2015 en [21], debido a la ausencia de herramientas preventivas del fenómeno de la corrupción en el gobierno colombiano; formuló mapas de riesgos de corrupción y señaló cómo estas inciden en su prevención; en el desarrollo de su trabajo demostraron que no se está tratando el tema de la corrupción de manera complementaria e integral; la información desarrollada en este antecedente fue valorada al momento del desarrollo de la presente investigación.

Del mismo modo, un antecedente importante fue realizado por Rodríguez en el 2019 en [22], donde señaló que los entornos en los que se desarrollan las empresas que brindan software como servicio son entornos expuestos a ataques y riesgos propios de su entorno y que podrían afectar su operación; en tal sentido presentó un MGR - TI de 6 fases como apoyo en la continuidad del negocio de las citadas empresas. Este antecedente es importante pues producto de la comparación de marcos y estándares internacionales de gestión de riesgos presenta un MGR - TI adaptado a empresas que brindan software como servicio; en tal sentido este antecedente fue considerado como punto de partida para la investigación realizada.

Callata en el 2018, presentó un estudio [23] donde planteó que la corrupción es un flagelo que menoscaba los gobiernos, dentro de ellos el gobierno peruano; en tal sentido, en su trabajo de investigación propuso una serie de políticas que deberían aplicarse en los organismos públicos: donde destacó la promoción del uso de las tecnologías y el gobierno electrónico; también señaló que es necesario la implementación de controles para frenar los eventos de corrupción en las instituciones públicas; como se observa este antecedente presentó datos valiosos los cuales fueron meritados al momento del desarrollo de esta investigación.

También se encontró la investigación [24] desarrollada por Banda en el 2019, donde señaló que las empresas agroindustriales de la región de

Lambayeque son blanco de constantes incidentes que impactan negativamente en sus activos de información; por lo que después de realizar un análisis de conceptos propuestos en las normas y marcos referidos a la gestión de riesgos, formuló un modelo que incluye 11 pasos los mismos que fueron adecuados a las citadas empresas, proporcionando las estrategias necesarias para atenuar los efectos del riesgo. Ya que en este antecedente se formuló una MGR - TI pero orientada a proporcionar seguridad, razón por la que fue que se tomó como referencia.

De igual forma, hay una investigación del 2018 realizada por Alva y Vásquez [25] observaron que existen problemas en las microfinancieras de la región de Lambayeque, debido a que observó problemas en la GR - TI que podrían poner en peligro sus operaciones. En el citado trabajo los investigadores desarrollaron un MGR - TI con 8 fases; dándole mayor énfasis al análisis de impacto de negocio y la normativa que las rige. Este antecedente es importante pues presenta un modelo producto de haber logrado realizar la armonización de diferentes estándares y metodologías de GR - TI.

Finalmente, Arangurí, Iman y León presentaron en el 2016 una investigación [26] donde realizaron un diagnóstico en centros de educación privada de la región Lambayeque llegando a determinar que la GR - TI no está implementada o está implementada de manera deficiente; en tal sentido propusieron un MGR - TI contextualizado al entorno de los citados centros de estudio. Así también en su segunda y tercera conclusión señalaron que en una de las instituciones identificaron 73 riesgos, categorizando 11 como alta prioridad, siendo tratados con proyectos que fomentan la toma de decisiones proactivas. Este antecedente es clave puesto que los autores formularon MGR - TI contribuyendo de esta manera a evitar el comportamiento reactivos; hechos que fueron merituados para esta investigación.

## **1.2. Base teórica conceptual**

En este acápite se ha expuesto los términos o expresiones que han sido aplicados, en el desarrollo de esta investigación, dentro de ellos tenemos:

**A. Corrupción:**

Como ya se comentó, tanto en el contexto internacional, nacional y local es frecuente escuchar sobre casos relacionados a la corrupción en las organizaciones estatales; pero ¿qué es corrupción?, la Convención de las Naciones Unidas contra la Corrupción en [27, p. iii] consideró que la corrupción es una tragedia que conspira contra el adelanto social; afecta directamente al ser humano (especialmente a los que menos tienen); provoca actividades al margen de la ley, deteriora la economía, genera inestabilidad y malestar social, así como fomenta la delincuencia de cuello blanco; pero sobre todo ocasiona que las personas pierdan la esperanza en sus gobernantes y funcionarios por ende los ciudadanos en general tienen la percepción que la administración pública no trabaja a favor de ellos.

Del mismo modo, Chaname en [28, p. 246], señaló que la corrupción de funcionarios o servidores está relacionada con el “delito ocasionado por un funcionario o servidor público de manera indebida e ilícita usa su función para servir y/o servirse contra la ley”. En conclusión, se habla de corrupción cuando un funcionario o servidor público usa u omite sus funciones inherentes a su cargo para sacar un beneficio propio; afectando de esta manera a las personas que más lo necesitan.

Frente a esto los gobiernos deberán ser más eficientes al identificar los riesgos de TI que conllevan a la corrupción con la finalidad de tener la posibilidad de poder gestionarlos y generar valor en el control de la corrupción; en esa línea de ideas, es vital entender el significado de riesgo.

**B. Riesgo:**

Este término se ha transformado en una cuestión de relevante interés, tal es así que podemos encontrar múltiples definiciones, por ejemplo: Hay quienes la definieron como la incertidumbre en la

materialización de un impacto negativo debido a la acción de alguna amenaza; lo que se condice con la definición presentada en el Diccionario la Lengua Española, en su primera acepción, [29] riesgo es la “Contingencia o proximidad de un daño.” Sin embargo, hay quienes manifiestan que el impacto del riesgo no solo es negativo (amenaza), sino que también puede ser positivo (oportunidad), lo que concuerda con lo expuesto en [30, p. 1], [31, p. 397] y [32, p. 15].

Ahora bien, de las definiciones presentadas en los párrafos anteriores se tiene que los riesgos están relacionados con la posibilidad de que suceda y el efecto que este provoque sea este negativo (dentro los están los efectos de la corrupción) o bien positivo (oportunidades).

Esta investigación se enfocó en los riesgos de impacto negativo provocados por la corrupción afectando el cumplimiento misional de las municipalidades; en tal sentido, es necesario comprender cómo pueden gestionarse.

### **C. Gestión del riesgo:**

El Diccionario de la Lengua Española [33] en su tercera acepción define a gestionar como “Manejar o conducir una situación problemática”; en tal sentido gestionar el riesgo está orientado a la ejecución de una serie de acciones tendentes a minimizar el impacto del riesgo en la consecución de los objetivos; lo cual se corrobora en [30, p. 1], [34, p. 8] y en [35, p. 131]; de lo expuesto la GR - TI está orientada a salvaguardar los activos de TI críticos de las instituciones.

Ahora bien, la GR - TI debe ser realizada de forma ordenada y sistematizada; de manera tal, que reduzca la improvisación y se logren los cumplir con los objetivos de la organización. Actualmente existen diversos estándares y marcos de referencia internacionales relacionados la GR - TI, aquellos que han sido utilizados en esta investigación se describieron en los ítems D y E.

## D. Estándares internacionales de riesgos

### a. Norma Internacional ISO<sup>2</sup> 31000:2018-02

La ISO ha publicado esta norma internacional denominada “Gestión del riesgo – Directrices” la cual puede aplicarse a cualquier organización, en su totalidad o a alguna parte de ella. Este estándar incluye tres componentes: 8 principios (orientados a la creación o protección del valor y de esta manera favorece el cumplimiento misional de las organizaciones); un marco de referencia empleado para estas actividades (lo que permite que la gestión de riesgo se sume a las labores de gobernanza de las entidades, hecho del cual dependerá su eficacia); y el último componente está con constituido por los procesos a través de los cuales se realiza la GR; como se ilustra a continuación:

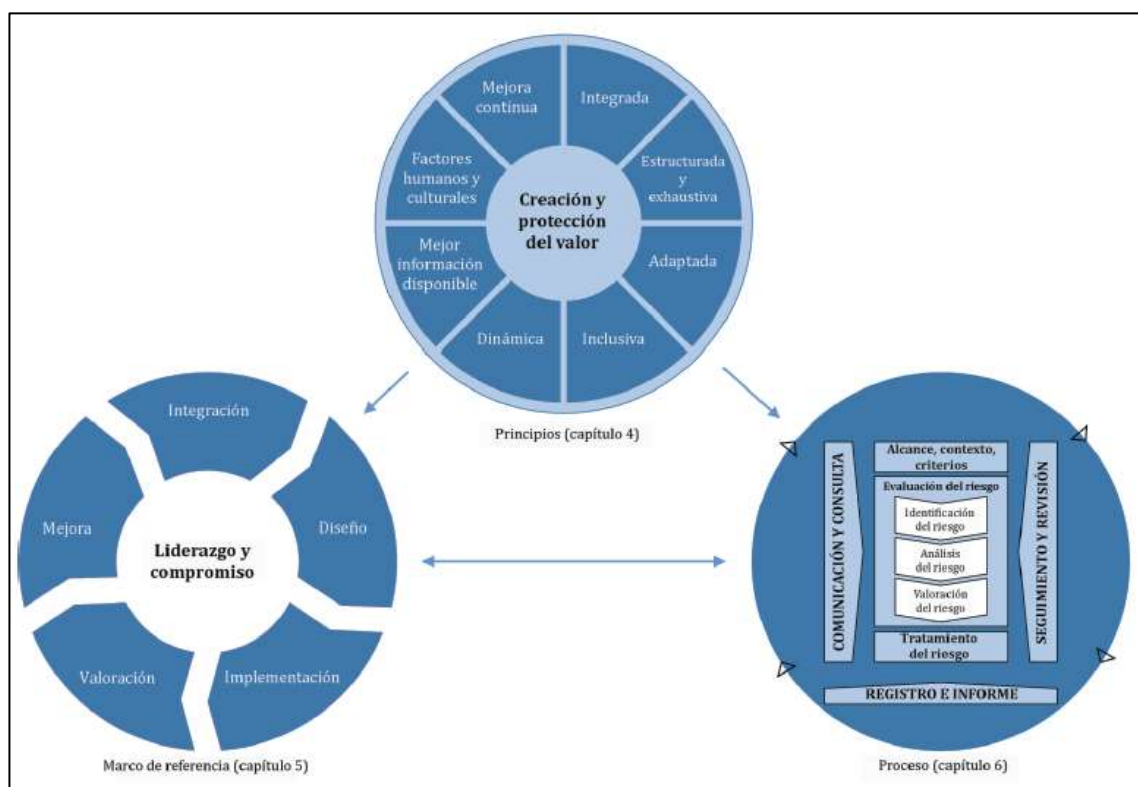


Gráfico n.º 1: Componentes de la ISO 31000:2018-02

Fuente: [30, p. vi]

<sup>2</sup> ISO acrónimo de International Organization for Standardization que en español se traduce como Organización Internacional de Normalización.

Además, esta norma internacional propuso tener en cuenta que el comportamiento humano no tiene naturaleza estática o rígida, sino más bien presenta una naturaleza dinámica. Este hecho complica las labores de gestión de riesgos, en tal sentido el modelo propuesto recoge esta recomendación.

Adicionalmente los procesos descritos en este estándar internacional han sido tomados como base en esta investigación pues fueron incluidos en el estudio comparativo realizado.

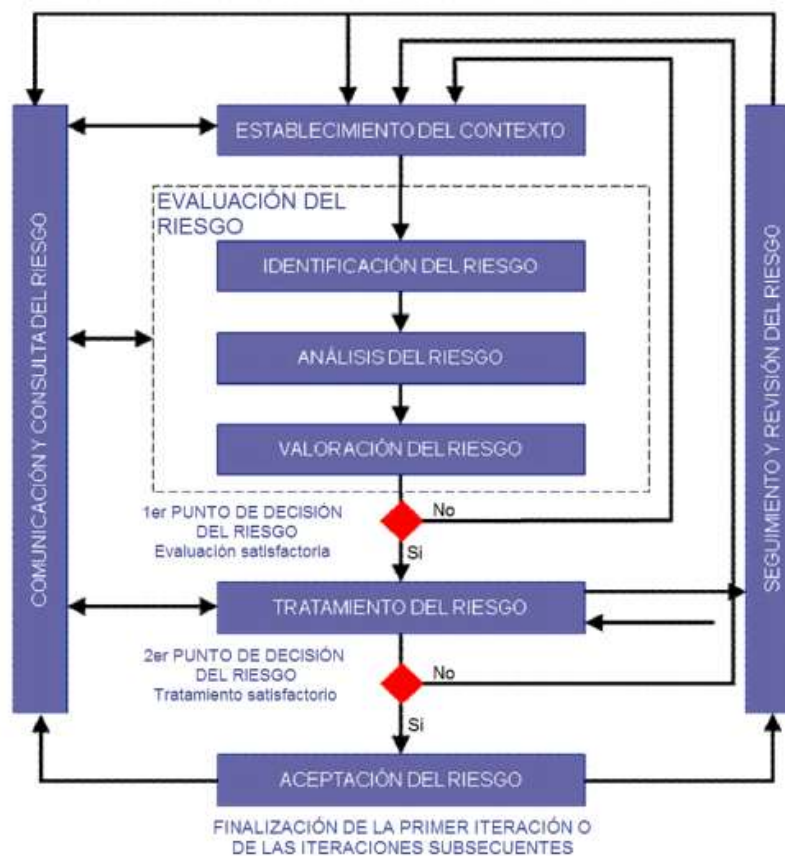
#### **b. ISO/IEC<sup>3</sup> 27005:2018**

Es uno de los documentos de la serie 27 000, que es la serie de estándares que se encuentra enfocada en la seguridad de la información. En este contexto este documento nace como complemento de los otros estándares de la serie; pues tiene como propósito proporcionar las directrices para la GR en el ámbito de seguridad de la información.

El 16 de enero de 2019 mediante Resolución Directoral n.º 047-2018-INACAL/DN se oficializó la “Norma Técnica Peruana NTP-ISO/IEC 27005:2018 Tecnología de la información. Técnicas de seguridad. Gestión de riesgo de la seguridad de la información, 2ª Edición”; la intención de esta norma no es presentar ningún método específico (que indique cómo hacerlo); sino más bien su contribución radica en que nos indica qué hacer cuando se gestionan los riesgos a nivel de seguridad de la información. En el gráfico siguiente se muestra el proceso que sigue esta norma, la cual toma como base lo expuesto en el estándar ISO 31000:2018-02:

---

<sup>3</sup> IEC acrónimo de International Electrotechnical Commission que en español significa Comisión Internacional Electrotécnica.



**Gráfico n.º 2: Fases de la NTP-ISO/IEC 27005:2018-02**

**Fuente:** [36, p. 7].

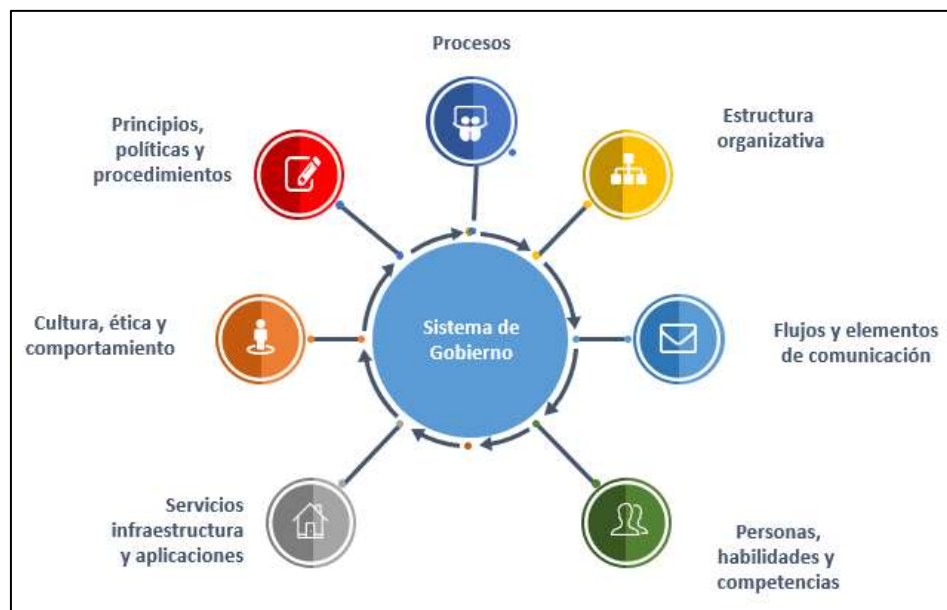
Durante el estudio comparativo realizado en esta investigación también se tomó en consideración los procesos descritos en esta norma internacional.

## **E. Marcos de referencia de gestión de riesgos.**

### **a. Cobit 2019**

Elaborado por Isaca<sup>4</sup>, este marco de trabajo aplica a todo tipo y tamaño de organizaciones y expone un sistema de gobierno de TI que es el punto partida para generar valor. El sistema de gobierno propuesto por Isaca está compuesto por varios componentes dentro de los que incluye:

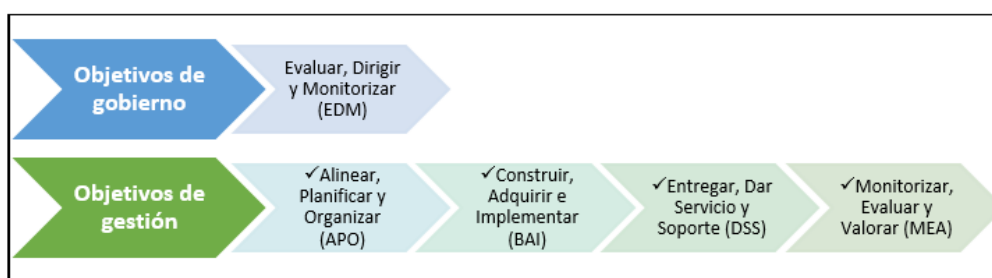
<sup>4</sup> ISACA del inglés Information Systems Audit and Control Association que en español significa Asociación de Auditoría y Control de Sistemas de Información



**Gráfico n.º 3: Componentes de Cobit 2019**

Fuente: Adaptación [35, p. 13]

Es de precisar, que para que el gobierno de TI sea eficiente y eficaz los elementos deben funcionar de manera sincronizada y armónica. Para esto el citado marco de trabajo plantea dos tipos de objetivos uno de gobierno (con un dominio) y otro de gestión (con cuatro dominios), tal como se ilustra a continuación:



**Gráfico n.º 4: Objetivos y dominios del Modelo Cobit 2019**

Fuente: Adaptación [35, p. 12]

Para esta investigación se tomó como referencia un objetivo del dominio “Evaluar, Dirigir y Monitorizar - EDM” y otro del dominio “Alinear, Planificar y Organizar – APO”, así como las prácticas de cada uno de estos objetivos, tal como se muestra en las siguientes gráficas:



**Gráfico n.º 5: Prácticas claves del objetivo de gobierno del riesgo**

**Fuente:** Adaptación [35, p. 43]



**Gráfico n.º 6: Prácticas claves del objetivo de gestión del riesgo**

**Fuente:** Adaptación [35, p. 134]

Debido a que en este documento se trata a la GR - TI como una herramienta para la consecución objetivos a través de la generación o preservación del valor fue tomado en consideración en el estudio comparativo realizado en esta investigación.

### **b. Magerit V 3.0**

Es la sigla del siguiente sintagma nominal: “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información” esta fue formulada por el gobierno español, con la finalidad de reducir los riesgos de la puesta en uso de las TI; esta metodología propone un conjunto de labores que permiten que las instancias de gobierno

puedan tomar decisiones tomando en consideración el riesgo que puede ocasionar el uso de tecnologías de información [37, p. 7]; está compuesta por:

En el libro I – Método, se basa en una secuencia de hechos que inicia con el análisis, seguido de las actividades para la selección de alternativas de tratamiento enfocados en estrategias de seguridad y en los aplicativos informáticos, ya que estos son puntos críticos en las organizaciones; finalmente da una serie de consejos prácticos para realizar estas actividades.

Se precisa, que la metodología propuesta toma en cuenta la aplicación de TI y busca la sensibilización a los responsables de información en relación a la existencia de riesgos asociados a esta, pero sobre todo en la obligación de gestionarlos y finalmente propone mantener los riesgos bajo control en base a su tratamiento oportuno, objetivos descritos en [37, p. 8]:

El libro II – Catálogo de Elementos, propone expresiones homogéneas para ser aplicados durante las labores de análisis de riesgos con la finalidad facilitar la integración de varios equipos [38, p. 6]; en tal sentido este documento nos permite determinar un inventario de elementos donde figuran tipos de activos, sus atributos, sus escalas de estimación, así como sus amenazas y las formas de cómo protegerlos.

En la guía de técnicas Magerit en su versión 3.0 presenta dos capítulos, en el primero explica técnicas específicas para la obtención de resultados: sencillas (como el uso de tablas) o complejas (como el empleo de algoritmos o la aplicación de árboles de ataque). En el segundo capítulo trata de técnicas generales tales como gráficas, sesiones de trabajo y técnicas de valoraciones

Magerit V 3.0 se utilizó durante el proceso de comparación desarrollado en la presente investigación, de allí su importancia.

### c. Octave

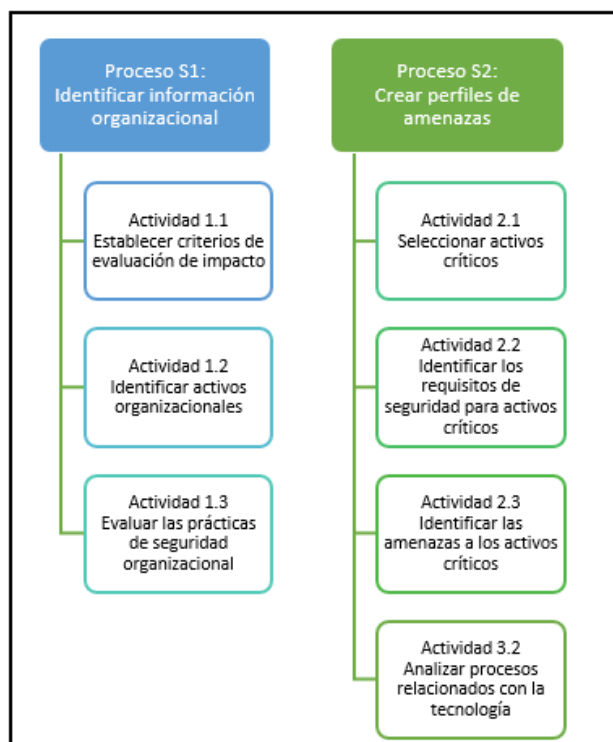
Octave fue desarrollado por el Software Engineering Institute<sup>5</sup> cuyo acrónimo se traduce al español en “Evaluación de Amenazas, Activos y Vulnerabilidades de Operaciones Críticas”. Octave marca la diferencia al enfocarse en cuatro puntos: la evaluación de riesgos de organizaciones; prácticas de seguridad; aspectos estratégicos de protección que no se enfocan únicamente en las debilidades de la infraestructura, sino se orienta en determinar cuáles de ellos son más críticos; además está dirigido por personal de la organización (pero también podría emplear expertos externos como personal de apoyo).

Octave-S es la versión orientada a pequeñas organizaciones, en esta variante de Octave, un grupo de personal multidisciplinario de la organización evalúa los riesgos basados en las prácticas de seguridad con la finalidad de definir las cuestiones estratégicas que conlleven a la protección de la información, para esto emplea tres fases:

La primera consiste en crear perfiles de amenazas basados en activos y se subdivide en dos procesos y siete actividades los cuales se muestran en el siguiente gráfico:

---

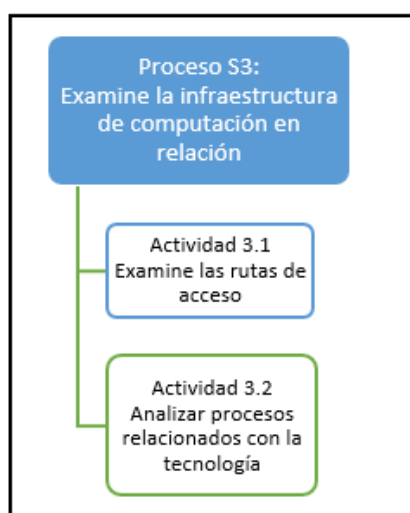
<sup>5</sup> Traducido al español significa Instituto de Ingeniería de Software



**Gráfico n.º 7: Octave – S – Fase 1**

**Fuente:** Adaptación [39, p. 10 a la 30 del Volumen 3]

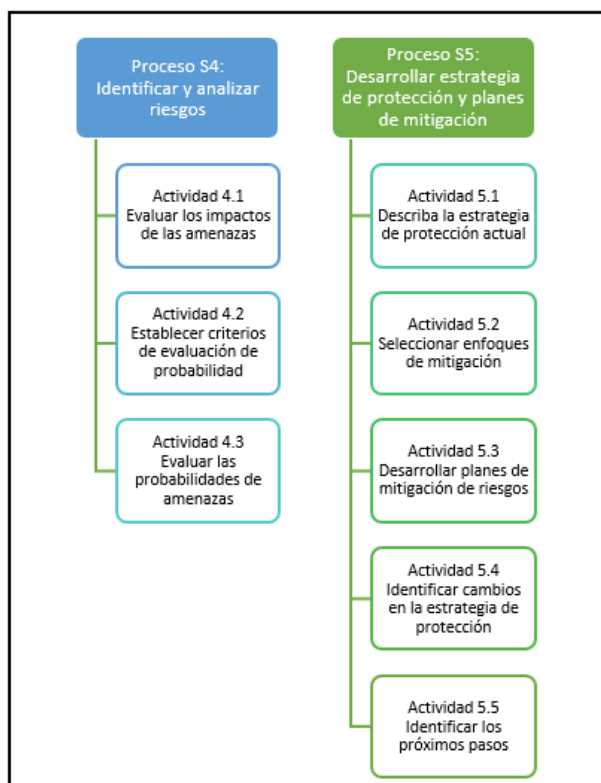
La segunda fase consiste en identificar las vulnerabilidades de infraestructura, basado en identificar cómo las personas usan la infraestructura informática y como logran acceso a los activos sobre todo a los críticos; se subdivide en un proceso y en dos actividades, las cuales son graficadas a continuación:



**Gráfico n.º 8: Octave – S – Fase 2**

**Fuente:** Adaptación [39, p. 31 a la 46 del Volumen 3]

Finalmente, la tercera fase se encarga de definir cuánto impactara la materialización de un riesgo y como desarrollar alternativas de tratamiento; se subdivide en dos procesos y ocho actividades tal como se ilustra a continuación:



**Gráfico n.º 9: Octave – S – Fase 3**

**Fuente:** Adaptación [39, p. 47 al 94 del Volumen 3]

Es de precisar que las hojas de trabajo desarrolladas en los volúmenes 4, 5, 6, 7, 8 y 9 son muy detalladas y han sido adaptadas para ser usadas en la presente investigación.

#### **d. Documentos de la serie NIST SP 800**

En el sitio web <https://csrc.nist.gov/publications/sp800>, a julio de 2020, se puede ubicar 183 documentos de la serie NIST<sup>6</sup> SP<sup>7</sup> 800 de libre descarga, los cuales fueron elaborados por el gobierno estadounidense a través de su Instituto Nacional de Estándares y

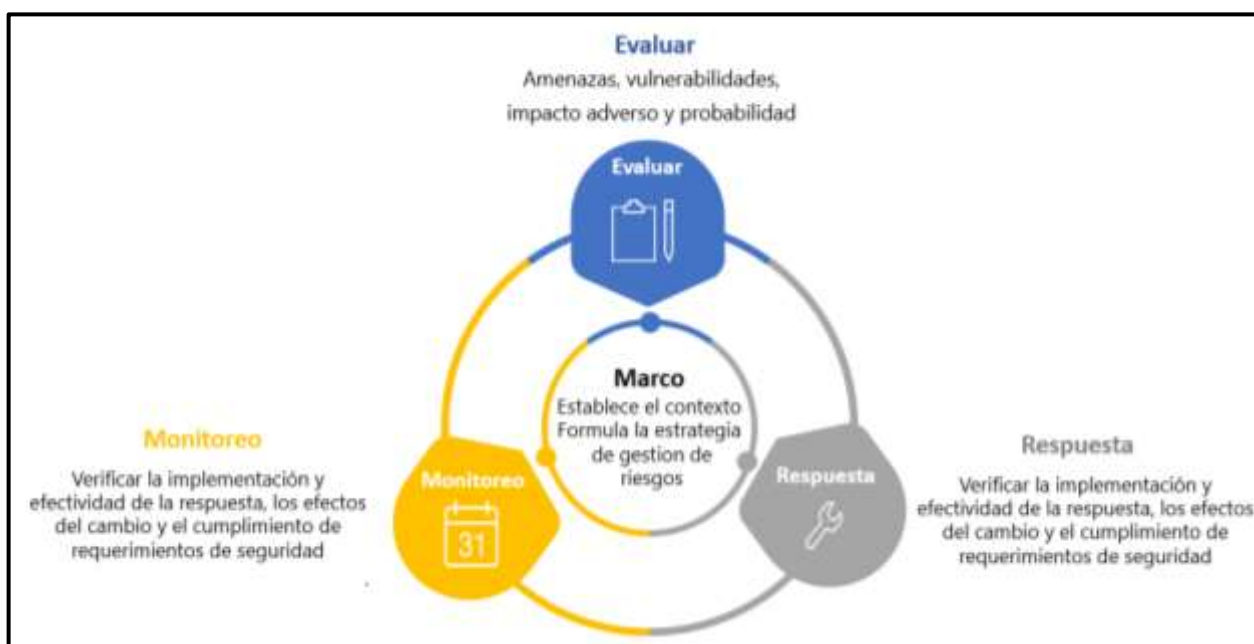
<sup>6</sup> NIST hace referencia a las palabras en inglés “National Institute of Standards and Technology” (que traducido al español significa el “Instituto Nacional de Estándares y Tecnología”)

<sup>7</sup> SP hace referencia a las palabras en inglés “Special Publication” (que traducido al español significa “Publicación Especial”)

Tecnología; en los cuales se exponen políticas, procedimientos y directrices de seguridad informática.

Para la presente investigación durante el proceso de comparación se han utilizado 3 de estos documentos NIST SP 800-30 R1, NIST SP 800-39 y NIST SP 800-53 R5, los cuales se comentan a continuación:

El documento NIST Special Publication 800-30 - Revision 1 Guide for Conducting Risk Assessments (que traducido al español significa “Guía para realizar evaluaciones de riesgos”) fue publicado el 17 de setiembre de 2012 y su propósito es orientar a los responsables de la realización del citado proceso en las labores de preparación, ejecución, respuesta al riesgo, así como las actividades de comunicación y de monitoreo continuo; tal como se grafica:



**Gráfico n.º 10: Evaluación de riesgos según NIST**

**Fuente:** Adaptación [40, p. 4]

El documento NIST Special Publication 800-39 Managing Information Security Risk (que traducido al español significa “Gestionar el riesgo de seguridad de la información”) fue publicado el

3 de enero de 2011; es un documento complementario en el que se detalla los siguientes procesos:



**Gráfico n.º 11: Procesos de la gestión de riesgos según NIST**

**Fuente:** Adaptación [41, pp. E-1]

El borrador del documento NIST Special Publication 800-53 Revision 5 “Security and Privacy Controls for Information Systems and Organizations” (que traducido al español significa “Controles de seguridad y privacidad para organizaciones y sistemas de información”) fue publicado el 16 de marzo de 2020; es un documento complementario en el que figuran 20 familias de controles orientados al cumplimiento de requisitos de seguridad y privacidad que se han definido en las organizaciones y sus sistemas información; a continuación se muestran los 20 familias de controles planteados:

ID	FAMILY	ID	FAMILY
<a href="#">AC</a>	Access Control	<a href="#">PE</a>	Physical and Environmental Protection
<a href="#">AT</a>	Awareness and Training	<a href="#">PL</a>	Planning
<a href="#">AU</a>	Audit and Accountability	<a href="#">PM</a>	Program Management
<a href="#">CA</a>	Assessment, Authorization, and Monitoring	<a href="#">PS</a>	Personnel Security
<a href="#">CM</a>	Configuration Management	<a href="#">PT</a>	PII Processing and Transparency
<a href="#">CP</a>	Contingency Planning	<a href="#">RA</a>	Risk Assessment
<a href="#">IA</a>	Identification and Authentication	<a href="#">SA</a>	System and Services Acquisition
<a href="#">IR</a>	Incident Response	<a href="#">SC</a>	System and Communications Protection
<a href="#">MA</a>	Maintenance	<a href="#">SI</a>	System and Information Integrity
<a href="#">MP</a>	Media Protection	<a href="#">SR</a>	Supply Chain Risk Management

**Gráfico n.º 12: Familias de riesgos propuestos por NIST**

Fuente: [42, p. 8]

De lo expuesto en los literales D y E surge la necesidad de realizar un estudio comparativo, para tal fin utilizaremos la armonización de los documentos comentados en estos literales.

