FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERA DE SISTEMAS

Autora

Bach. De Los Santos Guerrero Karina Carolina
ORCID: https://orcid.org/0000-0002-0969-7110

Asesor

Mg. Heber Mejía Cabrera
ORCID: https://orcid.org/0000-0002-0007-0928

Línea de Investigación

Ciencias de la información como herramientas multidisciplinares y estratégicas en el contexto industrial y de organizaciones

Sublínea de Investigación

Nuevas tendencias digitales orientadas al análisis y uso estratégico de la información

Pimentel – Perú

2025

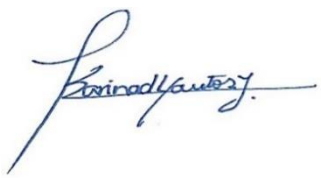
DECLARACIÓN JURADA DE ORIGINALIDAD

Quién suscribe la DECLARACIÓN JURADA, soy **De Los Santos Guerrero Karina Carolina** del Programa de Estudios de **Ingeniería de Sistemas** de la Universidad Señor de Sipán, declaro bajo juramento que soy autor del trabajo titulado:

DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firman:

De Los Santos Guerrero Karina Carolina	DNI: 43306449	

Pimentel, 27 de enero del 2025

REPORTE DE SIMILITUD TURINITIN

Karina Carolina De Los Santos Guerrero

Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una m

Universidad Señor de Sipan

Detalles del documento

Identificador de la entrega
trn:oid:::26396:429234680

Fecha de entrega
11 feb 2025, 6:41 p.m. GMT-5

Fecha de descarga
11 feb 2025, 6:47 p.m. GMT-5

Nombre de archivo
Turnitin Investigación_Karina Carolina De Los Santos Guerrero-1.docx

Tamaño de archivo
723.2 KB

95 Páginas

18,320 Palabras

91,960 Caracteres

13% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Fuentes principales

10% Fuentes de Internet
4% Publicaciones
9% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Caracteres reemplazados
57 caracteres sospechosos en N.º de páginas
Las letras son intercambiadas por caracteres similares de otro alfabeto.

Texto oculto
15 caracteres sospechosos en N.º de páginas
El texto es alterado para mezclarse con el fondo blanco del documento.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA

Aprobación del jurado

MG. GUEVARA ALBURQUEQUE LAURITA BELEN

Presidente del Jurado de Tesis

MG. ARCILA DIAZ JUAN CARLOS

Secretario del Jurado de Tesis

MG., MINGUILLO RUBIO CESAR AUGUSTO

Vocal del Jurado de Tesis

DEDICATORIA

El presente trabajo de investigación se lo dedico a Dios por escuchar mis peticiones y reconfortarme en cada momento, brindándome fortaleza, fe y paz.

A mis padres por su incondicional apoyo, amor, esfuerzo, y sacrificios diarios me han permitido llegar hasta aquí. Su esfuerzo y dedicación me han dado la fortaleza para enfrentar cada reto, y su ejemplo ha sido la guía que me ha acompañado en cada paso de este camino académico.

AGRADECIMIENTOS

Agradezco a Dios por guiar mi camino y bendecirme con mi familia que es lo maravilloso que tengo y ser mi apoyo incondicional, en especial a mis padres y el esfuerzo para lograr mi meta.

A mi tutor de tesis Dr. Ing. Carlos Alberto Chirinos Mundaca quien con su dirección, conocimiento y colaboración a formado parte de este trabajo de investigación.

A la Universidad Señor de Sipán, por habernos brindado una educación de calidad, con profesionales de alto nivel, de quienes he adquirido muchos conocimientos en lo profesional y en valores.

ÍNDICE

Resumen XII

Abstract XIII

I. INTRODUCCIÓN 14

II. MATERIALES Y MÉTODO 29

2.1 Materiales 29

2.2 Método 30

III. RESULTADOS Y DISCUSIÓN 80

3.1 Resultados 80

3.2 Discusión 105

IV. CONCLUSIONES Y RECOMENDACIONES 107

4.1 Conclusiones 107

4.2 Recomendaciones 108

REFERENCIAS 109

ANEXOS 113

ÍNDICE DE TABLAS

TABLA I LISTA DE MATERIALES 30

TABLA II IDENTIFICACION DE ROLES DE ACUERDO CON LOS OBJETIVOS COBIT2019 35

TABLA III TABLA FACTOR DE DISEÑO DE ESTRATEGIAS EMPRESARIALES 39

TABLA IV. TABLA FACTOR DE DISEÑO DE METAS EMPRESARIALES 40

TABLA V CATEGORÍA DE RIESGOS EN LA MUNICIPALIDAD 42

TABLA VI. NIVEL DE TOLERACIA DE RIESGOS 45

TABLA VII. TABLA DE FACTOR DE DISEÑO DE LOS PROBLEMAS QUE SE RELACIONAN CON TI 46

TABLA VIII. NIVELES DE IMPORTANCIA PARA EL DISEÑO 48

TABLA IX IDENTIFICACIÓN DE BRECHAS DE INFRAESTRUCTURA Y SERVICIOS DE TI/SI 49

TABLA X PRIORIDAD DE LOS OBJETIVOS DE GOBIERNO Y GESTIÓN OTORGADOS A UN ELEMENTO DEL DISEÑO DE LA ESTRATEGIA EMPRESARIAL 52

TABLA XI ALINEACIÓN DE LOS REQUERIMIENTOS Y PROCESOS DE LA MUNICIPALIDAD 55

TABLA XII ROLES ASIGNADOS AL PERSONAL PARA PARTICIPACIÓN EN EL DISEÑO DE COBIT 2019 60

TABLA XIII POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN 61

TABLA XIV TABLA DE PRIORIDAD DE OBJETIVOS DE GOBIERNO Y GESTIÓN EN EL ESCENARIO DE AMENAZAS 63

TABLA XV. TABLA DE PRIORIDAD DE OBETIVOS DE GOBIERNO Y GESTIÓ EN LOS REQUISITOS DE CUMPLIMIENTO 65

TABLA XVI. TABLA DE ROLES DE TI 65

TABLA XVII. TABLA DE ABASTECIMIENTO – PROVEEDORES PARA TI 67

TABLA XVIII. TABLA DE PRIORIDAD PARA CONSIDERAR LOS MÉTODOS DE IMPLEMENTACIÓN 68

TABLA XIX. 70
TABLA XX. TABLA PARA DEFINIR EL TAMAÑO DE LA EMPRESA 72
TABLA XXI. NIVEL DE VALORACIÓN PARA LOS OBJETIVOS Y SU CAPACIDAD DE PROCESOS 74
TABLA XXII. LISTA DE EXPERTOS EN COBIT 2019 76
TABLA XXIII. PUNTAJE DE VALORACIÓN DE LOS EXPERTOS PARA EL DISEÑO BASADO EN COBIT 2019 78
TABLA XXIV. VALIDEZ DE EXPERTOS POR V DE AIKEN 79
TABLA XXV RESULTADO DE PORCENTAJE DE PROCESOS - PRETEST 80
TABLA XXVI RESULTADO DE PORCENTAJE DE PROCESOS COBIT 2019 - POSTEST 83
TABLA XXVII Valoración de dominios COBIT 2019 – pretest y postest 86
TABLA XXVIII VALORACION CAPACIDAD DE CUMPLIMIENTO COBIT 2019 88
TABLA XXIX VALORACION CAPACIDAD DE CUMPLIMIENTO COBIT 2019 89
TABLA XXX RESULTADO PORCENTAJE DE INCIDENTES COBIT 2019 - PRESTEST 90
TABLA XXXI PORCENTAJE DE INCIDENTES COBIT 2019 - POSTEST 92
TABLA XXXII LISTA RESUMEN DE LOS ACTIVOS DE LA MUNICIPALIDAD DE LA VICTORIA 94
TABLA XXXIII PORCENTAJE DE ACTIVOS POR CRITICIDAD DE LA MUNICIPALIDAD DE LA VICTORIA - PRETEST 95
TABLA XXXIV CUADRO DE VALORACIÓN POR RANGO DE CRITICIDAD DE LOS ACTIVOS 95
TABLA XXXV PORCENTAJE DE ACTIVOS POR CRITICIDAD DE LA MUNICIPALIDAD DE LA VICTORIA - POSTEST 96
TABLA XXXVI RESULTADO DE LA ENCUESTA DE SATISFACCIÓN - PRETEST 101
TABLA XXXVII. RESULTADO DE LA ENCUESTA DE SATISFACCIÓN - POSTEST 104

ÍNDICE DE FIGURAS

Fig. 1.Proceso para la recolección de datos de acuerdo con los indicadores. 31

Fig. 2. Diseño de un sistema COBIT 2019.....31
Fig. 3. Factores de diseño de COBIT 2019.....32
Fig. 4.Metas empresariales de COBIT 2019.....41
Fig. 5.Mapa de calor para tolerancia al riesgo.....45
Fig. 6.Mapeo de procesos clave de la Municipalidad de la Victoria.....49
Fig. 7.Estrategia empresarial.....51
Fig. 8.Metas empresariales y la cascada de metas de COBIT.....53
Fig. 9.Perfil de riesgo de la empresa.....54
Fig. 10.Temas abiertos relacionados a TI.....55
Fig. 11. Gráfico de valoración para la conclusión del diseño.....73
Fig. 12.Porcentaje de procesos COBIT 2019 – pretest.....83
Fig. 13. Porcentaje de procesos COBIT 2019 - postest.....85
Fig. 14. Porcentaje de dominios de COBIT 2019 – Pretest y Postest.....87
Fig. 15. Porcentaje de incidentes de COBIT 2019 – Pretest.....92
Fig. 16.Porcentaje de incidentes de COBIT 2019 - Postest.....94
Fig. 17.Porcentaje de activos - Pretest.....96
Fig. 18.Porcentaje de activos - Postest.....97
Fig. 19. P1 ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad? – Pretest.....99
Fig. 20. P3 ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo? – Pretest.....99
Fig. 21. P9 ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información? – Pretest.....100
Fig. 22. P12 ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información? - Pretest.....100
Fig. 23. P1 ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad? – Postest.....102

Fig. 24.P3 ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo? – Postest 102
Fig. 25.P9 ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información? – Postest 103
Fig. 26. P12 ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información? – Postest 103

Resumen

Los desafíos a los que se enfrentan las empresas públicas y privadas son complejos, en el año 2021 se encuestó a un total de 62 000 usuarios de 22 empresas a nivel mundial, donde se pudo identificar que el 76% de ellas registraron paralizaciones de sus actividades debido a pérdida de información, fallos en sus sistemas, errores humanos, ataques cibernéticos y ataques interno. A pesar de que existen medidas como la aplicación de gobiernos de TI, donde la automatización llega a un 74% y es más rápido, siguen siendo vulnerables a diversos ataques. Por eso esta investigación propuso diseñar procesos de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en la municipalidad de la Victoria. La investigación se desarrolló en 05 etapas, primero se seleccionó la municipalidad, luego se diagnosticaron las actividades de la municipalidad, se caracterizaron los procesos, se diseñó el sistema de gestión de la seguridad basado en COBIT 2019 y posteriormente se validó mediante juicio de expertos. Se aplicó un cuestionario a 87 usuarios de TI. Como resultado se evidenció que el 97% de los usuarios estaban insatisfechos con respecto a gestión de fallos y para postest se llegó a un 79% de satisfacción de los usuarios con respecto a la adecuada gestión ante fallos. Finalmente se concluye que con el diseño se logró mejorar la gestión de la seguridad de la información basado en COBIT 2019 mejorando notablemente la gestión de la seguridad de la información

Palabras Clave: COBIT 2019, gobierno de TI, gestión de la seguridad.

Abstract

The challenges faced by public and private companies are complex, in 2021 a total of 62,000 users from 22 companies worldwide were surveyed, where it was identified that 76% of them recorded paralyzations of their activities due to loss of information, failures in their systems, human error, cyber-attacks and internal attacks. Despite the existence of measures such as the implementation of IT governance, where automation reaches 74% and is faster, they are still vulnerable to various attacks. That is why this research proposed to design IT governance processes based on COBIT 2019 to manage information security in the municipality of La Victoria. The research was developed in 05 stages, first the municipality was selected, then the activities of the municipality were diagnosed, processes were characterized, the security management system based on COBIT2019 was designed and then validated by expert judgment. A questionnaire was applied to 87 IT users. As a result, it was found that 97% of the users were dissatisfied with respect to failure management and for the post-test, 79% of the users were satisfied with respect to adequate failure management. Finally, it is concluded that the design was able to improve information security management based on COBIT2019, significantly improving information security management.

Keywords: COBIT 2019, IT governance, security management.

I. INTRODUCCIÓN

Los gobiernos trabajan de la mano con el desarrollo digital con la finalidad de crear una base sólida para una economía digital a futuro, por eso se consideran pilares clave al acceso a internet de forma rápida, segura, confiable y asequible, que permita generar, habilidades, aplicaciones y plataformas digitales que permitan a empresas, gobiernos y personas a ser partícipes de la economía digital [1].

Con respecto a economía a nivel mundial, se espera que entre los años 2022 y 2030 el crecimiento del producto bruto interno empiece a disminuir y se ubique alrededor del 2.2% por debajo del pronóstico anual, si hablamos de las economías que aún se están desarrollando, también presentarán una desaceleración abrupta de hasta el 4%, esto indica que podría haber otra crisis financiera mundial caracterizada por recesión, incertidumbre de inversión, caída de la productividad y desempleo en todos los países [2].

En Latinoamérica la brecha tecnológica está muy marcada, para el caso de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) la cual consta de 38 países exporta productos de alta tecnología con un valor de $ 891.18 per cápita y un valor de $ 942.25 en servicios de alta tecnología. En comparación con el resto de américa latina que exporta productos de alta tecnología con un valor de $ 99.78 per cápita y $66. 66 en servicios de alta tecnología, lo que demuestra que en comparación de la OCDE que exporta un 4.58%, américa latina exporta sólo un 3.98%. Con respecto a las medidas implementadas para el teletrabajo el 40% de los trabajadores puede trabajar desde casa, por otro lado en Latinoamérica y el Caribe, sólo el 21% cuenta con acceso a tecnologías que le permitan realizar teletrabajo, en el caso de los estudiantes cerca de 32 millones de niños y niñas no pueden acceder a opciones de teleeducación, esto debido a que de 33 países latinoamericanos, 14 de ellos tienen un bajo nivel de preparación en los gobiernos que permitan aprovechar todas las ventajas tecnologías actuales como la inteligencia artificial, dentro de ellos solo Argentina, Brasil , México, Chile y Uruguay han desarrollado políticas y estrategias lideradas por los propios gobiernos locales. Además cerca de 16 países de 33,

poseen reglamentos de protección de los datos personales de usuarios, 7 de esos países cuentan con leyes sectoriales y 10 ni siquiera cuentan con alguna legislación al respecto [3].

Para el caso de Perú, entre los meses enero – junio del 2014 habría acumulado un 0.5% de retroceso en el crecimiento de la economía, debido a una caída del 7.5% de inversión privada y a la caída del -15.6% pese al avance del 7.1% en inversión pública. Este bajo crecimiento se debe al estallido social, cambios de gobiernos y anomalías climáticas, por ahora el panorama es incierto debido a la alta probabilidad de que existan disrupciones en la cadena productiva debido al fenómeno del niño, donde los gobiernos vienen impulsando el gasto público en programas para la reactivación y emergencia climática [4].

Existen medidas que se implementan con la finalidad de abordar muchos problemas burocráticos actuales, uno de ellos es la aplicación de gobierno de TI en el proceso de trámites, pues si se automatizan llegan a ser hasta 74% más rápidos, entre el 1.5% y el 5% más baratos y son menos vulnerables a la corrupción, es por eso que muchas entidades públicas buscan la implementación de gobierno de TI enfocado en la generación de valor para la empresa y alineado a la mitigación de riesgos [5].

En Perú, la gobernanza digital fue un proceso que a finales del 2018 se considera de interés nacional como parte del desarrollo e innovación, ya para el año 2021 se crea el Sistema Nacional de Transformación Digital para englobar todas las materias de gobierno digital, es por eso que como medida se promulgan decretos a favor del gobierno y transformación digital con la finalidad de impulsar la economía digital, gracias a estas medidas para finales del 2021 el país logró crecer en indicadores de ciberseguridad y telecomunicaciones logrando subir 9 posiciones con respecto al año anterior ocupando el puesto 86 del total de 182 economías evaluadas [6].

Considerando al índice mundial de innovación en el año 2022, Perú se encuentra en el puesto 65 del total general de 132 países, donde se ocupó el puesto 61 a nivel de instituciones, el puesto 47 a nivel de capital humano e investigación, el puesto 79 a nivel de

infraestructura, el puesto 40 en desarrollo de mercado, el puesto 49 en desarrollo empresarial, el puesto 90 en producción de conocimientos y el puesto 65 tecnología productos creativos, pero eso no es suficiente en comparación con economías mundiales como Suiza en el puesto 1, Estados Unidos en el puesto 2 y Suecia en el puesto 3 respectivamente [7].

Para seguir creciendo en Perú, el presupuesto para inversión en infraestructura y equipamiento en la Comisión de Ciencia, Innovación y Tecnología (CITE) subió de 19.6 millones a 299 millones de soles, el gasto operativo subió de 18.7 millones a 47 Millones y el presupuesto actual asciende los 150.0 millones de soles, sólo el 39% está destinado a inversión y el 61% está destinado a gastos operativos. Se recalca también un impacto positivo para las pymes con pronósticos de que el 85% de las unidades productivas manejen eficazmente sus procesos, y que de ese porcentaje el 76% coloquen productos nuevos en el mercado, de esta forma buscan ofrecer 73. 657 servicios de TI para 26 588 unidades productivas que se verán beneficiadas [8].

En el año 2021, en una encuesta realizadas a 6200 usuarios de 22 empresas de diversos países, se pudo evidenciar que cerca del 76% de las organizaciones sufrieron paralizaciones por causas internas, del total del 76% de las empresas el 52% de ellas dijo que perdió información por fallos en el sistema, el 42% perdió información por errores humano, el 36% dijo que perdió información por ciberataques y el 20% dijo que perdió información por ataques internos. Otros datos importantes que considerar fueron que del total de los encuestados, el 50% de las organizaciones aseveró que asignan menos del 10% de su presupuesto total a inversión en seguridad de TI, sólo el 23% de las organizaciones a nivel mundial invierte más del 15% de su presupuesto total. Lo más impactante es que el 66% de los usuarios tienen incertidumbre solo si sus datos fueron modificados [9].