#### **F. Armonización:**

Este término se convierte en la piedra angular de este proyecto de investigación; según la primera acepción del Diccionario la Lengua Española [43] “armonizar es poner en armonía, o hacer que no discuerden o se rechacen dos o más partes de un todo, o dos o más cosas que deben concurrir al mismo fin”; en tal sentido parte de esta investigación estuvo orientada a mapear, comparar y analizar las discrepancias o los posibles puntos en común de los documentos revisados, para que sean integrados. Lo que permitió contar con el modelo deseado y que se pueda generar valor en el control de la corrupción.

#### **G. Generación de valor:**

Significa conseguir beneficios financieros y no financieros, mientras se realiza una distribución de recursos de manera suficiente, adecuada y eficaz, teniendo como base la optimización de la gestión del riesgo; lo que se condice con lo señalado por Isaca cuando se habla de creación de valor:



**Gráfico n.º 13: Resultados de la creación de valor**

**Fuente:** Adaptación [44, p. 11]

## **CAPÍTULO II MATERIALES Y MÉTODOS**

### **2.1. Tipo y nivel de investigación**

Debido a que el desarrollo del presente trabajo exige analizar datos objetivos los cuales orientados a obtener resultados generalizables y que puedan contrastarse y repetirse fue necesario emplear un tipo de investigación cuantitativo.

### **2.2. Diseño de investigación**

Para lograr cumplir con los objetivos de la investigación se empleará una investigación experimental - preprueba/posprueba; orientada en observar y analizar la realidad de los tres (3) gobiernos provinciales de la región de Lambayeque para luego proponer un MGR - TI para la generación de valor en el control de la corrupción en las citadas municipalidades, hecho que pondrá a prueba el planteamiento de la hipótesis.

### **2.3. Población, muestra y muestreo**

#### **2.3.1. Población:**

Está compuesta por tres (3), esto se debe a que son tres (3) las municipalidades provinciales que forman parte de la región de Lambayeque.

### 2.3.2. Muestra y muestreo

Se empleó un muestreo no probabilístico; al respecto se precisa que se seleccionaron como elementos de la muestra a un integrante del Comité de Implementación de Control Interno, un representante del Órgano de Control Institucional y finalmente un representante de la Oficina de Tecnologías de Información, de cada una de las municipalidades.

### 2.4. Criterios de selección

Se ha empleado un muestreo no probabilístico ya que en este caso en particular la selección de la muestra dependerá la experiencia de la persona a cargo de la investigación.

### 2.5. Técnicas e instrumentos de recopilación de datos

Se tomó como base a las técnicas e instrumentos detallados en el siguiente cuadro:

**Cuadro n.º 1:  
Técnicas e instrumentos de recopilación de datos**

N.º	Técnica	Instrumento
1	<b>Lectura analítica</b> Consiste en realizar una lectura que nos permita comprender la información de las metodologías y estándares de riesgos de tecnologías de información	<b>Representaciones gráficas</b> Tales como cuadros sinópticos, mapas mentales entre otros.
2	<b>Observación</b> Es una técnica que nos permite tomar conocimiento de varios aspectos relacionados con los objetivos propuestos.	<b>Lista de cotejo</b> Este instrumento es una tabla de doble entrada ideal para armonizar similitudes y diferencias de las metodologías y estándares de riesgos de TI
3	<b>Entrevistas</b> Nos permitirá obtener información de primera mano, la cual deberá de ser evaluada	<b>Cuestionario</b> Instrumento elaborado con la finalidad de recolectar datos referentes al tema de investigación se elaborarán preguntas las que serán aplicadas a los colaboradores responsables del área de TI, de los gobiernos provinciales de la región de Lambayeque.

## **2.6. Procedimientos**

- Revisión de información: Mediante este procedimiento se pudo examinar los documentos de las municipalidades, así como de los estándares, normas relacionadas a la GR – TI.
- Comparación de información: Este procedimiento nos permitió ver las similitudes y divergencias de los estándares, normas relacionadas a la GR – TI; obteniendo el material necesario para armonizarlos.
- Recolección de datos: El cual permitió el acopio de los datos fiables necesarios para esta investigación.
- Procesamiento y análisis de datos: Los datos recolectados con el procedimiento anterior fueron ordenados y tabulados permitiendo su fácil interpretación.
- Elaboración y revisión del informe: Este procedimiento nos permitió redactar y hacer los ajustes al informe.

## **2.7. Plan de procesamiento y análisis de datos**

Para esta labor, en algunos casos se utilizó el programa estadístico básico, y en otros una hoja de cálculo, con la finalidad de mostrar gráficos relacionados a la investigación realizada.

## **2.8. Consideraciones éticas**

Se obtuvo el consentimiento formal de los gobiernos provinciales, se informó a los responsables de la municipalidad el propósito del estudio, así como se les indicó que se mantuvo en secreto la denominación de las municipalidades y en cuanto a la confidencialidad de la información proporcionada se aclara que la información fue mostrada de manera general.

Del mismo modo, se precisa que la investigación cuidó de la validez y la confiabilidad de la información recogida y procesada.

## CAPÍTULO III RESULTADOS Y DISCUSIÓN

### 3.1. Diagnóstico del sector

Los gobiernos provinciales están orientados a la prestación de servicios públicos [45]; es de precisar que la región de Lambayeque tiene tres municipalidades provinciales: Chiclayo, Lambayeque y Ferreñafe; de las cuales se ha obtenido los documentos de aceptación para el desarrollo de la presente investigación, para mayor detalle revisar el **anexo n.º 1**.

Teniendo en cuenta este concepto y el análisis de la documentación de gestión<sup>8</sup> de las citadas municipalidades, se concluye que las citadas municipalidades son responsables de implementar servicios y proyectos acordes con las necesidades de su colectividad; asimismo la visión de cada una de ellas está fundamentada en la consecución de servicios públicos adecuados y de calidad; respecto a sus principios, estos están orientados a la transparencia, inclusión social y optimización de procesos; así como sus valores están basados en la honestidad e idoneidad; en cuanto a sus objetivos estratégicos resalta el fortalecimiento del gobierno y la gestión de los organismos provinciales; pues TI tiene incidencia directa en su implementación. En cuanto a la ubicación del área de TI o la que haga sus veces, estas no guardan relación entre ellas. Para mayor detalle de la revisión

---

<sup>8</sup> Los documentos de gestión están publicados en el portal web de cada una de las municipalidades provincial de la región de Lambayeque.

documental puede encontrarse en el **anexo n.º 2** donde se ha realizado un resumen comparativo de la información de las tres municipalidades provinciales de la región de Lambayeque.

Es de precisar que, se aplicó un cuestionario al responsable de las áreas de TI o las que hacen sus veces de las tres (03) entidades seleccionadas, con el fin de diagnosticar si las organizaciones cuentan con un MGR - TI; cuyo resultado se observa a continuación:

**Cuadro n.º 2:  
Diagnóstico en las municipalidades provinciales de Lambayeque**

Pregunta	Municipalidad		
	1	2	3
1. ¿Se ha implementado un sistema de gestión de riesgos de TI aplicando algún marco o estándar de trabajo?	No	No	No
2. ¿El Sistema de gestión de riesgos está integrado al gobierno de la municipalidad?	No	No	No
3. ¿Se han asignado roles y responsabilidades al personal respecto a la gestión de riesgos?	No	No	No
4. ¿Se cuenta con un inventario de activos de TI?	Si	Si	Si
5. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?	No	No	No
6. ¿Cuentan con un proceso de análisis de riesgo de TI que permita comprender su naturaleza del riesgo y determinar su nivel?	No	No	No
7. ¿Cuentan con un proceso de valoración de riesgo de TI?	No	No	No
8. ¿Cuentan con un proceso para modificar el nivel de impacto y probabilidad de ocurrencia del riesgo de TI?	No	No	No
9. ¿Existe un equilibrio entre los beneficios y costos de los controles a implementar?	No	No	No
10. ¿Tiene mecanismos de revisiones o supervisiones periódicas de las actividades u operaciones diarias relacionadas a TI?	No	No	No
11. ¿Tiene mecanismos de monitoreo para conocer oportunamente, si las operaciones relacionadas a TI se desarrollan de acuerdo con los procedimientos establecidos en la Municipalidad?	No	No	No
12. ¿Existe un plan de mejora continua de la gestión de riesgos de TI?	No	No	No
13. ¿Se han identificado los riesgos de TI asociados a la corrupción?	No	No	No
14. ¿Se ha cuantificado las pérdidas económicas relacionadas a la materialización de los riesgos de TI asociados a la corrupción?	No	No	No
15. ¿Las partes interesadas son informadas sobre la gestión de riesgos de TI asociados a la corrupción?	No	No	Si
16. ¿Se realiza actividades de monitoreo de los riesgos TI asociados a la corrupción?	No	No	No
17. ¿Tiene mecanismos que permitan identificar acontecimientos potenciales asociados a la corrupción que puedan afectar la ejecución de los procesos de TI con la consecuente afectación del logro de los objetivos institucionales?	No	No	No

**Nota:** Para mayor detalle respecto a la validación del cuestionario, así como a la aplicación de estos, se puede revisar el **anexo n.º 3**

Al respecto, se puede concluir que estas presentan inconvenientes en la GR - TI; dado que en 15 de las 17 interrogantes propuestas los entrevistados señalaron que las actividades a las cuales hacen alusión no se han implementado; es importante precisar, que algunos de los responsables comentaron que ciertas actividades las hacen; pero no siguen un procedimiento establecido, ni tampoco se documentan.

En relación con la interrogante del inventario de activos de TI, se señala que, si bien se constató que cuentan con un inventario de activos, este solo está compuesto del hardware y software de las entidades; sin embargo, este inventario no refleja su valor para las municipalidades.

Del mismo modo, se señala que un representante de una de las municipalidades respondió que las partes interesadas si son informadas sobre la GR - TI asociados a la corrupción (ver anexo n.º 3); sin embargo, la respuesta es cuestionable puesto que si no se tiene identificado los riesgos asociados a la corrupción como estos pueden ser comunicados.

Teniendo en cuenta que la CGR promueve la implementación del Control Interno en las entidades gubernamentales la cual contempla el componente denominado evaluación del riesgo que presenta cuatro principios: definición de los objetivos, gestión de riesgos (identificación, valoración y respuesta al riesgo), evaluación de la probabilidad de fraude en la gestión de riesgos y monitoreo del sistema de control interno; sin embargo, de lo expuesto por los integrantes del Comité de Control Interno en [15, p. 1] y [16, p. 27] y los resultados de aplicar el cuestionario al personal de las áreas de TI (o su equivalente) se constató la falta y la necesidad de contar de un MGR - TI en los citados gobiernos provinciales.

Del mismo modo, de la revisión de la documentación de gestión de las municipalidades, se han identificado que estas tienen los siguientes macroprocesos:



**Gráfico n.º 14: Macroprocesos de las municipalidades**

Estos macroprocesos presentes en los gobiernos provinciales permiten orientar el trabajo del personal en el cumplimiento de los objetivos estratégicos y la satisfacción de las necesidades de los ciudadanos y los actores de la localidad.

### 3.2. Estudio comparativo

Para realizar la propuesta del MGR - TI a los gobiernos provinciales de la región de Lambayeque, se han tomado en cuenta los siguientes estándares internacionales y marcos de referencia:

- Estándares de riesgos
  - A. ISO 31000:2018-02x
  - B. NTP-ISO/IEC 27005:2018-02
- Marcos de referencia:
  - A. Cobit 2019
  - B. Magerit V 3.0
  - C. Octave-S V1.0
  - D. NIST SP 800-30 R1, NIST SP 800-39 y NIST SP 800-53 R5

En el siguiente cuadro se muestra un análisis comparativo a nivel macro de las normas antes descritas:

**Cuadro n.º 3:  
Comparación a nivel macro**

Estándares, marcos de referencia o guías	Organización	País	Acceso a la documentación	Detalle	Importancia
<b>ISO 31000:2018-02</b>	Organización de estándares internacionales – ISO.	Suiza	Restringido	Estándar internacional involucra el trabajo con las buenas prácticas en la GR.	Estándar orientado a la creación o protección del valor y realización de objetivos. Se suma a la gobernanza de las entidades. Señala qué hacer. Indica que se debe tener en cuenta que el ser humano no tiene una naturaleza estática sino dinámica.
<b>NTP-ISO/IEC 27005:2018-02</b>	Organización de estándares internacionales – ISO.  Comisión Internacional Electrotécnica - IEC	Versión peruana	Restringido	Es uno de los documentos de la serie 27 000, que es la serie de estándares que se encuentra enfocada en la seguridad de la información. Se trabajo con la NTP-ISO/IEC 27005:2018-02.	Señala qué hacer. Agrega al estándar anterior puntos de decisión antes y después del tratamiento de riesgo. Enfocada en la seguridad de la información.
<b>Cobit 2019</b>	Isaca.	Estados Unidos	Restringido	Marco de referencia Cobit® 2019.	Elaborado por Isaca, este marco de trabajo aplica a todo tipo y tamaño de organizaciones y expone un sistema de gobierno de TI que es el punto partida para generar valor. Este marco de referencia en cuanto a la gestión de riesgos tiene dos componentes relacionados, uno de gobierno y otro de gestión: el <b>EDM03</b> - Asegurar la optimización del riesgo y el <b>APO12</b> - Gestionar el riesgo.
<b>Magerit V 3.0</b>	Consejo Superior de Administración Electrónica del Gobierno de España.	España	Público	Metodología de análisis y gestión de riesgos de los sistemas de información.	Finalidad de reducir los riesgos relacionado a la implementación de las TI; esta metodología propone un conjunto de labores orientadas a que las instancias de gobierno puedan tomar decisiones teniendo en consideración que el uso de tecnologías de información puede ocasionar riesgos.
<b>Octave-S V1.0</b>	Instituto de ingeniería de software de la Universidad Carnegie Mellon	Estados Unidos	Público	Evaluación de Amenazas, Activos y Vulnerabilidades de Operaciones Críticas.	Octave-S es la versión orientada a pequeñas organizaciones, en esta variante de Octave un grupo de personal multidisciplinario de la organización evalúa los riesgos basados en las prácticas de seguridad con la finalidad de definir las cuestiones estratégicas que conlleven a la protección de la información.
<b>NIST 800</b>	Instituto Nacional de Estándares y Tecnología de Estados Unidos.	Estados Unidos	Público	<b>NIST 800-30 R1:</b> Guía de Gestión de riesgos para sistemas de tecnologías de Información.	Su propósito es orientar a los responsables de la realización del citado proceso en las labores de preparación, ejecución, respuesta al riesgo, así como las actividades de comunicación y de monitoreo continuo.  Documento complementario de cuatro fases: marco de riesgo, evaluación, respuesta y

Estándares, marcos de referencia o guías	Organización	País	Acceso a la documentación	Detalle	Importancia
				<p><b>NIST 800-39:</b> Gestión del riesgo de seguridad de la información.</p> <p><b>NIST 800-53 R5:</b> Controles de seguridad y privacidad para organizaciones federales de sistemas e información.</p>	<p>monitoreo; los cuales orientan las labores de gestión del riesgo de seguridad de la información</p> <p>Documento complementario en el que figuran 20 familias de controles orientados al cumplimiento de requisitos de seguridad y privacidad que se han definido en las organizaciones y sus sistemas información</p>

**Fuente:** [30], [36], [35], [37], [38], [39], [40], [41] y [42].

En los párrafos siguientes, se muestra el estudio comparativo realizado entre los marcos de referencia y los estándares internacionales antes mencionados tomando como base las fases estipuladas en el ISO 31000:2018-02:

**a. Comunicación y consulta:**

Esta fase es uno de los tres componentes transversales que presenta el estándar. El propósito de esta fase es mantener informadas a las partes interesadas de las organizaciones, lo que se busca es que la comunicación se convierta en un catalizador en la toma de conciencia y en el entendimiento del riesgo por parte del personal.

En cuanto a la consulta está orientada a adquirir los aspectos de retroalimentación que nos ayuden a mejorar los aspectos de la gestión de riesgos a aplicar. Tanto para la comunicación como para la consulta la información deberá estar basada en hechos, oportunos, pertinentes, exactos y comprensibles.

En el siguiente cuadro se muestra en mayor detalle los aspectos comparados:

**Cuadro n.º 4:  
Análisis comparativo - fase de comunicación y consulta**

Comunicación y consulta			
Estándares, marcos de referencia	Aporte	Referencia	Nivel de aporte <sup>9</sup>
ISO 31000:2018-02	6.2 Comunicación y consulta	Página 11	Base
NTP-ISO/IEC 27005:2018-02	11. Comunicación y consulta del riesgo de seguridad de la información	Página 38	Media
Cobit 2019	EDM03.02 Actividad 2. Dirigir el desarrollo de planes de comunicación de riesgos  Comunicar de manera oportuna es fundamental pues permitirá tomar alguna decisión respecto a la identificación de alguna desviación.	<b>EDM03.02</b> Actividad 2 Página 42  <b>APO12.04</b> Articular el riesgo.	Alta
Magerit V3	4.2.6. Comunicación y consulta 5.4. PAR.3 – Comunicación de resultados	Página 59 Página 71 <b>del Libro I</b>	Alta
Octave-S V1.0	No se ubicó información relacionada	-----	Ninguno
NIST 800	3.3 Comunicación y compartir información de evaluación de riesgos	Página 37 del <b>NIST 800-30 R1</b>	Alta

**Fuente:** [30], [36], [35], [37], [38], [39] y [40].

#### **b. Alcance, contexto y criterios:**

Al respecto, en la ISO 31000:2018-02 se señala que es importante determinar el alcance, recordemos que la GR - TI puede ser aplicada a toda la organización o algunos procesos de ella, así mismo es importante el análisis de los elementos característicos que determinan la identidad de las instituciones tanto a nivel interno con externo, así como la determinación a priori de los criterios a aplicar; a esto la NTP-ISO/IEC 27005:2018-02 añade que se deber realizar una lista de restricciones que puedan afectar a las entidades.

Es importante mencionar que tanto COBTI 2019, MAGERIT V 3.0 y OCTAV-S V1.0 presentan una amplia variedad de criterios, los cuales serán expuestos a los representantes de las entidades para que se seleccionen los más indicados.

<sup>9</sup> Nivel de aporte tiene los valores

**Alto** cuando aporta más de dos factores importantes.

**Medio** cuando aporta hasta dos factores importantes.

**Similar** cuando no hay aporte.

**Ninguno** cuando no lo considera.

**Base** Estándar tomado como línea base.

En el siguiente cuadro se muestra en mayor detalle los aspectos comparados:

**Cuadro n.º 5:**  
**Análisis comparativo - fase de alcance, contexto y criterios**

Alcance, contexto y criterios			
Estándares, marcos de trabajo o guías	Aporte	Referencia	Nivel de aporte
<b>ISO 31000:2018-02</b>	5.4.1 Comprensión de la organización y de su contexto 6.3 Alcance, contexto y criterios 6.3.1 Generalidades 6.3.2 Definición del alcance 6.3.3 Contextos externo e interno 6.3.4 Definición de los criterios del riesgo	Página 6 Página 11 Página 11 Página 11 Página 12 Página 12	Base
<b>NTP-ISO/IEC 27005:2018-02</b>	7 Establecimiento el contexto 7.1 Consideraciones generales 7.3 El alcance y los límites 7.2 Criterios básicos 7.2.1 Enfoque de la gestión de riesgo 7.2.2 Criterio de valoración del riesgo 7.2.3 Criterios de impacto 7.2.4 Criterios de aceptación del riesgo 7.3 El alcance y los límites ANEXO A (INFORMATIVO) Definición del alcance y límites del proceso de gestión de riesgos de seguridad de la información ANEXO F (INFORMATIVO) Restricciones para la modificación del riesgo	Página 10 Página 10 Página 14 Página 11 Página 11 Página 11 Página 12 Página 12 Página 12 Página 14 Página 45  Página 88	Alta
<b>Cobit 2019</b>	Conocer la organización y su contexto en relación al riesgo de TI (actividad 1)  Define tres criterios de calidad principales para la información y 15 sub criterios	<b>EDM03.01</b> Evaluar la gestión de riesgos  <b>Páginas 41 y 42</b> Libro Introducción y metodología	Media
<b>Magerit V 3.0</b>	1.6. El análisis y el tratamiento de los riesgos en su contexto 4.2.2. Contexto 4.2.3. Criterios 7.2.2. Contexto  3. Dimensiones de valoración 4. Criterios de valoración	Página 10  Página 57 Página 57 Página 80 <b>del Libro I</b>  Página 15 Página 19 <b>del Libro II</b>	Alta
<b>Octave-S V1.0</b>	Proceso S1: Identificar información organizacional S1.1 Establecer criterios de evaluación de impacto  S1.3 Evaluar las prácticas de seguridad organizacional  Proceso S4: Identificar y analizar riesgos S4.2 Establecer criterios de evaluación de probabilidad	Página 11  Página 15  Página 53  <b>del Volumen 3</b>	Alta
<b>NIST 800</b>	2.1 Proceso de gestión de riesgos	Página 4 <b>del NIST 800-30 R1</b>	Medio

**Fuente:** [30], [36], [35], [37], [38], [39] y [40].

**c. Evaluación del riesgo.****i. Identificación del riesgo.**

Basados en la determinación del alcance, contexto y criterios realizados en la fase anterior se procede a la de determinación de los riesgos que pueden impactar negativamente en el cumplimiento misional de las organizaciones.

Es de recalcar que esta tarea no consiste en tan solo realizar un listado de activos, amenazas, vulnerabilidades y controles; sino debe estar abocada a detallar su valor e impacto en las actividades clave de las organizaciones.

En el siguiente cuadro se muestra en mayor detalle los aspectos comparados:

**Cuadro n.º 6:  
Análisis comparativo - fase de identificación del riesgo**

<b>Identificación del riesgo</b>			
<b>Estándares, marcos de referencia</b>	<b>Aporte</b>	<b>Referencia</b>	<b>Nivel de aporte</b>
<b>ISO 31000:2018-02</b>	6.4.2 Identificación del riesgo	Página 13	Base
<b>NTP-ISO/IEC 27005:2018-02</b>	8.2 Identificación de riesgos 8.2.1 Introducción a la identificación de riesgos 8.2.2 Identificación de activos 8.2.3 Identificación de las amenazas 8.2.4 Identificación de controles existentes 8.2.5 Identificación de vulnerabilidades 8.2.6 Identificación de consecuencias ANEXO B (INFORMATIVO) Identificación y evaluación de activos y evaluación de impacto ANEXO C (INFORMATIVO) Ejemplos de amenazas típicas ANEXO D (INFORMATIVO) Vulnerabilidades y métodos para evaluación de vulnerabilidades	Página 17 Página 17 Página 18 Página 19 Página 20 Página 21 Página 23 Página 53  Página 68 Página 71	Alta
<b>Cobit 2019</b>	Identificar y recopilar información con la finalidad de realizar una óptima labor de análisis y reporte de los riesgos de TI.  Mantener un inventario de los riesgos conocidos y los atributos de riesgo, incluidos la frecuencia esperada, impacto potencial y respuestas.	<b>APO12.01</b> Recopilar datos  <b>APO12.03</b> Mantener un perfil de riesgo	Media
<b>Magerit V 3.0</b>	3.1.1. Paso 1: Activos 3.2.1. Tarea MAR.1: Caracterización de los activos 8.2. Consejos prácticos: Para identificar activo 8.3. Consejos prácticos: Para descubrir y modelar las dependencias entre activos  2. Tipos de activos 5. Amenazas 6. Salvaguardas	Página 22 Página 37 Página 87 Página 88 <b>del Libro I</b>  Página 7 Página 25 Página 53 <b>del Libro II</b>	Media
<b>Octave-S V1.0</b>	Proceso S1: Identificar información organizacional S1.2 Identificar activos organizacionales  Proceso S2: Crear perfiles de amenazas S2.1 Seleccionar activos críticos S2.2 Identificar los requisitos de seguridad para activos críticos S2.3 Identificar las amenazas a los activos críticos	Página 13   Página 21 Página 23 Página 25  <b>del Volumen 3</b>	Alta
<b>NIST 800</b>	Paso 2: Evaluación de conducta Identificar fuentes y eventos de amenazas Identificar vulnerabilidades y condiciones predisponentes  Apéndice D Fuentes de amenaza Apéndice E Eventos de amenaza Apéndice F Vulnerabilidades y condiciones predisponentes	PROCESO DE EVALUACIÓN DE RIESGOS   Página D-1 Página E-1 Página F-1 <b>del NIST 800-30 R1</b>	Alta

**Fuente:** [30], [36], [35], [37], [38], [39] y [40].

## ii. Análisis del riesgo.

La ejecución del análisis del riesgo está orientada en entender al riesgo en toda su extensión. El personal a cargo de realizar esta labor determinará el grado de detalle y complejidad, el cual dependerá del alcance, contexto y criterios que se hayan propuesto inicialmente.

Es importante resaltar que MAGERIT V 3.0 en su “Libro III - Guía de Técnicas” detalla varias técnicas que podrían ser aprovechadas en esta labor.

En el siguiente cuadro se muestra en mayor detalle los aspectos comparados:

**Cuadro n.º 7:**  
**Análisis comparativo - fase de análisis del riesgo**

Análisis del riesgo			
Estándares, marcos de referencia	Aporte	Referencia	Nivel de aporte
<b>ISO 31000:2018-02</b>	6.4.3 Análisis del riesgo	Página 13	Base
<b>NTP-ISO/IEC 27005:2018-02</b>	8.3 Análisis de riesgos 8.3.1 Metodologías de análisis de riesgos 8.3.2 Evaluación de consecuencias 8.3.3 Evaluación de probabilidad de incidentes 8.3.4 Determinación del nivel de riesgos ANEXO E (INFORMATIVO) Enfoques a la evaluación de riesgos de seguridad de la información	Página 24 Página 24 Página 25 Página 27 Página 29 Página 78	Media
<b>Cobit 2019</b>	Actividades orientadas al análisis del riesgo de TI, que sirvan de apoyo a la toma de decisiones.	<b>APO12.02</b> Analizar el riesgo.	Media
<b>Magerit V 3.0</b>	3. Método de análisis de riesgos 5. Proyectos de análisis de riesgos 5.3. PAR.2 – Elaboración del análisis de riesgos 7.2.7. Operación: análisis y gestión dinámicos 7.2.8. Ciclos de mantenimiento: análisis marginal  Guía de Técnicas	Página 22 Página 62 Página 70 Página 83 Página 83 <b>del Libro I</b>  <b>Libro III</b>	Alta
<b>Octave-S V1.0</b>	Proceso S3: Examinar la infraestructura de computación relacionada a los activos críticos S3.1 Examinar las rutas de acceso S3.2 Analizar la tecnología relacionada a los procesos  Proceso S4: Identificar y analizar riesgos S4.1 Evaluar los impactos de las amenazas S4.3 Evaluar las probabilidades de amenazas	Página 33 Página 41  Página 49 Página 57  <b>del Volumen 3</b>	Alta
<b>NIST 800</b>	2.3.3 Enfoque de análisis 3.1 Preparación para la evaluación de riesgos 3.2 Realización de la evaluación de riesgos Apéndice G probabilidad de ocurrencia Apéndice H impacto Apéndice I determinación del riesgo	Página 15 Página 24 Página 29 Página G-1 Página H-1 Página I-1 <b>del NIST 800-30 R1</b>	Alta

Fuente: [30], [36], [35], [37], [38], [39] y [40].

### iii. Valoración del riesgo.

Esta fase tiene como finalidad apoyar a los órganos de gobierno a tomar decisiones; es importante no perder de vista que las actividades de esta fase están enfocadas en contrastar sus niveles de riesgo contra sus criterios (tanto de valoración como de aceptación).

En el siguiente cuadro se muestra en mayor detalle los aspectos comparados:

**Cuadro n.º 8:  
Análisis comparativo - fase de valoración del riesgo**

Valoración del riesgo			
Estándares, marcos de referencia	Aporte	Referencia	Nivel de aporte
<b>ISO 31000:2018-02</b>	6.4.4 Valoración del riesgo	Página 14	Base
<b>NTP-ISO/IEC 27005:2018-02</b>	8.4 Valoración de riesgos	Página 29	Media
<b>Cobit 2019</b>	Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	<b>APO12.05</b> Definir un portafolio con acciones de gestión de riesgos.	Media
<b>Magerit V 3.0</b>	4.1.1. Evaluación: interpretación de los valores de impacto y riesgo residuales 4.2.4. Evaluación de los riesgos Apéndice 4. Marco de evaluación y certificación  Guía de técnicas	Página 48 Página 58 Página 114 <b>del Libro I</b>  <b>Libro III</b>	Alta
<b>Octave-S V1.0</b>	Proceso S5: Desarrollar estrategia de protección y planes de mitigación S5.5 Identificar los próximos pasos	Página 93  <b>del Volumen 3</b>	Alta
<b>NIST 800</b>	3.1 Enfocando el riesgo Tarea 1 Suposiciones De Riesgo Tarea 2 Restricciones de riesgo Tarea 3 Tolerancia al riesgo Tarea 4 Prioridades y compensación  3.3 Evaluando el riesgo Tarea 1 identificación de amenaza y vulnerabilidad Tarea 2 determinación de riesgos	Página 33 del <b>NIST 800-39</b>  Página 37 del <b>NIST 800-39</b>	Alta

**Fuente:** [30], [36], [35], [37], [38], [39] y [41].

### d. Tratamiento del riesgo.

Esta fase tiene como intención responder de manera oportuna a eventos de riesgo materializados con medidas eficaces para limitar la magnitud de las pérdidas de las organizaciones.

Las actividades por realizar nos permitirán elegir las alternativas que mejor se adapten al tratamiento del riesgo también tomando en consideración el marco regulatorio de las organizaciones y no tan solo centrarse en la comparación entre los potenciales beneficios y el dinero que se tenga que invertir para su puesta en marcha.

También es importante precisar los aportes desarrollados en MAGERIT V 3.0 y OCTAVE-S V1.0 los cuales permiten ejecutar dicha fase.

En el siguiente cuadro se muestra en mayor detalle los aspectos comparados:

**Cuadro n.º 9:  
Análisis comparativo - fase de tratamiento del riesgo**

Tratamiento del riesgo			
Estándares, marcos de referencia	Aporte	Referencia	Nivel de aporte
<b>ISO 31000:2018-02</b>	6.5 Tratamiento del riesgo 6.5.1 Generalidades 6.5.2 Selección de las opciones para el tratamiento del riesgo 6.5.3 Preparación e implementación de los planes de tratamiento del riesgo	Página 15 Página 15 Página 15 Página 16	Base
<b>NTP-ISO/IEC 27005:2018-02</b>	9 Tratamiento del riesgo de seguridad de la información 9.1 Descripción general del tratamiento de riesgos 9.2 Modificación de riesgos 9.3 Retención de riesgos 9.4 Evitar el riesgo 9.5 Compartir el riesgo	Página 30 Página 30 Página 34 Página 36 Página 36 Página 37	Media
<b>Cobit 2019</b>	Responder de manera oportuna a eventos de riesgo materializados con medidas eficaces para limitar la magnitud de las pérdidas.	<b>APO12.06</b> Responder al riesgo.	Media
<b>Magerit V 3.0</b>	4.1.2. Aceptación del riesgo 4.1.3. Tratamiento 4.1.4. Estudio cuantitativo de costes / beneficios 4.1.5. Estudio cualitativo de costes / beneficios 4.1.6. Estudio mixto de costes / beneficios 4.1.7. Opciones de tratamiento del riesgo: eliminación 4.1.8. Opciones de tratamiento del riesgo: mitigación 4.1.9. Opciones de tratamiento del riesgo: compartición 4.1.10. Opciones de tratamiento del riesgo: financiación 4.2.5. Decisión de tratamiento  Guía de técnicas	Página 49 Página 49 Página 50 Página 53 Página 53 Página 53 Página 53 Página 54 Página 54 Página 58 <b>del Libro I</b>  <b>Libro III</b>	Alta
<b>Octave-S V1.0</b>	Proceso S5: Desarrollar estrategia de protección y planes de mitigación S5.1 Describa la estrategia de protección actual S5.2 Seleccionar enfoques de mitigación S5.3 Desarrollar planes de mitigación de riesgos S5.4 Identificar cambios en la estrategia de protección S5.5 Identificar los próximos pasos	Página 63 Página 75 Página 83 Página 87 Página 93  <b>del Volumen 3</b>	Alta

Tratamiento del riesgo			
Estándares, marcos de referencia	Aporte	Referencia	Nivel de aporte
<b>NIST 800</b>	Apéndice J respuesta de riesgo informativo  3.3 Respondiendo al riesgo Tarea 1 identificación de respuesta al riesgo Tarea 2 evaluación de alternativas Tarea 3 decisión de respuesta al riesgo Tarea 4 implementación de respuesta al riesgo  Controles de seguridad y privacidad para organizaciones federales de sistemas e información	Página J-1 del <b>NIST 800-30 R1</b>  Página 41 del <b>NIST 800-39</b>  <b>NIST 800-53 R5</b>	Alta

**Fuente:** [30], [36], [35], [37], [38], [39], [40], [41] y [42].

#### e. Seguimiento y revisión.

Este es el segundo componente transversal de los tres propuestos por el estándar, el cual tiene como finalidad advertir desviaciones o los problemas en la aplicación de este estándar, con la finalidad de corregir las brechas y asegurar el óptimo rendimiento del proceso.

En el siguiente cuadro se muestra en mayor detalle los aspectos comparados:

**Cuadro n.º 10:**  
**Análisis comparativo - fase de seguimiento y revisión**

Seguimiento y revisión			
Estándares, marcos de referencia	Aporte	Referencia	Nivel de aporte
<b>ISO 31000:2018-02</b>	6.6 Seguimiento y revisión	Página 16	Base
<b>NTP-ISO/IEC 27005:2018-02</b>	12 Seguimiento y revisión del riesgo de seguridad de la información 12.1 Seguimiento y revisión de los factores de riesgos 12.2 Seguimiento, revisión y mejora de la gestión de riesgos	Página 40 Página 40 Página 42	Alta
<b>Cobit 2019</b>	En cuenta al uso de TI examina periódicamente el efecto del riesgo; así como evalúa si el apetito al riesgo de la organización es adecuado, con la finalidad de obtener valor.  Revisa si las prácticas de GR-TI son adecuadas y si los riesgos de TI están por debajo de lo estipulado por las organizaciones (apetito de riesgo).  Revisa las metas y las métricas clave de los procesos de GR-TI. Determina las variaciones de lo real contra lo planificado, de ser el caso se procede a un reajuste	<b>EDM03.01</b> Evaluar la gestión de riesgos.  <b>EDM03.02</b> Dirigir la gestión de riesgos.  <b>EDM03.03</b> Monitorizar la gestión de riesgos.	Media
<b>Magerit V 3.0</b>	4.2.7. Seguimiento y revisión	Página 59 <b>del Libro I</b>	Alta
<b>Octave-S V1.0</b>	No se ubicó información relacionada		Ninguno
<b>NIST 800</b>	3.4 Mantenimiento de la evaluación de riesgos  3.4 Monitoreando el riesgo Tarea 1 Estrategia de monitoreo de riesgos Tarea 2 Monitoreo de riesgos	Página 38 <b>del NIST 800-30 R1</b>  Página 45 <b>del NIST 800-39</b>	Alta

**Fuente:** [30], [36], [35], [37], [38], [39], [40] y [41].

#### **f. Registro e informe.**

Este es tercer componente transversal que presenta el estándar, las actividades realizadas están abocadas a la documentación de cada una de las fases. Es importante precisar que tanto MAGERIT V 3.0 como OCTAVE-S V1.0 indican cómo el personal a cargo puede desarrollar esta labor.

En el siguiente cuadro se muestra en mayor detalle los aspectos comparados:

**Cuadro n.º 11:  
Análisis comparativo - fase de registro e informe**

<b>Registro e informe</b>			
<b>Estándares, marcos de referencia</b>	<b>Aporte</b>	<b>Referencia</b>	<b>Nivel de aporte</b>
<b>ISO 31000:2018-02</b>	6.7 Registro e informe	Página 17	Base
<b>NTP-ISO/IEC 27005:2018-02</b>	11. Comunicación y consulta del riesgo de seguridad de la información	Página 38	Media
<b>Cobit 2019</b>	Documentar los recursos, capacidades y actividades de control actuales relacionados con elementos de riesgo.	<b>APO12.03</b> Mantener un perfil de riesgo.	Alta
<b>Magerit V 3.0</b>	Apéndice 4. Informes	Página 72 <b>del Libro II</b>	Alta
<b>Octave-S V1.0</b>	<p>Documente los elementos de acción identificados durante el Proceso S1.  Documente los elementos de acción identificados durante el Proceso S2.  Documente los elementos de acción identificados durante el Proceso S3.  Documente los elementos de acción identificados en el Proceso S4.  Documente los elementos de acción identificados en el Proceso S5.</p> <p>Documente las notas y recomendaciones identificadas durante el Proceso S1.  Documente las notas y recomendaciones identificadas durante el Proceso S2.  Documente las notas y recomendaciones identificadas durante el Proceso S3.  Documente las notas y recomendaciones identificadas en el Proceso S4.</p>	<p>Volumen 9: Lista de acciones</p> <p>Volumen 9: Notas y recomendaciones</p>	Alta
<b>NIST 800</b>	Apéndice K informes de evaluación de riesgos	Página K-1 del <b>NIST 800-30 R1</b>	Alta

**Fuente:** [30], [36], [35], [37], [38], [39] y [40].

### 3.3. Propuesta de modelo.

En el gráfico siguiente podemos apreciar las fases del MGR - TI propuesto:



**Gráfico n.º 15: Fases del modelo propuesto**

El desarrollo de las fases del modelo propuesto seguirá el esquema presentado en el siguiente cuadro:

**Cuadro n.º 12:  
Cuadro presentación de los pasos del modelo propuesto**

Nombre de la etapa		Código
Concepto		
Entradas	Salidas	
Actividades específicas		
Formatos		

**Cuadro n.º 13:  
Fase 1: Actividades preliminares**

Nombre de la etapa		Código
ACTIVIDADES PRELIMINARES		P-1
Concepto		
Esta fase del modelo propuesto consiste en determinar el equipo que estará a cargo de la puesta en marcha del MGR-TI y cuáles será la forma de comunicación.		
Entradas	Salidas	
i. Cuadro de asignación de personal. ii. Resoluciones de designación de personal. iii. Informe de seguimiento y revisión.	i. Documento de conformación del equipo. ii. Matriz de comunicación. iii. Actualización de documentos	
Actividades específicas		
1. Conformación del equipo y asignación de roles por actividades. 2. Definir la matriz de comunicación. 3. Documentar y comunicar el trabajo realizado. 4. De ser el caso actualizar y comunicar los documentos.		
Formatos		
F-1 Formato del documento de conformación del equipo y asignación de responsabilidades por actividades. F-2 Formato movimiento de personal. F-3 Formato de la matriz de comunicación.		

**Cuadro n.º 14:**  
**Fase 2: Contexto, alcance y criterios**

Nombre de la fase		Código
CONTEXTO, ALCANCE Y CRITERIO		P-2
Concepto		
<p>Determinar los factores internos como externos de los gobiernos provinciales de la región de Lambayeque relevante para el MGRT -TI.</p> <p>Aquí también se fija el alcance para el MGR - TI, teniendo en consideración que se quiere abarcar: estrategias, operaciones, entre otras de menor complejidad; sin perder de vista las restricciones establecidas por la regulación que norma la operatividad de estas instituciones del sector público.</p> <p>Del mismo modo en esta fase las municipalidades provinciales deberán precisar el nivel de riesgo considerado como aceptable; así como, las pautas para evaluar cuán importante puede ser el riesgo tomando en consideración las ideas rectoras de las entidades y su disponibilidad de recursos.</p>		
Entradas	Salidas	
<ul style="list-style-type: none"> <li>i. Reglamento de organización y funciones (ROF).</li> <li>ii. Manual de organización y funciones (MOF).</li> <li>iii. Plan Estratégico.</li> <li>iv. Plan estratégico de gobierno electrónico.</li> <li>v. Cuadro de asignación de personal (CAP).</li> <li>vi. Organigrama.</li> <li>vii. Entrevistas.</li> <li>viii. Informe de seguimiento y revisión.</li> </ul>	<ul style="list-style-type: none"> <li>i. Documento de análisis del contexto interno y externo</li> <li>ii. Documento de establecimiento del alcance.</li> <li>iii. Documento de establecimiento de criterios.</li> <li>iv. Registro de documentos actualizados.</li> </ul>	
Actividades específicas		
<ul style="list-style-type: none"> <li>1. Determinar el contexto.</li> <li>2. Determinar el alcance.</li> <li>3. Determinar los criterios.</li> <li>4. Documentar y comunicar el trabajo realizado.</li> <li>5. De ser el caso actualizar y comunicar los documentos.</li> </ul>		
Formatos y repositorios		
<ul style="list-style-type: none"> <li>F-4 Formato de determinación de contexto.</li> <li>F-5 Formato de alcance.</li> <li>F-6 Formato de criterios y dimensiones</li> </ul>	<ul style="list-style-type: none"> <li>R-1 Repositorio de base legal aplicable a los gobiernos provinciales.</li> <li>R-2 Repositorio de restricciones.</li> <li>R-3 Repositorio de dimensiones y criterios.</li> </ul>	

**Cuadro n.º 15:**  
**Fase 3: Evaluación del riesgo - Identificación del riesgo**

Nombre de la sub fase	Código
IDENTIFICACIÓN DEL RIESGO	P-3.1
Concepto	
<p>La finalidad de esta fase es determinar los activos críticos, amenazas, vulnerabilidades, controles; así como valorar las posibles consecuencias en las actividades de las municipalidades.</p>	
Entradas	Salidas
<ul style="list-style-type: none"> <li>i. Catálogo de activos, amenazas, vulnerabilidades y controles propuestos en los marcos de referencia.</li> <li>ii. Entrevistas realizadas al personal de los grupos de control.</li> <li>iii. Informe de seguimiento y revisión.</li> </ul>	<ul style="list-style-type: none"> <li>i. Documento preliminar de valoración de activos críticos, amenazas y vulnerabilidades.</li> <li>ii. Registro de documentos actualizados.</li> </ul>
Actividades específicas	
<ul style="list-style-type: none"> <li>1. Identificar y valorar los activos críticos de las municipalidades.</li> <li>2. Identificar y valorar las amenazas a las que están expuestas.</li> <li>3. Identificar y valorar las vulnerabilidades.</li> <li>4. Documentar y comunicar el trabajo realizado.</li> <li>5. De ser el caso actualizar y comunicar los documentos.</li> </ul>	
Formatos y repositorios	
<ul style="list-style-type: none"> <li>F-7.1 Formato de identificación y valoración de activos críticos</li> <li>F-7.2 Formato de identificación y valoración de amenazas.</li> <li>F-7.3 Formato de identificación y valoración de vulnerabilidades.</li> </ul>	<ul style="list-style-type: none"> <li>R-4 Repositorio de activos</li> <li>R-5 Repositorio de amenazas y vulnerabilidades</li> </ul>

**Cuadro n.º 16:**  
**Fase 3: Evaluación del riesgo - Análisis y valoración del riesgo**

Nombre de la sub fase		Código
ANALISIS Y VALORACIÓN DEL RIESGO		P-3.2
Concepto		
<p>El análisis está orientado en entender al riesgo en toda su extensión. El personal a cargo de realizar esta labor determinará el grado de detalle y complejidad, el cual dependerá del alcance, contexto y criterios que se hayan propuesto inicialmente.</p> <p>La valoración tiene como finalidad apoyar la toma de acuerdos de la alta dirección de las organizaciones; es importante no perder de vista que las actividades de esta fase están enfocadas en contrastar sus niveles de riesgo contra sus criterios (tanto de valoración como de aceptación).</p>		
Entradas	Salidas	
<ul style="list-style-type: none"> <li>i. Documento preliminar de valoración de activos críticos, amenazas y vulnerabilidades.</li> <li>ii. Informe de seguimiento y revisión.</li> </ul>	<ul style="list-style-type: none"> <li>i. Escenarios de riesgos que conducen a un acto de corrupción.</li> <li>ii. Identificación de riesgo en un mapa de calor.</li> <li>iii. Registro de documentos actualizados.</li> </ul>	
Actividades específicas		
<ul style="list-style-type: none"> <li>1. Evaluación de consecuencias.</li> <li>2. Evaluación de probabilidad.</li> <li>3. Determinación del nivel de riesgos.</li> <li>4. Valorar los riesgos.</li> <li>5. Documentar y comunicar el trabajo realizado.</li> <li>6. De ser el caso actualizar y comunicar los documentos.</li> </ul>		
Formatos		
<ul style="list-style-type: none"> <li>F-7.4 Formato de análisis y valoración del riesgo.</li> <li>F-7.5 Formato del mapa de calor</li> </ul>		

**Cuadro n.º 17:  
Fase 4: Tratamiento del riesgo**

<b>Nombre de la fase</b>		<b>Código</b>
TRATAMIENTO DEL RIESGO		P-4
<b>Concepto</b>		
<p>Esta fase tiene como intención responder de manera oportuna a eventos de riesgo materializados con medidas eficaces con mecanismos con el afán de restringir la magnitud del impacto recibido.</p> <p>Las actividades por realizar nos permitirán elegir las alternativas que mejor se adapten al tratamiento del riesgo también tomando en consideración el marco regulatorio de las municipalidades y no tan solo centrarse en la comparación entre los potenciales beneficios y el dinero que se tenga que invertir para su puesta en marcha.</p>		
<b>Entradas</b>	<b>Salidas</b>	
<ul style="list-style-type: none"> <li>i. Mapas de calor con riesgos priorizados.</li> <li>ii. Esquemas de opciones de tratamiento del riesgo.</li> <li>iii. Informe de seguimiento y revisión.</li> </ul>	<ul style="list-style-type: none"> <li>i. Plan de tratamiento del riesgo</li> <li>ii. Plan de tratamiento del riesgo residual.</li> <li>iii. Registro de documentos actualizados.</li> </ul>	
<b>Actividades específicas</b>		
<ul style="list-style-type: none"> <li>1. Diseñar y ejecutar planes de tratamiento de riesgos.</li> <li>2. Identificar cambios en la estrategia de protección.</li> <li>3. Documentar y comunicar el trabajo realizado.</li> <li>4. De ser el caso actualizar y comunicar los documentos.</li> </ul>		
<b>Formatos y repositorios</b>		
<ul style="list-style-type: none"> <li>F-8.1 Formato de tratamiento del riesgo</li> <li>F-8.2 Formato de tratamiento del riesgo residual</li> </ul>	R-6 Repositorio de controles	

**Cuadro n.º 18:**  
**Componente transversal: Seguimiento o revisión**

Nombre del componente transversal		Código
SEGUIMIENTO O REVISIÓN		T-1
Concepto		
Este componente de carácter transversal tiene como finalidad advertir desviaciones o los problemas en la aplicación de este modelo, con la finalidad de corregir las brechas y asegurar el óptimo rendimiento de las actividades implementadas del MGR-TI.		
Entradas	Salidas	
i. Información obtenida de las actividades de gestión del riesgo.	i. Informe de seguimiento o revisión ii. Reporte de controversias	
Actividades específicas		
1. Ejecutar el seguimiento del resultado esperado de las actividades. 2. Ejecutar el seguimiento del modelo. 3. De ser el caso rediseñar el modelo propuesto.		
Formatos		
F-9 Formato de seguimiento o revisión de riesgos. F-10 Formato de acta de seguimiento o revisión. F-11 Formato de procedimiento y registro de controversias.		

En cuanto a los formatos y repositorios del MGR – TI estos se podrán encontrar en el **anexo n.ºs 4 y 5**.

### 3.4. Discusión

El MGR - TI propuesto permite determinar los riesgos que conllevan a un acto de corrupción, lo que permite asignarles controles como plan de tratamiento de riesgos y de esta manera preservar el valor de los activos y orientándonos a la optimización los recursos y obtención de los beneficios esperados generando valor como resultado de la lucha contra la corrupción.

Como es de conocimiento el 11 de marzo de 2020 la Organización Mundial de la Salud ha calificado el brote del COVID-19 como una pandemia; en tal sentido el mismo día el Gobierno Peruano mediante [46] declara la emergencia sanitaria a nivel nacional, por un periodo de noventa días, luego el 15 de marzo de 2020 el gobierno dispuso el aislamiento social obligatorio a través de [47], estas disposiciones fueron ampliadas a través de [48], [49], [50], [51], [52], [53] y [54] hasta el 31 de agosto de 2020; en consecuencia debido a las disposiciones dadas por el gobierno para probar la validez del MGR -TI propuesto en esta investigación se consultó con 3 expertos, los cuales vertieron sus opiniones en cuestionarios en los que se les consultó sobre la suficiencia, claridad, coherencia y relevancia de cada

una de las 28 actividades propuestas en el MGR – TI, para mayor detalle revisar el **anexo n.º 6**.

Al respecto se precisa, que se empleó el estadístico de W de Kendall con la finalidad de medir el nivel de concordancia de los expertos, donde se plantea una hipótesis nula que refleja la falta de concordancia entre los expertos (cuando el valor es cero) y una hipótesis alternativa donde se señala que la concordancia entre los datos proporcionados por los expertos (mientras el valor estadístico más se aproxime a uno, mayor será la concordancia). Los valores registrados como respuestas en los cuestionarios fueron ingresados al programa estadístico SPSS y los resultados fueron:

**Cuadro n.º 19:  
Resultados del estadístico de W de Kendall**

N	28
W de Kendall <sup>a</sup>	0,822
Chi-cuadrado	88,750
Gl	27
Sig. asintótica	0,000

En tal sentido si el estadístico W de Kendall es 0,822 por lo que se concluye que si existe concordancia entre los juicios emitidos por los expertos.

Del mismo modo se utilizó la V de Aiken el cual mide la importancia de cada actividad respecto al modelo siendo mejor cuando el valor se acerca a uno; el resultado obtenido se muestra en la siguiente tabla:

**Cuadro n.º 20:  
Resultados del estadístico de V de Aiken**

<b>Criterio</b>	<b>Valor de la V de Aiken</b>
Suficiencia	0,96
Claridad	0,98
Coherencia	0,98
Relevancia	0,99

Finalmente, para demostrar la confiabilidad modelo propuesto, se empleó el estadístico alfa de Cronbach, después de procesar los datos en el programa estadístico SPSS se obtuvo un valor de 0.727 y según [55, p. 12] su confiabilidad es alta.

## CONCLUSIONES

1. Se realizó un estudio comparativo de dos estándares y cuatro marcos de referencia internacionales relacionadas con la GR – TI. Como resultado se resalta que el modelo resultante recoge entre otros la naturaleza dinámica del comportamiento humano señalada en la ISO 31000:2018-02; así como tomó en cuenta el enfoque que realiza la NTP-ISO/IEC 27005:2018 en la gestión de riesgos orientada a la seguridad de la información; del mismo modo centra su atención en Cobit 2019 pues esta muestra cómo generar o preservar el valor al implementar la gestión de riesgos; de igual manera el modelo propuesto adecúa algunos de los recursos proporcionados por Magerit V.3 para reducir los riesgos de la puesta en uso de las TI; así como adaptó los formatos de Octave-S para la identificación, análisis de riesgos y el desarrollo de estrategias; y finalmente tomó como referencia varios de los recursos proporcionados por los documentos de la serie NIST SP 800 y se aplicaron al modelo.
2. Se formuló un MGR - TI el cual permitirá generar valor en el control de la corrupción de funcionarios o servidores en los gobiernos provinciales de la región de Lambayeque; pues permite identificar los riesgos que pueden ocasionar un acto de corrupción, optimizando el empleo de los recursos en la implementación de controles que mitiguen los mismos, permitiendo de esta manera la preservación del valor de sus activos.
3. Se un obtuvo un MGR -TI práctico, ágil y dinámico basado en formatos y repositorios y que fue validado por juicios expertos y sometido a indicadores estadísticos con resultados positivos.

## **RECOMENDACIÓN**

Automatizar el modelo de gestión de riesgos propuesto con la finalidad de masificar su uso.

## REFERENCIAS BIBLIOGRÁFICAS

- [1] Transparency International Secretariat, «Índice de percepción de la corrupción 2019,» Transparency International, 23 Enero 2020. [En línea]. Available: [https://files.transparency.org/content/download/2428/14734/file/2019\\_CPI\\_Report\\_EN.pdf](https://files.transparency.org/content/download/2428/14734/file/2019_CPI_Report_EN.pdf). [Último acceso: 8 Mayo 2020].
- [2] A. M. De Oliveira Guterres, «<https://www.unodc.org/bolivia/es/>,» 9 Diciembre 2018. [En línea]. Available: <https://www.unodc.org/bolivia/es/Mensaje-del-Secretario-General-de-la-Organizacion-de-las-Naciones-Unidas--Antonio-Guterres--en-el-Dia-Internacional-contr-la-Corrupcion---9-de-diciembre-de-2018.html#:~:text=La%20evasi%C3%B3n%20fiscal%2C%20el%20lavado,del>. [Último acceso: 10 Julio 2020].
- [3] Cybersecurity Ventures, «2019 Official Annual Cybercrime Report,» 2019. [En línea]. Available: <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>. [Último acceso: 15 Mayo 2020].
- [4] Polizia di Stato, «<https://www.poliziadistato.it/>,» 11 Abril 2016. [En línea]. Available: <https://www.poliziadistato.it/articolo/41918>. [Último acceso: 17 Agosto 2020].
- [5] Fondo Monetario Internacional, «Resumen Ejecutivo del Informe del Monitor Fiscal de Abril de 2019,» 30 Abril 2019. [En línea]. Available: <https://www.imf.org/~/media/Files/Publications/fiscal-monitor/2019/April/Spanish/execsum.ashx?la=es>. [Último acceso: 15 Mayo 2020].
- [6] T. Venezuela, «<https://transparencia.org.ve/>,» Transparencia Venezuela, 23 Agosto 2019. [En línea]. Available: <https://transparencia.org.ve/al-menos-20-paises-investigan-50-casos-de-corrupcion-con-dinero-de-venezuela/>. [Último acceso: 14 Mayo 2020].
- [7] Fiscalía General de la Nación - Colombia, «<https://www.fiscalia.gov.co/>,» 24 Agosto 2018. [En línea]. Available: <https://www.fiscalia.gov.co/colombia/seccionales/condenado-responsable-de-robo-informatico-a-la-oficina-de-predial-en-valledupar/>. [Último acceso: 13 Agosto 2020].
- [8] J. M. Harán, «<https://www.welivesecurity.com/>,» 20 Julio 2018. [En línea]. Available: <https://www.welivesecurity.com/la-es/2018/07/20/empleado-banco>.

- chile-estafa-informatica-transferencias-no-autorizadas/. [Último acceso: 13 Julio 2020].
- [9] Fiscalía General de la Nación de Colombia, «<https://www.fiscalia.gov.co/>,» 5 Noviembre 2019. [En línea]. Available: <https://www.fiscalia.gov.co/colombia/seccionales/asegurado-exsecretario-de-hacienda-de-baraya-huila-y-cuatro-particulares-mas-por-presunto-fraude-a-las-arcas-del-municipio-entre-2017-y-2018/>. [Último acceso: 27 Mayo 2020].
- [10] T. Internacional, «Barómetro Global de la Corrupción América Latina y el Caribe 2019 - Opiniones y Experiencias de los Ciudadanos en Materia de Corrupción,» 30 Setiembre 2019. [En línea]. Available: [https://files.transparency.org/content/download/2402/14630/file/2019\\_GCB\\_LAC\\_Report\\_ES.pdf](https://files.transparency.org/content/download/2402/14630/file/2019_GCB_LAC_Report_ES.pdf). [Último acceso: 8 Mayo 2020].
- [11] Contraloría General de la República del Perú, «Informe Ejecutivo Semestral de Gestión Julio – Diciembre 2019,» Gerencia de Comunicación Corporativa, Lima, 2020.
- [12] Contraloría General de la República del Perú, «Informe Ejecutivo Semestral de Gestión Julio – Diciembre 2018,» Servicios Gráficos Dinamo S.R.L., Lima, 2019.
- [13] Contraloría General de la República, «Buscador de Informes de la Contraloría General de la República,» 27 Agosto 2014. [En línea]. Available: <http://lfweb.contraloria.gob.pe/BuscadorInformes/DocView.aspx?id=3180505&cr=1>. [Último acceso: 15 Mayo 2020].
- [14] Contraloría General de la República, «INFORME N° 945 -2015-CG/CRN-EE - Carpeta de control n.° 122-2015-CG/CRN-EE-CC,» Contraloría General de la República, Chiclayo, 2015.
- [15] J. L. López Vásquez, «Informe de diagnóstico del sistema de control interno en la Municipalidad Provincial de Lambayeque,» Municipalidad Provincial de Lambayeque, Lambayeque, 2018.
- [16] Gerencia de Tecnología de la Información y Estadística, «Plan Estratégico de Gobierno Electrónico 2018 - 2020,» Municipalidad Provincial de Chiclayo, Chiclayo, 2017.
- [17] A. W. Quiroz Norris, «Historia de la corrupción en el Perú,» Instituto de Estudios Peruanos - Instituto de Defensa Legal, Lima, 2013.
- [18] Fiscalía Anticorrupción de Panamá, *Manual de investigación de delitos de corrupción*, Panamá: Editora Novo Art. S.A., 2007.
- [19] E. Crespo Martínez, «Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs,» *Enfoque UTE*, vol. 7, n° 1, pp. 107-121, 2017.
- [20] D. Arellano Gault, «[www.sciencedirect.com](http://www.sciencedirect.com),» 17 Setiembre 2016. [En línea]. Available: [www.sciencedirect.com](http://www.sciencedirect.com). [Último acceso: 10 Agosto 2019].
- [21] A. F. Cuesta Gómez, Los mapas de riesgos de corrupción incidencias en la prevención de la corrupción, Bogotá: Pontificia Universidad Javeriana, 2015.
- [22] J. M. Rodríguez Castro, Modelo de gestión de riesgos de tecnologías de la información como apoyo en la continuidad del negocio en una empresa que brinda software como servicio, Chiclayo: Universidad Católica Santo Toribio de Mogrovejo, 2019.

- [23] R. J. Callata Vega, Implementación de políticas públicas de gobierno Electrónico como un mecanismo de lucha contra la Corrupción en el Perú, 2016, Arequipa: Universidad Católica de Santa María, 2018.
- [24] J. C. Banda Santisteban, Modelo basado en metodologías de gestión de riesgos de ti para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque, Chiclayo: Universidad Católica Santo Toribio de Mogrovejo, 2019.
- [25] J. d. P. Alva Zapata y F. B. Vásquez Velásquez, Modelo de gestión de riesgos de TI para contribuir en la continuidad del negocio de las microfinancieras de la región de Lambayeque, Chiclayo: Universidad Católica Santo Toribio de Mogrovejo, 2018.
- [26] M. Y. Arangurí García, R. D. Iman Espinoza y G. M. León Tenorio, Modelo de gestión de riesgos de ti basados en estándares adaptados a las ti que soportan los procesos para contribuir a la generación de valor en las universidades privadas de la región Lambayeque, Chiclayo: Universidad Santo Toribio de Mogrovejo, 2016.
- [27] Oficina de las Naciones Unidas Contra la Droga y el Delito, Convención de las Naciones Unidas Contra la Corrupción, New York: Naciones Unidas, 2004.
- [28] R. Chaname Orbe, Diccionario Jurídico Moderno - Décima edición, Lima: Lex & Iuris, 2016.
- [29] Real Academia Española, «<https://dle.rae.es/>,» Real Academia Española, 2019. [En línea]. Available: <https://dle.rae.es/riesgo>. [Último acceso: 30 Junio 2020].
- [30] Organización Internacional de Normalización - ISO, ISO-31000-2018-02, Suiza: Secretaría Central de ISO, 2018.
- [31] Project Management Institute, La guía de los fundamentos para la dirección de proyectos (Guía del PMBOK), Estados Unidos: Project Management Institute, Inc., editor, 2017.
- [32] Isaca, Escenarios de riesgo - utilizando Cobit 5 para riesgos, Estados Unidos: Isaca, 2014.
- [33] Real Academia de la Lengua Española, «<https://dle.rae.es/>,» Real Academia de la Lengua Española, 2020. [En línea]. Available: <https://dle.rae.es/gestionar?m=form>. [Último acceso: 1 Julio 2020].
- [34] Instituto Nacional de Ciberseguridad del Gobierno de España, «<https://www.incibe.es/>,» 6 Julio 2015. [En línea]. Available: <https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario>. [Último acceso: 1 Julio 2020].
- [35] Isaca, Cobit 2019 - Objetivos de gobierno y gestión, Estados Unidos: Isaca, 2018.
- [36] ISO/IEC, Norma Técnica Peruana NTP-ISO/IEC 27005:2018 Tecnología de la información. Técnicas de seguridad. Gestión de riesgo de la seguridad de la información, Lima: Dirección de Normalización - INACAL, 2018.
- [37] Consejo Superior de Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas del Gobierno de España, Magerit - Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I - Método, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

- [38] Consejo Superior de Administración Electrónica del Ministerio de Hacienda y Administraciones Públicas del Gobierno de España, Magerit - Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II - Catálogo de elementos, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.
- [39] Software Engineering Institute, «<https://resources.sei.cmu.edu/>,» 31 Enero 2005. [En línea]. Available: [https://resources.sei.cmu.edu/asset\\_files/Handbook/2005\\_002\\_001\\_14273.pdf](https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14273.pdf). [Último acceso: 15 Julio 2020].
- [40] National Institute of Standards and Technology, «Guide for Conducting - Risk Assessments,» 3 Enero 2012. [En línea]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>. [Último acceso: 8 Julio 2020].
- [41] National Institute of Standards and Technology, «NIST Special Publication 800-39 Managing Information Security Risk,» 1 Marzo 2011. [En línea]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>. [Último acceso: 8 Julio 2020].
- [42] National Institute of Standards and Technology, «Draft NIST Special Publication 800-53 Revision 5,» 16 Marzo 2020. [En línea]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf>. [Último acceso: 8 Julio 2020].
- [43] Real Academia de la Lengua Española, «<https://dle.rae.es/>,» Real Academia de la Lengua Española, 8 Julio 2020. [En línea]. Available: <https://dle.rae.es/armonizar?m=form>. [Último acceso: 8 Julio 2020].
- [44] Isaca, Cobit 2019 Marco de referencia - Introducción y metodología, Estados Unidos: Isaca, 2018.
- [45] Congreso de la República, «<https://diariooficial.elperuano.pe/>,» 27 Mayo 2003. [En línea]. Available: <https://diariooficial.elperuano.pe/pdf/0015/3-ley-organica-de-municipalidades-1.pdf>. [Último acceso: 15 Marzo 2020].
- [46] G. Peruano, «<https://busquedas.elperuano.pe/>,» 11 03 2020. [En línea]. Available: <https://busquedas.elperuano.pe/download/url/decreto-supremo-que-declara-en-emergencia-sanitaria-a-nivel-decreto-supremo-n-008-2020-sa-1863981-2>. [Último acceso: 12 03 2020].
- [47] G. Peruano, «<https://cdn.www.gob.pe/>,» 15 03 2020. [En línea]. Available: [https://cdn.www.gob.pe/uploads/document/file/566448/DS044-PCM\\_1864948-2.pdf](https://cdn.www.gob.pe/uploads/document/file/566448/DS044-PCM_1864948-2.pdf). [Último acceso: 16 03 2020].
- [48] G. Peruano, «<https://cdn.www.gob.pe/>,» 27 03 2020. [En línea]. Available: [https://cdn.www.gob.pe/uploads/document/file/572157/DECRETO\\_SUPREMO\\_N%C2%BA\\_051-2020-PCM.pdf](https://cdn.www.gob.pe/uploads/document/file/572157/DECRETO_SUPREMO_N%C2%BA_051-2020-PCM.pdf). [Último acceso: 28 03 2020].
- [49] G. Peruano, «<https://cdn.www.gob.pe/>,» 09 04 2020. [En línea]. Available: [https://cdn.www.gob.pe/uploads/document/file/1021486/DS\\_N\\_\\_064-2020-PCM.pdf](https://cdn.www.gob.pe/uploads/document/file/1021486/DS_N__064-2020-PCM.pdf). [Último acceso: 09 04 2020].
- [50] G. Peruano, «<https://busquedas.elperuano.pe/>,» 25 04 2020. [En línea]. Available: <https://busquedas.elperuano.pe/download/url/decreto-supremo-que-prorroga-el->

- estado-de-emergencia-naciona-decreto-supremo-n-075-2020-pcm-1865780-1.  
[Último acceso: 26 04 2020].
- [51] G. Peruano, «<https://cdn.www.gob.pe>,» 09 05 2020. [En línea]. Available: [https://cdn.www.gob.pe/uploads/document/file/698139/DS\\_N\\_\\_083-2020-PCM.pdf](https://cdn.www.gob.pe/uploads/document/file/698139/DS_N__083-2020-PCM.pdf). [Último acceso: 10 05 2020].
- [52] G. Peruano, «<https://busquedas.elperuano.pe>,» 23 05 2020. [En línea]. Available: <https://busquedas.elperuano.pe/download/url/decreto-supremo-que-establece-las-medidas-que-debe-observar-decreto-supremo-n-094-2020-pcm-1866708-1>. [Último acceso: 24 05 2020].
- [53] G. Peruano, «<https://cdn.www.gob.pe>,» 26 06 2020. [En línea]. Available: [https://cdn.www.gob.pe/uploads/document/file/898487/DS\\_116-2020-PCM.pdf](https://cdn.www.gob.pe/uploads/document/file/898487/DS_116-2020-PCM.pdf). [Último acceso: 27 06 2020].
- [54] G. Peruano, «<https://busquedas.elperuano.pe>,» 31 07 2020. [En línea]. Available: <https://busquedas.elperuano.pe/download/url/decreto-supremo-que-prorroga-el-estado-de-emergencia-naciona-decreto-supremo-n-135-2020-pcm-1874483-1>. [Último acceso: 01 08 2020].