El costo mundial que genera la vulneración de los datos, para el año 2023 fue aproximadamente 4.45 millones de dólares con un claro aumento del 15% en 3 años a nivel mundial, es por eso que cerca del 51% de las organizaciones tiene planificado invertir en

seguridad como consecuencia, de haber sufrido algún tipo de vulneración, esto incluye las respuestas a incidencias, estrategias, capacitación al personal, herramientas de apoyo de detección y la respuesta oportuna a amenazas, esto representaría un ahorro promedio para las organizaciones de 1. 76 millones de dólares. A pesar de que se cuentan con herramientas basadas en inteligencia artificial para seguridad, sólo el 28% de las organizaciones la usan, por eso se necesita gestionar los servicios y reforzar las defensas para detener las amenazas. Además, cerca del 82% de vulnerabilidades afectaron directamente a datos almacenados en la nube, lo que sugiere que las organizaciones opten por soluciones híbridas que cubra, información en la nube, aplicaciones, servicios y base de datos [10].

En un informe realizado por ESET Security Report en Latinoamérica del total de 17 países, al 62% le preocupa el robo de su información, de entre ellos, el 36% aseguró que destinan presupuesto para el área de ciberseguridad, esto se refleja en que para el año 2021, se detectaron más de 22 mil reportes de vulnerabilidades, lo que resulta en 4100 explots que son detectados diariamente. Para detallar más el problema se consideraron los factores del ataque, las herramientas tecnológicas usadas, el personal humano y la gestión de la misma organización, como resultado obtuvieron que el 52% aduce no tener incidentes de seguridad independientemente de no tener la certeza de haberlo sufrido o no, el 24% sufrió infección de malware, el 5% sufrió filtración de información, el 8% sufrió explotación de sus vulnerabilidades, el 17% sufrió ataques de ingeniería social, el 13% identificó accesos no autorizados y donde 1 de cada 3 compañías afirma aplicar políticas de seguridad luego de haber sufrido al menos un ataque [11].

En el año 2022, la Asociación de Bancos (Asbanc) lanzó una alerta al gobierno peruano sobre la filtración de información del tipo personal que era administrada por entidades públicas, dicha data ha sido filtrada y vendida por redes sociales, afectando a la transacciones seguras; otra filtración se dio mediante la Plataforma de Interoperabilidad del Estado Peruano (PIDE) que actualmente viene siendo administrada por RENIEC, donde se podía extraer información personal que permitía ingresar a las cuentas de los usuarios y tener acceso a la

información de instituciones públicas. La filtración de datos afecta a las entidades públicas o privadas creando daño a la reputación de la empresa, pérdidas financieras, multas y otros, para el caso de los individuos afectados, pueden ser víctimas de extorsión o pérdida de su dinero [12].

A nivel regional la contraloría de la República, en este año, del 1 al 7 de marzo luego de realizar una auditoría en la Municipalidad de Olmos, determinó que existe un incumplimiento en la protección y conservación de archivos, pues existe un riesgo de sustracción, pérdida y degradación por el mal almacenamiento de los archivos, además de o contar con ventilación adecuada, zonas con mucha humedad, zonas como muebles y sillas llenas de archivos e impurezas, acumulación de información importante para la ciudadanía almacenada en cartones y sacos en mal estado y algunos hasta deteriorados [13].

En ese contexto, se formuló la pregunta de investigación ¿Cómo mejorar la gestión de la seguridad de la información en una municipalidad peruana? Ante esta pregunta se determinó la siguiente hipótesis, mediante el diseño de gobierno de TI basado en COBIT 2019 se mejora la gestión de la seguridad de la información en una municipalidad peruana. A partir de ello, el objetivo general de la investigación es diseñar procesos de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana. Los objetivos específicos: - Diagnosticar las actividades relacionadas con seguridad de la información en la municipalidad peruana. Caracterizar los procesos de TI relacionados a la seguridad de la información; diseñar mediante gobierno de TI los requerimientos necesarios para la seguridad de la información basado en COBIT 2019 y validar el diseño de gestión de la seguridad de la información con prueba empírica y por juicio de expertos.

Esta investigación se justifica en la necesidad de contar con un sistema de gestión de seguridad en la municipalidad de la Victoria como parte de minimizar los riesgos que puedan afectar a flujo de información entre áreas de la municipalidad. Existen diversos marcos de trabajo que apoyan a las empresas en la gestión de la seguridad, pero pocos marcos de

trabajo consideran la parte de gobernanza.

En respuesta a lo descrito anteriormente, esta investigación se avala en diversas investigaciones nacionales e internacionales como el trabajo de Miloslavkaya y Tolstaya. En su investigación titulada: “Information security Management maturity models” en Rusia [14]. Describen el problema de contar con varios modelos de madurez para la gestión de la seguridad, pero no existe una comparación para determinar cuál es el más apto para ser implementado con resultados eficaces. Por eso propusieron evaluar diversos modelos de madurez siguiendo modelos estandarizados, para esto compararon el modelo de madurez del banco de Rusia basado en COBIT 4.1 de 6 niveles. con el modelo de capacidad de madurez de los SGSI de 9 niveles, el modelo de madurez del NIST con 5 niveles, modelo de madurez de Open Group denominado SM3 de 5 niveles. El enfoque de Gartner que incluye gestión de riesgos con 5 niveles, el modelo de gestión de riesgos MMGR de 5 niveles, el modelo de gestión de incidentes de seguridad MM, de 3 niveles y finalmente el modelo de madurez del monitoreo de seguridad de la información SOC-UCMM. Como resultado generaron un cubo entre en nivel de madurez, los dominios y casos de uso, con proyecciones adicionales basadas en el SOC-UCMM. Llegaron a la conclusión que, al realizar este estudio, la comparación de modelos de madurez servirá para otros investigadores a determinar cuál de ellos es en que más se adecua a la realidad del caso que están investigando. Desde la perspectiva de Wulandari, et al. En su investigación titulada:” Risk assessment and recommendation strategy based on COBIT5 for Risk: Case study Sikn Jikn helpdesk service” en Indonesia [15]. Describen que el centro de SIKN JIKN, como todas las organizaciones, presentan riesgos incluidos riesgos tecnológicos que pueden generar pérdidas o efectos negativos para la empresa. Por eso propusieron un análisis de riesgos que permita que todos los riesgos se identifiquen y controlen como parte de un programa prioritario en el área de servicio de asistencia técnica de la empresa. Usaron el marco COBIT5 como referencia para evaluación de dichos riesgos, el método usado sigue 3 fases: Recopilación de datos, análisis de datos y análisis de riesgos. Como resultado pudieron determinar 7 categorías de riesgos

basado en COBIT5, se identificaron un total de 13 riesgos relacionados al servicio de asistencia técnica, esta escala de puntuación se afianzó con una entrevista de alta gerencia con un nivel de impacto de 3 niveles (bajo, medio y alto) donde finalmente en base a entrevistas y observaciones se encontró que en cada escenario el riesgo potencial era alto, es decir todos los riesgos necesitaban ser mitigados. Finalmente concluyeron que el centro de Sjikn necesita optimizar sus procesos mediante el plan de mitigación sugerido para que los servicios tengan continuidad. Así mismo, Irsheid, et al. En su investigación titulada: "Information security risk management models for cloud hosted systems: A comparative study" en Jordán [16]. Describieron que varias empresas en Jordan, comenzaron a migrar gran parte de sus activos de información a tecnología que tenía soporte en la nube, por tema de disponibilidad, escalabilidad y disponibilidad de la información, esto ha generado nuevos riesgos asociados al proceso de migración relacionada con la gestión, evaluación y gobernanza de riesgos. Por eso realizaron una investigación diversos modelos para la gestión de seguridad como ISO 27005, NIST SP 800-30, OCTAVE Allegro, CRAMM, CORAS y COBIT 5. Como resultado generaron una secuencia para la selección del mejor método con 4 fases: Selección de modelos de seguridad, comparación de estructuras (Aplicabilidad, adaptabilidad y participación), comparación de resultados y conclusión. Dentro de los principales hallazgos se determinó que ISO 27005, NIST SP 800-30 y CRAMM, usan enfoques abstractos de alto nivel con procesos generales para gestionar riesgos, pero alejados de la infraestructura basada en la nube, por otro lado, para el tipo de riesgos en la nube se recomienda OCTAVE, CORAS y COBIT 5, porque incluyen infraestructuras específicas de la nube, que se pueden evaluar, resaltaron el uso de COBIT5 porque cubre la parte de gobernanza al tratarse de sistemas en la nube. Concluyeron que OCTAVE Allegro es el preferido para gestión de riesgos en la nube, así como COBIT5 y CORAS con algunos ajustes. Por otro lado, Plant, Hillegersberg y Aldea. En su investigación titulada "Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps envirnment" en Netherlands [17]. Describen la problemática general de tienen las empresas para transformar los departamentos de TI mediante DevOps que es un enfoque innovador pero que la gran

mayoría de empresas tienen inconvenientes para controlar sus procesos dado al alto grado de exposición a riesgos que se pueden presentar en los equipos y departamentos de TI. Por eso propusieron un diseño basado en revisión de literatura y entrevistas a 17 empleados de 09 empresas holandesas que están en diferentes etapas de la transición a DevOps. Como resultados argumentaros que no existe una manera que permita implementar DevOps pues se debe adaptar a la situación de la empresa, además se pudo determinar que hay dos factores de riesgos que influyen en la gestión de controles que son la madurez de DevOps y el apetito de riesgo. Finalmente concluyeron que las empresas primero deberían establecer una cultura sólida de DevOps para no depender de las prácticas de automatización y que los auditores de TI deberían evaluar los mecanismos de gobierno blando para garantizar un mejor control interno en entornos DevOps. Complementando, Alvarado y Andrade. En su investigación titulada "Gestión de gobierno de Ti basado en COBIT 2019, para el colegio de bachillerato Sara Serrano de Maridueña" en Ecuador [18]. Describen el problema al que se enfrenta un auditor para determinar el estado actual de las instituciones y las mejoras que se pueden aplicar con apoyo de los gerentes de las organizaciones. Por eso propusieron un plan orientado en tecnología de la información basado en COBIT 2019 que apoye en la acciones correctivas y preventivas para mejoras en el área de TI. Usaron los lineamientos de COBIT 2019 para poder realizar una revisión de la situación actual y se plantean las mejoras en base a esa propuesta. Los resultados más importantes fueron que existían 3 tipos de servicios para toda la institución, con dicha información establecieron 06 metas empresariales donde 19 riesgos pueden afectar directamente al cumplimiento de dichas metas; el 63% del total tenían una valoración de muy peligrosos, el 21.05% eran riesgos altos, 10.5 % eran normales y el 5.26% considerados riesgos bajos. Con su propuesta ofrecieron 40 objetivos de COBIT 2019 que se pueden adecuar a cualquier empresa, con esto redujeron hasta en 65% la peligrosidad de ocurrencia de los riesgos. Concluyeron que dentro de cada proceso se deben considerar métricas que permitan evaluar las mejoras en la organización. Por otro lado, Cortés. En su investigación titulada: "Propuesta de método basado en COBIT 2019 para la evaluación de procesos tecnológicos en la municipalidad de Carrillo" en Costa Rica [19]. Describen que,

para las municipalidades de ese país, se promulgó una ley de telecomunicaciones y gobernanza que solicitaba a todos los municipios a modernizarse y aprovechar todos los recursos tecnológicos para satisfacer a usuarios internos y externos como los ciudadanos mediante la optimización de sus servicios. Por eso propusieron un método orientado con COBIT 2019 para que la municipalidad adopte y personalice su entorno organizacional para mantener, evaluar, mejorar y mantener el marco de gobierno de TI y gestionen la tecnología de forma eficaz. Dentro de los resultados obtenidos, considerando los niveles de capacidad institucional en cuanto a gestión y objetivos encontraron que para resguardar y afianzar el compromiso con todas las partes interesadas, para gestionar las relaciones y la gestión de riesgos, gestión de la seguridad, de capacidad y disponibilidad, gestión de configuración, gestión de peticiones e incidentes, gestión de problemas, gestión de servicios de seguridad y gestión del cumplimiento de requisitos el nivel de capacidad de la entidad llega a un valor de 1 que oscila entre 0% a 15%, siendo el más bajo en la escala, pero de acuerdo al análisis de capacidad la institución acordó llegar a un puntaje de 3 que oscila entre el 15% a 50% de cumplimiento para todos los objetivos. Finalmente concluyó que COBIT 2019 tiene una gran versatilidad permitiendo acoplarse a procesos evaluativos de TI que mejoran la madurez institucional a mediano y largo plazo. Al respecto, Malca. En su investigación titulada: “Modelo de gobierno de tecnologías de la información: Diseño para una facultad de ingeniería de una universidad pública peruana” [20]. A pesar de que esta institución es amplia, no gestiona de manera adecuada la tecnología de la información y no cuenta con un gobierno digital ofrezca un mejor servicio a estudiantes, docentes y administrativos. Por eso propuso un modelo de gestión de gobierno basado en COBIT 2019 que permita alinearse los objetivos institucionales en la parte estratégica mediante la optimización, escalabilidad y descubrimiento de mejoras que permitan disminuir la brecha tecnológica. Propuso un modelo que incluyan los niveles de madurez, cantidad de metas tecnológicas, avance de implementación de dominios y procesos COBIT alineados a los objetivos institucionales. La población se conformó por 89 personas entre personal directivo, de planificación, personal docente, unidad informática y personal administrativo. Dentro de los principales resultados encontró que sólo el 6% de los procesos

se implementaron, se aplicó el 14.26% del total de objetivos APO, sólo se contó el 7.5% de tecnología para la implementación, con respecto a la cantidad de objetivos, el 65% de la institución se encontró en un nivel 0, el 10% en un nivel 1 y el 25% se logró acentuar en el nivel 2 de madurez. Llegó a concluir que, con la implementación del modelo se mejoró la gestión de gobierno de TI, esto se puede mejorar siempre y cuando la involucre la alta dirección, se incrementen las políticas organizacionales, liderazgo y sobre todo el soporte financiero. Morán, Jimbo, Franco y Jimbo. En su investigación titulada: "Aplication of COBIT2019 to the government and management of information technologies in non-profit educational institutions" en Ecuador [21]. Describe el problema que enfrentan las instituciones sin fines lucro, pues se desenvuelven en un entorno incierto lo que genera una cantidad considerable de riesgos que permitan un continuo desarrollo del negocio para esta institución educativa religiosa. Por eso propusieron aplicar COBIT 2019 mediante una investigación focal donde se desarrolló el proceso de auditoría siguiendo los siguientes procesos, primero: determinar el alcance del sistema para luego delimitar el alcance, diseñar los sistemas de gobernanza para concluir con la evaluación de capacidad. Como principales resultados obtuvieron que es importante alinear los objetivos de TI con los objetivos de la empresa, se identificaron los principales riesgos, en este caso para aplicar el modelo de capacidad del proceso usaron matrices RACI que permitieron generar un informe de auditoría. Llegaron a concluir que COBIT 2019 permitió gestionar los riesgos mediante la identificación, evaluación y mitigación de los riesgos. Esto sin duda permitió que se asegure la integridad, disponibilidad y confidencialidad de los recursos tecnológicos en una institución sin fines de lucro. Complementando lo anterior, Nabeel, Rahmat y Widyayasya. En su investigación titulada: Transformasi digital InsurCo dengan merancang pengelolaan risiko teknologi informasi menggunakan framework COBIT2019 IT risk management focus área, en Estocolmo [22]. Describe que a pesar de que existen diferentes investigaciones sobre gobernanza y gestión de TI, no existen análisis profundos sobre la gestión de riesgos a pesar de que son muy importantes porque afectan directamente a las empresas. Por eso, propusieron usar el método basado en entrevistas denominado DRS (Investigación de ciencias del diseño) que

costa de tres partes: el entorno de investigación, la ciencia básica y el resultado de la investigación, todas las partes apoyadas en COBIT 2019, para poder diseñar la correcta gestión de riesgos, esto consideró además la evaluación de capacidades, posibles mejoras, impacto en base a estimaciones, y análisis de brechas dentro de la empresa InsurCo. Como resultado se evaluaron 40 objetivos TKM TI (Tecnología, conocimiento y management) referidos a la metodología de gestión de TI que se basa en COBIT con los 23 objetivos de las áreas prioritarias. Logrando considerar la capacidad de los componentes se seleccionaron el APO12 con 0% para de Gestión de riesgo, EDM03 con 6.12% en Garantía y optimización del riesgo y DSS04 Gestión de continuidad con 5.45%, obteniendo un promedio general de 3.75% de mejora en la gestión de riesgos. Llegaron a concluir que esta investigación se puede usar como base para los 7 componentes de gobernanza tomando como prioridad la gestión de riesgos que respalde la transformación digital. Así mismo, Syaputra, Kesuma, Saputra y Fitra. En su investigación titulada: "Design of information technology (IT) governance using framework COBIT 2019 subdomain APO01 (Case study: Instidla). En Indonesia [23]. Describe el problema del Instituto de Tecnología y Negocios Dniniyyah Lampung (INSTIDLA), que a pesar de ser un instituto reconocido, no plantica, no regula y no cuenta con políticas que evalúe la madurez de la implementación TI, además que no cuentan con la infraestructura de TI necesaria para un correcto acceso a la información, sumado la falta de cultura y disciplina organizacional. Por eso propusieron, diseñar y aplicar un modelo de gobernanza de TI con base en COBIT 2019 con el propósito de tener una visión holística del desempeño de gobierno de TI considerando la capacidad de TI de la institución. El método usado fue de acuerdo con el diseño de gobernanza de TI, parte con la iniciar la etapa del programa, definición de hojas guía, problemas, oportunidades y el programa según planificación. Los resultados de su investigación proporcionaron valores de madurez de gobernanza de 6 niveles, 5 escalas de creación de índices y un cuadro general de análisis y recomendaciones de brechas de acceso a la información contemplados en el APO01. Posterior a la implementación pudieron determinar que de un nivel 1 de capacidad se lograron cumplir varios objetivos institucionales alcanzando un nivel 3 de capacidad. Finalmente concluyeron que la gobernanza de TI se