## **ANEXOS**

**Anexo n.º 1:**  
**Documentos de aceptación de las municipalidades**

**1. Municipalidad provincial de Chiclayo.**

Documento de presentación



Chiclayo, 25 de noviembre 2019

CARTA N.º 054 – 2019 – USAT – PGRA

Sr. MARCOS ANTONIO GASCO ARROBAS  
ALCALDE  
MUNICIPALIDAD PROVINCIAL DE CHICLAYO  
Presente.-

*Asunto: Información de la Institución para proyecto de investigación*

Es grato dirigirme a usted para expresarle un cordial saludo a nombre de la Escuela de Posgrado de la Universidad Católica Santo Toribio de Mogrovejo y, a la vez, presentarle al maestrante ROGER GUSTAVO ABANTO ORTIZ, estudiante del Programa de Maestría en Ingeniería de Sistemas y Computación con Mención en Dirección Estratégica de Tecnologías de Información, quien solicita se le brinde información y permiso para aplicación de instrumentos en la institución, como parte de la investigación de su proyecto de tesis, denominado "Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de la región de Lambayeque".

Agradeciendo las facilidades otorgadas al estudiante para la realización de su trabajo de investigación, hago propicia la ocasión para reiterarle los sentimientos de consideración y estima.



Atentamente



Dña. Beatriz Isabel Ortega Pauta  
Directora Escuela de Posgrado – USAT

DIRECCIÓN  
ESCUELA DE POSGRADO

03 DIC. 2019

Registro Expositor: 668438  
Registro Expediente: 342129  
Firma: V.G.

Av. San José María Escobedo N°955, Chiclayo-Perú • Central telefónica: (074) 606200 – 606217 • Oficina de Información: (074) 606203  
Pna/USAT: (074) 606217 • www.usat.edu.pe • www.facebook.com/usat.peru

## Documento de aceptación

  
MUNICIPALIDAD PROVINCIAL DE CHICLAYO  
GERENCIA DE RECURSOS HUMANOS

**"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN Y LA IMPUNIDAD"**

Chiclayo, 05 de Noviembre del 2019.

**OFICIO N° 700 -2019-MPCH-G.RR.HH.**

Señora Dra.  
**BEATRIZ ISABEL ORTEGA PAUTA**  
Directora de la Escuela de Postgrado  
Universidad Católica Santo Toribio de Mogrovejo.

**Presente.-**

**REF.:** Carta N° 054-2019-USAT-PGRA - Rég. N°  
342129-2019-SISGEDO

De mi consideración:

Es grato dirigirme a usted, para expresarle mi saludo cordial a nombre de la Gerencia de Recursos Humanos de la Municipalidad Provincial de Chiclayo, y en atención al documento de la referencia, se da por aceptada la aplicación de su Proyecto de Tesis titulado **"MODELO DE GESTION DE RIESGOS DE TECNOLOGIAS DE INFORMACION PARA LA GENERACION DE VALOR EN EL CONTROL DE LA CORRUPCION DE FUNCIONARIOS Y SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES DE LA REGION LAMBAYEQUE"** para el Maestrante Sr. **ROGER GUSTAVO ABANTO ORTIZ**, el mismo que realizará en la Gerencia de Tecnologías de la Información y Estadística.

Es propicia la oportunidad para expresarle los sentimientos de mi consideración.

Atentamente


Cc.  
OTE  
Archivo

  
**Dr. P. G. Ortega Pauta**  
GERENCIA DE RECURSOS HUMANOS

  
SECRETARIA ACADÉMICA  
ESCUELA DE POSGRADO  
05/12/19

## 2. Municipalidad provincial de Lambayeque.

Documento de presentación




USAT  
Universidad Católica  
Santo Toribio de Mogrovejo

Chiclayo, 25 de noviembre 2019

CARTA N.º 055 – 2019 – USAT – PGRA

Sr. ALEXANDER RODRÍGUEZ ALVARADO  
ALCALDE  
MUNICIPALIDAD PROVINCIAL DE LAMBAYEQUE  
PRESENTE.-




*Asunto: Información de la Institución para proyecto de investigación*


Es grato dirigirme a usted para expresarle un cordial saludo a nombre de la Escuela de Posgrado de la Universidad Católica Santo Toribio de Mogrovejo y, a la vez, presentarle al maestrante ROGER GUSTAVO ABANTO ORTIZ, estudiante del Programa de Maestría en Ingeniería de Sistemas y Computación con Mención en Dirección Estratégica de Tecnologías de Información, quien solicita se le brinde información y permiso para aplicación de instrumentos en la institución, como parte de la investigación de su proyecto de tesis, denominado "Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de la región de Lambayeque".

Agradeciendo las facilidades otorgadas al estudiante para la realización de su trabajo de investigación, hago propicia la ocasión para reiterarle los sentimientos de consideración y estima.

Atentamente




Dra. Beatriz Isabel Ortega Pauta  
Directora Escuela de Posgrado – USAT



DIRECCIÓN  
ESCUELA DE POSGRADO

## Documento de aceptación

**SISTEMAS Y WEB**  
FOLIO N° 03

  
**MUNICIPALIDAD PROVINCIAL DE LAMBAYEQUE**  
**SECRETARIA GENERAL E IMAGEN INSTITUCIONAL**  
**AREA DE SISTEMAS - PAGINA WEB**

---

Lambayeque, 03 de Diciembre de 2019

INFORME N° 139-USG-AS-MPL-2019

A : ROGER GUSTAVO ABANTO ORTIZ  
MAESTRANTE EN INGENIERIA DE SISTEMAS Y COMPUTACION -USAT

DE : ENA MARIBEL CHERO SANTAMARIA  
JEFE DE AREA DE SISTEMAS - PAGINA WEB

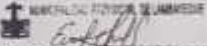
ASUNTO : INFORMACION DE LA INSTITUCION PARA EL PROYECTO DE  
INVESTIGACION

Ref. : NOTA DE ENVIO 17055/2019  
CARTA N° 1652-2019-MPL-SEGEIM  
CARTA N° 055-2019-USAT-PGRA


---

Es grato saludarlo y así mismo informarle que se le brindará la información necesaria para el desarrollo de su proyecto de investigación denominado "Modelo de Gestión de Riesgos de Tecnologías de Información para la Generación de Valor en el Control de la Corrupción de Funcionarios y Servidores en las Municipalidades Provinciales de la Región Lambayeque".

Atentamente,

  
Ing. Ena Maribel Chero Santamaria  
JEFE AREA DE SISTEMAS - PAGINA WEB

c.c. Archivo  
cc. Secretaría General e Imagen Institucional

*Recibido*  
03/12/2019  


### 3. Municipalidad provincial de Ferreñafe.

Documento de presentación



Chiclayo, 25 de noviembre 2019

CARTA N.º 056 – 2019 – USAT – PGRA

Sra. VIOLETA PATRICIA MURO MESONES  
ALCALDESA  
MUNICIPALIDAD PROVINCIAL DE FERREÑAFE  
PRESENTE.-

MUNICIPALIDAD PROVINCIAL DE FERREÑAFE  
ÁREA FUNCIONAL TRÁMITE DOCUMENTARIO

03 810 0000  
172459  
309032

*Asunto: Información de la institución para proyecto de investigación*

Es grato dirigirme a usted para expresarle un cordial saludo a nombre de la Escuela de Posgrado de la Universidad Católica Santo Toribio de Mogrovejo y, a la vez, presentarle al maestrante ROGER GUSTAVO ABANTO ORTIZ, estudiante del Programa de Maestría en Ingeniería de Sistemas y Computación con Mención en Dirección Estratégica de Tecnologías de Información, quien solicita se le brinde información y permiso para aplicación de instrumentos en la institución, como parte de la investigación de su proyecto de tesis, denominado "Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de la región de Lambayeque".

Agradeciendo las facilidades otorgadas al estudiante para la realización de su trabajo de investigación, hago propicia la ocasión para reiterarle los sentimientos de consideración y estima.

Atentamente



Sra. Beatriz Isabel Ortega Pauta  
Directora Escuela de Posgrado – USAT

DIRECCIÓN  
ESCUELA DE POSGRADO

Av. San Josémaría Escrivá N°855 Chiclayo-Perú | (074) 606200 - 606217 | www.usat.edu.pe

## Documento de aceptación



## MUNICIPALIDAD PROVINCIAL DE FERREÑA FE



*"Año de la Lucha Contra la Corrupción y la Impunidad"*

Ferreñafe, 04 de Diciembre de 2019

**OFICIO N° 066-2019-MPF/UGRH**

Señora:  
**DRA. BEATRIZ ISABEL ORTEGA PAUTA**  
**DIRECTORA ESCUELA DE POSGRADO - USAT**  
**Chiclavo.-**

**ASUNTO : AUTORIZACIÓN PARA REALIZACION DE INVESTIGACIÓN PARA PROYECTO DE TESIS**  
**REF. : EXPEDIENTE N° 172459**

De mi consideración:

Tengo a bien dirigirme a Usted, para saludarlo en nombre de la Municipalidad Provincial de Ferreñafe y por este intermedio manifestarle que en atención al documento de la referencia donde solicita permiso para que el estudiante **ROGER GUSTAVO ABANTO ORTIZ** realice su investigación para su Proyecto de Tesis, ha sido **ACEPTADO** por nuestra Institución; dicho Proyecto las realizará en la Unidad de Tecnología de Información y Comunicación.

Hago propicia la ocasión para reiterarle los sentimientos de mi sincera consideración y estima personal.

Atentamente,

c.c.: Archivo



**Chicho Polo**  
SECRETARIO GENERAL DE GOBIERNO REGIONAL



*PE. Braulio García*  
**COORDINACIÓN ACADÉMICA**  
**ESCUELA DE POSGRADO**  
 04-12-19

---

**CALLE NICANOR CARMONA N° 436 TELEFAX 287876 - FERREÑA FE**  
 Página Web: [www.muniferreñafe.gob.pe](http://www.muniferreñafe.gob.pe) - E-MAIL: [municipalidad@muniferreñafe.com.pe](mailto:municipalidad@muniferreñafe.com.pe)  
*"Juntos hacemos una ciudad digna y culta"*

**Anexo n.º 2:**  
**Información de las municipalidades provinciales.**

	<b>Municipalidad Provincial de Chiclayo</b>	<b>Municipalidad Provincial de Lambayeque</b>	<b>Municipalidad Provincial de Ferreñafe</b>
<b>Sector:</b>	Gobierno de nivel provincial.	Gobierno de nivel provincial.	Gobierno de nivel provincial.
<b>Norma y fecha de creación:</b>	El 18 de abril de 1835 el presidente coronel Felipe Santiago Salaverry bajo un dispositivo legal anuncia que se crea la provincia denominada Chiclayo, cuya capital será la ciudad del mismo nombre.	Acta de instalación del 9 de diciembre de 1883.	La provincia de Ferreñafe fue creada por ley 11590, del 17 de febrero de 1951, desmembrándose de la provincia de Lambayeque y en base al distrito de Ferreñafe y los caseríos de Inkawasi, Kañaris, Tres Tomas, Pueblo Nuevo y Pítipo que son elevados a la categoría de distritos teniendo como capitales los centros poblados de su nombre, a excepción de Kañaris que se asigna como capital al pueblo de Colaya. Por ley 16087 del 18 de marzo de 1966, al distrito de Tres Tomas y su capital cambian de nombre por Manuel Antonio Mesones Muro, y en 1954, Colaya deja de ser capital del distrito de Kañaris, reemplazándolo el pueblo homónimo.
<b>Dirección:</b>	La Municipalidad cuenta con varios locales, pero el palacio municipal se ubica en la Calle San José N° 823 / Chiclayo / Lambayeque; sin embargo, la Gerencia de Tecnología de la Información y Estadística está ubicado en la Calle Elías Aguirre N° 240 / Chiclayo / Lambayeque	El domicilio institucional, de la entidad, está ubicado en la AV. Bolívar 400 / Lambayeque / Lambayeque.	La entidad, está ubicada en la Calle Nicanor Carmona N° 436 - Ferreñafe – Lambayeque
<b>Representante legal:</b>	Alcalde: Marcos Antonio Gasco Arrobas	Alcalde: Alexander Rodríguez Alvarado	Alcalde: Violeta Patricia Muro Mesones
<b>Teléfonos de contacto:</b>	Coordinación de alcaldía: (074) 224933 Gerencia de Tecnología de la Información y Estadística (074) 208616	Central: (074) 282092 Área de Informática y Estadística: (074) 282092 - anexo 113 Área de sistemas y web: (074) 282092 - anexo 144	Central: (074) 287876
<b>Misión:</b>	Promover la adecuada prestación de los servicios públicos y el desarrollo integral y sostenible de la población de la Provincia de Chiclayo con calidad, transparencia y de manera participativa.	Somos una Municipalidad, que brinda servicios públicos de calidad a los ciudadanos y ciudadanas, con eficacia y eficiencia; desarrollando actividades orientadas a la inclusión social y equidad de género; que promueve y fomenta el desarrollo económico, turístico y socio cultural de las personas; conjuntamente con las organizaciones de la sociedad civil e instituciones públicas y privadas de la Provincia de Lambayeque; fortaleciendo nuestra identidad cultural, y condiciones ambientales, para mejorar la calidad de vida de los vecinos y vecinas, garantizando su tranquilidad, seguridad y bienestar	La Municipalidad Provincial de Ferreñafe, como órgano del Gobierno Local, representa a toda la población, que con su participación promueve la adecuada prestación de los servicios públicos, el desarrollo integral sostenible y económico de su jurisdicción.
<b>Visión:</b>	Chiclayo, tierra del Señor de Sipán, al 2030 es una provincia sostenible con servicios básicos, salud, seguridad y ornato adecuado; con organizaciones competitivas e inclusivas y socialmente responsable que promueve la igualdad de oportunidades.	Seremos una Municipalidad líder que brinda servicios de calidad a los vecinos y vecinas; con una gestión organizada, eficaz, inclusiva, transparente, participativa y con equidad de género, promoviendo la identidad cultural, el compromiso por la gestión de riesgo de desastres y la gestión ambiental; su personal es solidario, proactivo y competente, posicionando a Lambayeque como una provincia, moderna, ordenada, segura, turística, saludable, con una economía fluida; promoviendo el desarrollo integral de la ciudadanía Lambayecana.	La Provincia de Ferreñafe, signo histórico de la Cultura Sicán; busca elevar el nivel de vida de la población a través del acceso a la educación y salud de calidad, especialmente para las personas de escasos recursos.  Ferreñafe con una economía basada en el desarrollo sustentable de los sectores como turismo, agropecuario y agroindustria, se encuentra articulada a todos sus distritos y a la Región Lambayeque, mediante una gestión municipal democrática, transparente y eficiente, con plena participación ciudadana, equidad de género e igualdad de oportunidades.

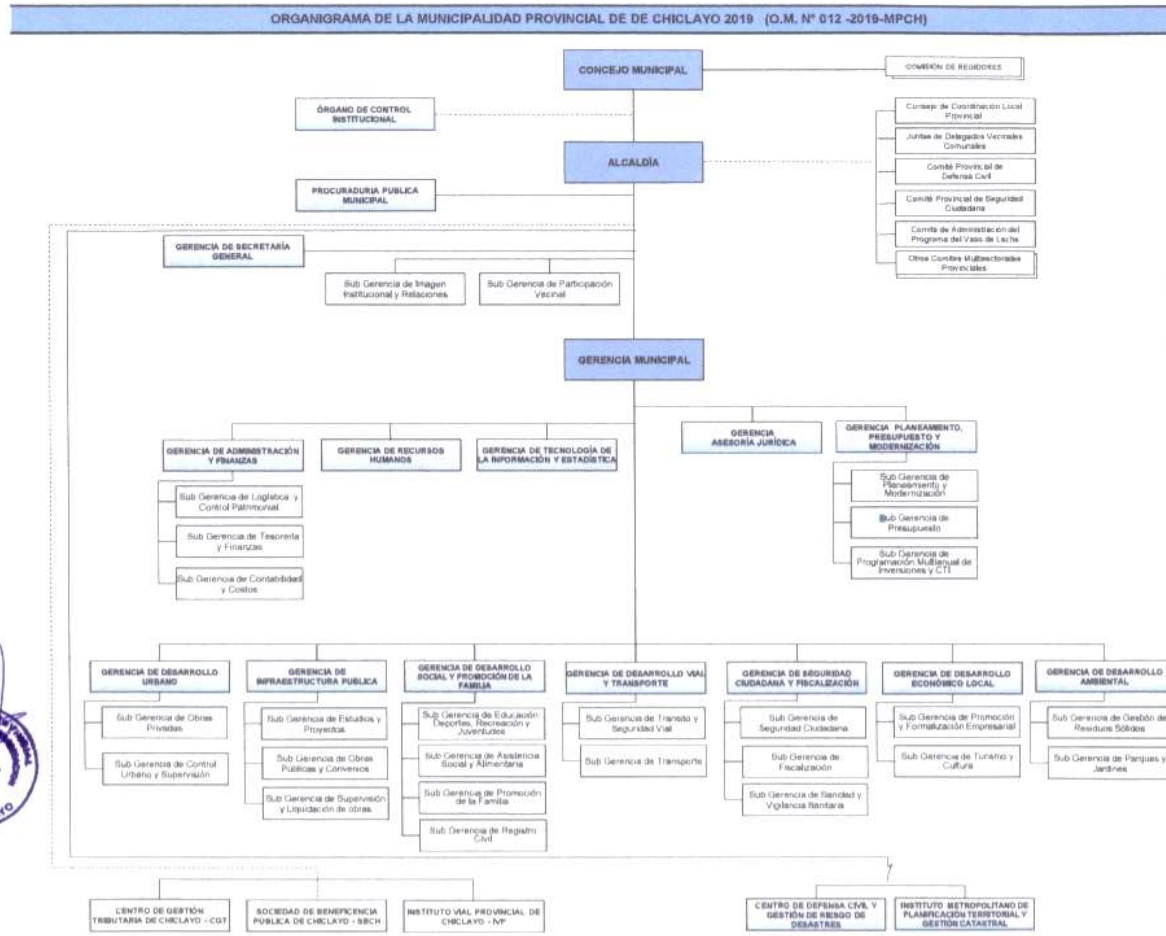
<p><b>Principios:</b></p>	<ol style="list-style-type: none"> <li>1. Respetuoso de los derechos humanos, por lo que impulsamos múltiples mecanismos de acceso ciudadano para acrecentar la actuación de los diversos grupos sociales.</li> <li>2. Promotor del acceso ciudadano a la gestión pública, en cuyo marco impulsamos una básica pero indeclinable apertura de mecanismos de accesibilidad a los diversos grupos poblacionales, con especial énfasis en aquellos que por años han permanecido excluidos de las políticas y atención públicas.</li> <li>3. Responsable del fortalecimiento y optimización de los procesos sociales que promueven el desarrollo local, para lo cual adopta un sólido compromiso demócrata de cooperación para la consolidación de la participación ciudadana en los ámbitos culturales, económicos, académicos, tributarios que afiancen la gobernabilidad en un contexto progresivo de descentralización.</li> <li>4. Impulsor de la incorporación de los enfoques de desarrollo humano, cogestión participativa, de resultados y, de equidad de género, en cuyas acciones se vienen involucrando todas las áreas orgánicas de la entidad edil, con énfasis en sus procesos de programación operativa y presupuestaria.</li> </ol>	<ol style="list-style-type: none"> <li>1. Participación. La gestión desarrollará y hará uso de instancias y estrategias concretas de participación ciudadana en las fases de formulación, seguimiento, fiscalización y evaluación de la gestión de gobierno y de la ejecución de los planes, presupuestos y proyectos locales, conforme a la normatividad vigente.</li> <li>2. Transparencia. Los planes, presupuestos, objetivos, metas y resultados del gobierno local serán difundidos a los vecinos. La implementación de portales electrónicos en Internet y cualquier otro medio de acceso a la información pública se rigen por la Ley de Transparencia y Acceso a la Información Pública N° 27806 y sus modificatorias y reglamentarias.</li> <li>3. Gestión moderna y rendición de cuentas. La administración pública está orientada bajo un sistema moderno de gestión y sometida a una evaluación de desempeño. Los gobiernos locales incorporan a sus programas de acción mecanismos concretos para la rendición de cuenta a los vecinos sobre los avances, logros, dificultades y perspectivas de su gestión. Los titulares de la administración pública local son gestores de los intereses de la colectividad y están sometidos a las responsabilidades que la Ley establezca.</li> <li>4. Inclusión. El gobierno local desarrolla políticas y acciones integrales de gobierno dirigidas a promover la inclusión económica, social, política y cultural de jóvenes o grupos sociales tradicionalmente excluidos y marginados del Estado, principalmente ubicada en el ámbito rural y organizado en comunidades campesinas y nativas, nutriéndose de sus perspectivas y aportes. Estas acciones también buscan promover los derechos de grupos vulnerables, impidiendo la discriminación por razones de etnia, religión o género.</li> <li>5. Eficacia. Los gobiernos locales organizan su gestión en torno a los planes y proyectos de desarrollo local concertados, al cumplimiento de objetivos y metas explícitos y de público conocimiento.</li> <li>6. Eficiencia. La política y la acción local se regirán por criterios de eficiencia, desarrollando las estrategias necesarias para consecución de los objetivos trazados con la utilización óptima de los recursos.</li> <li>7. Equidad. Las consideraciones de equidad también son componentes constitutivo y orientador de la acción local. Las acciones locales promocionan sin discriminación la igualdad de oportunidades y la identificación de grupos y sectores sociales que requieran ser atendidos de manera especial por la gestión municipal.</li> <li>8. Sostenibilidad. La gestión municipal se caracteriza por la búsqueda del equilibrio inter gerencial en el uso racional de los recursos naturales para lograr los objetivos de desarrollo, la defensa del ambiente y la protección de la biodiversidad.</li> <li>9. Imparcialidad y neutralidad. Los gobiernos locales garantizan la imparcialidad y neutralidad de la actuación de la administración pública local o general.</li> <li>10. Subsidiaridad. El gobierno más cercano a la población es el más idóneo para ejercer las distintas funciones que competen al Estado. Por consiguiente, el gobierno nacional no debe asumir competencias que pueden ser cumplidas más eficientemente por los gobiernos regionales y éstos a su vez no deben involucrarse en realizar acciones que pueden ser ejecutadas eficientemente por los gobiernos locales, evitando la duplicidad de funciones.</li> </ol>
---------------------------	---	---

<b>Valores:</b>	<ol style="list-style-type: none"> <li>1. Responsabilidad en la prestación de los servicios y la atención pública.</li> <li>2. Participación, cooperación y solidaridad como acción permanente que incorpore a la ciudadanía para la toma de decisiones.</li> <li>3. Transparencia, comunicación y justicia en las acciones de las autoridades, funcionarios y trabajadores.</li> <li>4. Compromiso, liderazgo e identidad como una característica constante en todo el personal.</li> <li>5. Integralidad y honestidad como actitud permanente en el quehacer institucional.</li> <li>6. Responsabilidad y organización en todos los niveles de gestión</li> </ol>	<ol style="list-style-type: none"> <li>1. Democracia y solidaridad. Valores que buscan reafirmar el gobierno de las mayorías, como expresión esencial de vida y condición indispensable de toda persona humana en su medio social, así como practica la solidaridad individual y organizativa ante el conjunto de personas desvalidas o en situación de pobreza.</li> <li>2. Identidad y compromiso con la institución y la provincia. Valores que buscan la reafirmación de lazos de pertenencia del trabajador municipal con la institución, sintiéndose parte, identificándose y comprometiéndose a brindar un mejor servicio con la finalidad de garantizar la satisfacción del vecino y contribuyendo de esta manera a consolidar la imagen de la administración municipal. Es el compromiso de trabajar en equipo, proporcionando un ambiente abierto, caracterizado por la igualdad de oportunidades en el desarrollo de la ciudad.</li> <li>3. Honradez, honestidad, ética y probidad. Valores que buscan internalizar la rectitud, integridad, y la honestidad en el desempeño de la función pública, con preminencia del interés público sobre el interés personal. La relación a establecerse con nuestros vecinos deberá conducirse con la mayor integridad, en la constante búsqueda de las más altas normas de ética y de justa conducta.</li> <li>4. Integridad y respeto. Valor que busca reafirmar la integridad como una conducta de vida con presencia en todos los actos públicos o privados, manteniendo una imagen de credibilidad, confianza y probidad; así como actuar en un marco de absoluto respeto de la persona con equidad de género, familia y sociedad en su conjunto, con derecho a exigir a los demás un trato similar.</li> </ol>	<ol style="list-style-type: none"> <li>1. Respeto. Adecua su conducta hacia el respeto de la Constitución y las Leyes, garantizando en todas las fases del proceso de toma de decisiones o en el cumplimiento de los procedimientos administrativos, se respeten los derechos a la defensa y al debido procedimiento.</li> <li>2. Probidad. Actúa con rectitud, honradez y honestidad, procurando satisfacer el interés general y desechando todo provecho o ventaja personal, obtenido por sí o por interpósita persona.</li> <li>3. Eficiencia. Brinda calidad en cada una de las funciones a su cargo, procurando obtener una capacitación sólida y permanente.</li> <li>4. Idoneidad. Entendida como aptitud técnica, legal y moral, es condición esencial para el acceso y ejercicio de la función pública. El servidor público debe propender a una formación sólida acorde a la realidad, capacitándose permanentemente para el debido cumplimiento de sus funciones.</li> <li>5. Veracidad. Se expresa con autenticidad en las relaciones funcionales con todos los miembros de su institución y con la ciudadanía, y contribuye al esclarecimiento de los hechos.</li> <li>6. Lealtad y obediencia. Actúa con fidelidad y solidaridad hacia todos los miembros de su institución, cumpliendo las órdenes que le imparta el superior jerárquico competente, en la medida que reúnan las formalidades del caso y tengan por objeto la realización de actos de servicio que se vinculen con las funciones a su cargo, salvo los supuestos de arbitrariedad o ilegalidad manifiestas, las que deberá poner en conocimiento del superior jerárquico de su institución.</li> <li>7. Justicia y equidad. Tiene permanente disposición para el cumplimiento de sus funciones, otorgando a cada uno lo que le es debido, actuando con equidad en sus relaciones con el Estado, con el administrado, con sus superiores, con sus subordinados y con la ciudadanía en general.</li> </ol>
-----------------	---	---	---

<b>Objetivos Estratégicos:</b>	<ol style="list-style-type: none"> <li>1. Mejorar las condiciones de habitabilidad en la Provincia.</li> <li>2. Promover la gestión ambiental en la Provincia.</li> <li>3. Reducir los índices de inseguridad ciudadana en la Provincia.</li> <li>4. Contribuir con la calidad de los servicios de salud en la Provincia.</li> <li>5. Promover la gestión de riesgo de desastres en la Provincia.</li> <li>6. Promover la competitividad económica en la Provincia.</li> <li>7. Fortalecer la gestión institucional.</li> <li>8. Promover el desarrollo urbano territorial ordenado y sostenible en la Provincia.</li> <li>9. Mejorar el servicio de transporte y tránsito en la Provincia.</li> <li>10. Incrementar la oferta turística con enfoque cultural en la Provincia.</li> <li>11. Promover el desarrollo humano y hábitos saludables en la Provincia.</li> </ol>	<ol style="list-style-type: none"> <li>1. Mejorar las condiciones de vida de la población mediante la ampliación y mejor calidad de los servicios como salud, educación, alimentación saneamiento, electrificación, seguridad ciudadana y protección social, con enfoque de igualdad de oportunidades y de equidad.</li> <li>2. Contribuir a la protección, conservación y mejoramiento del medio ambiente y al desarrollo de una cultura ambiental y de prevención de riesgos en la población y en las instituciones.</li> <li>3. Contribuir a mejorar los índices de competitividad de Lambayeque, basado en el desarrollo de las potencialidades y capacidades locales y en el marco del desarrollo humano sostenible.</li> <li>4. Promover acciones, programas y proyectos para mejorar sensiblemente la calidad de la gestión pública municipal y su mejor articulación con la sociedad civil y empresariado, reduciendo las distancias que lo separan.</li> </ol>	<ol style="list-style-type: none"> <li>1. Fortalecer las capacidades de los Recursos Humanos de la Municipalidad Provincial de Ferreñafe, a fin de mejorar su desempeño y productividad para que la Gestión Local logre Eficiencia y Eficacia.</li> <li>2. Dotar a la Municipalidad Provincial de Ferreñafe de mejores condiciones en cuanto a su infraestructura, equipamiento y tecnología que le permita modernizarse y estar en condiciones de mejorar sus procesos, y ser más eficiente y eficaz.</li> <li>3. Lograr que los Servicios Públicos Locales, brindados por la Municipalidad Provincial de Ferreñafe, sean de estándares altos en calidad, optimizando sus recursos logísticos, financieros y humanos para beneficio de los usuarios, contribuyentes y vecinos en general.</li> <li>4. Implementar de manera eficiente los diferentes Programas y Proyectos Sociales, Educativos y de Salud, dirigidos prioritariamente al sector de pobreza y pobreza extrema para alcanzar el desarrollo Humano, el aprovechamiento del turismo, la conservación ambiental, fomento</li> </ol>
<b>Naturaleza:</b>	La Municipalidad Provincial de Chiclayo es el órgano de Gobierno Local de la Provincia de Chiclayo que emana de la voluntad popular, cuenta con personería jurídica de derecho público, con autonomía política, económica y administrativa en los asuntos de su competencia, conforme a Ley, facultada a ejercer actos de gobierno en mérito a esa autonomía, en estricto cumplimiento a las leyes y disposiciones que de manera general le son aplicables y conforme a la Constitución Política del Perú.	Es un Gobierno Provincial promotor del desarrollo provincial, que emana de la voluntad popular. Tiene personería jurídica de derecho público con autonomía política, económica y administrativa en los asuntos municipales de su competencia, es promotor del desarrollo local con plena capacidad para el cumplimiento de sus fines; ejerce las funciones y atribuciones que le señala la Constitución Política del Perú y la Ley Orgánica de Municipalidades.	La Municipalidad Provincial de Ferreñafe, de acuerdo a lo establecido en la Constitución Política del Perú, modificado por la Ley de Reforma Constitucional N° 27680, es un organismo con personería jurídica de derecho público y goza de autonomía política, económica y administrativa en los asuntos de su competencia y ejerce actos de gobierno, actos de administración y actos administrativos en sujeción al marco jurídico nacional, en concordancia al Título II de la Ley N° 27972 – Ley Orgánica de Municipalidades, en virtud a ello está sujeta a las leyes y disposiciones que de manera general regulan las actividades y funcionamiento del sector público y de los sistemas administrativos del Estado que son de observancia y cumplimiento obligatorio.
<b>Jurisdicción:</b>	La Municipalidad Provincial de Chiclayo, tiene jurisdicción provincial sobre los veinte distritos de la provincia, incluyendo el distrito del mismo nombre, promoviendo su desarrollo y es el canal inmediato de participación vecinal en los asuntos políticos.	Representa a la Provincia de Lambayeque conformada por sus once distritos, la cual está ubicada en el norte de la costa peruana, aproximadamente entre las coordenadas geográficas 5°28'36" y 7°14'37" de latitud Sur y 79°41'30" y 80°37'23" de longitud oeste del meridiano de Greenwich, específicamente, en el noroeste y este de la región Lambayeque; al lado izquierdo del río Lambayeque a una altura de 18 m.s.n.m. y a 11,4 km. de la ciudad de Chiclayo.	Ejerce las competencias exclusivas y compartidas que le asigna la Ley Orgánica de Municipalidades en materia de organización y uso del espacio físico; saneamiento ambiental, salubridad y salud; tránsito, vialidad y transporte; educación, cultura, deportes, y recreación; abastecimientos y comercialización de productos y servicios; programas sociales, defensa y promoción de derechos; seguridad ciudadana y defensa civil; promoción del desarrollo económico local y otros servicios públicos que estén de acuerdo a sus posibilidades y no estén reservadas a otras entidades de nivel nacional o regional.
<b>Descripción de su área de TI:</b>	Según el artículo 70° del Reglamento de Organización y Funciones, la Gerencia de Tecnología de la Información y Estadística es el órgano de apoyo que depende de la Gerencia Municipal, encargado de administrar actividades referidas al proceso de planificación, organización, dirección, coordinación, comunicación y control, acerca del uso adecuado de los recursos informáticos físicos y lógicos y la utilización de las tecnologías de información y comunicación en la institución, desarrollando, implementando y manteniendo los sistemas de información	El Área de Informática y Estadística depende de la Sub Gerencia de Racionalización que es el órgano de asesoramiento, encargado de conducir y asesorar los procesos de planeamiento y de racionalización de las actividades y procedimientos administrativos de las unidades orgánicas, de corto y mediano plazo, así como de la elaboración de documentos de gestión institucional. La Sub Gerencia de Racionalización depende jerárquicamente de la Gerencia de Planeamiento y Presupuesto.	La Sub Gerencia de Tecnología de Información y Comunicación depende jerárquicamente de la Gerencia de Administración, esta tiene por objeto promover el desarrollo y mantenimiento de las TICs para la gestión de los procesos y procedimientos de la gestión municipal, así como promover su máximo acceso y uso de estas tecnologías de la información para ofrecer un óptimo servicio al ciudadano y mejorar la gestión municipal, así como formular los planes estratégicos y operativos, en sujeción al marco legal sobre la materia.

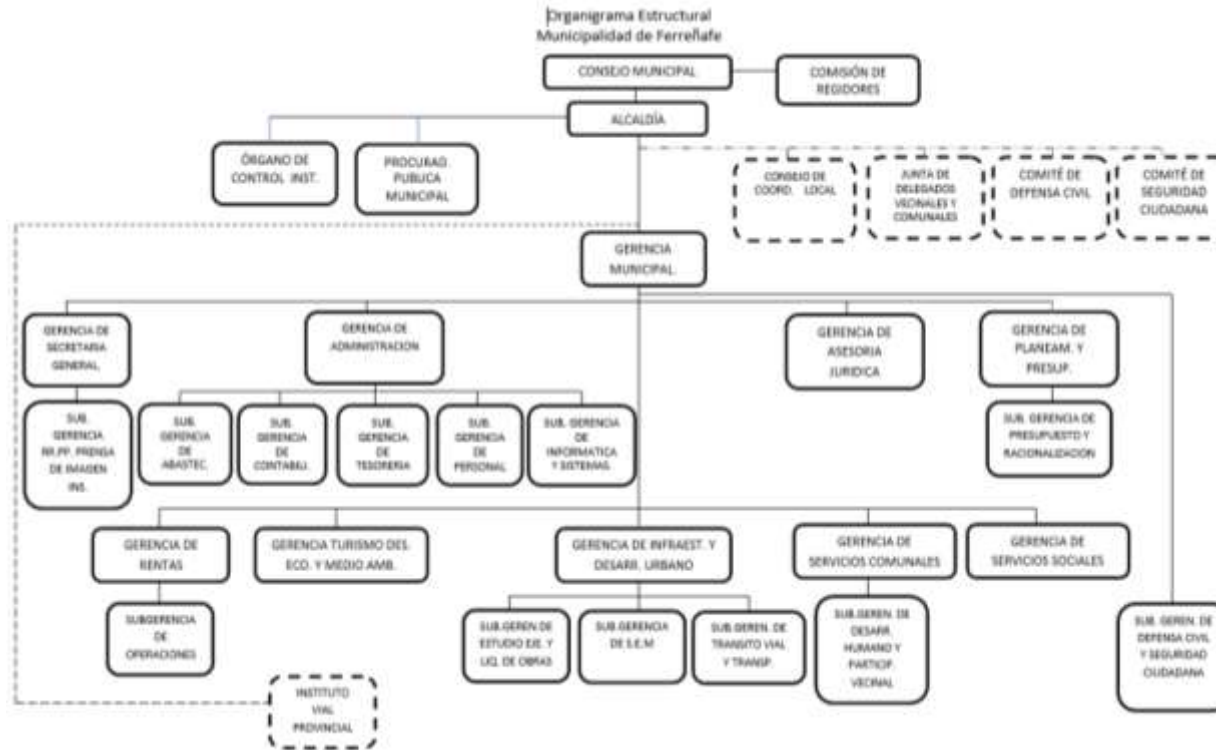
	<p>integrados, así como la elaboración de los procesos y acciones referentes a la estadística de la Municipalidad. Aprobado mediante Ordenanza Municipal N° 012 -2019-MPCH del 13 de agosto de 2019.</p>	<p>El Área de Sistemas y Página WEB depende de la Secretaría General e Imagen Institucional, que es el órgano de apoyo, entre otros, responsable del trámite, certificación y control de la correspondencia institucional, orientación y atención al público en general, así como de la administración y actualización del sistema de trámite documentario y archivo central de la municipalidad.</p>	
--	--	---	--

**Organigrama de la Municipalidad Provincial de Chiclayo.**





**Organigrama de la Municipalidad Provincial de Ferreñafe:**



### Anexo n.º 3:

#### Documentos relacionados a los cuestionarios

#### Validación del instrumento de recolección a aplicar.

En su mayoría las preguntas del instrumento de recolección de información han sido adaptadas de lo establecido en la ISO 31000 Segunda edición – 2018 “Gestión del Riesgo – Directrices”, tal como se muestra en el siguiente cuadro:

**Cuadro n.º 1**  
**Cuestionario adaptado tomando en cuenta el ISO 31000:02- 2018**

Pregunta \ Referencia	Referencia según ISO 31000 – segunda edición 2018
1. ¿Se ha implementado un sistema de gestión de riesgos de TI aplicando algún marco o estándar de trabajo?	5.4.2 Articulación del compromiso con la gestión del riesgo
2. ¿El Sistema de gestión de riesgos está integrado al gobierno de la municipalidad?	5.4.2 Articulación del compromiso con la gestión del riesgo
3. ¿Se han asignado roles y responsabilidades al personal respecto a la gestión de riesgos?	5.4.3 Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización
4. ¿Se cuenta con un inventario de activos de TI?	6.4.2 Identificación del riesgo
5. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?	6.4.2 Identificación del riesgo
6. ¿Cuentan con un proceso de análisis de riesgo de TI que permita comprender su naturaleza del riesgo y determinar su nivel?	6.4.3 Análisis del riesgo
7. ¿Cuentan con un proceso de valoración de riesgo de TI?	6.4.4 Valoración del riesgo
8. ¿Cuentan con un proceso para modificar el nivel de impacto y probabilidad de ocurrencia del riesgo de TI?	6.5 Tratamiento del riesgo
9. ¿Existe un equilibrio entre los beneficios y costos de los controles a implementar?	6.5 Tratamiento del riesgo
10. ¿Tiene mecanismos de revisiones o supervisiones periódicas de las actividades u operaciones diarias relacionadas a TI?	6.6 Seguimiento y revisión
11. ¿Tiene mecanismos de monitoreo para conocer oportunamente, si las operaciones relacionadas a TI se desarrollan de acuerdo con los procedimientos establecidos en la Municipalidad?	6.6 Seguimiento y revisión
12. ¿Existe un plan de mejora continua de la gestión de riesgos de TI?	6.5.3 Preparación e implementación de los planes de tratamiento del riesgo
13. ¿Se han identificado los riesgos de TI asociados a la corrupción?	Propio
14. ¿Se ha cuantificado las pérdidas económicas relacionadas a la materialización de los riesgos de TI asociados a la corrupción?	Propio
15. ¿Las partes interesadas son informadas sobre la gestión de riesgos de TI asociados a la corrupción?	6.2 Comunicación y consulta
16. ¿Se realiza actividades de monitoreo de los riesgos TI asociados a la corrupción?	Propio
17. ¿Tiene mecanismos que permitan identificar acontecimientos potenciales asociados a la corrupción que puedan afectar la ejecución de los procesos de TI con la consecuente afectación del logro de los objetivos institucionales?	Propio

Fuente: ISO 31000 Segunda edición – 2018 “Gestión del Riesgo – Directrices”

Elaborado por: Maestrante

Debido a que no todas las preguntas han sido adaptadas del ISO 31000 Segunda edición – 2018 “Gestión del Riesgo – Directrices”, se ha procedido a realizar la validación de esta por tres (3) expertos, los cuales se detallan a continuación:

### **FICHA DE VALIDACIÓN DE EXPERTOS**

Estimado(a) experto(a), remito el presente el cuestionario relacionado al proyecto de tesis “Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de la región de Lambayeque”, con la finalidad de que valide el instrumento que pretende obtener información que sirva de punto de partida para el desarrollo del presente trabajo.

### **DATOS DEL CUESTIONARIO**

#### **Objetivo del cuestionario:**

El objetivo principal es identificar si las municipalidades provinciales de la región de Lambayeque gestionan los riesgos de tecnologías de información relacionados a corrupción.

## Validación por la Ing. Mgtr. MÓNICA VILLAVICENCIO MONTOYA

### Instrucción:

A continuación, sírvase identificar si el ítem o pregunta cumple con los criterios de validez de suficiencia, claridad, coherencia y relevancia marcando con un aspa en la casilla que usted considere conveniente; del mismo modo de creerlo conveniente consignar sus comentarios; agradezco de antemano la atención al presente.

N° de ítem de la encuesta	Validez							
	Suficiencia		Claridad		Coherencia		Relevancia	
	SI	NO	SI	NO	SI	NO	SI	NO
1. ¿Se ha implementado un sistema de gestión de riesgos de TI aplicando algún marco o estándar de trabajo?	X		X		X		X	
2. ¿El Sistema de gestión de riesgos está integrado al gobierno de la municipalidad?	X		X		X		X	
3. ¿Se han asignado roles y responsabilidades al personal respecto a la gestión de riesgos?	X		X		X		X	
4. ¿Se cuenta con un inventario de activos de TI?	X		X		X		X	
5. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?	X		X		X		X	
6. ¿Cuentan con un proceso de análisis de riesgo de TI que permita comprender su naturaleza del riesgo y determinar su nivel?	X		X		X		X	
7. ¿Cuentan con un proceso de valoración de riesgo de TI?	X		X		X		X	
8. ¿Cuentan con un proceso para modificar el nivel de impacto y probabilidad de ocurrencia del riesgo de TI?	X		X		X		X	
9. ¿Existe un equilibrio entre los beneficios y costos de los controles a implementar?	X		X		X		X	
10. ¿Tiene mecanismos de revisiones o supervisiones periódicas de las actividades u operaciones diarias relacionadas a TI?	X		X		X		X	
11. ¿Tiene mecanismos de monitoreo para conocer oportunamente, si las operaciones relacionadas a TI, se desarrollan de acuerdo con los procedimientos establecidos en la Municipalidad?	X		X		X		X	
12. ¿Existe un plan de mejora continua de la gestión de	X		X		X		X	

riesgos de TI?							
13. ¿Se han identificado los riesgos de TI asociados a la corrupción?	X		X		X		X
14. ¿Se ha cuantificado las pérdidas económicas relacionadas a la materialización de los riesgos de TI asociados a la corrupción?	X		X		X		X
15. ¿Las partes interesadas son informadas sobre la gestión de riesgos de TI asociados a la corrupción?	X		X		X		X
16. ¿Se realiza actividades de monitoreo de los riesgos TI asociados a la corrupción?	X		X		X		X
17. ¿Tiene mecanismos que permitan identificar acontecimientos potenciales asociados a la corrupción que puedan afectar la ejecución de los procesos de TI con la consecuente afectación del logro de los objetivos institucionales?	X		X		X		X

**Comentarios:**

En cuanto a la pregunta 8, se entiende que está enfocada a indagar si la institución posee procedimientos para el establecimiento de opciones de tratamiento de riesgo y de las medidas pertinentes; por ello se sugiere que se reemplace la frase "modificar el nivel de impacto y probabilidad" por "disminuir el nivel de impacto y/o probabilidad", entendiendo que con las medidas/controles se podrían disminuir ambas o al menos una de las características del riesgo.

  
 MÓNICA VILLAVIENCIO MONTOYA

Fecha: 1 de noviembre de 2019

## Validación por el Ing. Dr. OSCAR ZOCON ALVA

### Instrucción:

A continuación, sírvase identificar si el ítem o pregunta cumple con los criterios de validez de suficiencia, claridad, coherencia y relevancia marcando con un aspa en la casilla que usted considere conveniente; del mismo modo de criterio conveniente consignar sus comentarios; agradezco de antemano la atención al presente.

N° de ítem de la encuesta	Validez							
	Suficiencia		Claridad		Coherencia		Relevancia	
	SI	NO	SI	NO	SI	NO	SI	NO
1. ¿Se ha implementado un sistema de gestión de riesgos de TI aplicando algún marco o estándar de trabajo?	X				X		X	
2. ¿El Sistema de gestión de riesgos está integrado al gobierno de la municipalidad?	X				X		X	
3. ¿Se han asignado roles y responsabilidades al personal respecto a la gestión de riesgos?	X				X		X	
4. ¿Se cuenta con un inventario de activos de TI?	X				X		X	
5. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?	X				X		X	
6. ¿Cuentan con un proceso de análisis de riesgo de TI que permita comprender su naturaleza del riesgo y determinar su nivel?	X				X		X	
7. ¿Cuentan con un proceso de valoración de riesgo de TI?	X				X		X	
8. ¿Cuentan con un proceso para modificar el nivel de impacto y probabilidad de ocurrencia del riesgo de TI?	X			X	X		X	
9. ¿Existe un equilibrio entre los beneficios y costos de los controles a implementar?	X			X	X		X	
10. ¿Tiene mecanismos de revisiones o supervisiones periódicas de las actividades u operaciones diarias relacionadas a TI?	X				X		X	
11. ¿Tiene mecanismos de monitoreo para conocer oportunamente si las operaciones relacionadas a TI, se desarrollan de acuerdo con los procedimientos establecidos en la Municipalidad?	X				X		X	



12. ¿Existe un plan de mejora continua de la gestión de riesgos de TI?	X		X		X		X	
13. ¿Se han identificado los riesgos de TI asociados a la corrupción?	X		X		X		X	
14. ¿Se ha cuantificado las pérdidas económicas relacionadas a la materialización de los riesgos de TI asociados a la corrupción?	X		X		X		X	
15. ¿Las partes interesadas son informadas sobre la gestión de riesgos de TI asociados a la corrupción?	X		X		X		X	
16. ¿Se realiza actividades de monitoreo de los riesgos TI asociados a la corrupción?	X		X		X		X	
17. ¿Tiene mecanismos que permitan identificar acontecimientos potenciales asociados a la corrupción que puedan afectar la ejecución de los procesos de TI con la consecuente afectación del logro de los objetivos institucionales?	X		X		X		X	

**Comentarios:**

En las preguntas 8 y 9 se recomienda que sean modificadas utilizando un lenguaje más coloquial, con la finalidad que sea entendible por el interlocutor.

- Asimismo la implementación de la recomendación planteada se concluye que las preguntas propuestas en el cuestionario están enfocadas en los objetivos del proyecto de tesis y cumplen con los aspectos de suficiencia, claridad, coherencia y relación.



Dr. Ing. OSCAR ZOCÓN ALVA

CIP 58444

Fecha: 2 de noviembre de 2019

**Ing. Mgtr. GONZALO MARTÍN VALDIVIA BENITES**

**Instrucción:**

A continuación, sírvase identificar si el ítem o pregunta cumple con los criterios de validez de suficiencia, claridad, coherencia y relevancia marcando con un aspa en la casilla que usted considere conveniente; del mismo modo de creerlo conveniente consignar sus comentarios; agradezco de antemano la atención al presente.


Falta las respuestas

N° de ítem de la encuesta	Validez							
	Suficiencia		Claridad		Coherencia		Relevancia	
	SI	NO	SI	NO	SI	NO	SI	NO
1. ¿Se ha implementado un sistema de gestión de riesgos de TI aplicando algún marco o estándar de trabajo?	X		X		X		X	
2. ¿El Sistema de gestión de riesgos está integrado al gobierno de la municipalidad?	X		X		X		X	
3. ¿Se han asignado roles y responsabilidades al personal respecto a la gestión de riesgos? <i>↓ TI</i>	X		X		X		X	
4. ¿Se cuenta con un inventario de activos de TI?	X							
5. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?		X		X		X		X
6. ¿Cuentan con un proceso de análisis de riesgo de TI que permita comprender su naturaleza del riesgo y determinar su nivel?	X		X	X	X		X	
7. ¿Cuentan con un proceso de valoración de riesgo de TI?	X		X		X		X	
8. ¿Cuentan con un proceso para <i>revisión</i> modificar el nivel de impacto y probabilidad de ocurrencia del riesgo de TI?	X		X		X		X	
9. ¿Existe un equilibrio entre los beneficios y costos de los controles a implementar?	X			X	X		X	
10. ¿Tiene mecanismos de revisiones o supervisiones periódicas de las actividades u operaciones diarias relacionadas a TI? <i>revisión</i>	X		X		X		X	
11. ¿Tiene mecanismos de monitoreo para conocer oportunamente, si las operaciones relacionadas a TI, se desarrollan de acuerdo con los procedimientos establecidos en la Municipalidad?	X		X		X		X	
12. ¿Existe un plan de mejora continua de la gestión de riesgos de TI?	X		X		X		X	

13. ¿Se han identificado los riesgos de TI asociados a la corrupción?	X		X		X		X	
14. ¿Se ha cuantificado las pérdidas económicas relacionadas a la materialización de los riesgos de TI asociados a la corrupción?	X		X		X		X	
15. ¿Las partes interesadas son informadas sobre la gestión de riesgos de TI asociados a la corrupción?	X		X		X		X	
16. ¿Se realiza actividades de <sup>revisión</sup> <del>revisión</del> de los riesgos TI asociados a la corrupción?	X			X	X		X	
17. ¿Tiene mecanismos que permitan identificar acontecimientos potenciales asociados a la corrupción que puedan afectar la ejecución de los procesos de TI con la consecuente afectación del logro de los objetivos institucionales?	X		X		X		X	

**Comentarios:**

- Se sugiere especificar dependencias en las preparatas.
- El ítem 5 está incluido en el ítem 6
- El ítem 8 se debe modificar o reducir
- el ítem 14 se debe modificar a revisión
- El ítem 16 " " " " "

  
GONZALO MARTÍN VALDIVIA BENITES

Fecha: 2 de noviembre de 2019g

## Resultados del Cuestionario aplicado en la Municipalidad 1

**CUESTIONARIO**

**Instrucciones:**

Gracias por su participación, el presente cuestionario tiene por finalidad recoger información de interés para el proyecto de tesis denominado "Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de la región de Lambayeque".

Al respecto, se le solicita que en las preguntas que a continuación se acompaña, elija la alternativa que considere adecuada, marcando para tal fin con una X en el espacio correspondiente.

Es de precisar, que el cuestionario es anónimo, además los datos proporcionados serán utilizados con fines académicos; en cuanto a la confidencialidad de la información proporcionada se aclara que la información será mostrada de manera general manteniendo en reserva la denominación de la entidad.

N° de ítem de la encuesta	Respuesta		Comentario
	SI	NO	
1. ¿Se ha implementado un sistema de gestión de riesgos de TI aplicando algún marco o estándar de trabajo?		X	
2. De ser afirmativa su respuesta anterior ¿El Sistema de gestión de riesgos está integrado al gobierno de la municipalidad?			NO Aplica
3. ¿Se han asignado roles y responsabilidades al personal respecto a la gestión de riesgos de TI?		X	
4. ¿Se cuenta con un inventario de activos de TI? <sup>1</sup>	X		SE Proporciono el Plan Operativo Institucional el que contiene la Información requerida.
5. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?		X	
6. ¿Cuentan con un proceso de análisis de riesgo <sup>2</sup> de TI que permita comprender su naturaleza del riesgo y determinar su nivel?		X	
7. ¿Cuentan con un proceso de valoración <sup>3</sup> de riesgo de TI?		X	

<sup>1</sup> De ser afirmativa su respuesta alcanzar el inventario de hardware y software según el formato entregado. Adicionalmente alcanzar el diagrama de red.

<sup>2</sup> El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia.

<sup>3</sup> Cuando se habla de valoración no se está hablando de lo que cuestan las cosas, sino de lo que vales.

N° de ítem de la encuesta	Respuesta		Comentario
	SI	NO	
8. ¿Cuentan con un proceso para reducir el nivel de impacto y probabilidad de ocurrencia del riesgo de TI?		X	
9. ¿Existe en un equilibrio entre los costos de los controles a implementar y los beneficios a obtener?		X	
10. ¿Tiene mecanismos de revisiones periódicas de las actividades u operaciones diarias relacionadas a TI?		X	
11. ¿Tiene mecanismos de revisión para conocer oportunamente, si las operaciones relacionadas a TI, se desarrollan de acuerdo con los procedimientos establecidos en la Municipalidad?		X	
12. ¿Existe un plan de mejora continua de la gestión de riesgos de TI?		X	
13. ¿Se han identificado los riesgos de TI asociados a la corrupción?		X	
14. ¿Se ha cuantificado las pérdidas económicas relacionadas a la materialización de los riesgos de TI asociados a la corrupción?		X	
15. ¿Las partes interesadas son informadas sobre la gestión de riesgos de TI asociados a la corrupción?		X	
16. ¿Se realiza actividades de revisión de los riesgos TI asociados a la corrupción?		X	
17. ¿Tiene mecanismos que permitan identificar acontecimientos potenciales asociados a la corrupción que puedan afectar la ejecución de los procesos de TI con la consecuente afectación del logro de los objetivos institucionales?		X	

## Resultados del cuestionario aplicado en la Municipalidad 2

### CUESTIONARIO

#### Instrucciones:

Gracias por su participación, el presente cuestionario tiene por finalidad recoger información de interés para el proyecto de tesis denominado "Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de la región de Lambayeque".

Al respecto, se le solicita que en las preguntas que a continuación se acompaña, elija la alternativa que considere adecuada, marcando para tal fin con una X en el espacio correspondiente.

Es de precisar, que el cuestionario es anónimo, además los datos proporcionados serán utilizados con fines académicos; en cuanto a la confidencialidad de la información proporcionada se aclara que la información será mostrada de manera general manteniendo en reserva la denominación de la entidad.

N° de ítem de la encuesta	Respuesta		Comentario
	SI	NO	
1. ¿Se ha implementado un sistema de gestión de riesgos de TI aplicando algún marco o estándar de trabajo?		X	
2. De ser afirmativa su respuesta anterior ¿El Sistema de gestión de riesgos está integrado al gobierno de la municipalidad?			No Aplica
3. ¿Se han asignado roles y responsabilidades al personal respecto a la gestión de riesgos de TI?		X	
4. ¿Se cuenta con un inventario de activos de TI? <sup>1</sup>	X		
5. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?		X	
6. ¿Cuentan con un proceso de análisis de riesgo <sup>2</sup> de TI que permita comprender su naturaleza del riesgo y determinar su nivel?		X	
7. ¿Cuentan con un proceso de valoración <sup>3</sup> de riesgo de TI?		X	

<sup>1</sup> De ser afirmativa su respuesta alcanzar el inventario de hardware y software según el formato entregado. Adicionalmente alcanzar el diagrama de red.

<sup>2</sup> El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia.

<sup>3</sup> Cuando se habla de valoración no se está hablando de lo que cuesten los roles, sino de lo que valen.

N° de ítem de la encuesta	Respuesta		Comentario
	SI	NO	
8. ¿Cuentan con un proceso para reducir el nivel de impacto y probabilidad de ocurrencia del riesgo de TI?		X	
9. ¿Existe en un equilibrio entre los costos de los controles a implementar y los beneficios a obtener?		X	
10. ¿Tiene mecanismos de revisiones periódicas de las actividades u operaciones diarias relacionadas a TI?		X	
11. ¿Tiene mecanismos de revisión para conocer oportunamente, si las operaciones relacionadas a TI, se desarrollan de acuerdo con los procedimientos establecidos en la Municipalidad?		X	
12. ¿Existe un plan de mejora continua de la gestión de riesgos de TI?		X	
13. ¿Se han identificado los riesgos de TI asociados a la corrupción?		X	
14. ¿Se ha cuantificado las pérdidas económicas relacionadas a la materialización de los riesgos de TI asociados a la corrupción?		X	
15. ¿Las partes interesadas son informadas sobre la gestión de riesgos de TI asociados a la corrupción?		X	
16. ¿Se realiza actividades de revisión de los riesgos TI asociados a la corrupción?		X	
17. ¿Tiene mecanismos que permitan identificar acontecimientos potenciales asociados a la corrupción que puedan afectar la ejecución de los procesos de TI con la consecuente afectación del logro de los objetivos institucionales?		X	

### Resultados del cuestionario aplicado en la Municipalidad 3

#### CUESTIONARIO

##### Instrucciones:

Gracias por su participación, el presente cuestionario tiene por finalidad recoger información de interés para el proyecto de tesis denominado "Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de la región de Lambayeque".

Al respecto, se le solicita que en las preguntas que a continuación se acompaña, elija la alternativa que considere adecuada, marcando para tal fin con una X en el espacio correspondiente.

Es de precisar, que el cuestionario es anónimo, además los datos proporcionados serán utilizados con fines académicos; en cuanto a la confidencialidad de la información proporcionada se aclara que la información será mostrada de manera general manteniendo en reserva la denominación de la entidad.

N° de ítem de la encuesta	Respuesta		Comentario
	SI	NO	
1. ¿Se ha implementado un sistema de gestión de riesgos de TI aplicando algún marco o estándar de trabajo?		X	Se realiza buenas practicas
2. De ser afirmativa su respuesta anterior ¿El Sistema de gestión de riesgos está integrado al gobierno de la municipalidad?		X	no, aplica
3. ¿Se han asignado roles y responsabilidades al personal respecto a la gestión de riesgos de TI?		X	Mejorar o Realizar Directiva..
4. ¿Se cuenta con un inventario de activos de TI?	X		
5. ¿Se han identificado los riesgos a los que están expuestos los activos de TI?	X		NO encuentra Documentos
6. ¿Cuentan con un proceso de análisis de riesgo <sup>2</sup> de TI que permita comprender su naturaleza del riesgo y determinar su nivel?		X	
7. ¿Cuentan con un proceso de valoración <sup>3</sup> de riesgo de TI?		X	

<sup>1</sup> De ser afirmativa su respuesta alcanzar el inventario de hardware y software según el formato entregado. Adicionalmente alcanzar el diagrama de red.

<sup>2</sup> El análisis del riesgo implica una consideración detallada de inestabilidades, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia.

<sup>3</sup> Cuando se habla de valoración no se está hablando de lo que cuesten las cosas, sino de lo que valen.