puede mejorar con el proceso APO01 de COBIT 2019, pues se redujeron las brechas de acceso a la información y se incrementó la capacidad de madurez de la institución. Considerando el estudio de, Klucka y Grünbichler. En su investigación titulada: Enterprise risk management - approaches determining its application and relation to business performance, en Eslovaquia y Estados Unidos [24]. Describe el problema presente en Eslovaquia donde la gestión de riesgos no está establecida de forma legal y tampoco es obligatoria para todas las empresas, estos riesgos se pueden manejar de forma positiva o negativa dependiendo la planificación y el tratamiento que se les da. El método usado fue aplicar una serie de entrevistas para recopilar información y posteriormente analizar los resultados en base a las actividades de gestión de riesgos y desempeño de las empresas. Realizaron un cuestionario a 55 empresas de Norteamérica, encontraron que el 44% tuvo ventas inferiores a 500 millones de dólares y el 40% tenía menos de mil empleados. Para el caso de Eslovaquia se encuestó a 162 empresas de las cuales el 95% son entre medianas y pequeñas empresas. Dentro de los resultados más importantes encontraron que el 36% aseguró tener un director de riesgos, el 25% dijo que a pesar de tener un jefe, no cubre todo el programa de gestión de riesgos, el 8% atribuye tal responsabilidad al gestor de riesgos, cerca del 42% dijeron que no tenían documentación sobre gestión de riesgos, el 33% afirmó que existe control interno, el 31% cuenta con sistema organizativo y el 28% se enfoca en la calidad de la empresa. Por el lado de Eslovaquia a diferencia de Norteamérica, el 65% considera que gestionar los riesgos corresponde a una tarea de la alta dirección. Identificaron 5 tipos de riesgos, el riesgo operacional. El riesgo de cumplimiento, el riesgo de imagen institucional, el riesgo financiero y el riesgo estratégico. Llegaron a la conclusión de que existe una relación fuerte entre el rendimiento y el riesgo y que en la opinión de los trabajadores, el control y gestión de riesgos recae en el director de la empresa, pues las decisiones de alta gerencia o dirección influyen de forma en las tareas y obligaciones de sus empleados. Por su parte, Juiz, Duhamel, Gutiérrez y Luna. En su investigación titulada: IT managers´ framing of IT governance roles and responsibilities in Ibero-American Higher Education Institutions en Suiza [25]. Describieron que a pesar de la existencia de guías para gestión de gobierno corporativo muy

pocas organizaciones lo realizan de forma efectiva, donde muchos de ellos no tienen una asignación de responsabilidades y roles estratégicos ni para gobierno ni para gestión de TI. Por eso propusieron usar ISO/IEC 38500 y COBIT para indagar sobre las actividades, roles y responsabilidades que deben tener los gerentes de TI, los órganos de gobierno y otros niveles gerenciales. El método que usó tiene lo siguientes pasos, se realizó una revisión para seleccionar las mejores prácticas, mediante juicio de expertos, se aplicó la encuesta a 43 institutos, se realizó una regresión estándar MCO para estimar el impacto de los factores, posteriormente se realizaron preguntas a responsables de TI entre los años 2019 y 2020. Como resultados consideraron 212 prácticas para las 212 preguntas, obtuvieron que sólo el 10% de la instituciones cuenta con programas de gobierno efectivos, el 60% tienen programas algo efectivos y el restante tiene programas ineficientes, con estos resultados y la opinión de los expertos se obtuvo una coincidencia del 70% en que existe una separación de roles donde los gerentes son los que toman las riendas de actividades gobernanza y donde los gerentes no aceptan desarrollar actividades de gestión. Concluyeron que los resultados contribuyen en la identificación y detección de posibles problemas considerando el nivel organizacional, las condiciones culturales y las responsabilidades tecnológicas de los directivos. Así mismo, Kandasamy, Srinivas, Achuthan y Rangan, en su investigación titulada: IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. En India [26]. Abordan el problema que representan los ataques de IoT en las tres capas principales de red, hardware y red propiamente identificadas, estos ataques forman parte de un conjunto de riesgos que surgen como parte de la heterogeneidad de tecnología y datos. Por eso propusieron realizar un análisis holístico sobre marcos internacionales que permitan evaluar y clasificar los riesgos cibernéticos para posteriormente presentar un método de clasificación y cuantificación de riesgos para proponer estrategias y técnicas que mitiguen esos riesgos. Identificaron 4 riesgos: riesgos éticos, riesgos de privacidad, riesgos de seguridad y riesgos técnicos. Como parte del análisis se revisaron marcos de riesgos de seguridad cibernética (CSRF), entre ellos OCTAVE, NIST, ISO en combinación con COBIT5 que fue seleccionado para gestionar los riesgos, procesos, roles, áreas de riesgo y

operaciones, para esto realizaron una encuesta a 230 personas de 700 que era la población. Dentro de los hallazgos más importantes encontraron que existen 7 vectores de riesgo relacionados con la nube, y 4 categorías para la evaluación del riesgo, y que cerca del 882% de las industrias de salud han sufrido ataques de ciberseguridad; en base a eso se encontraron un total de 72 como puntuación a los riesgos identificados en el caso de estudio, lo que representa un nivel de riesgo muy alto, posterior a la evaluación encontraron que el riesgo disminuyó a 36 lo que representa que ahora se encuentra en un nivel de riesgo medio. Llegaron a la conclusión que para calcular de forma correcta el riesgo que se genera luego de multiplicar la probabilidad de ocurrencia por el impacto que puede tener. Complementando por su parte, Hakim, Fauzi y Santosa. En su investigación titulada: Analisis dan perancangan proses manajement risikó ti eggunakan kerangka kerja COBIT 2019 di PT iti (PERSERO), en Indonesia [27]. Describieron el problema de gestión que necesitan tener las empresas estatales, pues en indonesia, el gobierno evalúa constantemente a las instituciones, si obtienen una buena calificación y control, el estado les proporciona presupuesto, en ese contexto la empresa trabajaba con COBIT 4.1. Por eso en el afán de mejorar la gestión propusieron un análisis para la gestión de riesgos en la empresa PT INTI en el departamento de servicios de TI, los autores realizaron una evaluación de la versión más actual que es COBIT 2019 como una guía para la gestión de riesgos. La metodología usada tiene 04 fases: la primera fase se describen los hallazgos sobre problemas de TI, en la fase 2 se realizó la evaluación de COBIT 2019 para determinar las capacidades del proceso, la fase 3 explican los objetivos alineados al APO12 para gestión de riesgos, en la fase 4 se determina la prioridad de recomendaciones en base a la fase anterior. Dentro de los resultados más importantes encontraron 5 puntos de riegos empresariales, 5 puntos críticos de TI, para eso seleccionaron el APO12 para gestión de riesgo según COBT 2019, de los cuales evaluaron 7 apartados, 1 para políticas y 6 para el tema de registros, posteriormente establecieron prioridades a los riesgos, considerando las probabilidades de ocurrencias encontraron que 12 riesgos eran <20% (muy bajo), 24 riegos entre 20% y 40%(bajo), 36 riesgos mayores a 40% y menores a 60% (normales), 48 riesgos entre 60% y 80% (alto) y 60 riesgos entre 80% y

100% (muy grande). Para mejorar estos hallazgos establecieron una matriz de riesgo que permitió proporcionar una lista de controles para ser implementados. Llegaron a concluir que el APO12 para gestión de riesgos basado en COBIT 2019, permite identificar y evaluar los riegos de forma más eficiente que las versiones anteriores de COBIT. Además, Safitri, Syafii y Adi. En su investigación titulada: "Measuring the performance of information system governance using framework COBIT 2019" en Indonesia [28]. Describieron el problema de una entidad gubernamental en la oficina de vivienda en Salatiga con respecto a considerar gestionar la tecnología con el objetivo de tener agua de mejor calidad, los servicios de vivienda y el saneamiento de los ciudadanos. Por eso propusieron usar el marco COBIT 2019 para medir el desempeño de los sistemas de información alineados a mejorar la gobernanza. Cómo método usó 6 procesos relacionados a la investigación: Identificación de problemas, literatura de estudio, observación y entrevista, mapeo de dominios, cálculo del nivel de capacidad y recomendaciones. Dentro de los resultados más importantes, encontró que el departamento municipal de Salatiga tienen un 70% de amenazas debido a la falta de informes, con respecto al mapeo para el diseño se consideró que el 20% necesita contar con requisitos de cumplimiento de forma urgente, en base a eso determinaron los siguientes requisitos de cumplimiento de COBIT 2019: EDM03, APO12, DSS05 y MEA03 para los procesos de apoyo, fábrica, giro de negocio, y estratégico, con respecto al diseño de TI, se consideró tipos de abastecimiento, donde el 30% se debe subcontratar, el 50% se debe considerar como servicios en la nube y sólo el 20% se debe considerar de forma interna. Teniendo en cuenta los métodos para la implementación se consideró trabajar en 50% de forma ágil, 30% con apoyo de DevOps y 20% de forma tradicional. Concluyeron que el diseño de gobierno con COBIT 2019 con el kit de herramientas para 4 procesos fueron APO12, APO13, APO09, DSS02, DSS3, por es para mejorar la gobernanza y gestión en una entidad estatal y municipal se recomienda el uso de estos apartados. Finalmente, Russo, Reis, Silveira y Mamede. En su investigación titulada: "Towards a comprehensive framework for the multidisciplinary evaluation of organizational maturity on business continuity program management: A Systematic literature review." En Portugal [29]. Describieron el problema de continuidad de

negocio que atraviesan las empresas en los procesos comerciales en un tiempo determinado; a pesar de que existen una serie de lineamientos y guías, es muy complejo determinar el mejor plan para la continuidad del negocio. Por eso propusieron una revisión literaria a fin de proponer un marco integral para poder evaluar la madurez organizacional para continuidad de negocio. Para esto realizaron el método de revisión literaria que sigue los siguientes 03 procesos: Plan de revisión, realizar la revisión y finalmente documentar las revisiones, entre estándares internacionales como ISO 22301:2019, NFPA 1600 2019, CMMI V2.0, COBIT 2019 e ITIL V4. Dentro de los principales resultados de una revisión de 1 254 artículos se pudo encontrar que el 10% de ellos hacen referencias a directrices estratégicas que se pueden aplicar en las organizaciones, el otro 90% consideraban a la población y el contexto por lo tanto se dejaron de lado en la evaluación de calidad por lo tanto solo consideraron 393 publicaciones. Como dato adicional encontraron que el 19% del total de los artículos revisados, el tratamiento de los desastres sólo representa el 7%, y el uso de una metodología llega al 15%. Concluyeron que las métricas e interpretación de resultados son sumamente necesarios para tener medidas de contingencia ante incidentes o interrupciones en las funciones del negocio.

II. MATERIALES Y MÉTODO

2.1 Materiales

En cuanto a los materiales usados se consideran equipos dado en el enfoque de la investigación, se usaron materiales de oficina en su mayor parte, dentro del equipo de trabajo se contempló una laptop y el marco de trabajo COBIT 2019 como parte crucial para el desarrollo de esta investigación.

TABLA I
LISTA DE MATERIALES

COMPONENTE	DESCRIPCIÓN
Dispositivo de trabajo	Procesador: Intel Core i5-1165G7 a 2.50 GHz, RAM: 16GB, Sistema Operativo: Windows 10 de 64 bits
Marco de trabajo	COBIT 2019
Papelería	Papel bond A4 75g
Impresora	EPSON L3250

2.2 Método

El proceso metodológico para la recolección de la información parte desde la presentación en la Municipalidad, continúa la realización de la encuestas para el personal, además de tener reuniones continuas, se realizó la recolección de información mediante los documentos relacionados con los procesos y actividades que realiza la municipalidad para poder evaluar un antes y un después de aplicar el diseño de gestión de la seguridad propuesto. Como apartado final, se aplicaron cuestionarios al personal que tiene acceso a información relevante dentro de la municipalidad. Con respecto a la cantidad del personal encuestado se realizó un cálculo de población finita siendo un total de 87 personas encuestadas.

Fig. 1.Proceso para la recolección de datos de acuerdo con los indicadores.

Con respecto a la metodología propiamente relacionada con COBIT 2019 y la municipalidad se estableció la gestión de gobierno y seguridad de la información vinculado a los procesos segregados de los objetivos de esta investigación.

Fig. 2. Diseño de un sistema COBIT 2019

Como parte del diseño se detallan los subprocesos que COBIT 2019 recomienda para un sistema de gestión de la seguridad de la información considerando el Anexo 11.

Fig. 3. Factores de diseño de COBIT 2019.

2.2.1. Diagnosticar las actividades relacionadas con seguridad de la información en la municipalidad peruana.

2.2.1.1. Identificar actividades relacionadas a gobierno de TI

Como parte de la identificación de las actividades se consideró listar los objetivos empresariales de las estrategias de gobierno de la municipalidad de la Victoria.

Objetivos empresariales

- Cultivar la competitividad económica en el distrito Victoriano.
- Disminuir la vulnerabilidad que se puede presentar ante algún tipo de desastre.
- Optimizar las condiciones de habitabilidad en el distrito.
- Gestionar la institucional de la municipalidad.

- Apoyar el desarrollo humano y estilos saludables de vida en la ciudadanía.
- Consolidar la gestión ambiental en el distrito.

Estrategias de gobierno

- Coordinación de acciones con instituciones especializadas en seguridad, enfocadas en el bienestar de la comunidad.
- Provisión de asistencia técnica en seguridad ciudadana de forma eficiente y dirigida a la población.
- Implementación de patrullajes sectorizados para mejorar la seguridad de los habitantes.
- Desarrollo de programas vecinales de seguridad ciudadana con un enfoque específico en las necesidades locales.
- Organización de ferias económicas integrales para promover la formalización entre los ciudadanos.
- Soporte técnico especializado para emprendedores del distrito de La Victoria.
- Asesoramiento en la formalización de negocios informales, orientado a comerciantes de manera eficiente.
- Fortalecimiento de la plataforma de defensa civil para el beneficio del distrito.
- Identificación, prevención e intervención en áreas de riesgo focalizadas, asegurando la protección de los residentes del distrito de La Victoria.
- Elaboración de análisis técnicos exhaustivos sobre vulnerabilidades en diversas áreas del distrito.
- Supervisión integral de obras públicas, garantizando su correcta ejecución en espacios comunitarios.
- Monitoreo puntual de la infraestructura urbana en favor de los ciudadanos.
- Promoción de medidas de seguridad vial integrales, orientadas al bienestar de la población.

- Reorganización del espacio urbano vial mediante proyectos de inversión pública y campañas de concienciación ciudadana en el distrito.
- Actualización del sistema catastral para una mejor gestión en el distrito.
- Implementación de mecanismos internos de control en la gestión municipal.
- Implementación de un sistema de gestión institucional basado en procesos dentro de la Municipalidad.
- Fortalecimiento de las capacidades del personal municipal.
- Refuerzo de los mecanismos de participación ciudadana en la gestión municipal.
- Simplificación de procesos y trámites administrativos en la Municipalidad.
- Implementación de mecanismos legales y de defensa alineados con las competencias municipales.
- Prestación de servicios sociales integrales para atender a las poblaciones más vulnerables.
- Ejecución de programas de salud preventiva dirigidos a sectores en situación de vulnerabilidad.
- Promoción de actividades deportivas y programas de reinserción juvenil para el desarrollo comunitario.
- Fomento de una cultura inclusiva como parte del desarrollo educativo de la población.
- Gestión integral de residuos sólidos para el beneficio colectivo.
- Separación en origen y recolección diferenciada de residuos sólidos.
- Capacitación técnica en educación ambiental para los habitantes del distrito de La Victoria.
- Servicios continuos de mantenimiento y conservación de áreas verdes públicas para el disfrute de la comunidad.

2.2.1.2. Identificar roles

Como parte de la identificación de los roles se contemplaron las siguientes necesidades y responsabilidades:

TABLA II
IDENTIFICACION DE ROLES DE ACUERDO CON LOS OBJETIVOS COBIT2019

Objetivo COBIT 2019	**¿Por qué es necesario?**	**¿Quién podría ser el responsable y por qué?**
GOBIERNO	Se necesitan procedimientos que mantengan el establecimiento de políticas y control de rendimiento en el área de sistemas, generando valor a la Municipalidad.	Gerente de TI, porque necesita establecer políticas para el área de sistemas basado en las necesidades de la Municipalidad.
	Se necesitan procedimientos de jefatura de área para gestionar adecuadamente los recursos que permitan el cumplimiento de las políticas dictados por el gobierno de TI de la Municipalidad.	Jefe de Sistemas, porque necesita tener liderazgo y compromiso con el cumplimiento de las políticas de la Municipalidad a nivel de sistemas de información.
GESTIÓN	Se necesitan procedimientos enfocados en la seguridad de la información según los dictámenes de la jefatura de sistemas.	Oficial de seguridad de la información, porque trabajará apoyando al Jefe de Sistemas con las operaciones relacionadas a seguridad de la información y ciberseguridad.
	Se necesita monitorear la gestión de manera independiente para informar al Gerente de TI sobre el	Auditor interno de TI. Porque la persona encargada del monitoreo no debe ser juez ni parte en el

rendimiento de la gestión de seguridad de la información.	proceso de gobierno.

2.2.1.3. Entender los problemas de la Municipalidad de la Victoria

Para poder entender los problemas que presenta la Municipalidad de la Victoria se realizaron una serie de preguntas:

a. ¿Cuál es la preocupación más relevante para cumplir la misión de la Municipalidad?. Explicación: La opción seleccionada es debido a que la Municipalidad distrital de la Victoria es una organización estatal, su preocupación principal es el servicio a la ciudadanía.

   Estas metas fueron analizadas anteriormente, y se encuentran alineadas a los objetivos de la municipalidad.

b. ¿Cuáles son las amenazas informáticas más preocupantes en la Municipalidad?. Explicación: La opción seleccionada es debido a que el área de sistemas brinda mayormente servicios de soporte en las otras áreas de la Municipalidad, además no cuenta con un área madura de desarrollo ni de seguridad.

c. ¿Cuál cree que son las causas que posibiliten el perfil de riesgo anterior?. Explicación: La opción seleccionada se debe a la creciente evolución tecnológica de la organización y el poco recurso que el área de gerencia general asigna al área de sistemas. Se manifiesta que todos los trabajadores del área de sistemas deben hacer todo tipo de labor.

d. ¿En qué nivel considera que la Municipalidad está amenazada en temas informáticos a comparación de otras Municipalidades? ¿Normal o Alto?. Explicación: La Municipalidad considera estar dentro de lo normal respecto a amenazas como hacking, violación a la privacidad de datos, robo de equipos, entre otros.

e. ¿En qué nivel considera Ud. que la Municipalidad se encuentra respecto a exigencias u obligaciones legales a comparación de otras Municipalidades? ¿Bajo, Normal o Alto?. Explicación: La Municipalidad considera estar dentro de lo normal con otras Municipalidades distritales. Sin embargo es consciente que las Municipalidades Provinciales manifiestan mayores exigencias por el Gobierno Central y Gobierno Regional.
f. ¿Considera que el área de TI brinda a la Municipalidad apoyo de soporte, de fábrica de soluciones, de cambio para innovaciones tecnológicas o de estrategias empresariales?. Explicación: La opción seleccionada se debe a que el área de TI brinda servicios como limpieza de equipos, copias de seguridad de archivos, revisión de puertos USB, revisión de conexión de internet, escaneos, instalación de sistemas del gobierno regional y central.
g. ¿Los servicios y tecnologías para la gestión de dominio, hosting y correo electrónico son externos, en la nube, internos o híbrido?. Explicación: La opción seleccionada se debe a que la mayoría de los servicios y las tecnologías son gestionadas por plataformas del gobierno regional y central, que para la Municipalidad distrital de la victoria se considerarían como entes externos.
h. ¿Cómo desarrollan software en el área de TI?. Explicación: La opción seleccionada se debe a que la Municipalidad, a pesar de no contar con un área de desarrollo maduro, atiende requisitos de software bajo el método de cascada.
i. ¿Qué tanto demora el área de TI de la Municipalidad en adoptar una nueva tecnología como por ejemplo Inteligencia Artificial?. Explicación: La opción seleccionada se debe a que el área de TI al tener poco personal capacitado en nuevas tendencias tecnológicas, no puede ser ágil en la implementación de estas tendencias.
j. ¿Cuántos trabajadores tiene la Municipalidad?. Explicación: La opción seleccionada se basa en los parámetros de COBIT 2019, ya que la Municipalidad

cuenta con 83 trabajadores, y al ser menor a 150, se ubica en la clasificación de Mediana empresa.

Como parte de los procesos de COBIT 2019, se describieron los procesos de forma detallada como parte del diseño del sistema de gestión de la seguridad:

A. Entender el contexto y la estrategia empresarial

Para entender y conocer las actividades y procesos que involucra el proceso de diseño y construcción de un sistema de gestión de la seguridad de la información, es importante analizar los objetivos de gobierno y los objetivos de gestión de COBIT 2019 para determinar cuáles son los más necesarios para la municipalidad:

- Primero se realizó una entrevista con el gerente general como representante del alcalde, para determinar cuáles son los requerimientos de la municipalidad que se relaciona con la gestión de la seguridad de la información. A ese listado de necesidades se denominaron objetivos de negocio.
- Segundo, se realizó una entrevista con el encargado del área de sistemas para conocer y definir los objetivos que tiene el área para poder optimizar los servicios que ofrece a los ciudadanos con apoyo de la tecnología, a esa lista de objetivos se le denominó objetivos de TI.

a. Entender la estrategia empresarial

Para entender la estrategia empresarial, se tomó en consideración los objetivos Dentro de las reuniones se detallaron las estrategias empresariales de forma general las cuales fueron avaladas por el gerente.

- Minimizar la cantidad de índices por falta de seguridad pública.
- Incrementar y fortalecer la economía en el distrito.
- Reducir puntos vulnerables ante riesgos y desastres en el distrito.

- Mejorar las condiciones de vivienda para los ciudadanos.
- Mejorar la gestión institucional.
- Promover estilos de vida saludable y humano para los ciudadanos
- Promover la conciencia ambiental en el distrito.

TABLA III
TABLA FACTOR DE DISEÑO DE ESTRATEGIAS EMPRESARIALES

Estrategia	**Meta/Objetivo**
Crecimiento	Incrementar y fortalecer la economía en el distrito.
Innovación	Mejorar la gestión institucional.
Servicio al cliente	- Minimizar los índices de desprotección ciudadana que afecta a los ciudadanos - Reducir puntos vulnerables ante riesgos y desastres en el distrito. - Promover estilos de vida saludable y humano para los ciudadanos - Promover la conciencia ambiental en el distrito

b. Entender las metas empresariales

Las metas empresariales son las que respaldan las estrategias y se articulan en aspectos asociados con balanced scorecard, estas metas están basadas en los servicios de TI y la seguridad de la información qué es importante como apoyo en el logro de las estrategias empresariales, estas se detallan a continuación:

TABLA IV.
TABLA FACTOR DE DISEÑO DE METAS EMPRESARIALES

Meta	Dimensión Balanced ScoreCard	Detalle de la meta empresarial
EG01	Finanzas	Portafolio de servicios – Proteger información como datos personales de los ciudadanos dentro de los sistemas internos del área de sistemas.
EG02	Finanzas	Gestión de riesgos de negocio – Proteger la información relacionada a tributos que se procesan dentro del portal web institucional.
EG03	Finanzas	Adherencia a las normativas y disposiciones externas – Proteger la información financiera de forma que sea confidencial y transparente de acuerdo con los lineamientos del Gobierno Regional.
EG06	Cliente	Cumplimiento con la disponibilidad y continuidad de servicio – Proteger la continuidad del servicio web que ofrece trabajadores y ciudadanos.
EG11	Interno	Cumplimiento de políticas internas – Salvaguardar la información personal y laboral de los trabajadores.

Fig. 4.Metas empresariales de COBIT 2019

c. Comprender el perfil de riesgo

Es necesario comprender el perfil de riego de la empresa centrados en los tipos de riesgos de TI a los que la empresa está expuesta para determinar el apetito de riego y listar las áreas más vulnerables. Para este caso de tomaron los riesgos que pueden afectar con un mayor impacto y probabilidad con respecto a la situación de la municipalidad, por eso se dejó de lado los demás riesgos y escenarios de riesgo.

TABLA V
CATEGORÍA DE RIESGOS EN LA MUNICIPALIDAD

Riesgos por categoría	**Escenarios de riesgos**	**Impacto (1-5)**	**Probabilidad (1-5)**	**Valoración**
Toma de decisiones de TI	Falta de inversión en TI que respalde estrategias digitales en la municipalidad.	4	5	Muy alto
	Poca gestión de recursos debido a la incongruencia de prioridades de negocio.	3	4	Alto
Gestión del ciclo de vida de proyectos.	Poco presupuesto en proyectos de TI.	5	4	Muy alto
	Falta de calidad en los proyectos de TI.	4	3	Alto
	Entrega de proyectos fuera de tiempo.	4	4	Muy alto
Supervisión y costo	Requerimientos de acuerdos de SLA inadecuados.	3	3	Medio
	Falta de inversión en TI	4	2	Medio
Habilidades y conocimiento de TI	Falta de formación y capacitación en TI.	4	3	Alto
	Dependencia del personal de TI para prestación solución de problemas.	4	2	Medio
Infraestructura	Falla en la adopción de	5	5	Muy alto

de TI	nueva infraestructura de TI.			
	Poca o nula documentación de arquitectura empresarial que conduce a la duplicidad.	4	4	Muy alto
Incidentes de infraestructura	Daño accidental de equipos y dispositivos de TI.	3	3	Medio
operativa	Errores de personal en backup y actualizaciones de sistemas.	5	3	Muy alto
	Interrupción de servicios alojados en la nube por parte de los proveedores.	4	3	Alto
Acciones no autorizadas	Modificación de software de forma no intensional que genera resultados inexactos	4	2	Medio
	Errores en la gestión de cambios y configuración no intencionada.	4	2	Medio
Incidentes de hardware	Fallo de servicios de internet y electricidad.	4	3	Alto
	Retraso de atención a incidentes de hardware por el área de soporte.	5	4	Muy alto
Incidentes de terceros o proveedores	Soporte inadecuado donde los servicios proporcionados por los	4	2	Medio

	proveedores no se alinean a los SLA.			
	Detalle de SLA inadecuado.	4	3	Alto
Incumplimiento	Poca relevancia a los cambios que pueden afectar al entorno empresarial.	5	3	Muy alto
Desastres naturales	Inundación (Fenómeno del niño)	5	2	Medio
Innovación tecnológica	No se han identificado tecnologías actuales que aporten valor.	3	3	Medio
	No considerar a la nueva infraestructura de TI como parte de la optimización de procesos.	5	4	Muy alto
	No se proporcionan soporte a los nuevos modelos de negocio considerando la tecnología.	4	5	Muy alto
Gestión de la información y datos	Revelación de datos sensibles a personal no autorizado por el deficiente archivamiento de la información.	5	3	Muy alto

Donde:

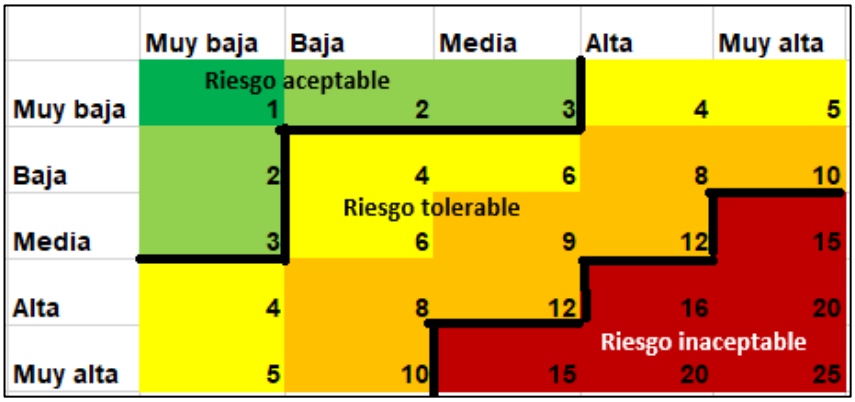


Fig. 5.Mapa de calor para tolerancia al riesgo.

Y donde el nivel de tolerancia al riesgo es el siguiente:

TABLA VI.
NIVEL DE TOLERACIA DE RIESGOS

Zona	Criterio	Descripción
Inaceptable	>=15	Nivel de riesgo inaceptable para la empresa. Debe aplicarse medidas de gestión de riesgo de forma obligatoria y ser consideradas como prioritarias.
Tolerable	<15 - >=4	Nivel de riesgo tolerable para la empresa. Pueden aplicarse medidas de tratamiento de riesgo.
Aceptable	<4	Nivel de riesgo aceptable para la empresa. No es necesario medidas de tratamiento de riesgo adicionales. Por otra parte, se puede aplicar medidas para gestionar las oportunidades.

d. Entender los temas pendientes relacionados a TI

Para poder entender los problemas relacionados con TI, se realizó una valoración de riesgos basados en los problemas frecuentes relacionados con TI.

TABLA VII.
TABLA DE FACTOR DE DISEÑO DE LOS PROBLEMAS QUE SE RELACIONAN CON TI

Referencia	Descripción	Importancia (1-3)	Valoración
A	Dificultades entre unidades de TI porque da la impresión de que genera poco aporte de valor para el negocio.	2	
B	Dificultades entre el área de TI y las áreas de negocio por fallas en aplicación de iniciativas que generan impresión de poca contribución de valor al negocio.	2	
C	Incidentes de cuidado vinculados con TI como la pérdida de información, grietas de seguridad, errores de aplicaciones, proyectos sin éxito, etc.	3	
D	Inconvenientes por parte de terceros en la entrega de servicios.	3	
E	Incumplimiento con regulaciones, requisitos o contratos vinculados a TI	3	
F	Hallazgos frecuentes en evaluaciones o informes de auditoría sobre la disminución de indicadores de desempeño de TI o problemas con el servicio y la calidad.	2	
G	Gastos significativos fraudulentos u ocultos en TI	1	
H	Duplicidad o superposición entre diversas iniciativa o pérdida de recursos	1	

I	Personal agotado o insatisfecho con recursos de TI escasos.	3	
J	Cambios realizados por TI que no cubren las necesidades del negocio porque se ejecutan de forma tardía o son muy costosos	1	
K	Resistencia y falta de compromiso de alta gerencia a involucrarse con decisiones de TI	1	
L	Modelos complejos con decisiones poco claras relacionadas con TI	1	
M	Coste excesivamente alto de TI	1	
N	Implementación fallida de ideas novedosas debido a la arquitectura usada en los sistemas de TI.	3	
O	Grietas entre el conocimiento empresarial y tecnológico que genera confusión en la comunicación entre usuarios y especialistas de TI	2	
P	Problemas constantes con la integración de la información derivada de diversas fuentes.	3	
Q	Elevado nivel de computación del usuario final que promueve falta de supervisión y control sobre el desarrollo de las aplicaciones	1	
R	La áreas de negocio ponen en operación soluciones propias sin la consulta o participación del área de TI.	3	
S	Poco conocimiento sobre normas y políticas de privacidad y seguridad.	3	

T	Limitaciones para la exploración de nuevas tecnologías apoyadas en I&T.	3	

Línea base de la referencia (2)

Donde:

TABLA VIII.
NIVELES DE IMPORTANCIA PARA EL DISEÑO

Importancia	
Sin problema	
Problema	
Problema grave	

2.2.2. Caracterizar los procesos de TI relacionados a la seguridad de la información

Como parte de la caracterización de los procesos de TI relacionados con la seguridad de la información, se realizó un mapeo de los procesos clave, además de la identificación de brechas en la infraestructura de tecnolgía en la Municipalidad de la Victoria.

2.2.2.1. Mapeo de procesos clave

Dentro de los procesos clave, se consideraron 03 componentes: Gobierno, Gestión operativa y gestión supervisora.

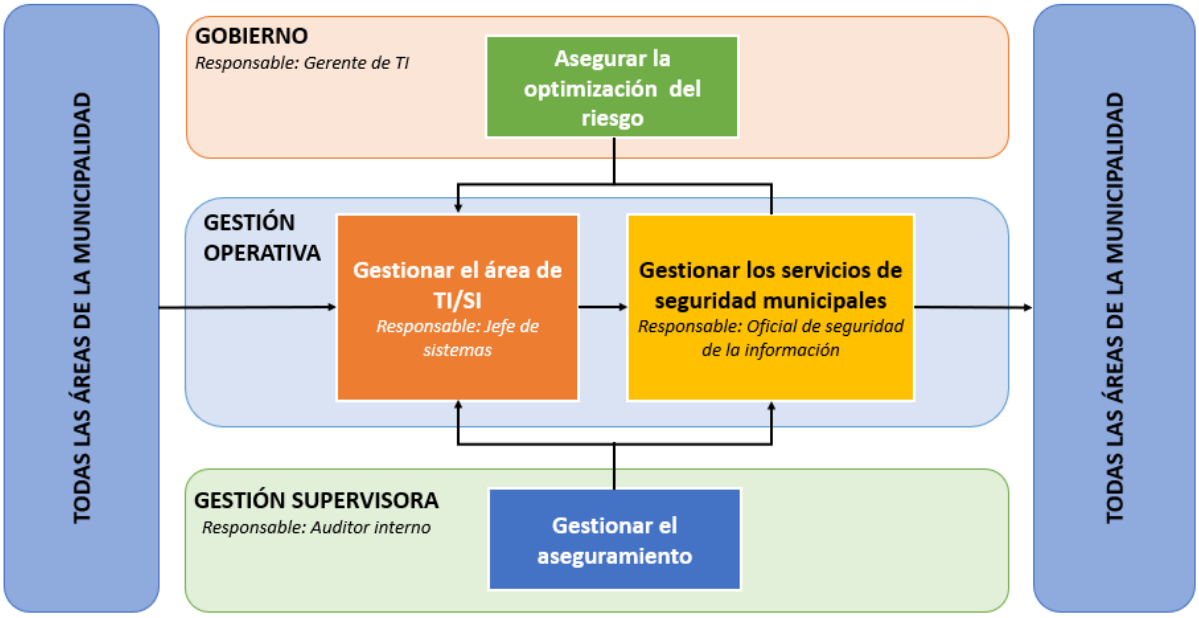


Fig. 6.Mapeo de procesos clave de la Municipalidad de la Victoria.

2.2.2.2. Identificar brechas

Como parte de la identificación de brechas, se consideraros los avances de ejecución con respecto a la infraestructura y servicios de TI/SI de acuerdo con la Resolución de alcaldía N° 119 – 2021 MDLV/A en la Municipalidad de la Victoria.

TABLA IX
IDENTIFICACIÓN DE BRECHAS DE INFRAESTRUCTURA Y SERVICIOS DE TI/SI

Actividad/Tarea	Meta anual	% Ejecución
Implementación de sistemas informáticos	4	100%
Actualización del portal de consultas en línea	4	100%
Actualización de la información del portar de consultas en línea	360	88%
Elaboración de un Plan Operativo Informático	1	0%
Actualización del portal institucional	1	100%
Actualización del portar del estado peruano	48	100%

Soporte técnico de servidores	12	83%
Mantenimiento de computadoras	120	100%
Mantenimiento de impresoras	240	46%
Mantenimiento de la red de cómputo	2	100%
Ampliación del sistema de red de cómputo	4	100%
Mantenimiento de una base de datos del sistema integral	12	83%
Mantenimiento de la base de datos del sistema de Renta y Cajas	121	83%
Mantenimiento de la base de datos del registro civil	12	83%
Mantenimiento de la data del sistema documentario.	121	83%
Copias que respaldan las bases de datos de los sistemas de rentas y caja	312	100%
Copias que permiten respaldar la data del sistema del sistema de registro civil	312	100%
Respaldo de seguridad de la base de datos del sistema de trámite documentario	312	100%
Respaldo de seguridad de la base de datos del sistema integral	312	100%
Respaldo de seguridad de la base de datos del sistema SIAF	312	100%
Documentos remitidos	360	60%
Total de porcentaje de ejecución		86%

B. Determinar el alcance inicial del sistema de gobierno

Parte importante para caracterizar los procesos de TI van relacionados con conocer el alcance del sistema de gobierno y gestión, para este estudio se basó en un enfoque cuantitativo donde se consideran los objetivos más importantes para cada factor del diseño.

En cuanto a la valoración para las tablas de asignación se consideran valores entre 0 – 5, donde 5 es máxima relevancia y cero es no relevante.

a. Considerar la estrategia empresarial

Para considerar las estrategias de la empresa y poder transmitirlas mediante prototipos, es importante considerar las diversas estrategias a nivel de crecimiento, innovación constante como parte de la individualidad en los productos que se ofrecen a los clientes, otro punto importante es el liderazgo en cuanto al manejo de los costos que deberían ser mínimos a corto plazo.

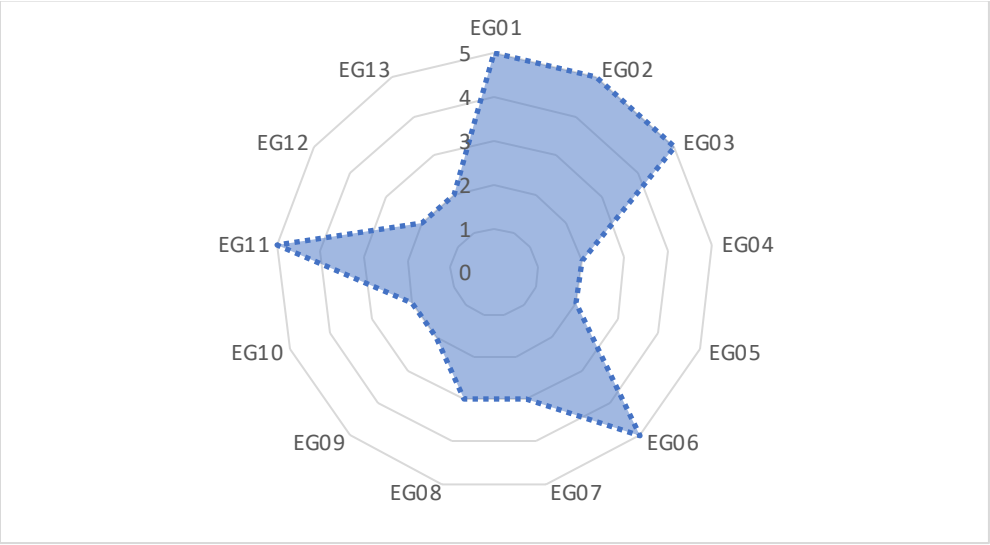


Fig. 7.Estrategia empresarial

Como se puede visualizar en el gráfico anterior con respecto a las estrategias, el EG01, EG02, EG03, EG06 y EG12 son los que obtuvieron una mayor puntuación, posteriormente se consideró los objetivos priorizados con respecto a las estrategias.