N° de ítem de la encuesta	Respuesta		Comentario
	SI	NO	
8. ¿Cuentan con un proceso para reducir el nivel de impacto y probabilidad de ocurrencia del riesgo de TI?		X	Realizan buenas Prácticas
9. ¿Existe en un equilibrio entre los costos de los controles a implementar y los beneficios a obtener?		X	
10. ¿Tiene mecanismos de revisiones periódicas de las actividades u operaciones diarias relacionadas a TI?		X	Realizar eventualmente Buenas Prácticas
11. ¿Tiene mecanismos de revisión para conocer oportunamente, si las operaciones relacionadas a TI, se desarrollan de acuerdo con los procedimientos establecidos en la Municipalidad?		X	Realiza Buenas Prácticas
12. ¿Existe un plan de mejora continua de la gestión de riesgos de TI?		X	Aceptar el Proyecto de Investigación para mejorar e implementar Gestión Riesgo
13. ¿Se han identificado los riesgos de TI asociados a la corrupción?		X	Proyecto contribuye a la identificación de los mismos
14. ¿Se ha cuantificado las pérdidas económicas relacionadas a la materialización de los riesgos de TI asociados a la corrupción?		X	
15. ¿Las partes interesadas son informadas sobre la gestión de riesgos de TI asociados a la corrupción?	X		INFO-GERENCIA
16. ¿Se realiza actividades de revisión de los riesgos TI asociados a la corrupción?		X	
17. ¿Tiene mecanismos que permitan identificar acontecimientos potenciales asociados a la corrupción que puedan afectar la ejecución de los procesos de TI con la consecuente afectación del logro de los objetivos institucionales?		X	

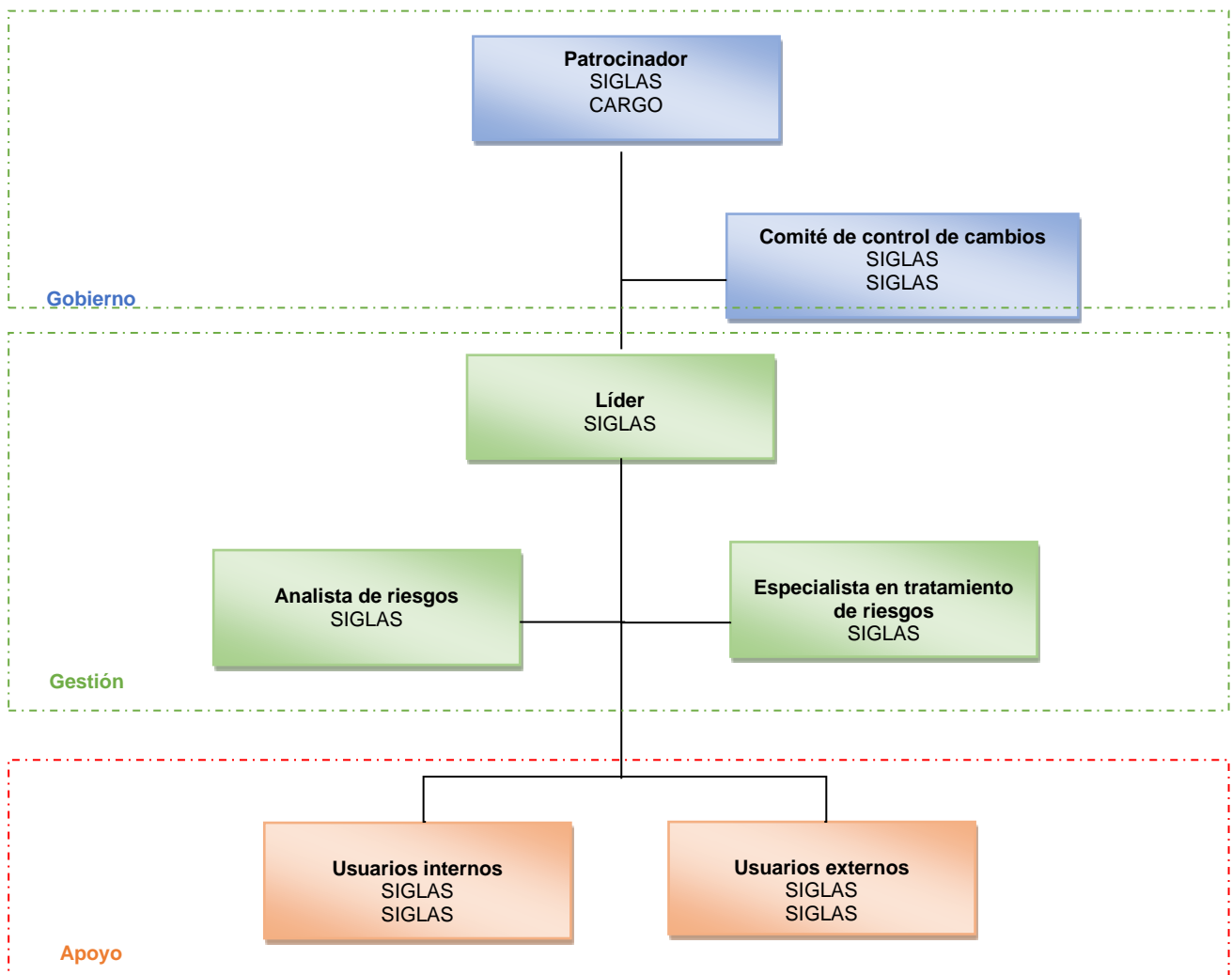
**Anexo n.º 4:**  
**Formatos del modelo**

**F-1**  
**Formato del documento de conformación del equipo y**  
**asignación de responsabilidades por actividades.**

**CUADRO DE ADQUISICIONES DEL PERSONAL**

Rol	Siglas de la persona	Origen	Fecha	
			Inicio	Fin
Patrocinador				
Comité de Control de cambios				
Líder				
Analista de riesgo				
Especialista de tratamiento de riesgos				
Usuarios internos				
Usuarios externos				

## ORGANIGRAMA



**Leyenda:**

- Azul** : Gobierno
- Verde** : Gestión
- Naranja** : Apoyo

## MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES

FASE	Actividades	Gobierno		Gestión			Apoyo		
		P	CCC	L	AR	ETR	UI	UE	
ACTIVIDADES PRELIMINARES	Conformación del equipo y asignación de roles por actividades.								
	Definir la matriz de comunicación.								
	Documentar y comunicar el trabajo realizado.								
	De ser el caso actualizar y comunicar los documentos.								
CONTEXTO, ALCANCE Y CRITERIO	Definir el contexto externo.								
	Establecer el alcance.								
	Determinar los criterios.								
	Documentar y comunicar el trabajo realizado.								
	De ser el caso actualizar y comunicar los documentos.								
EVALUACIÓN DEL RIESGO	Identificación del riesgo	Identificar y valorar los activos críticos de las municipalidades.							
		Identificar y valorar las amenazas a las que están expuestas.							
		Identificar y valorar las vulnerabilidades.							
		Documentar y comunicar el trabajo realizado.							
		De ser el caso actualizar y comunicar los documentos.							
	Análisis y valoración del riesgo	Evaluación de consecuencias.							
		Evaluación de probabilidad de escenarios.							
		Determinación del nivel de riesgos.							
		Valorar los riesgos.							
		Documentar y comunicar el trabajo realizado.							
		De ser el caso actualizar y comunicar los documentos.							
TRATAMIENTO DEL RIESGO	Diseñar y ejecutar planes de mitigación de riesgos.								
	Documentar y comunicar el trabajo realizado.								
	Identificar cambios en la estrategia de protección.								
	Documentar y comunicar el trabajo realizado.								
	De ser el caso actualizar y comunicar los documentos.								
SEGUIMIENTO O REVISIÓN	Seleccionar enfoques de seguimiento o revisión.								
	Ejecutar el seguimiento y revisión de los riesgos.								
	De ser el caso rediseñar el modelo propuesto.								

### LEYENDA DE CÓDIGOS

Responsabilidades	Gobierno	Gestión	Apoyo
Responsable (R) ¿Quién realiza la tarea? ¿Quién dirige la tarea? Quien rinde cuentas (A) ¿Quién rinde cuentas por el éxito y la consecución de la tarea? Consultado (C) ¿Quién está proporcionando información? Informado (I) ¿Quién está recibiendo información?	P = Patrocinador CCC = Comité de Control de Cambios	L = Líder AR= Analista de riesgo ETR= Especialista de tratamiento de riesgo	UI = Usuarios internos UE = Usuarios externos

<b>OBSERVACIONES</b>		
<b>AUTORIZACIÓN</b>		
<b>Alcalde</b>	<b>Gerente Municipal</b>	<b>Gerente de Recursos Humanos</b>
Fecha:	Fecha:	Fecha:

**F-2**  
**Formato movimiento de personal.**

**FORMATO DE MOVIMIENTO  
DE PERSONAL**

1. TIPO DE MOVIMIENTO		
Ingreso <input type="radio"/>	Retiro <input type="radio"/>	Reemplazo <input type="radio"/>
2. TIPO DE PUESTO		
Patrocinador <input type="radio"/>	Líder <input type="radio"/>	Analista de riesgo <input type="radio"/>
Especialista de tratamiento de riesgos <input type="radio"/>	Usuarios internos <input type="radio"/>	Usuarios externos <input type="radio"/>
3. MOTIVO		
Renuncia <input type="radio"/>	Cambio de funciones <input type="radio"/>	Nueva asignación <input type="radio"/>
Aumento de trabajo <input type="radio"/>	Otro <input type="radio"/>	_____
4. DATOS PERSONALES		
DNI n.º	Nombres	Apellidos
5. OBSERVACIONES		
6. AUTORIZACIÓN		
<b>Gerente Municipal</b>	<b>Gerente de Recursos Humanos</b>	<b>Líder</b>
Fecha:	Fecha:	Fecha:





OBSERVACIONES		
AUTORIZACIÓN		
<b>Gerente Municipal</b>	<b>Líder</b>	<b>Usuario Interno</b>
Fecha:	Fecha:	Fecha:

**F-4**  
**Formato de determinación de contexto.**

## FORMATO DE DETERMINACIÓN DE CONTEXTO

7. FACTORES INTERNOS (Revisar Plan Estratégico u otros relacionados)		
MISION	VISION	VALORES
		1.
		2.
		3.
		4.
		5.
OBJETIVOS ESTRATEGICOS		
1.		
2.		
3.		
4.		
FACTORES CRÍTICOS DE ÉXITO		
1.		
2.		
3.		
4.		
ROLES Y FUNCIONES RELEVANTES DE LOS INVOLUCRADOS (Revisar el Manual de Organización y Funciones)		
CARGO _____		
DNI n.º	Nombres	Apellidos
Relación contractual		Dependencia laboral
Descripción del rol		
Funciones relevantes		
1.		
2.		
3.		
Habilidades y conocimientos	Sistemas relacionados	Activos relacionados

Opinión del personal relacionada a la implementación de la gestión de riesgos		
CARGO _____		
DNI n.º	Nombres	Apellidos
Relación contractual		Dependencia laboral
Descripción del rol		
Funciones relevantes		
1. 2. 3.		
Habilidades y conocimientos	Sistemas relacionados	Activos relacionados
Opinión del personal relacionada a la implementación de la gestión de riesgos		
8. FACTORES EXTERNOS (Revisar el repositorio de factores externos)		
a. SOCIALES		
REGIONAL	NACIONAL	INTERNACIONAL
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.
b. CULTURALES		
INTERNACIONAL	NACIONAL	REGIONAL
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.

<b>c. POLITICOS</b>		
INTERNACIONAL	NACIONAL	REGIONAL
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.
<b>d. FINANCIEROS</b>		
INTERNACIONAL	NACIONAL	REGIONAL
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.
<b>e. TECNOLOGICOS</b>		
INTERNACIONAL	NACIONAL	REGIONAL
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.
6.	6.	6.
<b>f. AMBIENTALES</b>		
INTERNACIONAL	NACIONAL	REGIONAL
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.
<b>g. OTROS: _____</b>		
INTERNACIONAL	NACIONAL	REGIONAL
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.
<b>9. CUMPLIMIENTO NORMATIVO (Revisar el repositorio de base legal)</b>		
<b>a. NORMA DE CREACIÓN</b>		
1.		

<b>b. NORMAS GENERALES</b>	
1.	
2.	
3.	
4.	
5.	
<b>c. NORMAS PRESUPUESTALES</b>	
1.	
2.	
3.	
4.	
5.	
<b>d. NORMAS DE CONTRATACIONES</b>	
1.	
2.	
3.	
4.	
5.	
<b>e. NORMAS DE RECURSOS HUMANOS</b>	
1.	
2.	
3.	
4.	
5.	
<b>f. NORMAS DE ADMINISTRACIÓN TRIBUTARIA</b>	
1.	
2.	
3.	
4.	
<b>g. NORMAS DE CONTROL</b>	
1.	
2.	
3.	
4.	
5.	
<b>h. NORMAS RELACIONADAS A TECNOLOGÍAS DE INFORMACIÓN</b>	
1.	
2.	
3.	
4.	

<b>i. NORMAS TÉCNICAS PERUANAS RELACIONADAS A TECNOLOGÍAS DE INFORMACIÓN</b>		
1.		
2.		
3.		
4.		
5.		
<b>j. OTRAS NORMAS</b>		
1.		
2.		
3.		
4.		
5.		
<b>k. NORMAS FUNCIONAMIENTO</b>		
1.		
2.		
3.		
<b>l. NORMAS INTERNAS</b>		
1.		
2.		
3.		
4.		
<b>DATOS RELEVANTES DE LOS INVOLUCRADOS EXTERNOS (Ciudadanos, sociedad civil organizada, proveedores, Ministerio Público, Poder Judicial, etc)</b>		
<b>ENTIDAD</b> _____		
<b>Datos del representante</b>		
<b>DNI n.º</b>	<b>Nombres</b>	<b>Apellidos</b>
<b>Descripción del rol de la entidad</b>		
<b>DATOS RELEVANTES DE LOS INVOLUCRADOS EXTERNOS (Ciudadanos, sociedad civil organizada, proveedores, Ministerio Público, Poder Judicial, etc)</b>		
<b>ENTIDAD</b> _____		
<b>Datos del representante</b>		
<b>DNI n.º</b>	<b>Nombres</b>	<b>Apellidos</b>
<b>Descripción del rol de la entidad</b>		

10. MACROPROCESOS		
11. OBSERVACIONES		
12. AUTORIZACIÓN		
Patrocinador	Líder	Analista de riesgos
Fecha:	Fecha:	Fecha:

**F-5**  
**Formato de alcance.**  
**FORMATO DE ALCANCE**

13. OBJETIVO								
14. RESULTADOS ESPERADOS POR ACTIVIDAD			15. TIPO DE RECURSOS					
FASE	ACTIVIDAD	RESULTADOS ESPERADOS	PERSONAL			MATERIALES O MAQUINARIA		
			SIGLAS	UNIDAD	CANTIDAD	DESCRIPCION	UNIDAD	CANTIDAD
<b>ACTIVIDADES PRELIMINARES</b>	1. Conformación del equipo y asignación de roles por actividades.							
	2. Definir la matriz de comunicación.							
	3. Documentar y comunicar el trabajo realizado.							
	4. De ser el caso actualizar y comunicar los documentos.							
<b>CONTEXTO, ALCANCE, RESTRICCIONES Y CRITERIOS</b>	1. Determinar el contexto.							
	2. Determinar el alcance.							
	3. Determinar los criterios.							
	4. Documentar y comunicar el trabajo realizado.							
	5. De ser el caso actualizar y comunicar los documentos.							

<b>EVALUACIÓN DEL RIESGO</b>	<b>IDENTIFICACIÓN DEL RIESGO</b>	1. Identificar y valorar los activos críticos de las municipalidades.							
		2. Identificar y valorar las amenazas a las que están expuestas.							
		3. Identificar y valorar las vulnerabilidades.							
		4. De ser el caso actualizar los documentos.							
		5. Documentar y comunicar el trabajo realizado.							
	<b>ANÁLISIS Y VALORACIÓN DEL RIESGO</b>	1. Evaluación de consecuencias.							
		2. Evaluación de probabilidad de escenarios.							
		3. Determinación del nivel de riesgos.							
		4. Valorar los riesgos.							
		5. Documentar y comunicar el trabajo realizado.							
		6. De ser el caso actualizar y comunicar los documentos.							
<b>TRATAMIENTO DEL RIESGO</b>	1. Diseñar y ejecutar planes de mitigación de riesgos.								
	2. Documentar y comunicar el trabajo realizado.								
	3. Identificar cambios en la estrategia de protección.								
	4. Documentar y comunicar el trabajo realizado.								
	5. De ser el caso actualizar y comunicar los documentos.								

<b>SEGUIMIENTO REVISIÓN</b>	1. Ejecutar el seguimiento del resultado esperado de las actividades.							
	2. Ejecutar el seguimiento del modelo.							
	3. De ser el caso rediseñar el modelo propuesto							
<b>16. EXCLUSIONES</b>								
1.	2.	3.						
4.	5.	6.						
<b>17. RESTRICCIONES</b>								
<b>ORGANIZACIONALES</b>			<b>TÉCNICAS</b>			<b>ECONOMICAS</b>		
<b>LEGALES</b>			<b>OTRO _____</b>					
<b>18. CRITERIOS DE ACEPTACIÓN</b>								
<b>TECNICOS</b>			<b>CALIDAD</b>			<b>ADMINISTRATIVO</b>		

**19. OBSERVACIONES****20. AUTORIZACIÓN**

<b>20. AUTORIZACIÓN</b>			
<b>PATROCINADOR</b>	<b>LIDER</b>	<b>ANALISTA DE RIESGOS</b>	<b>ESPECIALISTA EN TRATAMIENTO DEL RIESGO</b>
Fecha:	Fecha:	Fecha:	Fecha:

**F-6**  
**Formato de criterios y dimensiones**

**FORMATO DE SELECCIÓN DE CRITERIOS Y  
DIMENSIONES**

<b>1. CRITERIOS</b>		
Antisoborno <input type="radio"/>		
Bajo	Medio	Alto
Multas <input type="radio"/>		
Bajo	Medio	Alto
Demandas <input type="radio"/>		
Bajo	Medio	Alto
Investigaciones <input type="radio"/>		
Bajo	Medio	Alto
Tiempo máximo de inactividad <input type="radio"/>		
Bajo	Medio	Alto
Tiempo de recuperación del servicio <input type="radio"/>		
Bajo	Medio	Alto
Productividad <input type="radio"/>		
Bajo	Medio	Alto
Financiero <input type="radio"/>		
Bajo	Medio	Alto
Reputación <input type="radio"/>		
Bajo	Medio	Alto
Seguridad <input type="radio"/>		
Bajo	Medio	Alto
Salud <input type="radio"/>		
Bajo	Medio	Alto

Tipo de información <input type="radio"/>		
Bajo	Medio	Alto
Otro <input type="radio"/> _____		
Bajo	Medio	Alto
2. DIMENSIONES		
Disponibilidad <input type="radio"/>	Integridad <input type="radio"/>	Confidencialidad <input type="radio"/>
Trazabilidad <input type="radio"/>	Autenticidad <input type="radio"/>	Otro _____
3. OBSERVACIONES		
4. AUTORIZACIÓN		
Patrocinador	Líder	Analista de riesgos

Logo de la municipalidad

**F-8.1**  
**Formato de**  
**identificación y**  
**valoración de**  
**activos críticos**

**F-7.1**

**Formato de identificación y valoración de activos críticos**

**FORMATO DE IDENTIFICACIÓN DE ACTIVOS**

<b>Procesos</b>	<b>Personas</b>	<b>Información</b>	<b>Software</b>	<b>Hardware</b>	<b>Servicios</b>	<b>Otro activo</b>
¿Qué procesos realizan las personas de la municipalidad para cumplir con sus funciones?	¿Qué personas se necesitan para realizar estos procesos?	¿Qué información necesitan las personas de la municipalidad para realizar su trabajo?	¿Qué software necesita las personas de la municipalidad para realizar su trabajo?	¿Qué hardware necesitan las personas de la municipalidad para realizar su trabajo?	¿Qué servicios necesitan las personas de la municipalidad para realizar su trabajo?	¿Qué otros activos están estrechamente relacionados con estos activos?

## FORMATO DE VALORACIÓN DE ACTIVOS CRÍTICOS

Activos por clase	Clase de activos relacionados											Responsable de	Quién lo usa	Dimensiones de valoración				Valoración	Activo crítico	Justificación de la selección
	Personal	Datos	Servicios	Software interno	Software externo	Hardware	Redes internas	Redes externas	Almacenamiento	Equipamiento auxiliar	Instalaciones			Otros	Disponibilidad	Integridad	Confidencialidad			

[P] Personal																				

[D] Datos																				

[S] Servicios																				





OBSERVACIONES		
AUTORIZACIÓN		
<b>Sponsor</b>	<b>Líder</b>	<b>Analista de riesgos</b>
Fecha:	Fecha:	Fecha:

En cuanto a los formatos:

- F-7.2 Formato de identificación y valoración de amenazas.
- F-7.3 Formato de identificación y valoración de vulnerabilidades.
- F-7.4 Formato de análisis y valoración del riesgo.
- F-7.5 Formato del mapa de calor
- F-8.1 Formato de tratamiento del riesgo
- F-8.2 Formato de tratamiento del riesgo
- F-9 Formato de seguimiento o revisión de riesgos.

Estos se encontrarán en archivo en Excel

**F-10**  
**Formato de acta de seguimiento o revisión.**

**FORMATO ACTA DE SEGUIMIENTO O CONTROL N.º XX**

<b>Fecha y hora</b>	<i>Registrar la fecha de aprobación en el formato dd/mm/aaaa y la hora en formato de 24 horas</i>	<b>Realizada por</b>	<i>Registrar las iniciales de la persona que realiza el seguimiento o control</i>
<b>Lugar</b>	<i>Registrar el lugar donde se llevó a cabo el seguimiento</i>	<b>Objetivo</b>	<i>Registrar lo que se quiere conseguir con el seguimiento o control</i>

<b>Asistentes</b>		
Persona	Cargo	Área
<i>Registrar el nombre de la persona asistente</i>	<i>Registrar su cargo</i>	<i>Registrar área</i>
<b>Antecedentes</b>		
<b>Qué se debe leer previamente</b>	<b>Responsable</b>	
<i>Registrar los documentos que se deben de leer previamente</i>	<i>Registrar el nombre de la persona responsable de la lectura de los antecedentes</i>	
<b>Qué se debe presentar en la reunión</b>	<b>Responsable</b>	
<i>Registrar los documentos que se deben de presentar en la reunión</i>	<i>Registrar el nombre de la persona que debe traer los documentos a la reunión</i>	

<b>Agenda</b>		
Actividad	Responsable	Tiempo
<i>Registrar las actividades a realizarse durante la reunión dentro de estos se puede tratar riesgos actuales potenciales, riesgos actuales sucedidos, o nuevos riesgos detectados</i>	<i>Registrar las siglas del responsable de dirigir la actividad</i>	<i>Registrar el tiempo asignado a la actividad</i>

<b>Conclusiones</b>	
<b>01</b>	<i>Registrar las conclusiones a las que se arriben</i>
<b>02</b>	
<b>03</b>	
<b>04</b>	
<b>05</b>	

<b>Acciones</b>	<b>Responsable</b>	<b>Fecha Límite</b>	<b>Observaciones</b>
<i>Registrar las acciones producto de las conclusiones arribadas</i>	<i>Registrar las siglas del responsable de dirigir las acciones</i>	<i>Registrar la fecha límite para culminar las acciones en formato dd/mm/aaa</i>	<i>De ser el caso registrar observaciones</i>

<i>Acciones</i>	<i>Responsable</i>	<i>Fecha Límite</i>	<i>Observaciones</i>

<i>Notas especiales</i>	
01	De ser el caso registrar anotaciones especiales
02	
03	

<b>OBSERVACIONES</b>		
<b>AUTORIZACIÓN</b>		
<b>Líder</b>	<b>Analista de riesgos</b>	<b>Especialista en tratamiento de riesgos</b>
Fecha:	Fecha:	Fecha:

**F-11**  
**Formato de procedimiento y registro de controversias.**

**FORMATO DE PROCEDIMIENTO Y REGISTRO  
DE CONTROVESIAS N.º XX**

<b>Procedimiento</b>					
1. Se captan las controversias a través de la observación, o alguna otra evidencia que lo exprese. 2. Se registran las controversias:					
<b>Registro de control de controversias</b>					
Código de polémica	Descripción	Acciones de solución	Responsable	Fecha	Resultado obtenido
3. Se revisa el Registro de Control de Controversias en la reunión programada <ol style="list-style-type: none"> <li>a) Determinar las soluciones</li> <li>b) Revisar si las soluciones programadas</li> <li>c) Si la controversia ha sido resuelta</li> <li>d) Si la controversia no ha sido resuelta se vuelve al paso a)</li> </ol> 4. En caso de que una polémica no pueda ser resuelta o en caso se haya vuelto un problema, deberá ser abordada con el siguiente método no deberá de demorar más de 3 días: <ol style="list-style-type: none"> <li>a) Se tratará de resolver por el Gerente de Administración</li> <li>b) En última instancia será resuelta Comité de Control de Controversias.</li> </ol>					
<b>Procedimiento para actualizar el Modelo.</b>					
El Modelo de Gestión de Riesgos deberá ser revisado y/o actualizado cada vez que: <ol style="list-style-type: none"> <li>1. Haya una solicitud de cambio aprobada que impacte el mismo.</li> <li>2. Haya evidencias de resistencia al cambio.</li> <li>3. Haya evidencias de deficiencias en el modelo.</li> </ol>					

<b>OBSERVACIONES</b>		
<b>AUTORIZACIÓN</b>		
<b>Patrocinador</b>	<b>Líder</b>	<b>Analista de riesgos</b>
Fecha:	Fecha:	Fecha:

**Anexo n.º 5:****Repositorios del modelo****R-1****Repositorio de base legal aplicable a los gobiernos provinciales****REPOSITORIO DE BASE LEGAL**

La normativa principal que la Municipalidad debe cumplir en el desarrollo de sus actividades y operaciones, así como relacionadas con el proceso en donde se aplicará el modelo, podrían ser las siguientes:

<b>1. NORMAS GENERALES</b>	
1.	Constitución Política del Perú de 1993 de 29 de diciembre de 1993.
2.	Ley de Bases de la Descentralización, aprobada con Ley n.º 27783 de 17 de julio de 2002.
3.	Ley del Procedimiento Administrativo General, aprobada con Ley n.º 27444 de 10 de abril de 2001.
4.	Ley General del Sistema Nacional de Tesorería, aprobada mediante Ley n.º 28693 de 21 de marzo de 2006.
5.	Ley Marco del Empleo Público, aprobada mediante Ley n.º 28175 de 18 de febrero de 2004.
6.	Ley del Código de Ética de la Función Pública, aprobada mediante Ley n.º 27815 de 12 de agosto de 2002.
7.	Reglamento de la Ley del Código de Ética de la Función Pública, aprobada mediante Decreto Supremo n.º 033-2005-PCM de 18 de abril de 2005.
8.	
<b>2. NORMAS PRESUPUESTALES</b>	
1.	Texto Único Ordenado de la Ley n.º 28411, Ley General del Sistema Nacional de Presupuesto, aprobado con Decreto Supremo n.º 304-2012-EF de 29 de diciembre de 2012.
2.	Ley de Presupuesto del Sector Público para el año fiscal 2014, aprobada con Ley n.º 30114 de 30 de noviembre de 2013.
3.	Ley del Presupuesto del Sector Público para el año fiscal 2015, aprobada con Ley n.º 30281 de 30 de noviembre de 2014.
4.	Ley del Presupuesto del Sector Público para el año fiscal 2016, aprobada con Ley n.º 30372 de 30 de noviembre de 2015.
5.	Ley del Presupuesto del Sector Público para el año fiscal 2017, aprobada con Ley n.º 30518 de 30 de noviembre de 2016.
6.	Directiva n.º 005-2010-EF/76.01, Directiva para la ejecución presupuestaria, aprobada con Resolución Directoral n.º 030-2010-EF/76.01 de 27 de diciembre de 2010, modificada por Resolución Directoral n.º 022-2011-EF/50.01 de 20 de diciembre de 2011.
7.	
<b>3. NORMAS DE CONTRATACIONES</b>	
1.	Ley de Contrataciones del Estado aprobada por Ley n.º 1017, de 3 de junio de 2008, vigente a partir de 1 de febrero de 2009 y sus modificatorias.
2.	Reglamento de la Ley de Contrataciones del Estado aprobado mediante Decreto Supremo n.º 184-2008-EF, de 31 de diciembre de 2008, vigente a partir de 1 de febrero de 2009 y sus modificatorias.
3.	Ley de Contrataciones del Estado, aprobada por Ley n.º 30225, de 10 de julio de 2014, vigente a partir de 9 de enero de 2016 y sus modificatorias.
4.	Reglamento de la Ley de Contrataciones del Estado aprobado mediante Decreto Supremo n.º 350-2015-EF de 9 de diciembre de 2015, vigente a partir de 9 de enero de 2016 y sus modificatorias.
5.	

<b>4. NORMAS DE RECURSOS HUMANOS</b>	
1.	Ley de Bases de la Carrera Administrativa y de Remuneraciones del Sector Público, aprobada por Decreto Legislativo n.° 276 de 6 de marzo de 1984.
2.	Reglamento de la Ley de Bases de la Carrera Administrativa y de Remuneraciones del Sector Público, aprobado por Decreto Supremo n.° 005-90-PCM de 15 de enero de 1990.
3.	Régimen Especial de Contratación Administrativa de Servicios, aprobado por Decreto Legislativo n.° 1057 de 27 de junio de 2008.
4.	Reglamento del Decreto Legislativo n.° 1057, aprobado mediante Decreto Supremo n.° 075-2008-PCM de 24 de noviembre de 2008.
5.	
<b>5. NORMAS DE ADMINISTRACIÓN TRIBUTARIA</b>	
1.	Texto Único Ordenado de la Ley de Tributación Municipal, aprobado mediante Decreto Supremo n.° 156-2004-EF de 11 de noviembre de 2004
2.	
<b>6. NORMAS DE CONTROL</b>	
1.	Ley de Control Interno de las Entidades del Estado, aprobada por Ley n.° 28716 de 16 de abril de 2006.
2.	Normas de Control Interno, aprobadas por Resolución de Contraloría n.° 302-2006-CG de 30 de octubre de 2006.
3.	Guía para la Implementación del Sistema de Control Interno en las entidades del Estado, aprobada por Resolución de Contraloría n.° 458-2008-CG, de 28 de octubre de 2008.
4.	
<b>7. NORMAS RELACIONADAS A TECNOLOGÍAS DE INFORMACIÓN</b>	
1.	Ley n.° 28612, Ley que norma el uso, adquisición y adecuación del software en la administración pública.
2.	Decreto Supremo n.° 024-2006-PCM, de fecha 24 de mayo de 2006, que aprueba el Reglamento de la Ley n.° 28612, Ley que norma el uso, adquisición y adecuación de software en la administración pública.
3.	Decreto Supremo n.° 004-2013-PCM, publicado el 09 de enero de 2013, que aprueba la Política Nacional de Modernización de la Gestión Pública.
4.	Decreto Supremo n.° 081-2013-PCM, publicado el 10 de julio del 2013, que aprueba la Política Nacional de Gobierno Electrónico 2013-2017.
5.	Decreto Supremo n.° 026-2016-PCM, publicada el 24 de abril del 2016, que aprueba Medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado
6.	Resolución Ministerial n.° 073-2004-PCM, de fecha 16 de marzo del 2004, que aprueba la "Guía para la Administración Eficiente del Software Legal en la Administración Pública".
7.	Resolución Ministerial n.° 139-2004-PCM, de fecha 27 de mayo de 2004, que aprueba la "Guía Técnica sobre evaluación de software para la Administración Pública".
8.	Resolución de Contraloría General n.° 320-2006-CG, de fecha 30 de octubre de 2006, que aprueba las Normas de Control Interno de aplicación en todas las entidades del Estado, de conformidad con lo establecido por la Ley n.° 28716, Ley de Control Interno de las Entidades del Estado.
9.	Resolución de Contraloría General n.° 458-2008-CG, de fecha 28 de octubre del 2008, que aprueba la "Guía para la implementación del Sistema de Control Interno de las entidades del Estado".
10.	
<b>8. NORMAS TÉCNICAS PERUANAS RELACIONADAS A TECNOLOGÍAS DE INFORMACIÓN</b>	
1.	ETP-ISO/IEC TS 22237-1:2019. Tecnología de la información. Instalaciones e infraestructuras de centros de datos. Parte 1: Conceptos generales. 1ª Edición
2.	ETP-ISO/IEC TS 22237-2:2019. Tecnología de la información. Instalaciones e infraestructuras de centros de datos. Parte 2: Construcción de edificio. 1ª Edición
3.	ETP-ISO/IEC TS 22237-3:2019. Tecnología de la información. Instalaciones e infraestructuras de centros de datos. Parte 3: Distribución de energía. 1ª Edición
4.	ETP-ISO/IEC TS 22237-4:2019. Tecnología de la información. Instalaciones e infraestructuras de centros de datos. Parte 4: Control ambiental. 1ª Edición