TABLA X
PRIORIDAD DE LOS OBJETIVOS DE GOBIERNO Y GESTIÓN OTORGADOS A UN ELEMENTO DEL DISEÑO DE LA ESTRATEGIA EMPRESARIAL

Estrategia	**Meta/Objetivo**
Crecimiento	Incentivar la competitividad económica en el distrito.
Innovación	Mejorar la gestión institucional.
Servicio al cliente	- Minimizar los índices de inseguridad ciudadana que afecta a los ciudadanos - Reducir puntos vulnerables ante riesgos y desastres en el distrito. - Promover estilos de vida saludable y humano para los ciudadanos - Fortalecer la gestión ambiental en el distrito

b. Considerar las metas de la empresa y aplicar la cascada de metas de COBIT 2019

Las metas de la empresa apoyan a las estrategias, esto se puede lograr mediante la identificación de metas desde 03 dimensiones (Internos, crecimiento y finanzas), relacionadas con el balanced scordcard que pueda considerar las empresa de forma independiente y pueda mostrarse de forma resumida las metas, la denominación y la dimensión que tienen mayor relación con las estrategias en este caso de la Municipalidad.

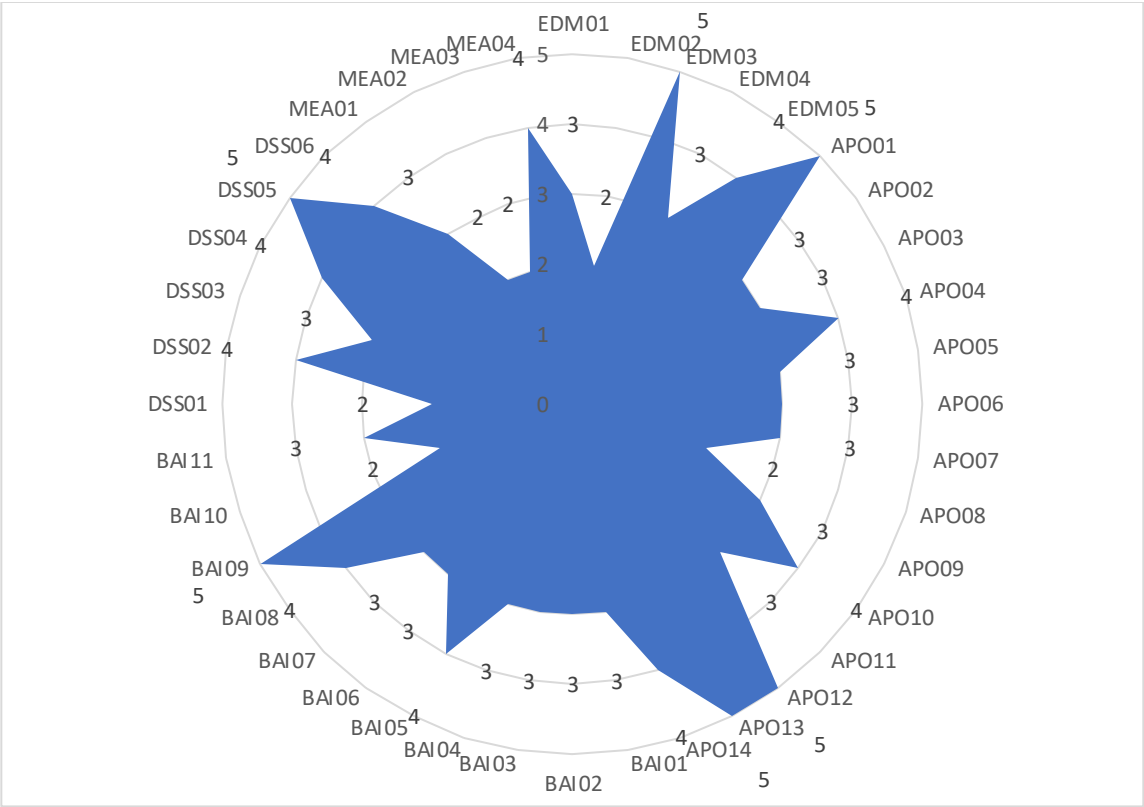


Fig. 8.Metas empresariales y la cascada de metas de COBIT

Como se puede deducir del cuadro anterior, los objetivos de gobierno que tienen mayor puntaje son EDM03, APO01, APO12, APO13, BAI09 y DSS05 con un puntaje de 5 de acuerdo con los valores anteriormente indicados.

c. Considerar el perfil de riesgo de la empresa

Para identificar y asociar el riesgo y los problemas por los cuales atraviesa la empresa es importante primero poder reconocer el tipo de riesgo que se relaciona a TI y a los riegos a los que se encuentra vulnerable actualmente, además de eso se debe considerar qué áreas o departamentos están más expuesto por sobre el apetito de riesgo que se debe detallar para cada empresa.

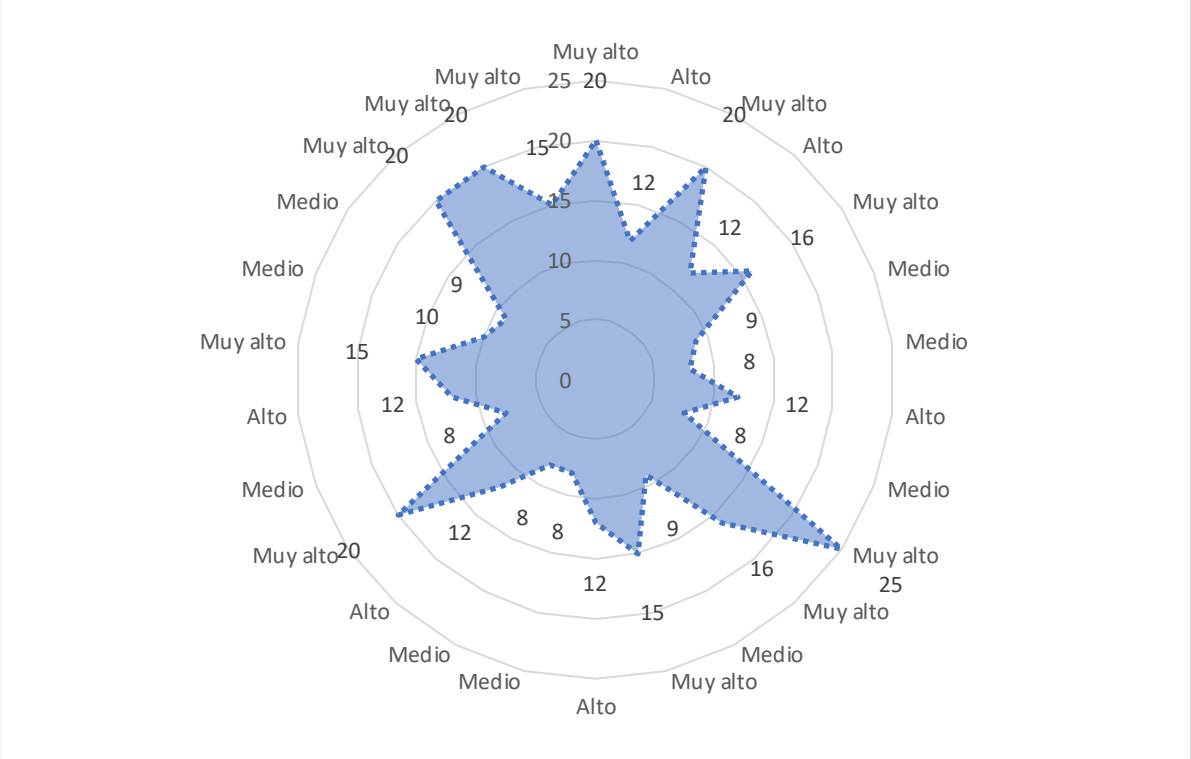


Fig. 9.Perfil de riesgo de la empresa

En la figura anterior, se puede observar a mayor detalle que hay riesgos que tienen una puntuación muy alto y que pueden a la larga afectar en mayor medida a le seguridad de la información de la municipalidad.

d. Considerar problemas relacionados a TI

En este apartado, se refleja el resúmen con respecto a la valoración que se le asignó a los riesgos, en específicos los que están relacionados de forma directa con TI, en el caso de que el riesgo ya materializado se covierte en un problema.

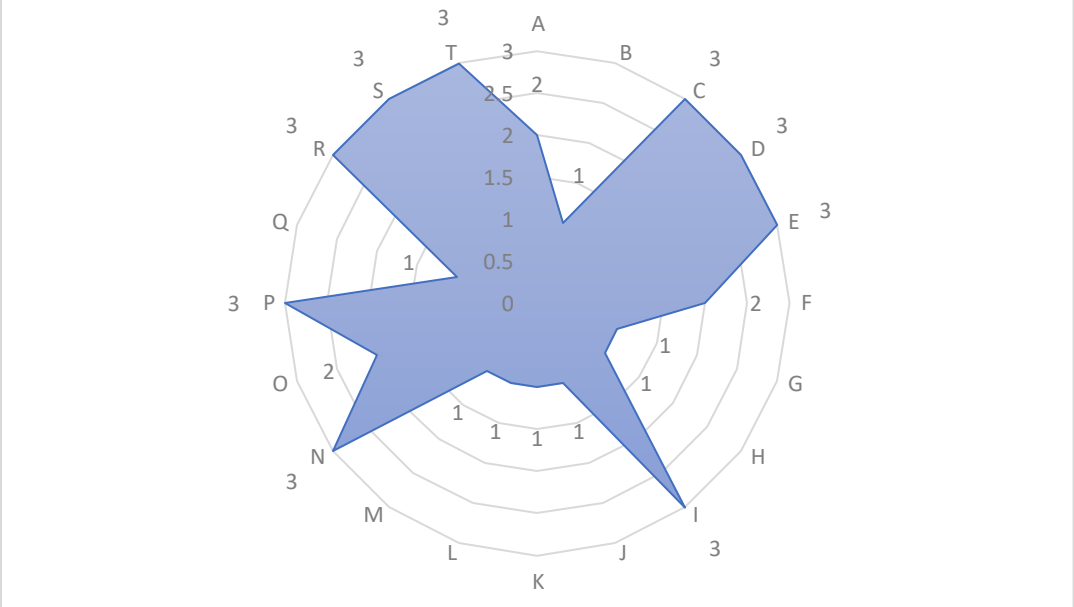


Fig. 10.Temas abiertos relacionados a TI

De la figura anterior se puede deducir que hay problemas con una valoración muy alta, lo que puede generar que la municipalidad esté vulnerable a perder su información.

2.2.3. Diseñar mediante gobierno de TI los requerimientos necesarios para la seguridad de la información basado en COBIT 2019.

2.2.3.1. Alineación de requerimientos y procesos

A continuación se detalla la alineación de los requerimientos y procesos de la municipalidad de la victoria, cada uno de ellos con el proveedor y cliente.

TABLA XI
ALINEACIÓN DE LOS REQUERIMIENTOS Y PROCESOS DE LA MUNICIPALIDAD

Requerimiento	Proveedor	Proceso	Cliente
Asegurar la optimización del riesgo	Alcalde Consejo	- Analizar la estructura y contexto de la organización en relación con los riesgos asociados a I&T.	Área de Sistemas

	regional Gobierno regional Gobierno central	- Identificar el nivel de riesgo que la organización está dispuesta a aceptar en el ámbito de I&T como parte de sus objetivos estratégicos. - Establecer márgenes de tolerancia al riesgo en función del nivel de riesgo aceptado, considerando posibles desviaciones temporales. - Evaluar la alineación entre la estrategia de riesgos en I&T y la estrategia general de riesgos de la organización, asegurando que el nivel de riesgo aceptado no supere la capacidad de riesgo. - Informar sobre cualquier problema de gestión de riesgos al consejo directivo o al comité ejecutivo.	
Gestionar el marco de gestión de I&T	Gerente de TI	- Comprender la visión, dirección y estrategia corporativa junto con el contexto empresarial y sus desafíos actuales. - Tener en cuenta el entorno interno, incluidos la cultura organizacional, la	Áreas de Sistemas Oficial de seguridad de la información

		política de seguridad, los valores éticos y la tolerancia al riesgo.. - Utilizar la cascada de metas y los factores de diseño de COBIT para determinar prioridades en el sistema de gestión y los objetivos de implementación. - Diseñar un modelo de procesos de gobierno de I&T adaptado a la organización, basado en los objetivos de gestión seleccionados. - Asegurar la definición clara de roles y responsabilidades para garantizar la rendición de cuentas.	
Gestionar los servicios de seguridad	Gerente de TI	- Implementar herramientas de protección contra software malicioso en todos los sistemas de procesamiento y mantener sus definiciones actualizadas automáticamente.. - Filtrar el tráfico entrante, como correos electrónicos y descargas, para bloquear contenido no solicitado o potencialmente dañino.	Áreas de la Municipalidad

(p.ej. spyware, correos electrónicos de phishing).

- Restringir el acceso a la información corporativa y la red solo a dispositivos autorizados, configurándolos para requerir contraseñas.

- Establecer controles de red mediante firewalls y sistemas de detección de intrusos, además de aplicar políticas para gestionar el tráfico de datos.

- Asegurar que las conexiones de red utilicen protocolos de seguridad aprobados.

- Configurar equipos y sistemas operativos siguiendo prácticas seguras.

- Gestionar el acceso a través de navegadores y correos electrónicos, bloqueando sitios web específicos y desactivando enlaces peligrosos en dispositivos móviles.

		- Regular los derechos de acceso de los usuarios según sus roles y las políticas de seguridad, aplicando los principios de menor privilegio y necesidad justificada. - Realizar revisiones periódicas de registros de eventos para identificar posibles incidentes.	
Gestionar el aseguramiento	Gerente de TI	- Entender la estrategia y prioridades de la empresa. - Comprender las prioridades estratégicas de la organización y el contexto interno para evaluar mejor los objetivos y amenazas críticas. - Incluir todos los componentes de gobierno en las revisiones, tales como principios, políticas, estructuras, procesos, comportamientos éticos, información, servicios, infraestructura y habilidades. - Diseñar un plan detallado para recopilar y evaluar información sobre controles de gestión, enfocándose en la aplicación de	Gerente de TI

buenas prácticas y el cumplimiento de objetivos de control.

- Documentar las implicaciones de las debilidades detectadas en los controles de gestión.

- Coordinar e implementar acciones correctivas dentro de la organización para abordar las debilidades identificadas.

- Realizar seguimientos internos para verificar que las acciones correctivas hayan solucionado las brechas en los controles internos.

2.2.3.2. Roles

A continuación se detallan los roles involucrados en el diseño de gestión de la seguridad de la información basado en COBIT 2019.

TABLA XII
ROLES ASIGNADOS AL PERSONAL PARA PARTICIPACIÓN EN EL DISEÑO DE COBIT 2019

Etapas para diseño de sistema de gobierno COBIT2019	**Roles**
Entender y contextualizar	Gerente de TI Jefe de Sistemas
Determinar el alcance	Gerente de TI

Afinar el alcance	Gerente de TI Jefe de Sistemas
Concluir el sistema	Gerente de TI Jefe de Sistemas Oficial de seguridad de la información Auditor interno de TI

2.2.3.3. Políticas

Se detallaron las siguientes políticas con sus respectivos objetivos relacionados con la seguridad de la información en la Municipalidad de la Victoria.

TABLA XIII
POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Política	Objetivos
Política de gestión de operaciones	- Asegurar el uso correcto de los recursos TIC. - Implementar y mantener niveles de tolerancia de riesgos. - Minimizar fallas en los sistemas - Protección del software. - Proteger la infraestructura de redes. - Monitorear actividades no autorizadas en procesamiento de información.
Política de control de accesos	- Asegurar, que el personal pueda acceder a la información conforme a sus atribuciones y funciones. - Controlar y restringir los accesos. - Registrar al personal y su nivel de autorización.

	- Prevenir accesos no autorizados.
Política de desarrollo y mantenimiento de aplicaciones informáticas	- Asegurar, que los sistemas desarrollados tengan los requisitos mínimos de seguridad. - Evitar la manipulación de la información dentro de los aplicativos. - Proteger la información con los principios de confidencialidad, integridad y autenticidad.
Política de gestión de incidentes	- Identificar los incidentes de acuerdo con el nivel de ocurrencia. - Controlar las debilidades presentes en la municipalidad. - Transmitir de forma oportuna cualquier incidente.
Política del uso de correos electrónicos	- Capacitar a los usuarios sobre el uso de los correos institucionales. - Identificar de forma oportuna correos electrónicos de dudosa procedencia. - Controlar los accesos de los usuarios a los correos institucionales.
Política para protección de equipos de comunicaciones	- Establecer configuraciones avanzadas en los equipos de comunicaciones.
Política de medios extractables	- Minimizar el uso indebido de medios extractables.
Política de seguridad de red	- Establecer controles de seguridad de acuerdo con los niveles de servicio.

	- Promover configuraciones seguras para el acceso a la red.
Política de auditorías	- Registrar mediante evidencias si la municipalidad cumple con los requisitos de seguridad planteados.
Política para la instalación de software	- Promover un entorno seguro para la instalación de sistemas informáticos. - Cumplir con la instalación y actualización de licencias de software.

B. Afinar el alcance del sistema de gobierno

Permite identificar si un factor de diseño es aplicable para la empresa, es importante mencionar que si un factor no es aplicable se puede ignorar. Para el caso donde los factores sean aplicables se van a considerar desde el factor 5 de diseño.

a. Considerar el panorama de amenazas

Cuando se consideran los valores que mejor se adecúan al entorno actual de la empresa, por eso es importante definir las entradas para los objetivos, áreas prioritarias, componente y gestión que servirán para el diseño y la conclusión.