5.	ETP-ISO/IEC TS 22237-5:2019. Tecnología de la información. Instalaciones e infraestructuras de centros de datos. Parte 5: Infraestructura de cableado de telecomunicaciones. 1ª Edición
6.	ETP-ISO/IEC TS 22237-7:2019. Tecnología de la información. Instalaciones e infraestructuras de centros de datos. Parte 7: Información de administración y operación. 1ª Edición
7.	NTP 291.100-1:2009. INGENIERÍA DE SOFTWARE. Modelos de procesos y evaluación para desarrollo y mantenimiento de software. Parte 1: Definición de conceptos y productos 1a Edición
8.	NTP 291.100-2:2009. INGENIERÍA DE SOFTWARE. Modelos de procesos y evaluación para desarrollo y mantenimiento de software. Parte 2: Requisitos de procesos (MoProSoft) 1a Edición
9.	NTP 291.100-3:2009. INGENIERÍA DE SOFTWARE. Modelos de procesos y evaluación para desarrollo y mantenimiento de software. Parte 3: Guía de implantación de procesos 1a Edición
10.	NTP 291.100-4:2009. INGENIERÍA DE SOFTWARE. Modelos de procesos y evaluación para desarrollo y mantenimiento de software. Parte 4: Directrices para la evaluación de procesos (EvalProSoft)
11.	NTP ISO/IEC 12119 2005. TECNOLOGIA DE LA INFORMACION. Paquetes software. Requerimientos de calidad y pruebas.
12.	NTP ISO/IEC 12119 2005. TECNOLOGIA DE LA INFORMACION. Paquetes software. Requerimientos de calidad y pruebas.
13.	NTP ISO/IEC 12207: 2016. Ingeniería de software y sistemas. Procesos del ciclo de vida del software. 3ª Edición
14.	NTP ISO/IEC 14598-1 2005. TECNOLOGIA DE LA INFORMACION. Evaluación del producto software. Parte 1: Visión general. 1a. ed.
15.	NTP ISO/IEC 14598-1 2005. TECNOLOGIA DE LA INFORMACION. Evaluación del producto software. Parte 1: Visión general. 1a. ed.
16.	NTP ISO/IEC 14598-2 2005. INGENIERIA DE SOFTWARE. Evaluación del producto. Parte 2: Planificación y gestión
17.	NTP ISO/IEC 14598-2 2005. INGENIERIA DE SOFTWARE. Evaluación del producto. Parte 2: Planificación y gestión
18.	NTP ISO/IEC 14598-3 2005. INGENIERIA DE SOFTWARE. Evaluación del producto. Parte 3: Proceso para desarrolladores
19.	NTP ISO/IEC 14598-3 2005. INGENIERIA DE SOFTWARE. Evaluación del producto. Parte 3: Proceso para desarrolladores
20.	NTP ISO/IEC 14598-4 2006. INGENIERIA DE SOFTWARE. Evaluación del producto. Parte 4: Proceso para adquirientes
21.	NTP ISO/IEC 14598-4 2006. INGENIERIA DE SOFTWARE. Evaluación del producto. Parte 4: Proceso para adquirientes
22.	NTP ISO/IEC 14598-5 2007. TECNOLOGÍA DE LA INFORMACIÓN. Evaluación del producto software. Parte 5: Proceso para evaluadores
23.	NTP ISO/IEC 14598-5 2007. TECNOLOGÍA DE LA INFORMACIÓN. Evaluación del producto software. Parte 5: Proceso para evaluadores
24.	NTP ISO/IEC 15288:2014. INGENIERÍA DE SISTEMAS Y SOFTWARE: Procesos del ciclo de vida del sistema
25.	NTP ISO/IEC 15419:2016. Tecnología de la información. Identificación automática y técnicas de captura de datos. Imagen digital de código de barras y pruebas de rendimiento de impresión. 2ª Edición (EQV. ISO/IEC 15419:2009)
26.	NTP ISO/IEC 20000-2:2008. Tecnología de la Información. Gestión del servicio. Parte 2: Código de buenas prácticas. 1a Edición
27.	NTP ISO/IEC 2382-1:2004 (revisada el 2013). CÓDIGO DE BARRAS. Tecnología de la información. Vocabulario. Parte 1: Términos básicos
28.	NTP ISO/IEC 27006:2009. EDI. Tecnología de la información. Técnicas de seguridad. Requisitos para los organismos que realizan auditorías y certificaciones de los sistemas de gestión de la seguridad de la información
29.	NTP ISO/IEC 38500:2016. Tecnología de información. Gobernanza de TI para la organización. 2ª Edición

30. NTP ISO/IEC 38500:2016. Tecnología de información. Gobernanza de TI para la organización. 2ª Edición
31. NTP ISO/IEC 90003:2008(revisada el 2013). INGENIERÍA DE SOFTWARE. Guía para la aplicación de la ISO 9001:2000 al software
32. NTP ISO/IEC 9126-1 2004. INGENIERIA DE SOFTWARE. Calidad del producto. Parte 1: Modelo de calidad.
33. NTP ISO/IEC-TR 15271 2007. TECNOLOGÍA DE LA INFORMACIÓN. Guía para la NTP-ISO/IEC 12207 (Proceso del ciclo de vida del software)
34. NTP ISO/IEC-TR 9126-2 2004. INGENIERIA DE SOFTWARE. Calidad del producto. Parte 2: Métricas externas.
35. NTP ISO/IEC-TR 9126-3:2005. INGENIERIA DE SOFTWARE. Calidad del producto. Parte 3: Métricas internas. 1a. ed.
36. NTP ISO/IEC-TR 9126-4:2005. INGENIERIA DE SOFTWARE. Calidad del producto. Parte 4: Métricas de calidad en uso.
37. NTP RT ISO/IEC-TR 27008:2013. TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Lineamientos para auditores sobre controles de seguridad de la información
38. NTP-IEC 60950-1: 2016. Equipos de tecnología de la información. Seguridad. Parte 1: Requisitos generales
39. NTP-ISO 14298: 2015. Tecnología gráfica. Gestión de los procesos de impresión de seguridad. 1ª Edición
40. NTP-ISO 25237:2019. Informática en la salud. Seudonimización. 1ª Edición
41. NTP-ISO/IEC 14598-6:2008 (revisada el 2019). Ingeniería de software. Evaluación del producto. Parte 6: Documentación de módulos de evaluación. 1ª Edición
42. NTP-ISO/IEC 15416:2015. Tecnología de la información. Técnicas para la identificación automática y captura de datos. Especificación de las pruebas de calidad para impresión de código de barras. Símbolos lineales
43. NTP-ISO/IEC 15438:2004 (revisada el 2019). Tecnología de la información. Técnicas de identificación y captura automática de datos. Especificaciones de simbología de código de barras. PDF417. 1ª Edición
44. NTP-ISO/IEC 15459-2:2019. Tecnología de la información. Técnicas de identificación automática y captura de datos. Identificación única. Parte 2: Procedimientos de registro. 3ª Edición
45. NTP-ISO/IEC 15963:2006(revisada el 2017). Tecnología de la información. Identificación por radio frecuencia para control de productos. Identificación única de etiquetas de RF. 1ª Edición. (EQV. ISO/IEC 15963:2004)
46. NTP-ISO/IEC 27001:2014. TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos
47. NTP-ISO/IEC 27002:2017. Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. 1a Edición
48. NTP-ISO/IEC 27003:2019. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Orientación. 2ª Edición
49. NTP-ISO/IEC 27004:2018. Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación. 2ª Edición
50. NTP-ISO/IEC 27005:2018. Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información. 2ª Edición
51. NTP-ISO/IEC 27007:2019. Tecnología de la información. Técnicas de seguridad. Directrices para la auditoría de los sistemas de gestión de la seguridad de la información. 2ª Edición
52. NTP-ISO/IEC 27017:2018. Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de la seguridad de la información basado en la ISO/IEC 27002 para los servicios de nube. 1ª Edición
53. NTP-ISO/IEC 27031:2012 (revisada el 2017). Tecnología de la información. Técnicas de seguridad. Directrices para la adecuación de las tecnologías de la información y las comunicaciones para la continuidad del negocio. 1ª Edición
54. NTP-ISO/IEC 27035-1:2019. Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 1: Principios de la gestión de incidencias. 1ª Edición

55. NTP-ISO/IEC 27035-2:2019. Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de la seguridad de la información. Parte 2: Directrices para planificar y prepararse para la respuesta a incidentes. 1ª Edición
56. NTP-ISO/IEC/IEEE 16326:2015. Ingeniería de software y sistemas. Procesos de ciclo de vida Gestión de proyectos
57. NTP-ISO/IEC/IEEE 16326:2015. Ingeniería de software y sistemas. Procesos de ciclo de vida. Gestión de proyectos
58. RTP-ISO/IEC TR 27103:2019. Tecnología de la información. Técnicas de seguridad. Ciberseguridad y Normas ISO e IEC. 1ª Edición
59. NTP ISO/IEC 38500:2016. Tecnología de información. Gobernanza de TI para la organización. 2ª Edición
60.
<b>9. NORMA DE CREACIÓN</b>
1. Consignar la norma de creación.
2.
<b>10. NORMAS DE FUNCIONAMIENTO</b>
1. Ley Orgánica de Municipalidades, aprobada con Ley n.º 27972 de 26 de mayo de 2003.
2. Reglamento de Organización y Funciones, aprobado con Ordenanza Municipal n.º xxx de xx de xxxxx de xxxx.
3. Manual de Organización y Funciones, aprobado con Ordenanza Municipal n.º xxx de xx de xxxxx de xxxx.
4.
<b>11. NORMAS INTERNAS</b>
1. Reglamento interno de trabajo
2. Manual de procedimientos del área de Tecnologías de Información y Comunicaciones o las que haga sus veces.
3. Otros manuales de procedimientos
4.
<b>12. OBSERVACIONES</b>

**R-2**  
**Repositorio de restricciones**

## **REPOSITORIO DE RESTRICCIONES**

<b>1. RESTRICCIONES ORGANIZACIONALES</b>
1. Jurisdicción
2. Estructurales
3. Relativas al personal
4. Plazos
5. Formas de trabajo
6.
7.
8.
9.
10.
<b>2. RESTRICCIONES TÉCNICAS</b>
1. Restricciones de acceso al internet
2. Compatibilidad de software
3. Compatibilidad de hardware
4. Interfaces tecnología - hombre
5. Integración de controles
6.
7.
8.
9.
10.
<b>3. RESTRICCIONES ECONÓMICAS</b>
1. Presupuestaria
2.
3.
4.
5.
6.
7.
8.
9.
10.

<b>4. RESTRICCIONES LEGALES</b>	
1.	Dadas por normas
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
<b>5. OTRO TIPO DE RESTRICCIONES: _____</b>	
1.	De carácter ambiental
2.	Culturales
3.	Éticas
4.	Huelgas
5.	Crisis nacionales o internacionales
6.	
7.	
8.	
9.	
10.	
<b>6. OBSERVACIONES</b>	

**R-3**  
**Repositorio de dimensiones y criterios**

**REPOSITORIO DE CRITERIOS Y SUS IMPACTOS**

<b>1. CRITERIOS</b>		
<b>Antisoborno</b>		
Bajo	Medio	Alto
Montos de menos de S/ _____.	Montos entre S/ _____ y S/ _____.	Montos superiores a S/ _____.
<b>Multas</b>		
Bajo	Medio	Alto
Se imponen multas de menos de S/ _____.	Se imponen multas entre S/ _____ y S/ _____.	Se imponen multas superiores a S/ _____.
<b>Demandas</b>		
Bajo	Medio	Alto
Se presenta una demanda menor de S/ _____ contra la municipalidad.	Una demanda entre S/ _____ y S/ _____ se presenta contra la municipalidad.	Una demanda mayor de S/ _____ se presenta contra la municipalidad.
<b>Investigaciones</b>		
Bajo	Medio	Alto
Entidades gubernamentales solicitan información o registros de rutina.	Entidades gubernamentales solicitan información o registros no rutinaria	Entidades gubernamentales inician una investigación sobre las prácticas organizacionales.
<b>Tiempo máximo de inactividad</b>		
Bajo	Medio	Alto
La municipalidad puede seguir operando por un periodo de inactividad máximo de __ días.	La municipalidad puede seguir operando por un periodo de inactividad entre __ hasta __ días.	La municipalidad puede seguir operando por un periodo de inactividad máximo de __ horas.
<b>Tiempo de recuperación del servicio</b>		
Bajo	Medio	Alto
La municipalidad puede esperar la recuperación del activo hasta __ días.	La municipalidad puede esperar la recuperación del activo entre ____ hasta __ días	La municipalidad puede esperar la recuperación del activo hasta ____ horas.
<b>Productividad</b>		
Bajo	Medio	Alto
Las horas de trabajo del personal se incrementan en menos del _____% en _____ día (s).	Las horas de trabajo del personal se incrementan entre _____% y _____% en _____ día (s).	Las horas de trabajo del personal aumentan en más de _____% en _____ día (s).

Financiero		
Bajo	Medio	Alto
Menos del _____% de pérdida de ingresos mensuales.	_____ a _____% de pérdida de ingresos mensuales.	Pérdida de ingresos mensuales superior al _____%.
Reputación		
Bajo	Medio	Alto
La reputación se ve mínimamente afectada.	La reputación está dañada y se requiere cierto esfuerzo y gasto para recuperarse.	La reputación se destruye o daña irrevocablemente.
Seguridad		
Bajo	Medio	Alto
Seguridad cuestionada	Seguridad afectada	Seguridad violada
Salud		
Bajo	Medio	Alto
Sin pérdida o amenaza significativa para la vida de los ciudadanos o del personal	Las vidas de los ciudadanos o del personal están amenazadas, pero se recuperarán después de recibir tratamiento médico.	Pérdida de la vida de los ciudadanos o del personal.
Tipo de información		
Bajo	Medio	Alto
Información pública	Información personal	Información confidencial
2. DIMENSIONES		
Disponibilidad	Integridad	Confidencialidad
Trazabilidad	Autenticidad	Otro _____

Fuente: Adaptación de Magerit V 3.0 y NIST

**R-4**  
**Repositorio de activos**

**REPOSITORIO DE ACTIVOS**

- [D] Datos / Información
- [S] Servicios
- [SW] Software - Aplicaciones informáticas
- [HW] Equipamiento informático (hardware)
- [COM] Redes de comunicaciones
- [Media] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Personal

**Fuente:** Magerit V 3.0

**R-5**

**Repositorio de amenazas y vulnerabilidades**

Ver archivo Excel

## **R-6 Repositorio de controles**

### **R-6 Repositorio de controles**

- Protecciones generales u horizontales
- Protección de los datos / información
- Protección de las claves criptográficas
- Protección de los servicios
- Protección de las aplicaciones (software)
- Protección de los equipos (hardware)
- Protección de las comunicaciones
- Protección en los puntos de interconexión con otros sistemas
- Protección de los soportes de información
- Protección de los elementos auxiliares
- Seguridad física – Protección de las instalaciones
- Salvaguardas relativas al personal
- Salvaguardas de tipo organizativo
- Continuidad de operaciones
- Externalización
- Adquisición y desarrollo

**Fuente:** Magerit V 3.0

**Anexo n.º 6:**  
**Validación del modelo por expertos**

**CUESTIONARIO DE JUICIO DE EXPERTOS**

**1. OBJETIVO DE CUESTIONARIO:**

Recoger opinión de juicio de expertos en relación con el "MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN PARA LA GENERACIÓN DE VALOR EN EL CONTROL DE LA CORRUPCIÓN DE FUNCIONARIOS Y SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES DE LA REGIÓN DE LAMBAYEQUE".

**2. DATOS PERSONALES:**

Ingrese los datos solicitados:

2.1. APELLIDOS Y NOMBRES: ZOCÓN ALVA, OSCAR GILBERTO

2.2. PROFESIÓN: Ingeniero de Computación y Sistemas

2.3. CÓDIGO DEL COLEGIO DE INGENIEROS: 38444

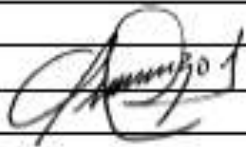
2.4. AÑOS DE EXPERIENCIA PROFESIONAL: 21 años

**3. CUESTIONARIO PARA CONOCER OPINIÓN:**

El cuestionario presenta un conjunto de actividades que se pretende lograr con el modelo propuesto. Coloque un valor según las escalas que se indica a continuación con la finalidad de conocer su nivel de conformidad respecto a las actividades planteadas.

Suficiencia: El ítem contribuye al cumplimiento de la fase.				
1	2	3	4	5
En total desacuerdo El ítem no corresponde a la fase propuesta.	En desacuerdo El ítem no es suficiente	Neutral El ítem debe de mejorarse	De acuerdo El ítem contribuye al cumplimiento de lo planificado en la fase, pero puede mejorarse	Totalmente de acuerdo El ítem cuenta con el detalle suficiente para contribuir con el cumplimiento de lo planificado en la fase
Claridad: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.				
1	2	3	4	5
En total desacuerdo El ítem no es claro	En desacuerdo El ítem presenta dificultad para entenderse	Neutral Claridad del ítem debe de mejorarse	De acuerdo El ítem se entiende, pero puede mejorarse	Totalmente de acuerdo El ítem es claro.
Coherencia: El ítem tiene relación lógica con la fase.				
1	2	3	4	5
En total desacuerdo El ítem no es coherente con lo planificado en la fase	En desacuerdo El ítem tiene una mínima relación con lo planificado en la fase	Neutral El ítem tiene una relación moderada con lo planificado en la fase, debe de mejorarse	De acuerdo El ítem guarda una relación lógica con lo planificado en la fase, pero puede mejorarse.	Totalmente de acuerdo El ítem guarda una estrecha relación lógica con lo planificado en la fase
Relevancia: El ítem es esencial o importante, es decir, debe ser incluido.				
1	2	3	4	5
En total desacuerdo El ítem no es relevante y debe de ser eliminado	En desacuerdo El ítem tiene una mínima relevancia y puede ser sustituido por otro	Neutral El ítem tiene una relevancia moderada, debe de mejorarse	De acuerdo El ítem es relevante, pero puede ser mejorado	Totalmente de acuerdo El ítem es esencial para lo planificado en la fase.



Fase o componente	Actividades	Suficiencia	Claridad	Coherencia	Relevancia	Comentarios		
ACTIVIDADES PRELIMINARES	1. Conformación del equipo y asignación de roles por actividades.	5	5	5	5			
	2. Definir la matriz de comunicación.	5	5	5	5			
	3. Documentar y comunicar el trabajo realizado.	5	5	5	5			
	4. De ser el caso actualizar y comunicar los documentos.	5	5	5	5			
CONTEXTO, ALCANCE Y CRITERIO	1. Definir el contexto externo.	5	5	5	5			
	2. Establecer el alcance.	5	5	5	5			
	3. Determinar los criterios.	5	5	5	5			
	4. Documentar y comunicar el trabajo realizado.	5	5	5	5			
	5. De ser el caso actualizar y comunicar los documentos.	5	5	5	5			
EVALUACIÓN DEL RIESGO	Identificación del riesgo.	1. Identificar y valorar los activos críticos de las municipalidades.	5	5	5	5		
		2. Identificar y valorar las amenazas a las que están expuestas.	4	4	4	5		
		3. Identificar y valorar las vulnerabilidades.	4	4	4	5		
		4. Documentar y comunicar el trabajo realizado.	5	5	5	5		
		5. De ser el caso actualizar y comunicar los documentos.	5	5	5	5		
	Sub fase Análisis y valoración del riesgo.	1. Evaluación de consecuencias.	5	5	5	5		
		2. Evaluación de probabilidad de escenarios.	5	5	5	5		
		3. Determinación del nivel de riesgos.	5	5	5	5		
		4. Implementar un mecanismo de análisis predictivo de identificación de riesgos.	3	5	5	5		
		5. Valorar los riesgos.	5	5	5	5		
		6. Documentar y comunicar el trabajo realizado.	5	5	5	5		
		7. De ser el caso actualizar y comunicar los documentos.	5	5	5	5		
		TRATAMIENTO DEL RIESGO	1. Diseñar y ejecutar planes de mitigación de riesgos.	4	4	4	5	
			2. Identificar cambios en la estrategia de protección.	4	4	4	5	
3. Documentar y comunicar el trabajo realizado.	5		5	5	5			
4. De ser el caso actualizar y comunicar los documentos.	5		5	5	5			

Fase o componente	Actividades	Suficiencia	Claridad	Coherencia	Relevancia	Comentarios
SEGUIMIENTO Y REVISIÓN	1. Ejecutar el seguimiento del resultado esperado de las actividades.	5	5	5	5	
	2. Ejecutar el seguimiento del modelo.	5	5	5	5	
	3. De ser el caso rediseñar el modelo propuesto	5	5	5	5	

#### 4. RESULTADO

X	FAVORABLE		DEBE DE MEJORAR		DESFAVORABLE
---	-----------	--	-----------------	--	--------------

#### 5. COMENTARIO FINAL

El modelo propuesto presenta actividades suficientes, claras, coherentes y relevantes para el logro del objetivo propuesto. Este modelo de gestión de riesgos es un modelo dinámico que se retroalimenta. Se recomienda fortalecer las actividades de identificación y valoración de amenazas y vulnerabilidades, así como las actividades relacionadas al tratamiento del riesgo residual.



### CONSTANCIA DE JUICIO DE EXPERTO

Yo, ZOCÓN ALVA, OSCAR GILBERTO, identificado con DNI n.º 26706422 doy constancia que realicé el juicio de experto del cuestionario diseñado por ABANTO ORTIZ ROGER GUSTAVO en la investigación titulada: MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN PARA LA GENERACIÓN DE VALOR EN EL CONTROL DE LA CORRUPCIÓN DE FUNCIONARIOS Y SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES DE LA REGIÓN DE LAMBAYEQUE, el día miércoles, 22 de Julio de 2020.



ZOCÓN ALVA, OSCAR GILBERTO



PERÚ

Ministerio de Educación

Superintendencia Nacional de  
Educación Superior UniversitariaDirección de Documentación e  
Información Universitaria y  
Registro de Grados y Títulos

## REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

GRADUADO	GRADO O TÍTULO	INSTITUCIÓN
ZOCON ALVA, OSCAR GILBERTO DNI 26706422	DOCTOR EN INGENIERIA DE SISTEMAS  Fecha de Diploma:12/07/19	UNIVERSIDAD NACIONAL DE PIURA
ZOCON ALVA, OSCAR GILBERTO DNI 26706422	MAESTRO EN INGENIERIA DE SISTEMAS SISTEMAS DE INFORMACION  Fecha de Diploma:12/05/2006	UNIVERSIDAD PRIVADA ANTENOR ORREGO
ZOCON ALVA, OSCAR GILBERTO DNI 26706422	INGENIERO DE COMPUTACION Y SISTEMAS  Fecha de Diploma:13/11/1998	UNIVERSIDAD PRIVADA ANTENOR ORREGO
ZOCON ALVA, OSCAR GILBERTO DNI 26706422	BACHILLER EN INGENIERIA DE COMPUTACION Y  Fecha de Diploma:26/04/1996	UNIVERSIDAD PRIVADA ANTENOR ORREGO
ZOCON ALVA, OSCAR GILBERTO DNI 26706422	BACHILLER EN INGENIERIA DE COMPUTACION Y SISTEMAS  Fecha de Diploma:26/04/1996	UNIVERSIDAD PRIVADA ANTENOR ORREGO



#### CURRICULUM VITAE

Apellidos y Nombres	:	ZOCÓN ALVA, OSCAR GILBERTO
Grado Académico	:	Doctor en Ingeniería de Sistemas
Fecha de Nacimiento	:	07 de Noviembre de 1974
Lugar de Nacimiento	:	Trujillo – La Libertad
Estado Civil	:	Casado
Documento de Identidad	:	26705422
Dirección	:	Jr. Luis Portilla 470 – Dpto 202. Urb. San Luis Cajamarca.
Teléfono	:	976458747
Email	:	oscarzocon@hotmail.com

#### 1.- GRADOS Y TÍTULOS:

Doctor en Ingeniería de Sistemas –Universidad Nacional de Piura. - Julio 2019.

Magister en Ingeniería de Sistemas Mención en Sistemas de Información.  
Universidad Privada Antenor Orrego . Trujillo – Mayo del 2005.

Maestría en Educación – con Especialización en Educación Superior. Universidad Privada San Pedro 2007

Ingeniero de Computación y Sistemas. Universidad Privada Antenor Orrego. Trujillo – Octubre de 1998.

Bachiller en Ingeniería de Computación y Sistemas. Universidad Privada Antenor Orrego. Trujillo - Marzo de 1996.

## 2.- CAPACITACIÓN ACADÉMICA Y PROFESIONAL

2.1.- Certificación Internacional como Trainer en la Metodología activa CEFE para Empresarios, Innovadores, Startup y demás, autorizado por CEFE Internacional con una duración de 115 Horas. CEFE es la metodología desarrollada por la Fundación Alemana de Cooperación Técnica (GTZ) para implementar proyectos de Capacitación a nivel mundial.

2.2.- Certificación Internacional IYB TRAINER de MESUN (Mejora su Negocio) creada por la OIT (Organización Internacional del Trabajo). MESUN es una de las certificaciones internacionales desarrollada por la Organización Internacional del Trabajo dirigida a la capacitación de empresarios, Innovadores y Negocios a nivel mundial.

2.3.- Certificación Internacional Laureate en Educación del Adulto Trabajador - Laureate International Universities. Laureate es la red de universidades más grandes del mundo y dueña de UPC y UPN.

2.4.- Certificación Internacional Laureate en Educación Online, Híbrida y Blended- Laureate International Universities. Laureate es la red de universidades más grandes del mundo y dueña de UPC y UPN.

2.5.- Auditor Interno Certificado en ISO 27001 AENOR (Asociación Española de Normalización y Certificación) – Gestión de la Seguridad de la Información.

2.6.- Certificación como DBA - Administrador de Base de Datos DB2 de IBM, especializado en Big Data, Data Warehouse y Data Mining.

2.7.- Certificación Yellow Belt en Gestión y Mejora de Procesos empresariales bajo LEAN SIX SIGMA Newmont Corp.

2.8.- Especialización en Gestión Empresarial, Gestión de Procesos y gestión de Calidad bajo Iso 9001 y CertiPyme (Certificación Nacional de Calidad para Pequeñas y Medianas Empresas) – Proyecto Fundación Suiza de Cooperación Técnica – Minera GoldFields la Cima.

2.9.- Especialización en Gestión de Ventas, Gestión de Compras, Gestión de Almacenes e Inventarios, módulo de Finanzas, Gestión de Clientes y Marketing a través del Enterprise Resource Planning (ERP) con SAP – Proyecto Newmont Yanacocha- Soluciones Globales Empresariales.

2.10.- Especialización en Gestión de Proyectos y Gestión de la Calidad empresarial, Pontificia Universidad Católica del Perú.

2.11.- Certificación Internacional ITIL en Gestión de Servicios Empresariales de Tecnologías de Información, ITIL – AXELOS.

2.12.- Certificación en Gestión y Desarrollo de Proyectos Agiles Certified Scrum Developer Open Edge.

2.13.- Miembro Fundador del Project Management Institute – Chapter Cajamarca Vicepresidente de Membresía – PMI Capítulo Cajamarca- Abril 2018 – a la Fecha.

2.14.- Instructor Internacional Certificado Laureate - Laureate Internacional Universities 2015 International Universities

2.15.- Certificación Internacional Laureate en Educación Superior -Laureate International Universities 2011.

### 3. EXPERIENCIA CONSULTOR, CAPACITADOR

3.1.- Gerente General en Soluciones Globales Empresariales, empresa dedicada a proyectos en Minería y tecnología. Desarrollando proyectos con Minera Yanacocha, Minera Antamina, Minera Goldfields la Cima y Otros.

3.2.- Consultor y capacitador del proyecto Innova y Emprende II, financiado por Fondo Empleo y la Cámara de comercio de Cajamarca, en el que se brindó capacitación Presencial y luego Virtual a más de 200 Empresarios de la región Cajamarca. Febrero 2020 – a la Fecha

3.3.- Consultor y Capacitador Proyecto Emprende Cajamarca, Asociación los Andes Cajamarca. Diciembre 2019 – Marzo 2020. Capacitación en Mejora de Procesos y Elaboración de Planes de Mejora de Negocios de 29 empresas Cajamarquinas.

3.4.- Consultor y Capacitador en el "Programa empresario de éxito- creando valor compartido" en las áreas de Comercialización, Producción Logística, calidad, finanzas, recursos humanos. Proyecto Fundación Sulza de Cooperación Técnica – Minera GoldFields la Cima. Desarrollando el Plan de Mejora de Negocio para 14 Empresas. marzo 2017 – diciembre 2017

3.5.- Consultor en mejora de Proyectos Empresariales: Centro de Proyectos SRL . Enero 2013 – Diciembre 2014.

3.6.- Consultor en Mejorar de Procesos y Calidad Empresarial, Implementación de ISO 9001: Ipsycom Ingenieros SRL marzo 2010 – diciembre 2011

3.7.- Consultor y Capacitador en Procesos Empresariales SAP. Proyecto: Entrenamiento y Migración ERP Corporativo Newmont ( Minera Yanacocha) Ellipse a SAP - Soluciones Globales Empresariales. Abril 2012 – Diciembre 2012:

3.8.- Consultor y Capacitador en Procesos Empresariales a través de Prospector y Mejora de Soluciones Ofimáticas con Microsoft Office 2010 en el proyecto: Migración Intranet Sharepoint 2010, Office 2010 – Minera Yanacocha - Soluciones Globales Empresariales. Setiembre 2011 – Abril 2012

3.9.- Docente Principal de la Facultad de Ingeniería. Escuela Profesional de Ingeniería de Sistemas De la Universidad Nacional de Cajamarca. Octubre de 1996 – a la Fecha.

3.10.- Docente Postgrado Universidad Nacional de Cajamarca – Maestría en Gerencia de Proyectos - Julio 2018 – A la Fecha.

3.11.- Docente Invitado de la Escuela de Postgrado Maestría en Gestión de TI UNITEC Sede – Tegucigalpa Honduras – Laureate International University - Julio 2014 - a la Fecha.

3.12.- Docente Invitado de la Escuela de Postgrado Maestría en Dirección de Proyectos UNITEC Sede – Tegucigalpa Honduras – Laureate International University Periodo Julio 2014 - A la fecha.

3.13.- Docente Invitado de la Escuela de Postgrado Maestría en Dirección de Proyectos UPAGU Periodo 2019 - A la fecha.

3.14.- Docente de la Facultad de Ingeniería de Sistemas de la Universidad Privada del Norte- Cajamarca - Marzo del 2003 – Julio 2018.

3.15.- Docente de la Escuela de Post Grado de la Universidad Nacional de Trujillo Maestría en Ing. De Sistemas - Enero del 2006 – Diciembre 2008.

#### **4. EXPERIENCIA EN CARGOS ADICIONALES CON EMPRENEDORES Y PROFESIONALES**

- Presidente Capítulo de Ingeniería de Sistemas, Computación e Informática Colegio de Ingenieros Cajamarca
- Vicepresidente del Área de Membresía del Project Management Institute - PMI, Capítulo Norte Perú.
- Director de Escuela de Ingeniería de Sistemas – Universidad Nacional de Cajamarca.

#### **5. CONOCIMIENTO DE IDIOMAS**

5.1.- Estudios de Inglés Nivel Básico en el Centro de Idiomas de la Universidad Privada Antenor Orrego.

5.2.- Estudios de Inglés Intermedio en el Centro de Idiomas de la UNC.

5.3.- Estudios de Inglés Intermedio Acreditado para el Nivel de Maestría Centro de Idiomas de la Universidad Privada Antenor Orrego.

5.4.- Estudios de Portugués Nivel Básico Acreditado para el Nivel de Maestría Centro de Idiomas de la Universidad Nacional de Cajamarca

5.5.- Estudios de Portugués Nivel Intermedio Acreditado para el Nivel de Maestría Centro de Idiomas de la Universidad Nacional de Cajamarca

5.6.- Estudios de Portugués Nivel Avanzado Acreditado para el Nivel de Maestría Centro de Idiomas de la Universidad Nacional de Cajamarca

## 6.- PRODUCCIÓN CIENTÍFICA Y HUMANÍSTICA

Proyectos de Investigación realizados y publicados en la Revista de Investigación de la Universidad Nacional de Cajamarca

6.1.- "Diseño e Implementación de una Aplicación Móvil para la Consulta Académica de la Universidad Nacional de Cajamarca, en base a servicios web" Año 2013

6.2.- Aplicación de la Tecnología Informática en la Gestión Educativa de la Universidad Nacional de Cajamarca. Año 2012

6.3.- Inteligencia de Negocios (BI) como soporte de decisiones en las Pymes de Cajamarca, aplicación en Marketing y Dirección de la Producción. Año 2011

6.4.- Propuesta de Implementación de una Solución CRM (Customer Relationship Management) usando Software Libre para fines académicos en la Universidad Nacional de Cajamarca. Año 2010

6.5.- Integración de Información utilizando Servicio WEB y Tecnologías Semánticas. Año 2009

6.6.- Factores Críticos de éxito que influyen en el Network Marketing. Año 2007

6.7.- Guía de Aprendizaje para Desarrollar Proyectos en Ingeniería de Software Utilizando el Lenguaje de Modelado Unificado (UML). Año 2006

6.8.- Propuesta de Diseño e Implementación de Redes de Área Local Gireles (WLAN) para accesos Públicos a Internet – Hot Spot- En la Universidad Nacional de Cajamarca. Año 2005.

6.9.- Diseñar una Base de Datos Orientada a Objetos, Implementar y Evaluar el Rendimiento de un OODBMS. Año 2002.