TABLA XIV
TABLA DE PRIORIDAD DE OBJETIVOS DE GOBIERNO Y GESTIÓN EN EL ESCENARIO DE AMENAZAS

Valor	Prioridad	Componentes	Área prioritaria
Alto 90%	Considerando los objetivos de gobierno más importantes se consideraron: APO12,	Los componentes más importantes son:	Área prioritaria de seguridad de la información

	APO13, BAI09 y DSS05.	- Organizar un comité de seguridad de la información. - Poder contar con un director de seguridad de la información, Aspectos de cultura y comportamientos: - Generar conciencia sobre la seguridad de la información Información en flujos: - Políticas de seguridad. - Estrategias de seguridad.	
Normal 10%	Basado en la definición de alcance inicial.	N/A	Modelo Core de COBIT

b. Considerar los requerimientos regulatorios

Cuando se consideró este factor, primero se decidió valorar el factor de diseño en un rango de 3 niveles (Alto, normal y najo) considerando la prioridad de cada uno y descartando de la lista los que no se consideraron alineados a la municipalidad.

TABLA XV.
TABLA DE PRIORIDAD DE OBETIVOS DE GOBIERNO Y GESTIÓ EN LOS REQUISITOS DE CUMPLIMIENTO.

Valor	Prioridad	Componentes	Área prioritaria
80% Alto	Los más importante son: APO12, APO13, BAI09 y DSS05.	En función del cumplimiento: - Importancia en documentación, políticas y procedimientos	Modelo Core de COBIT
20% Bajo	Basado en la definición de alcance inicial.	N/A	Modelo Core de COBIT

c. Considerar el rol de las TI

Con respecto al rol de TI, se consideraron aspectos como soporte, cambio y fábrica, tomando en consideración los valores del alcance inicial.

TABLA XVI.
TABLA DE ROLES DE TI

Valor	Prioridad	Componentes	Área Prioritaria
Soporte 5 – 5	Entre los objetivos más importantes se tiene: BAI09	-	Seguridad de la información
Estratégico 5 -5	Entre los objetivos más importantes se	Ente ellos encontramos:	

	tiene: APO12, APO13	- A nivel organizativo: director de tecnología. - A nivel de habilidades y competencias: Personas que pueden combinar la exploración y explotación. - A nivel de procesos: Un portafolio y proceso innovador.	
Cambio 3 – 5	Entre los objetivos más importantes se tiene: DSS05	-	DevOPs
Fábrica 1 – 3	-	-	-

d. Considerar el modelo de aprovisionamiento

El modelo de aprovisionamiento o de proveedores ayudó a determinar factores como la externalización del servicio, servicio en la nube, el personal interno o una combinación de 2 de ellos o más considerado como un híbrido dependiendo de los objetivos.

TABLA XVII.
TABLA DE ABASTECIMIENTO – PROVEEDORES PARA TI

Objetivos de gobierno	Externalización (Outsourcing)	Nube	Personal Interno (Insoursing)
EDM01	1	1	1
EDM02	1	1	1
EDM03	1	1	3
EDM04	1	1	2
EDM05	1	1	1
APO01	1	1	3
APO02	1	1	2
APO03	1	2	1
APO04	1	1	2
APO05	1	1	1
APO06	1	1	2
APO07	1	1	3
APO08	1	1	3
APO09	1	1	2
APO10	1	1	1
APO11	1	1	2
APO12	1	1	3
APO13	1	2	4
APO14	1	1	2
BAI01	1	1	1
BAI02	1	1	2
BAI03	1	1	2
BAI04	1	1	1
BAI05	1	1	2

BAI06	1	1	1
BAI07	1	1	1
BAI08	1	1	2
BAI09	1	1	3
BAI10	1	1	1
BAI11	1	1	1
DSS01	1	1	1
DSS02	1	1	2
DSS03	1	1	1
DSS04	1	1	1
DSS05	1	2	3
DSS06	1	1	1
MEA01	1	1	1
MEA02	1	1	1
MEA03	1	1	1
MEA04	1	1	1

e. Considerar los métodos de implementación para las TI

Para considerar los métodos, se basó en el factor de diseño de método ágil, DevOps, método tradicional o híbrido que dependen de los roles vinculados a las directrices.

TABLA XVIII.
TABLA DE PRIORIDAD PARA CONSIDERAR LOS MÉTODOS DE IMPLEMENTACIÓN.

Objetivos de gobierno	Agile	DevOps	Tradicional
EDM01	2	1	1
EDM02	1	1	1

EDM03	1	1	1
EDM04	2	1	1
EDM05	1	1	1
APO01	1	1	1
APO02	2	1	1
APO03	1	1	1
APO04	1	1	1
APO05	2	1	1
APO06	1	1	1
APO07	1	1	1
APO08	1	1	1
APO09	2	2	1
APO10	1	2	1
APO11	1	1	1
APO12	3	1	1
APO13	3	1	1
APO14	1	1	1
BAI01	1	1	1
BAI02	1	1	1
BAI03	1	1	1
BAI04	1	1	1
BAI05	1	1	1
BAI06	2	1	1
BAI07	1	1	1
BAI08	1	1	1
BAI09	3	2	1
BAI10	1	1	1

BAI11	3	1	1
DSS01	1	1	1
DSS02	1	1	1
DSS03	1	1	1
DSS04	1	1	1
DSS05	3	1	1
DSS06	1	1	1
MEA01	1	2	1
MEA02	1	1	1
MEA03	1	1	1
MEA04	1	1	1

f. Considerar la estrategia de adopción de las TI

En este caso se consideró el impacto que tiene considerar la manera en que se adopta una nueva tecnología de TI basado en un rango de prioridad.

TABLA XIX.

TABLA DE LA ESTRATEGIA PARA ADAPTAR NUEVAS TECNOLOGÍAS

Objetivos de gobierno	First mover (Primero en reaccionar)	Follower (Segidor)	Slow adopter (Adoptador lento)
EDM01	1	1	1
EDM02	1	1	1
EDM03	4	2	1
EDM04	1	1	1
EDM05	1	1	1
APO01	4	3	1
APO02	1	1	1
APO03	1	1	1

APO04	1	1	1
APO05	1	1	1
APO06	1	1	1
APO07	1	1	1
APO08	1	1	1
APO09	1	1	1
APO10	1	1	1
APO11	1	1	1
APO12	4	3	1
APO13	5	2	1
APO14	1	1	1
BAI01	1	1	1
BAI02	1	1	1
BAI03	1	1	1
BAI04	1	1	1
BAI05	1	1	1
BAI06	1	1	1
BAI07	1	1	1
BAI08	1	1	1
BAI09	5	2	1
BAI10	1	1	1
BAI11	1	1	1
DSS01	1	1	1
DSS02	1	1	1
DSS03	1	1	1
DSS04	1	1	1
DSS05	5	2	1

DSS06	1	1	1
MEA01	1	1	1
MEA02	1	1	1
MEA03	1	1	1
MEA04	1	1	1

g. Considerar el tamaño de la empresa

Para este caso se consideró una empresa grande debido al número de empleados, aunque independiente del tamaño que tenga una empresa no genera un cambio en los objetivos de gobierno.

TABLA XX.
TABLA PARA DEFINIR EL TAMAÑO DE LA EMPRESA

Tamaño de la empresa		Resultado
Empresa grande	Más de 250 empleados trabajando en horario regular.	Sí
Pequeñas y medianas empresas	Entre 50 a 250 empleados trabajando en horario regular.	No

C. Concluir el diseño del sistema de gobierno

Como parte de la conclusión se consideran los valores entre -100% y 100% para la valoración de cada uno de los factores.

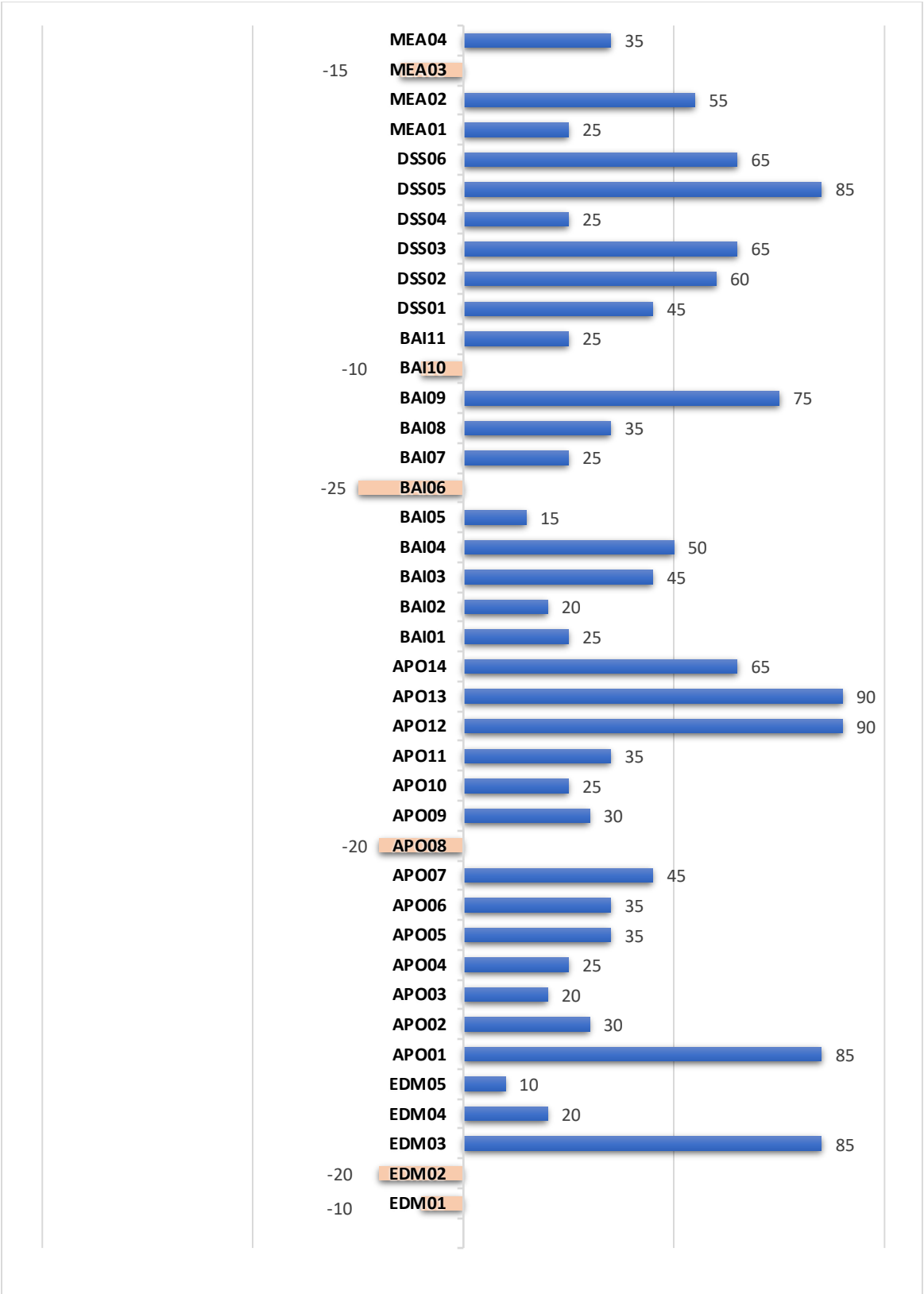


Fig. 11. Gráfico de valoración para la conclusión del diseño.

Como parte de la conclusión se dio una valoración a los objetivos de gobierno y gestión.

TABLA XXI.
NIVEL DE VALORACIÓN PARA LOS OBJETIVOS Y SU CAPACIDAD DE PROCESOS.

Objetivos de gobierno	**Nivel objetivo sugerido de capacidad de procesos**	**Nivel objetivo sugerido de capacidad de procesos**
EDM01	3	2
EDM02	2	1
EDM03	5	4
EDM04	3	2
EDM05	4	3
APO01	5	4
APO02	3	2
APO03	3	2
APO04	4	3
APO05	3	2
APO06	3	2
APO07	3	2
APO08	2	1
APO09	3	2
APO10	4	3
APO11	3	2
APO12	5	4
APO13	5	4
APO14	4	3
BAI01	3	2
BAI02	3	2
BAI03	3	2

BAI04	3	2
BAI05	4	3
BAI06	3	2
BAI07	3	2
BAI08	4	3
BAI09	5	4
BAI10	2	1
BAI11	3	2
DSS01	2	1
DSS02	4	3
DSS03	3	2
DSS04	4	3
DSS05	5	4
DSS06	4	3
MEA01	3	2
MEA02	2	1
MEA03	2	1
MEA04	4	3

2.2.4. Validar el diseño de gestión de la seguridad de la información con prueba empírica por expertos.

En cuanto a la validación del diseño se elaboró un resumen donde se detalla el objetivo de la investigación, así como una descripción corta de la propuesta, se planteó y se realizó la evaluación del diseño basado en el juicio de 3 expertos que tienen conocimientos y experiencia trabajando con COBIT2019. La validación fue valorada de acuerdo con los ítems como la claridad, adecuación funcional y claridad de las tablas que sirvieron para la elaboración del diseño. Anexo 13.

Luego de presentar el diseño basado en COBIT2019, se procedió con el envío del formato para que los expertos puedan validar el diseño, se pudo contar con la participación de 03 expertos los cuales en su mayoría son profesionales reconocidos y afiliados a ISACA y pudieron dar su apreciación con respecto a los factores de diseño presentados.

Además de eso se pudo presentar el perfil de cada profesional, donde cuentan con grado de magister y doctor en ingeniería de sistemas y tienen estudios y formación independiente en otras áreas de TI y COBIT 2019. Anexo 14.

TABLA XXII.
LISTA DE EXPERTOS EN COBIT 2019

Apellido y nombre	**Grado/Profesión**	**Especialización**	**Cargo actual**
Ernesto Karlo Celi Arévalo	✓ Ingeniero de Computación y Sistemas. ✓ Doctorado en Administración	✓ SCRUM Fundamentals. ✓ Especialización en Gestión de Servicios de Tecnologías de Información con ITIL. ✓ Especialización en Auditoría de Tecnologías de Información y	Director del Instituto de Investigación de la Universidad Nacional Pedro Ruiz Gallo

		Seguridad Informática.	
Carlos Alberto Chirinos Mundaca	✓ Ingeniería de Computación y Sistemas. ✓ Maestría en Informática y Sistemas. ✓ Doctorado en Tecnologías de la Información y Comunicaciones.	✓ Auditoria de Sistemas de Información. ✓ Sistemas Inteligentes. ✓ Programación Lógica.	Consultor TI - Peritajes en Sistemas – Poder Judicial
Alberto Enrique Samillan Ayala	✓ Ingeniero de Computación y Sistemas. ✓ Magister en Ciencias de la Educación. ✓ Doctorado, Ciencias Ambientales.	✓ Investigador RENACYT P0063355. ✓ MBA, ✓ COBIT ✓ Project Management Professional.	Catedrático Universitario de la Universidad Nacional Pedro Ruiz Gallo

Debido a la distancia y las ocupaciones de cada uno de los expertos se usaron medios de comunicación para explicar la propuesta del diseño basado en COBIT2019, estas reuniones se llevaron a cabo mediante llamadas telefónicas y correos electrónicos como se puede verificar en el Anexo 12, a continuación, se muestran las respuestas que los expertos ofrecieron en base a su experiencia y conocimientos.

TABLA XXIII.
PUNTAJE DE VALORACIÓN DE LOS EXPERTOS PARA EL DISEÑO BASADO EN COBIT 2019

Técnica	Experto 1	Experto 2	Experto 3	Total
Ficha para el experto	4.5	4.4	4.5	4.5

Nota. El nivel 5 representa un alto nivel de cumplimiento.

En este caso, primero se realizó el cálculo de los estadísticos Inter jueces para posteriormente revisar los criterios de validez, en esta oportunidad se trabajó con la validación V de Aiken debido a que es un método que permite tener un enfoque amplio orientado a una valoración positiva alineado al objeto que se valora, puede ser usado como criterio indicativo para precisar el sentido de pertenencia para revisar o quitar ítems. Este procedimiento permitió calcular el nivel de probabilidad adecuada al contenido de los grupos, es decir, a cada juez participante.

De la tabla siguiente, se puede evidenciar que los resultados cumplen con el criterio mínimo de valides que debe ser un valor de 0.8 en adelante hasta un total de 1 para que sea considerado como adecuado. En este caso se obtuvo un valor de V de Aiken mayor a 0.9 lo que indica que el modelo es adecuado según la opinión de los expertos.

TABLA XXIV.
VALIDEZ DE EXPERTOS POR V DE AIKEN

Ítem	Categoría	V de Aiken	Interpretación
	Claridad	1	Válido
		1	Válido
		1	Válido
	Objetividad	1	Válido
		1	Válido
		1	Válido
		1	Válido
		1	Válido
- Entender y contextualizar	Coherencia	1	Válido
		1	Válido
- Determinar el alcance		1	Válido
		1	Válido
- Afinar el alcance	Pertenencia	1	Válido
- Concluir el sistema		1	Válido
		1	Válido
		1	Válido
	Suficiencia	1	Válido
		1	Válido
		1	Válido
		1	Válido
	Relevancia	1	Válido
		1	Válido
		1	Válido

III. RESULTADOS Y DISCUSIÓN

3.1 Resultados

Se realizó el cálculo y medición de los indicadores, producto de eso se muestran los resultados a continuación:

a. Marco de trabajo COBIT 2019:

- **Porcentaje procesos:** Se realizó con la finalidad de tener una mejor perspectiva del porcentaje total de procesos que se va a considerar en este estudio en comparación al total de procesos que se maneja en COBIT 2019. Por ese motivo se realizó una valoración en un rango de 1 – 5 para determinar qué procesos son los que tienen más impacto en este estudio, para lograr esto se propuso la siguiente fórmula:

$$PC = \frac{N° \, Objetivos}{Total \, de \, objetivos} * 100\%$$

Para la valoración de los objetivos se consideraron la lista de todos los objetivos, se calculó mediante una valoración entre 1 a 5 de acuerdo con el Problema general aporte en cuanto a claridad, relación e importancia de los objetivos COBIT aportan a mejorar la seguridad de la información en la Municipalidad.