6.10.- Perú Zona Norte: Análisis Comparativo Multivariado de los Niveles de Empleo según ENAHO en el periodo de 1997-2001. Año 2001.

6.11.- Proyecto de Planificación, Diseño, Construcción y Publicación de la Página Web de la Oficina General de Investigación de la U.N.C. Año 2001.

6.12.- Proyecto de Desarrollo del Sistema Informático para el Control de Proyectos de Investigación: Oficina General de Investigación de la U.N.C. Año 2000.

6.13.- Desarrollo del Sistema de Registro de Evaluación de Alumnos De la Escuela Profesional de Ingeniería de Sistemas de la U.N.C usando Tecnología Cliente/Servidor. Año 2000.

6.14.- Análisis Estadístico: Que Factores Limitan el crecimiento Económico en la Sub Región IV Cajamarca. Año 1999.

### CUESTIONARIO DE JUICIO DE EXPERTOS

#### 1. OBJETIVO DE CUESTIONARIO:

Recoger opinión de juicio de expertos en relación con el "MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN PARA LA GENERACIÓN DE VALOR EN EL CONTROL DE LA CORRUPCIÓN DE FUNCIONARIOS Y SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES DE LA REGIÓN DE LAMBAYEQUE".

#### 2. DATOS PERSONALES:

Ingrese los datos solicitados

2.1. APELLIDOS Y NOMBRES: VILLACORTA CHAVEZ PAUL MARTIN

2.2. PROFESIÓN: INGENIERO ADMINISTRATIVO

2.3. CÓDIGO DEL COLEGIO DE INGENIEROS: 127097

2.4. AÑOS DE EXPERIENCIA PROFESIONAL: +15 AÑOS

#### 3. CUESTIONARIO PARA CONOCER OPINIÓN:

El cuestionario presenta un conjunto de actividades que se pretende lograr con el modelo propuesto. Coloque un valor según las escalas que se indica a continuación con la finalidad de conocer su nivel de conformidad respecto a las actividades planteadas.

Suficiencia: El ítem contribuye al cumplimiento de la fase.				
1	2	3	4	5
En total desacuerdo El ítem no corresponde a la fase propuesta.	En desacuerdo El ítem no es suficiente	Neutral El ítem debe de mejorarse	De acuerdo El ítem contribuye al cumplimiento de lo planificado en la fase, pero puede mejorarse	Totalmente de acuerdo El ítem cuenta con el detalle suficiente para contribuir con el cumplimiento de lo planificado en la fase
Claridad: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.				
1	2	3	4	5
En total desacuerdo El ítem no es claro	En desacuerdo El ítem presenta dificultad para entenderse	Neutral Claridad del ítem debe de mejorarse	De acuerdo El ítem se entiende, pero puede mejorarse	Totalmente de acuerdo El ítem es claro.
Coherencia: El ítem tiene relación lógica con la fase.				
1	2	3	4	5
En total desacuerdo El ítem no es coherente con lo planificado en la fase	En desacuerdo El ítem tiene una mínima relación con lo planificado en la fase	Neutral El ítem tiene una relación moderada con lo planificado en la fase, debe de mejorarse	De acuerdo El ítem guarda una relación lógica con lo planificado en la fase, pero puede mejorarse.	Totalmente de acuerdo El ítem guarda una estrecha relación lógica con lo planificado en la fase
Relevancia: El ítem es esencial o importante, es decir, debe ser incluido.				
1	2	3	4	5
En total desacuerdo El ítem no es relevante y debe de ser eliminado	En desacuerdo El ítem tiene una mínima relevancia y puede ser sustituido por otro	Neutral El ítem tiene una relevancia moderada, debe de mejorarse	De acuerdo El ítem es relevante, pero puede ser mejorado.	Totalmente de acuerdo El ítem es esencial para lo planificado en la fase.



Fase o componente	Actividades	Suficiencia	Claridad	Coherencia	Relevancia	Comentarios	
ACTIVIDADES PRELIMINARES	1. Conformación del equipo y asignación de roles por actividades.	5	5	5	5		
	2. Definir la matriz de comunicación.	5	5	5	5		
	3. Documentar y comunicar el trabajo realizado.	5	5	5	5		
	4. De ser el caso actualizar y comunicar los documentos.	5	5	5	5		
CONTEXTO, ALCANCE Y CONTENIDO	1. Definir el contexto externo.	5	5	5	5		
	2. Establecer el alcance.	5	5	5	5		
	3. Determinar los criterios.	5	5	5	5		
	4. Documentar y comunicar el trabajo realizado.	5	5	5	5		
	5. De ser el caso actualizar y comunicar los documentos.	5	5	5	5		
EVALUACIÓN DEL RIESGO	Identificación del riesgo	1. Identificar y valorar los activos críticos de las municipalidades.	5	5	5	5	
		2. Identificar y valorar las amenazas a las que están expuestas.	5	5	5	5	
		3. Identificar y valorar las vulnerabilidades.	5	5	5	5	
		4. Documentar y comunicar el trabajo realizado.	5	5	5	5	
		5. De ser el caso actualizar y comunicar los documentos.	5	5	5	5	
	Sub-fase Análisis y valoración del riesgo	1. Evaluación de consecuencias.	5	5	5	5	
		2. Evaluación de probabilidad de escenarios.	5	5	5	5	
		3. Determinación del nivel de riesgos.	5	5	5	5	
		4. Implementar un mecanismo de análisis predictivo de identificación de riesgos.	5	5	5	5	
		5. Valorar los riesgos.	5	5	5	5	
		6. Documentar y comunicar el trabajo realizado.	5	5	5	5	
		7. De ser el caso actualizar y comunicar los documentos.	5	5	5	5	
TRATAMIENTO DEL RIESGO	1. Diseñar y ejecutar planes de mitigación de riesgos.	4	4	4	4		
	2. Identificar cambios en la estrategia de protección.	5	5	5	5		
	3. Documentar y comunicar el trabajo realizado.	5	5	5	5		
	4. De ser el caso actualizar y comunicar los documentos.	5	5	5	5		

Fase o componente	Actividades	Suficiencia	Claridad	Coherencia	Relevancia	Comentarios
SEGUIMIENTO O REVISIÓN	1. Ejecutar el seguimiento del resultado esperado de las actividades.	5	5	5	5	
	2. Ejecutar el seguimiento del modelo.	5	5	5	5	
	3. De ser el caso rediseñar el modelo propuesto	5	5	5	5	

#### 4. RESULTADO

X	FAVORABLE		DEBE DE MEJORAR		DESFAVORABLE
---	-----------	--	-----------------	--	--------------

#### 5. COMENTARIO FINAL

El modelo cumple con su objetivo y las actividades (formatos y repositorios) son suficientes, claros, coherentes y relevantes. El modelo tiene el detalle suficiente para ser puesto en operatividad de manera práctica, es un modelo que se ajusta a las necesidades de las municipalidades; así como está orientado a la retroalimentación. Se recomienda tomar en consideración labores de sensibilización para la puesta en marcha del modelo, así como determinar los responsables de las actualizaciones de los repositorios.



#### CONSTANCIA DE JUICIO DE EXPERTO

Yo, VILLACORTA CHAVEZ PAUL MARTIN, identificado con DNI n.º 07879132 doy constancia que realicé el juicio de experto del cuestionario diseñado por ABANTO ORTIZ ROGER GUSTAVO en la investigación titulada: MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN PARA LA GENERACIÓN DE VALOR EN EL CONTROL DE LA CORRUPCIÓN DE FUNCIONARIOS Y SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES DE LA REGIÓN DE LAMBAYEQUE, el día miércoles, 29 de julio de 2020.



PAUL MARTÍN VILLACORTA CHAVEZ



PERÚ

Ministerio de Educación

Superintendencia Nacional de  
Educación Superior UniversitariaDirección de Documentación e  
Información Universitaria y  
Registro de Grados y Títulos

## REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

GRADUADO	GRADO O TÍTULO	INSTITUCIÓN
VILLACORTA CHAVEZ, PAUL MARTIN DNI 07879132	<b>MAESTRO EN EDUMÁTICA Y DOCENCIA UNIVERSITARIA</b>  Fecha de Diploma:12/08/19	<b>UNIVERSIDAD TECNOLÓGICA DEL PERÚ S.A.C.</b>
VILLACORTA CHAVEZ, PAUL MARTIN DNI 07879132	<b>GRADO DE MAESTRÍA EN ADMINISTRACIÓN DE EMPRESAS INTERNACIONALES</b> Fecha de diploma: No aplica <i>TIPO:</i>  • <b>RECONOCIMIENTO</b>  Fecha de Resolución de Reconocimiento:18/07/2014	<b>Universidad Tecnológica de América</b>
VILLACORTA CHAVEZ, PAUL MARTIN DNI 07879132	<b>INGENIERO ADMINISTRATIVO</b>  Fecha de Diploma:11/08/2010	<b>UNIVERSIDAD INCA GARCILASO DE LA VEGA ASOCIACIÓN CIVIL</b>
VILLACORTA CHAVEZ, PAUL MARTIN DNI 07879132	<b>BACHILLER EN INGENIERIA ADMINISTRATIVA</b>  Fecha de Diploma:11/12/2007	<b>UNIVERSIDAD INCA GARCILASO DE LA VEGA ASOCIACIÓN CIVIL</b>

**Contactar**

999298706 (Home)  
 ing\_paulvillacorta@hotmail.com

[www.linkedin.com/in/ing%C2%BD-adm-cip-paul-villacorta-pmp-mba-11233a26](http://www.linkedin.com/in/ing%C2%BD-adm-cip-paul-villacorta-pmp-mba-11233a26) (LinkedIn)  
[ingpaulvillacorta.blogspot.com/](http://ingpaulvillacorta.blogspot.com/)  
 (Blog)

**Aptitudes principales**

PMP

MOS EXPERT

CIP

**Certifications**

ING° ADM COLEGIADO (CIP)  
 PMP

**Honors-Awards**

Mejor Catedrático Año 2012

Premio CIP 2012

Premio al Desempeño Académico  
 Año 2016

**Publications**

Video Introducción a las Buenas  
 Prácticas: Que es el PMI?

Boletín Oceano Azul aplicada a la  
 Gestión de Proyectos

Boletín Buenas Prácticas PMI  
 Rentabilidad Educativa

# Ing° Adm. CIP Paul Villacorta, PMP, MBA

PastPresidente en PMI LIMA PERU CHAPTER

**Extracto**

Presidente PMI Lima Peru Chapter 2016.

Presidente Electo PMI Lima Peru Chapter 2015.

Especialista en Gestión de Proyectos - ONPE 2014 - Proyecto "Voto Electrónico".

VicePresidente de Educación PMI Lima Perú 2013-2014.

Director Instituto de Gestion de Proyectos - IGP.

Miembro Comité Consultivo de las Universidades: ESAN, USIL y PUCP.

Catedrático Postgrado - UNMSM, UNFV y UPAGU (Cajamarca)

Catedrático Pregrado - UPC, USMP, UTP y UCSUR.

Consultor y Facilitador en Proyectos con 20 años de experiencia.

Profesor Diplomatura de Proyectos - Instituto de Calidad de la PUCP.

Profesor Diplomado Proyectos - CIP, URP y BSGrupo

Profesor Invitado Escuela de Ciencias e Ingeniería Continental

(Lima), Universidad Antunez de Mayolo (Huaraz), Universidad del Santa (Chimbote).

Gestor de Capacitación - MEF - Proyecto "MEF sin Papeles"

Jefe de Capacitación - COMSA-INDRA - Proyecto en ONP

"Calificación Expedientes Pensionables".

Jefe del Centro de Cómputo - Asociación Judía del Perú.

Ingeniero Administrativo Colegiado.

Magister en Proyectos Empresariales.

Magister en Educación.

Master Business Administrator.

Project Management Professional.

Especialista en Gestión de Proyectos.

Especialista en Informática Empresarial y Competencias Ejecutivas.

Premio IC-PUCP 2015.

Premio CIP 2012.

Premio UTP 2012.

Premio IPAE 1993.

Conferencista en: UPC, UNT, UPT, UL, UP, UPN, UTP, UNAC, UNI, UNMSM, USMP, UIGV, UNE, UNLM, PUCP, UCV, UNFV, UESAN, UNTELS, USIL, Senati, Tecsup AQP.

---

## Experiencia

### INSTITUTO DE GESTION DE PROYECTOS

Director de Proyectos  
enero de 2013 - Present

Lima

Responsable de Dirigir los Proyectos de Outsourcing para las áreas de Tecnología (TI) y Recursos Humanos (RRHH), así como desarrollar y poner en marcha los planes de entrenamiento y capacitación de cada uno de los proyectos encomendados, contribuyendo a la mejora de las competencias del Talento Humano de cada una de las organizaciones clientes.

### Universidad Nacional Mayor de San Marcos

Catedrático Postgrado  
octubre de 2012 - Present

Lima

Catedrático en Gestión de Proyectos - PMI en la escuela de postgrado de la facultad de ing<sup>o</sup> electrónica y de telecomunicaciones de la UNMSM.

### Instituto para la Calidad - PUCP

Profesor Diplomatura  
septiembre de 2012 - Present

Lima

Profesor en la Diplomatura de Gestión de Proyectos PMI del Instituto de Calidad de la PUCP, además de profesor inhouse a nivel nacional.

### COLEGIO DE INGENIEROS DEL PERU (CIP)

Consultor & Facilitador Proyectos (PMI)  
marzo de 2012 - Present

CIP Lima (San Isidro)

Consultor & Facilitador en Proyectos (PMI) para los capítulos de Ing<sup>o</sup> Económica - Administrativa, Ing<sup>o</sup> Alimentarias - Agroindustrial e Ing<sup>o</sup> Química.

### PMI Lima Peru Chapter

Presidente  
enero de 2016 - diciembre de 2016 (1 año)

Institución Mundial, Líder en los Estándares de Dirección de *Proyectos*, que propone las Buenas Prácticas en la Dirección de *Proyectos*.

#### PMI LIMA PERU CHAPTER

2 años 11 meses

Presidente Electo

enero de 2016 - diciembre de 2016 (1 año)

Lima

Institución Internacional sin fines de lucro cuya finalidad es seguir extendiendo las buenas prácticas en la gestión de *proyectos*.

#### VP EDUCACION

febrero de 2013 - enero de 2015 (2 años)

LIMA

Vice Presidente de Educación Electo para el periodo 2013-2014 del Capítulo PMI Lima PERU

#### ONPE

Especialista en Gestión de *Proyectos* - Proyecto "Voto Electrónico"  
julio de 2014 - diciembre de 2014 (6 meses)

Lima, Peru

Especialista en la Gestión del *Proyecto* para el *Proyecto* "Voto Electrónico" con vistas a las Elecciones Municipales y Regionales Perú 2014

#### UNIVERSIDAD TECNOLOGICA DEL PERU - UTP

Profesor de TI & Gestión & *Proyectos* (PMI)

noviembre de 2011 - diciembre de 2014 (3 años 2 meses)

Lima

Tengo a mi cargo las cátedras del curso de Administración y Gestión Empresarial de VII Ciclo e Informática Empresarial del VIII Ciclo para alumnos de Ing. Económica y del curso de Taller PMP & Gestión de *Proyecto* PMI, para alumnos del IX Ciclo de Ing. de Sistemas e Ing. Industrial

#### Universidad Mayor de San Marcos - UNMSM

Profesor de TI & *Proyectos* (PMI)

marzo de 2007 - marzo de 2012 (5 años 1 mes)

Dicho cursos de TI aplicado a gestión, negocios y *proyectos*, ahora con la certificación PMP!

#### Camara de Comercio de Lima

Expositor TI Aplicado a Negocios y Gestión

marzo de 2004 - diciembre de 2011 (7 años 10 meses)

Lima

Dictor cursos de Informática aplicada, como herramientas financieras con excel, base de datos con excel & access *f* excel aplicado a control logístico.

MEF

Gestor de Capacitación & Capacitador

enero de 2011 - julio de 2011 (7 meses)

Actualmente asignado al Proyecto "MEF Sin Papeles - NSTD"

COM S.A.

Coordinador de Capacitación

abril de 2009 - marzo de 2010 (1 año)

Coordinador de Capacitación para el Proyecto ONP (Servicio de Calificación de Expedientes Pensionables)

New Horizons Peru

Instructor TI

1997 - 2000 (4 años)

Dicte cursos de TI en general!

Cosapi Data

Instructor TI

1993 - 1996 (4 años)

Instructor & Facilitador TI & Proyectos (PMI)

---

## Educación

TECHNOLOGICAL UNIVERSITY OF AMERICA - TUA

Master of Business Administration (MBA), Administración *f* gestión de empresas - (2012 - 2013)

UNIVERSIDAD TECNOLÓGICA DEL PERU - UTP

MAESTRIA EN EDUCACION, Educación, Edumática, Docencia Universitaria - (2011 - 2013)

Universidad Nacional Federico Villarreal

Egresado de la Maestría en Proyectos Empresariales (PMI), Gestión *f* Dirección de Proyectos - (2008 - 2010)

Universidad Inca Garcilaso de la Vega  
Ingeniero Administrativo, Gestión, Ingeniería, Tecnología - (1998 - 2006)

## CUESTIONARIO DE JUICIO DE EXPERTOS

### 1. OBJETIVO DE CUESTIONARIO:

Recoger opinión de juicio de expertos en relación con el "MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN PARA LA GENERACIÓN DE VALOR EN EL CONTROL DE LA CORRUPCIÓN DE FUNCIONARIOS Y SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES DE LA REGIÓN DE LAMBAYEQUE".

### 2. DATOS PERSONALES:

Ingrese los datos solicitados

2.1. APELLIDOS Y NOMBRES: Villavicencia Montoya Mónica Yalanda

2.2. PROFESIÓN: Ingeniera de Sistemas y Computación

2.3. CÓDIGO DEL COLEGIO DE INGENIEROS: 158003

2.4. AÑOS DE EXPERIENCIA PROFESIONAL: 09 años

### 3. CUESTIONARIO PARA CONOCER OPINIÓN:

El cuestionario presenta un conjunto de actividades que se pretende lograr con el modelo propuesto. Marque con un aspa ("X") un valor según la escala que se indica a continuación con la finalidad de conocer su nivel de conformidad respecto a las actividades planteadas.

Suficiencia El ítem contribuye en la identificación de la situación problemática.				
1	2	3	4	5
En total desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Claridad El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.				
1	2	3	4	5
En total desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Coherencia El ítem tiene relación lógica con la fase.				
1	2	3	4	5
En total desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
Relevancia El ítem es esencial o importante, es decir, debe ser incluido.				
1	2	3	4	5
En total desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

Fase o componente	Actividades	Suficiencia	Claridad	Coherencia	Relevancia	Comentarios	
ACTIVIDADES PRELIMINARES	1. Conformación del equipo y asignación de roles por actividades.	5	5	5	5		
	2. Definir la matriz de comunicación.	5	5	5	5		
	3. Documentar y comunicar el trabajo realizado.	5	5	5	5		
	4. De ser el caso actualizar y comunicar los documentos.	5	5	5	5		
CONTEXTO, ALCANCE Y CRITERIO	1. Definir el contexto externo.	5	5	5	5		
	2. Establecer el alcance.	5	5	5	5		
	3. Determinar los criterios.	5	5	5	5		
	4. Documentar y comunicar el trabajo realizado.	5	5	5	5		
	5. De ser el caso actualizar y comunicar los documentos.	5	5	5	5		
EVALUACIÓN DEL RIESGO	Identificación del riesgo	1. Identificar y valorar los activos críticos de las municipalidades.	5	5	5	5	
		2. Identificar y valorar las amenazas a las que están expuestas.	5	5	5	5	
		3. Identificar y valorar las vulnerabilidades.	5	5	5	5	
		4. Documentar y comunicar el trabajo realizado.	5	5	5	5	
		5. De ser el caso actualizar y comunicar los documentos.	5	5	5	5	
	Subtarea: Análisis y valoración del riesgo	1. Evaluación de consecuencias.	5	5	5	5	
		2. Evaluación de probabilidad de escenarios.	5	5	5	5	
		3. Determinación del nivel de riesgos.	4	5	5	5	No se observó el desarrollo de esta parte en las plantillas.
		4. Implementar un mecanismo de análisis predictivo de identificación de riesgos.	5	5	5	5	No se observó esta actividad en el modelo propuesto.
		5. Valorar los riesgos.	4	5	5	5	No se observó el desarrollo de esta parte en las plantillas.
		6. Documentar y comunicar el trabajo realizado.	5	5	5	5	
		7. De ser el caso actualizar y comunicar los documentos.	5	5	5	5	
TRATAMIENTO DEL RIESGO	1. Diseñar y ejecutar planes de mitigación de riesgos.	4	5	5	5	No se observó el desarrollo de esta parte en las plantillas.	
	2. Identificar cambios en la estrategia de protección.	4	5	5	5	No se observó el desarrollo de esta parte en las plantillas.	
	3. Documentar y comunicar el trabajo realizado.	5	5	5	5		
	4. De ser el caso actualizar y comunicar los documentos.	5	5	5	5		

Fase o componente	Actividades	Suficiencia	Claridad	Coherencia	Relevancia	Comentarios
SEGUIMIENTO O REVISIÓN	1. Ejecutar el seguimiento del resultado esperado de las actividades.	5	5	5	5	
	2. Ejecutar el seguimiento del modelo.	5	5	5	5	
	3. De ser el caso rediseñar el modelo propuesto	5	5	5	5	

#### 4. OBSERVACIONES

X	FAVORABLE		DEBE DE MEJORAR		DESFAVORABLE
---	-----------	--	-----------------	--	--------------

#### 5. OBSERVACIONES

El modelo cumple con su propósito y cuenta con el detalle suficiente para ser aplicado de forma práctica. Se recomienda culminar el desarrollo de los formatos pendientes/en proceso, asociados a las actividades "Determinación de nivel de riesgos", "Implementar un mecanismo de análisis predictivo de identificación de riesgos", "Valorar los riesgos", "Diseñar y ejecutar planes de tratamiento de riesgos" e "Identificar cambios en la estrategia de protección".

### CONSTANCIA DE JUICIO DE EXPERTO

Yo, Villavicencio Montoya Mónica Yolanda, identificado con DNI n.º 45824265 doy constancia que realicé el juicio de experto del cuestionario diseñado por ROGER GUSTAVO ABANTO ORTIZ en la investigación titulada: MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN PARA LA GENERACIÓN DE VALOR EN EL CONTROL DE LA CORRUPCIÓN DE FUNCIONARIOS Y SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES DE LA REGIÓN DE LAMBAYEQUE, el día viernes, 24 de julio de 2020.



\_\_\_\_\_  
Villavicencio Montoya Mónica Yolanda


**PERÚ**

Ministerio de Educación

 Superintendencia Nacional de  
Educación Superior Universitaria

 Dirección de Documentación e  
Información Universitaria y  
Registro de Grados y Títulos

**REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES**

GRADUADO	GRADO O TÍTULO	INSTITUCIÓN
VILLAVICENCIO MONTOYA DE PALOMINO, MONICA YOLANDA DNI 45824265	MAGÍSTER EN ADMINISTRACIÓN ESTRATÉGICA DE EMPRESAS  Fecha de Diploma:10/10/18	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
VILLAVICENCIO MONTOYA, MONICA YOLANDA DNI 45824265	INGENIERO DE SISTEMAS Y COMPUTACION  Fecha de Diploma:13/12/2010	UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
VILLAVICENCIO MONTOYA, MONICA YOLANDA DNI 45824265	BACHILLER EN INGENIERIA DE SISTEMAS Y COMPUTACION  Fecha de Diploma:05/05/2010	UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

## Mónica Yolanda Villavicencio Montoya

Ingeniera de sistemas y computación, Magíster en Administración Estratégica de Empresas, certificada en ITIL Foundations, con más de 7 años de experiencia en consultoría de tecnología vinculada con seguridad de la información, ley de protección de datos personales, evaluación de la Matriz SOX (Sarbanes Oxley) para Control Interno, evaluación de procesos de tecnología e implementación de sistemas de información, principalmente en empresas del sector Banca, Infraestructura, Energía, Industria y Salud. Así mismo, cuenta con experiencia en el análisis, diseño, desarrollo e implementación de software. Responsable de las auditorías de los principales grupos económicos del país, con experiencia internacional en Chile.



### Experiencia

**Docente universitario.** Marzo 2019 a la actualidad.

USAT, CHICLAYO, PERÚ. Educación | [www.usat.edu.pe/](http://www.usat.edu.pe/)

Docente perteneciente a la Escuela de Ingeniería de Sistemas y Computación, Facultad de Ingeniería y Arquitectura, responsable del dictado de las asignaturas Auditoría de Sistemas de Información, Auditoría de Controles Generales de TI y Desarrollo de Competencias Digitales a estudiantes de pregrado y postgrado.

**Auditor y Consultor Senior.** Febrero 2013 a la actualidad.

EY PERÚ, ADVISORY SERVICES. LIMA, PERÚ. Asesoría de negocios y auditoría | [www.ey.com](http://www.ey.com)

Líder responsable del planeamiento, ejecución y administración de proyectos sobre seguridad de la información, revisión de adecuación a la ley de protección de datos personales, evaluación de matriz SOX para Control interno, evaluaciones de los procesos de tecnología y mejora de procesos de negocio, en Perú (Lima, Chiclayo, Trujillo, Piura, Pacasmayo y Cajamarca) y Chile (Santiago de Chile). Revisión de las siguientes tecnologías: SAP ERP, SAP HANA, Oracle EBS, SQL Server, Oracle 11g, Informix, DB2, AIX, Red Hat Linux Enterprise, Linux SUSE, Windows Server. Manejo de aspectos administrativos de los proyectos, gestión de equipos de trabajo multidisciplinarios, entrenamiento a personal junior, ejecución de capacitaciones a los clientes, experiencia comercial en la detección de oportunidades de venta, elaboración y presentación de propuestas.

### Principales proyectos:

- Asistencia en el Análisis de Riesgos y Requisitos de Seguridad de la Información en base a la norma ISO 27002 para **Clinica Internacional**.
- Asistencia en la formulación de una propuesta de procesos TIC en base a COBIT 5 en **Petroperú S.A.**
- Revisión de la adecuación a la Ley de Protección de Datos Personales en la **Cámara de Compensación Electrónica**.
- Revisión y diagnóstico de los procesos de TI en empresas del sector financiero: **Edpyme Alternativa, Financiera Efectiva, Cámara de Compensación Electrónica e IM Trust S.A. Administradora General de Fondos** (Chile).
- Revisión y evaluación de controles SOX en el **Grupo Graña y Montero** (GyM; Concar; Viva GyM; Stracom GyM; GyM Ferrovías; Vial y Vives – DSD, sede Chile) y en **Luz del Sur**.
- Evaluación y prueba de controles de accesos lógicos y cambios a programas de los sistemas de información, y revisión de la seguridad en equipos perimetrales y correo electrónico de **Luz del Sur**.
- Revisión y diagnóstico de los principales procesos de TI en **Grupo Gloria, Alicorp, Grupo Centenario, Cementos Pacasmayo, Empresa Editorial El Comercio, Soldex, CENTRIA, Electricidad del Perú Electroperú, Distriluz, Adinelsa, Urbi Propiedades, MODASA, EOM Grupo, Tecnología de Alimentos S.A., Protisa, Agroindustrial Laredo, Grupo EFE** (Financiera Efectiva y Tiendas Efe), **Universidad de Piura, Universidad Cayetano Heredia, Técnica Avícola**.
- Relevamiento y estandarización a la estrategia de negocio de los principales procesos de negocio de

**Agrícola Cerroprieto (Chepén, La Libertad).**

**Consultor de Implementación de Sistemas. 2012 - 2013.**

ISOFT, LIMA, PERÚ. Servicios | [www.isothealth.com/es-es/Partners/SIS.aspx](http://www.isothealth.com/es-es/Partners/SIS.aspx)

Implementación de un sistema ERP en grupo AUNA (Oncosalud). Responsable del planeamiento y ejecución de capacitaciones sobre el uso del sistema.

**Principales funciones:**

- Entendimiento de los procesos de admisión y atención médica ambulatoria, hospitalaria y de urgencias de la Clínica.
- Entendimiento de la funcionalidad del sistema ERP xHIS de ISOFT, respecto al ciclo de atención médica ambulatoria, hospitalaria y de urgencias, desde la admisión, pasando por la atención médica, recetas de medicamentos, toma de exámenes médicos, cirugía, asignación de habitaciones y salas de operación, y culminando con el alta del paciente.
- Revisión de manuales de usuario y ejecución de pruebas funcionales para comprender la funcionalidad del sistema.
- Coordinación de pruebas funcionales e implantación en el ambiente de calidad.
- Resolución y escalamiento de incidentes reportados por los Analistas funcionales de la Clínica.
- Exposiciones ante la Gerencia de Procesos y Líderes funcionales de la Clínica sobre el funcionamiento de los módulos del sistema.
- Diseño y dictado del programa de capacitación sobre el uso del sistema ERP dirigido a la Gerencia de Procesos y Líderes Funcionales de la Clínica.

**Analista y Desarrollador de Sistemas. 2011 - 2012.**

USAT, CHICLAYO, PERÚ. Educación | [www.usat.edu.pe/](http://www.usat.edu.pe/)

Responsable de la implementación y soporte de los sistemas de información de la Universidad. Garantizar la disponibilidad de los servicios de la institución para los usuarios.

**Principales funciones:**

- Análisis de procesos de la Universidad y de requerimientos de las áreas usuarias.
- Diseño de soluciones para satisfacer las necesidades identificadas.
- Desarrollo de software utilizando los lenguajes de programación Visual Basic .NET, HTML y PHP, y base de datos SQL Server y MySQL.
- Elaboración de casos de prueba para los usuarios finales.
- Mantenimiento de las soluciones de tecnología necesarias para soportar los procesos de la Universidad.
- Elaboración de políticas y procedimientos del área de Desarrollo de Sistemas.

**Ponencias**

Expositor en las siguientes ponencias dictadas durante la ejecución de proyectos sobre riesgos y seguridad de la información.

**Revisión de controles de tecnologías de información en la función de Auditoría Interna**

DANPER. TRUJILLO. 2018.

**Requisitos tecnológicos de seguridad de la información en base a ISO 27001 Y 27002**

CLÍNICA INTERNACIONAL. 2017.

**Certificaciones**

**Certificación ITIL Foundations**

APMG - INTERNATIONAL LIMA CHAPTER. 2013.

#### Estudios

##### **MBA Gerencial Internacional**

CENTRUM CATÓLICA. CHICLAYO. 2015 - 2018.

##### **Ingeniería de Sistemas y Computación**

UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO. CHICLAYO. 2005-2010. Ingeniera titulada. Quinto superior.

##### **COBIT 5**

NEW HORIZONS. LIMA. 2014

##### **Business Intelligence con SQL Server 2012**

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO. CHICLAYO. 2012

##### **Programa de Especialización en Auditoría de Tecnologías de Información y Seguridad informática**

USAT. CHICLAYO. 2011

#### Conocimientos adicionales

**Marcos de referencia:** PMBOK, ISO 27001, ISO 27002.

**Inglés:** Escucha intermedio, Lectura intermedio, Escrito intermedio, Oral intermedio.

**Ofimática:** Microsoft Power Point Intermedio, Microsoft Word Intermedio, Microsoft Excel Intermedio

#### Información adicional

Fecha de nacimiento: 02 Setiembre 1988

Miembro activo del Colegio de Ingenieros del Perú

#### Contacto

**Teléfono:** +51949911248

**Email:** [monicavm88@gmail.com](mailto:monicavm88@gmail.com)

**LinkedIn:**

<https://pe.linkedin.com/in/m%C3%B3nica-villavicencia-montoya-3477834a>

#### Referencias

- **Elder Cama** | Socio de EY | 993 530 306
- **Isabel Torres** | Gerente de EY | 993 773 092
- **Orlando Núñez** | Gerente de EY | 993 530 381
- **Víctor Campos** | Gerente de EY | 993 206 146
- **Diana Castillo** | Gerente de everis - Technology | 943 025 738