TABLA XXV
RESULTADO DE PORCENTAJE DE PROCESOS - PRETEST

N°	Identificador	Claridad	Relación	Importancia	Total
1	EDM01	3	3	2	2.7
2	EDM02	3	3	2	2.7
3	EDM03	5	4	4	4.3
4	EDM04	3	3	3	3.0
5	EDM05	3	3	3	3.0
6	APO01	3	4	3	3.3
7	APO02	3	3	3	3.0
8	APO03	3	3	3	3.0
9	APO04	3	3	3	3.0

10	APO05	4	3	3	3.3
11	APO06	3	3	3	3.0
12	APO07	4	3	3	3.3
13	APO08	4	2	2	2.7
14	APO09	5	3	2	3.3
15	APO10	5	3	2	3.3
16	APO11	4	3	3	3.3
17	APO12	5	5	5	5.0
18	APO13	5	5	5	5.0
19	APO14	5	4	4	4.3
20	BAI01	4	4	2	3.3
21	BAI02	3	3	3	3.0
22	BAI03	4	3	3	3.3
23	BAI04	4	3	3	3.3
24	BAI05	4	3	2	3.0
25	BAI06	4	3	2	3.0
26	BAI07	3	3	2	2.7
27	BAI08	3	4	2	3.0
28	BAI09	5	5	5	5.0
29	BAI10	3	3	2	2.7
30	BAI11	4	4	2	3.3
31	DSS01	4	3	3	3.3
32	DSS02	5	4	3	4.0
33	DSS03	4	4	3	3.7
34	DSS04	4	3	2	3.0
35	DSS05	5	5	5	5.0
36	DSS06	5	4	2	3.7

37	MEA01	4	3	2	3.0
38	MEA02	4	3	2	3.0
39	MEA03	3	3	2	2.7
40	MEA04	3	3	2	2.7

Donde se delimita por la siguiente tabla de valoración para el porcentaje de procesos COBIT2019

Valoración rango 1-5	
1	Muy bajo
2	bajo
3	medio
4	alto
5	Muy alto

Siguiendo los principios de seguridad y en coordinación con el área de TI de la Municipalidad se realizó la valoración de los objetivos que generan mayor impacto en la seguridad de la información tomando como referencia el Anexo 6.

Se consideraron los objetivos que tienen una puntuación entre alto y muy alto entre ellos los objetivos: EDM03 - Asegurar la optimización del riesgo, APO12 - Gestionar el riesgo, APO13 - Gestionar la seguridad, APO14 - Gestionar los datos, BAI09 - Gestionar los activos, DSS0 - Gestionar las solicitudes e incidentes de servicio y DSS05 - Gestionar los servicios de seguridad, siendo un total de 7 objetivos con más alta puntuación de un total de 35 objetivos como se resume en el siguiente gráfico:

$$.PC = \frac{7}{35} * 100\% = 20\%$$

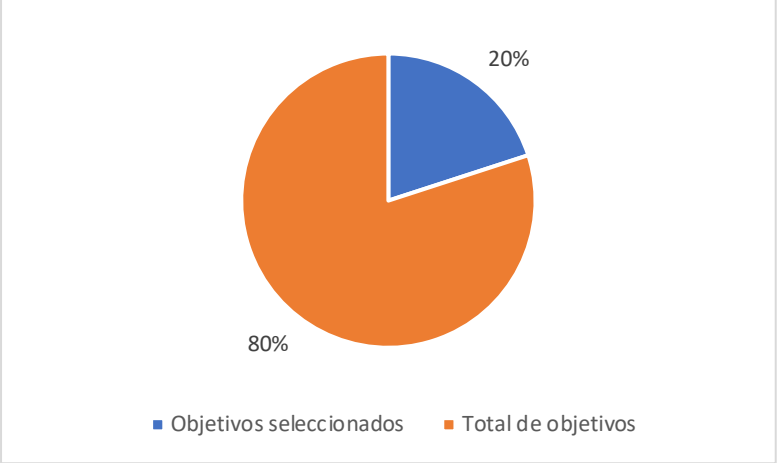


Fig. 12.Porcentaje de procesos COBIT 2019 – pretest

Resultados postest

Siguiendo los principios de seguridad y en coordinación con el área de TI de la Municipalidad se realizó un análisis más exhaustivo para volver a reconsiderar la valoración de los objetivos que generan mayor impacto y sean más urgentes en respaldo para la seguridad como se muestra en la siguiente tabla:.

TABLA XXVI
RESULTADO DE PORCENTAJE DE PROCESOS COBIT 2019 - POSTEST

N°	ID	Claridad	Relación	Importancia	Total
1	EDM01	3	3	2	2.7
2	EDM02	3	3	2	2.7
3	EDM03	5	4	4	4.3
4	EDM04	3	3	3	3.0
5	EDM05	3	3	3	3.0
6	APO01	3	4	3	3.3
7	APO02	3	3	3	3.0
8	APO03	3	3	3	3.0
9	APO04	3	3	3	3.0
10	APO05	4	3	3	3.3
11	APO06	3	3	3	3.0

12	APO07	4	3	3	3.3
13	APO08	4	2	2	2.7
14	APO09	5	3	2	3.3
15	APO10	5	3	2	3.3
16	APO11	4	3	3	3.3
17	APO12	5	5	5	5.0
18	APO13	5	5	5	5.0
19	APO14	5	4	4	4.3
20	BAI01	4	4	2	3.3
21	BAI02	3	3	3	3.0
22	BAI03	4	3	3	3.3
23	BAI04	4	3	3	3.3
24	BAI05	4	3	2	3.0
25	BAI06	4	3	2	3.0
26	BAI07	3	3	2	2.7
27	BAI08	3	4	2	3.0
28	BAI09	5	5	5	5.0
29	BAI10	3	3	2	2.7
30	BAI11	4	4	2	3.3
31	DSS01	4	3	3	3.3
32	DSS02	5	4	3	4.0
33	DSS03	4	4	3	3.7
34	DSS04	4	3	2	3.0
35	DSS05	5	5	5	5.0
36	DSS06	5	4	2	3.7
37	MEA01	4	3	2	3.0
38	MEA02	4	3	2	3.0

39	MEA03	3	3	2	2.7
40	MEA04	3	3	2	2.7

Se consideraron los objetivos que tienen una puntuación de muy alto entre ellos los objetivos: APO12 - Gestionar el riesgo, APO13 - Gestionar la seguridad, BAI09 - Gestionar los activos y DSS05 - Gestionar los servicios de seguridad, siendo un total de 4 objetivos con más alta puntuación de un total de 35 objetivos como se muestra en el siguiente gráfico:

$$PC = \frac{5}{35} * 100\% = 11.4\%$$

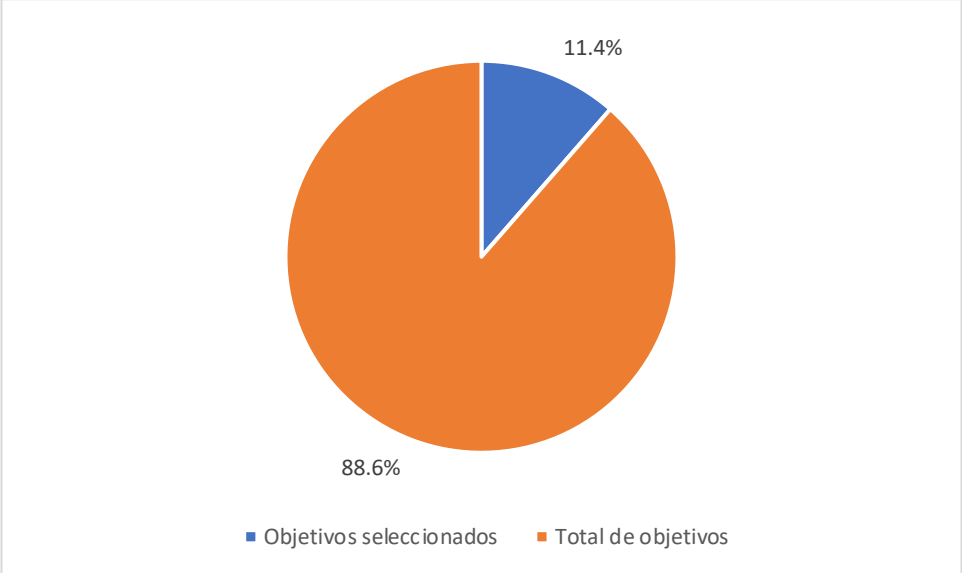


Fig. 13. Porcentaje de procesos COBIT 2019 - postest

- **Porcentaje de dominios:** Se realizó con la finalidad de tener una mejor perspectiva del porcentaje de dominios que se va a considerar en este estudio en comparación al total de procesos APO (Alinear – Planificar – Organizar) que se maneja en COBIT 2019. Por ese motivo se realizó una valoración en un rango de 1 – 5 para determinar qué dominios son los que tienen más impacto en este estudio, para lograr esto se propuso la siguiente fórmula:

$$DOM = \frac{APO\ COBIT}{Total\ APO} * 100\%$$

Para la valoración de los objetivos se consideraron la lista de todos los dominios, se calculó mediante una valoración entre 1 a 5 de acuerdo con el aporte en cuanto a claridad, relación e importancia de los objetivos COBIT aportan a la seguridad en la Municipalidad.

Donde se delimita por la siguiente tabla de valoración:

Cuadro de valoración para el porcentaje de dominios pretest y postest

Valoración rango 1-5	
1	Muy bajo
2	bajo
3	medio
4	alto
5	Muy alto

Siguiendo los principios de seguridad y en coordinación con el área de TI de la Municipalidad se realizó un análisis más exhaustivo para considerar la valoración de los dominios APO que generan mayor impacto como parte principal para alinear, planificar y organizar tomando como referencia el Anexo 7.

TABLA XXVII
VALORACIÓN DE DOMINIOS COBIT 2019 – PRETEST Y POSTEST

Id	**Claridad**	**Relación**	**Importancia**	**Total**
APO01	3	4	3	3.3
APO02	3	3	3	3.0
APO03	3	3	3	3.0
APO04	3	3	3	3.0
APO05	4	3	3	3.3
APO06	3	3	3	3.0

APO07	4	3	3	3.3
APO08	4	2	2	2.7
APO09	5	3	2	3.3
APO10	5	3	2	3.3
APO11	4	3	3	3.3
APO12	5	5	5	5.0
APO13	5	5	5	5.0
APO14	5	4	4	4.3

Se consideraron los dominios que tienen una puntuación de muy alto entre ellos los dominios: APO12 - Gestionar el riesgo y APO13 – Gestionar que son los 2 dominios con más alta puntuación de un total de 14 que se listan en COBIT 2019.

$$PC = \frac{2}{14} * 100\% = 14\%$$

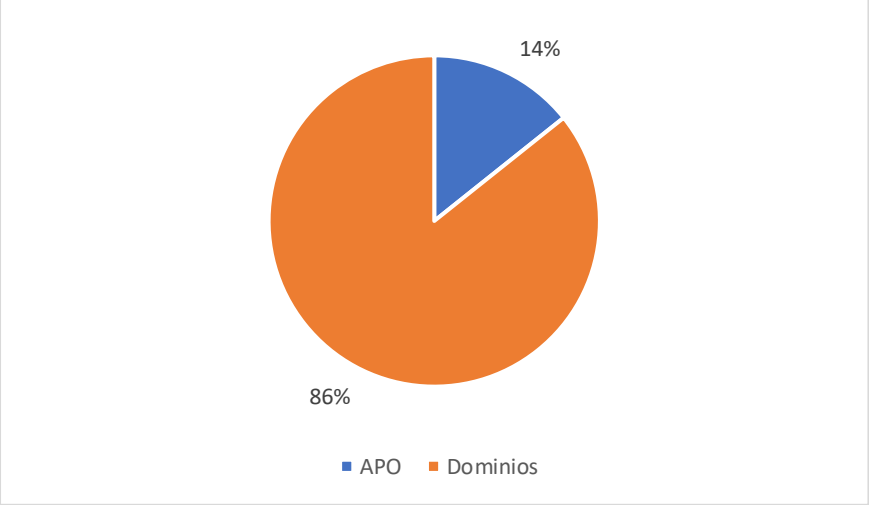


Fig. 14. Porcentaje de dominios de COBIT 2019 – Pretest y Postest

Para pre y postest se consideraron los 2 dominios como los más importantes que permitieron lograr la parte de identificación, evaluación, la mitigación de los riesgos de acuerdo con el nivel de tolerancia, además para poder definir, monitorear y operar el sistema de seguridad de la información para poder mantener el impacto y las ocurrencias de incidentes que puedan vulnerar a la seguridad de la información.

- **Capacidad de cumplimiento:** Se realizó con la finalidad de alinear los objetivos por nivel de madurez dentro de la municipalidad, para esto se realizó una revisión entre los objetivos estratégicos empresariales institucionales cada uno de ellos con las acciones estratégicas institucionales que permitan cumplir a mediano plazo con los objetivos, para lograr esto se propuso la siguiente fórmula:

$$KC = \frac{N° \ Objetivos}{Nivel \ Madurez} * 100\%$$

TABLA XXVIII
VALORACION CAPACIDAD DE CUMPLIMIENTO COBIT 2019

Objetivos COBIT 2019	Nivel	Cantidad de objetivos	Porcentaje
DSS05	2	4	57%
BAI09	1	1	14%
APO12	1	1	14%
APO 13	1	1	14%
Total			100%

Donde el nivel de madurez se encuentra en un rango entre 0-5 y se detalla a continuación:

Nivel de madurez	
5	Optimizado
4	Establecido
3	Definido
2	Repetible

1	Inicializado
0	No

Y donde el total de objetivos institucionales son 7 en total detallados en el Anexo 8. Para la valoración se realizó un análisis de los objetivos y el nivel de madurez en el que se encuentra cada uno, se multiplicó por la cantidad de objetivos COBIT 2019 asociados al nivel, se dividió por los 7 objetivos institucionales de la municipalidad y se multiplicó por el 100% para obtener el porcentaje por objetivo COBIT 2019.

Tal como se muestra en la tabla anterior, los objetivos empresariales relacionados con el objetivo de COBIT 2029 DSS05 son 4.

$$KC = \frac{4}{7} * 100\% = 57\%$$

Resultados postest

Se muestra en la tabla anterior, los objetivos empresariales relacionados con el objetivo de COBIT 2029 DSS05 son 3.

$$KC = \frac{3}{7} * 100\% = 43\%$$

Esto debido a que 3 objetivos alcanzaron un nivel 3 de madurez alineado al objetivo COBIT2019 y 1 objetivo alcanzó un nivel 2 de madurez en relación con el objetivo COBIT 2019 como se muestra a continuación:

TABLA XXIX
VALORACION CAPACIDAD DE CUMPLIMIENTO COBIT 2019

Objetivos COBIT 2019	Nivel	Cantidad de objetivos	Porcentaje
DSS05	3	3	43%
DSS05	2	1	14%
BAI09	3	1	14%
APO12	3	1	14%

APO 13	3	1	14%
Total			100%

b. Marco de trabajo COBIT 2019:

- **Porcentaje de incidentes:** Se realizó con la finalidad de tener una mejor perspectiva del porcentaje de incidentes corporativos que afectan de forma directa a la seguridad de la información en la municipalidad, para lograr esto se propuso la siguiente fórmula:

$$KC = \frac{Inc.corporativos}{Total\ Incidentes} * 100\%$$

Para el conteo de los incidentes se realizaron fichas resumen en las cuales se anotaron la cantidad de incidencias de la municipalidad, esto se realizó con la aprobación del jefe del área de TI que tenía un registro en Excel de la cantidad aproximada de los incidentes que se atendían de forma diaria, semanal, mensual y anual como se detalla en el Anexo 9.

Los resultados se resumen en la siguiente tabla:

TABLA XXX
RESULTADO PORCENTAJE DE INCIDENTES COBIT 2019 - PRESTEST

N°	Incidencias	Periodo	Incidencias diarias	Incidencias al mes	Tipo	Total mensual
1	Actualización en el portal de consultas en línea	Diario	3	15	1	15
2	Actualización mensual para el estado peruano	1 mes	4	6		
3	Actualización diaria del portal institucional	Diario	3	6		
4	Mantenimiento de BD (4)	1 semana	2	4	1	4

5	Back-up de la diferentes BD (Rentas-caja, Registro civil, Trámite documentario y SIAF)	Diario	1	13	1	13
6	Mantenimiento de servidores (3)	3 meses	1	1	1	1
7	Mantenimiento de impresoras (55)	6 meses	1	10	1	10
8	Mantenimiento de equipos cómputo (135)	6 meses	2	13	1	13
9	Sistema de mesa de partes virtual	Diario	1	18	1	18
10	Consultas en línea de mesa de partes virtual por usuarios	Diario	3	24	1	24
11	Migración del portal GOB.PE a la PCM	2 mese	4	8		
12	Mantenimiento de computadoras de escritorio (110)	6 meses	4	15	1	15
13	Mantenimiento de laptops (35)	6 meses	2	17	1	17
14	Reemplazo de equipos (20)	1 año	2	4	1	4
				154	11	134

.

Realizando el conteo respectivo se obtuvieron un total de 154 incidentes, siendo 134 corporativos y tenían más impacto en la seguridad de la información de la municipalidad. Se aplicó el siguiente cálculo:

$$KC = \frac{134}{154} * 100\%$$

KC= 87%

Se puede deducir que del 100% de incidentes detectados en la Municipalidad de la

Victoria, el 87% de ellos son incidentes corporativos, por tanto, afectan en gran medida a la seguridad de la información de la Municipalidad y el 13% son otros tipos de incidentes como se muestra en el siguiente gráfico:.

Fig. 15. Porcentaje de incidentes de COBIT 2019 – Pretest

Los resultados se resumen en la siguiente tabla:

TABLA XXXI
PORCENTAJE DE INCIDENTES COBIT 2019 - POSTEST

N°	Incidencias	Periodo	Incidencias diarias	Incidencias al mes	Tipo	Total mensual
1	Actualización en el portal de consultas en líneas	Diario	3	8	1	8
2	Actualización mensual para el estado peruano	1 mes	4	6		
3	Actualización diaria del portal institucional	Diario	3	6		
4	Mantenimiento de BD (4)	1 semana	2	2	1	2
5	Back-up de la diferentes BD	Diario	1	4	1	4

	(Rentas-caja, Registro civil, Trámite documentario y SIAF)					
6	Mantenimiento de servidores (3)	3 meses	1	1	1	1
7	Mantenimiento de impresoras (55)	6 meses	1	4	1	4
8	Mantenimiento de equipos cómputo (135)	6 meses	2	5	1	5
9	Sistema de mesa de partes virtual	Diario	1	8	1	8
10	Consultas en línea de mesa de partes virtual por usuarios	Diario	3	8	1	8
11	Migración del portal GOB.PE a la PCM	2 mese	4	4		
12	Mantenimiento de computadoras de escritorio (110)	6 meses	4	8	1	8
13	Mantenimiento de laptops (35)	6 meses	2	8	1	8
14	Reemplazo de equipos (20)	1 año	2	2	1	2
				74	11	58

Realizando el conteo respectivo se obtuvieron un total de 74 incidentes, siendo 58 incidentes corporativos y tenían más impacto en la seguridad de la información de la municipalidad. Se aplicó el siguiente cálculo:

$$KC = \frac{58}{74} * 100\%$$

KC= 78%

Se puede deducir que del 100% de incidentes detectados en la Municipalidad de la Victoria, el 78% son incidentes corporativos y el 22% son otro tipo de incidentes como se muestra a continuación:

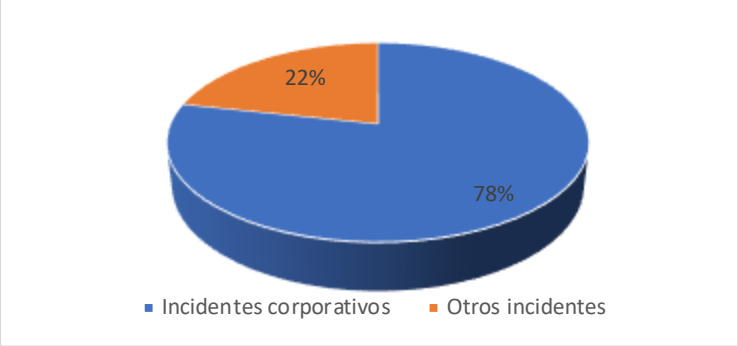


Fig. 16.Porcentaje de incidentes de COBIT 2019 - Postest

Realizando el análisis se puede evidenciar que con existe una reducción significativa del 87% al 78% con respecto al porcentaje de incidentes corporativos que inicialmente se detectaron pasando de un total de 134 a 58 incidentes corporativos.

- **Porcentaje de activos:** Se realizó con la finalidad de tener una mejor perspectiva de la criticidad de realizar un análisis de riesgo basado en la criticidad de todos los activos de la municipalidad, para lograr esto se propuso la siguiente fórmula:

$$AI = \frac{(N°\ Activos) * 100\%}{total}$$

Para identificar el total de activos de la municipalidad se realizaron fichas resumen en las cuales se anotaron el nombre del activo y la cantidad detallado en el Anexo 10, esto se realizó con la información de inventario de equipos que maneja la Municipalidad de la Victoria.

Se puede observar que hay un total de 206 activos con los que cuenta la municipalidad de la Victoria de los cuales 110 son computadoras en la siguiente tabla:

TABLA XXXII
LISTA RESUMEN DE LOS ACTIVOS DE LA MUNICIPALIDAD DE LA VICTORIA

Resumen lista de activos	
Servidores	3
Impresoras	55

Computadoras	110
Laptops	35
Data center	1
UPS	2
TOTAL	206

Se realizó el cálculo respectivo para poder identificar el porcentaje de activos y la descripción de cuántos estaban más críticos de acuerdo con los valores del cuadro que se muestra a continuación:

TABLA XXXIII
PORCENTAJE DE ACTIVOS POR CRITICIDAD DE LA MUNICIPALIDAD DE LA VICTORIA - PRETEST

Criticidad	**Activos**	**Porcentaje**
Muy alto	99	48%
Alto	71	34%
Normal	32	16%
Bajo	4	2%
	206	100%

Realizando el conteo respectivo se obtuvieron un total de 206 activos, de los cuales el 48% tenían una criticidad alta, el 34% tenían criticidad alta, el 16% tenía criticidad normal y sólo el 2% tenía una criticidad baja. Se aplicó siguiente cálculo:

$$pAI = 99 * 100/206 = 48\%$$

TABLA XXXIV
CUADRO DE VALORACIÓN POR RANGO DE CRITICIDAD DE LOS ACTIVOS

	Rango de criticidad			
Valor	4	3	2	1
Rango	Muy alto	Alto	Normal	Bajo

Se puede deducir que del 100% de los activos con los que cuenta la Municipalidad de la Victoria, el 48% tienen un valor de criticidad muy alto, el 34% tiene un valor de criticidad alto, el 16% tiene un valor de criticidad normal % y sólo el 2% tiene una criticidad baja, por tanto, se considera un porcentaje considerable de ser afectado por algún tipo de riesgo que pueda afectar a la seguridad de la información como se muestra a continuación:

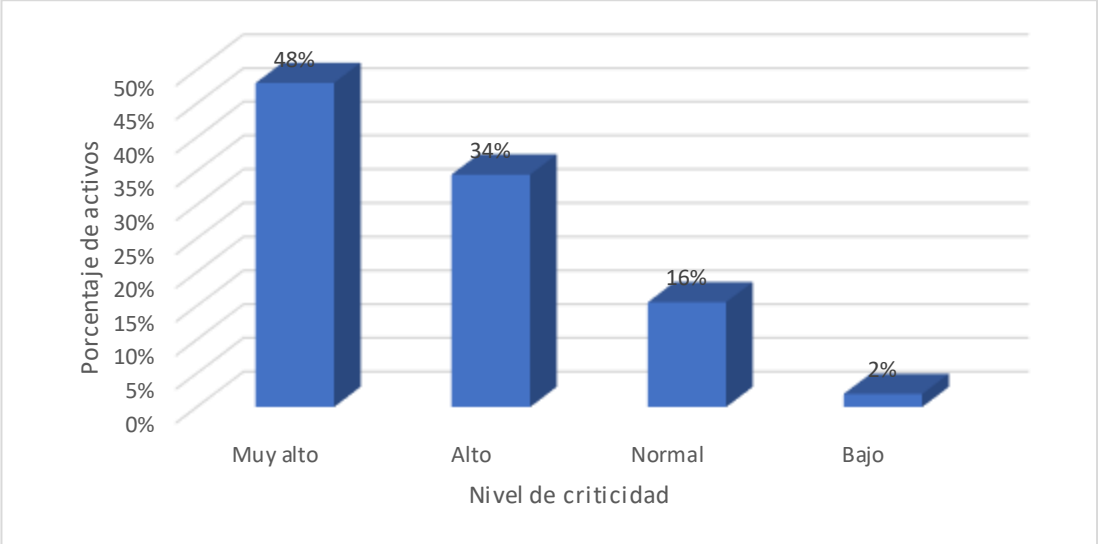


Fig. 17.Porcentaje de activos - Pretest

Los resultados se resumen en la siguiente tabla:

TABLA XXXV
PORCENTAJE DE ACTIVOS POR CRITICIDAD DE LA MUNICIPALIDAD DE LA VICTORIA - POSTEST

Criticidad	Activos	Porcentaje
Muy alto	0	0%
Alto	55	27%
Normal	131	64%
Bajo	20	10%
	206	100%

Realizando el conteo respectivo se obtuvieron un total de 206 activos. Se aplicó siguiente cálculo:

$$pAI = 55 * 100/206 = 27\%$$

Se realizó el cálculo para los activos donde se consideró la criticidad que le correspondía a cada activo entre el total de activos para poder segregarlos en grupo de acuerdo con el rango de prioridad. Del 100% de los activos con los que cuenta la Municipalidad de la Victoria, el 0% tienen un valor de criticidad muy alto, el 27% tiene un valor de criticidad alto, el 64% tiene un valor de criticidad normal y sólo el 10% tiene una criticidad baja, con esto se evidencia una reducción en cuanto a la criticidad de que el activo pueda ser afectado por algún tipo de riesgo.

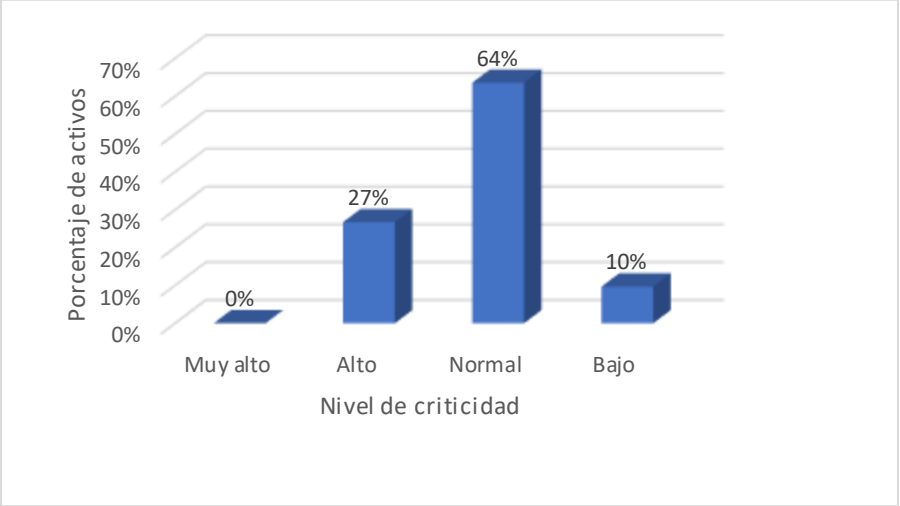


Fig. 18.Porcentaje de activos - Postest

- **Nivel de satisfacción:** Se realizó con la finalidad de tener una mejor perspectiva de los usuarios con respecto a la seguridad de la seguridad de la información en la Municipalidad de la Victoria, para lograr esto se propuso la siguiente fórmula:

$$NS = \frac{\%Usuarios\ con\ alta\ satisfacción}{\%\ Total\ de\ Usuarios}$$

Para identificar el total de personas que se relacionan directamente con activos que guardan relación con la seguridad, de la información se realizó la recolección de información en el directorio institucional, con esa información se

consideró la aplicación de la fórmula finita que sirvió para determinar cuánto era la cantidad de la muestra de usuarios a los que se iba a encuestar.

La fórmula finita es la siguiente:

$$n = \frac{N * Z_{\alpha}^{2} * p * q}{e^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

Donde se tiene en consideración lo siguiente:

n= Tamaño de la muestra

N=Tamaño del universo o población

Z=Parámetro estadísticos dependiente del nivel de confianza

e=Error máximo de estimación aceptado.

p=Probabilidad de que suceda el evento con éxito.

q=(1-p) Es decir, la probabilidad de que el evento no suceda con éxito.

$$\mathrm{n} = \frac{112 * 1.96^{2} * 0.5 * 05}{0.05^{2} * (112-1) + 1.96^{2} * 0.5 * 0.5}$$

$$\mathrm{n} = \frac{107.5648}{1.2379} = 86.89 = 87$$

La encuesta de satisfacción se muestra en el Anexo 5.

Los resultados más relevantes se muestran a continuación:

En la siguiente figura el 97% del personal encuestado está insatisfecho con la atención del área de TI ante fallas de equipos o sistemas, el 2% está totalmente insatisfecho y sólo el 1% está algo satisfecho con la atención.

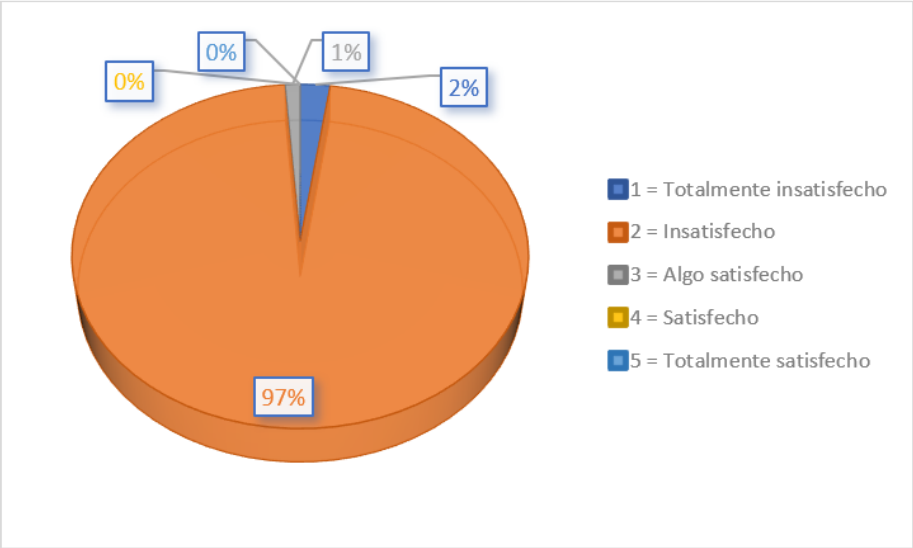


Fig. 19. P1 ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad? – Pretest

Como se puede ver en la siguiente figura, el 95% del personal encuestado está insatisfecho con los métodos actuales para protección ante robo de información en su espacio de trabajo, el 3% está totalmente insatisfecho y sólo el 1% está algo satisfecho.

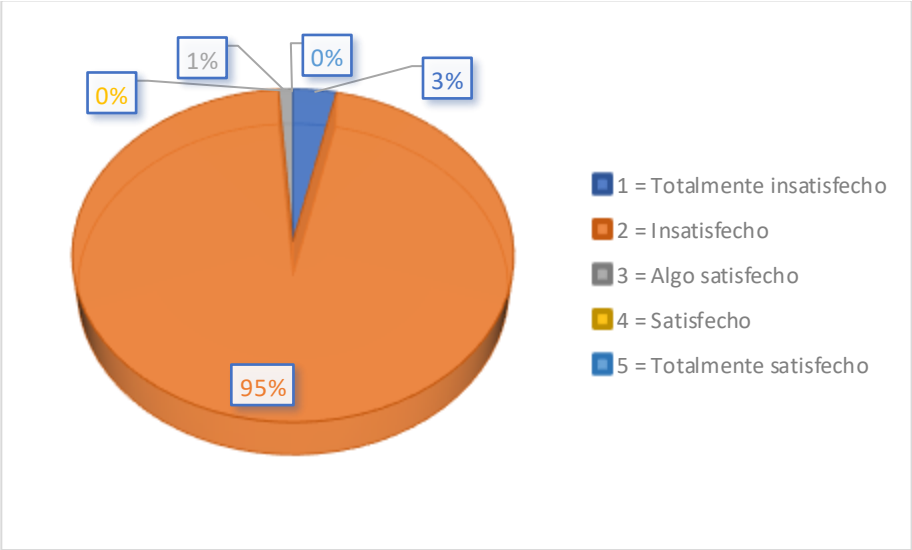


Fig. 20. P3 ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo? – Pretest

Como se puede ver en la siguiente figura el 93% del personal encuestado está insatisfecho con el desempeño del área de informática con respecto al

resguardo de la información y el 7% está totalmente insatisfecho.

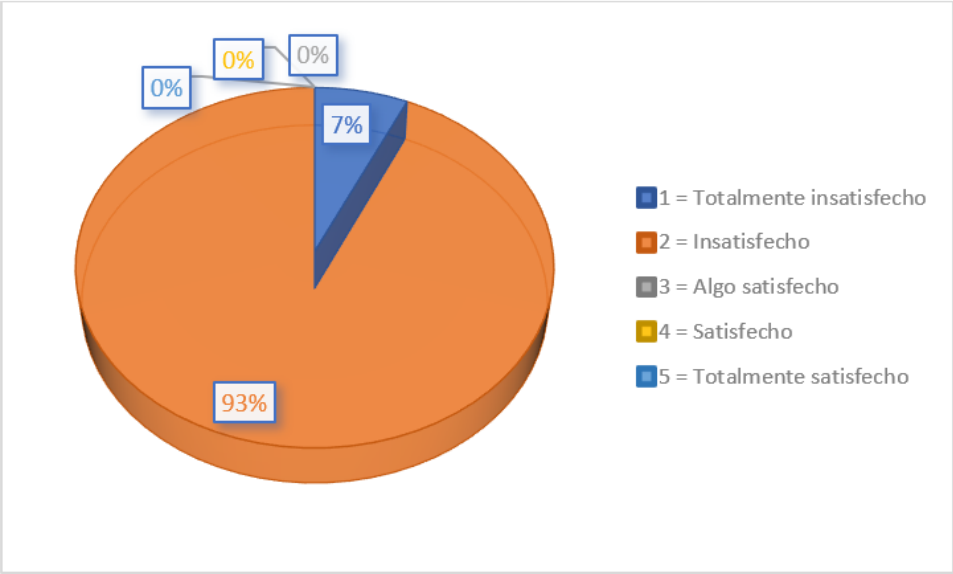


Fig. 21. P9 ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información? – Pretest

Como se puede ver en la siguiente figura el 95% del personal encuestado está insatisfecho con la poca proporción de guías o políticas que les permita actuar ante robos, ataques o fallos y el 5% está totalmente insatisfecho.

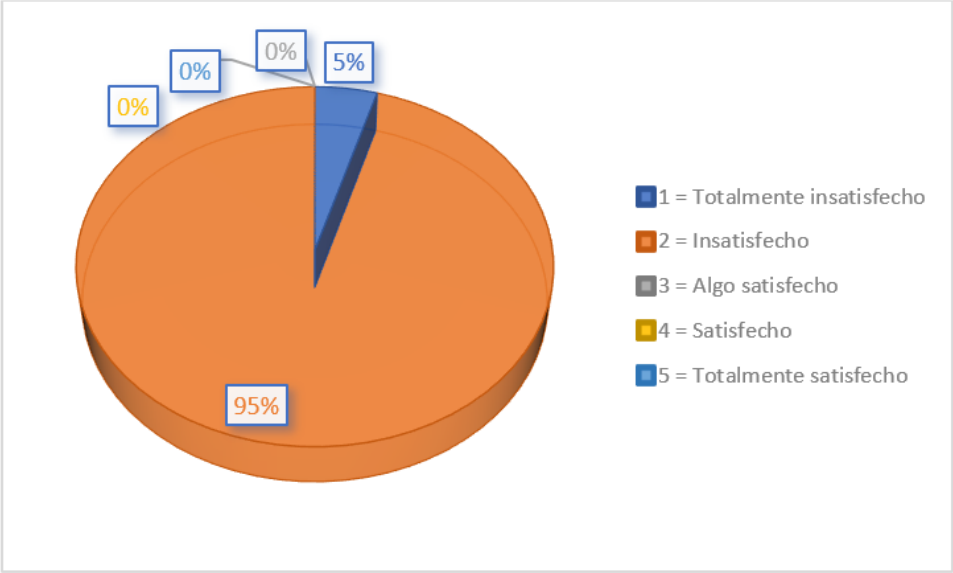


Fig. 22. P12 ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información? – Pretest

TABLA XXXVI
RESULTADO DE LA ENCUESTA DE SATISFACCIÓN - PRETEST

	Totalmente insatisfecho	**Insatisfecho**	**Algo satisfecho**	**Satisfecho**	**Totalmente satisfecho**
P1	2%	97%	1%	0%	0%
P2	2%	98%	0%	0%	0%
P3	3%	95%	1%	0%	0%
P4	2%	98%	0%	0%	0%
P5	2%	98%	0%	0%	0%
P6	2%	97%	1%	0%	0%
P7	0%	98%	2%	0%	0%
P8	3%	95%	1%	0%	0%
P9	7%	93%	0%	0%	0%
P10	6%	93%	1%	0%	0%
P11	5%	93%	2%	0%	0%
P12	5%	95%	0%	0%	0%
P13	5%	95%	0%	0%	0%
P14	1%	98%	1%	0%	0%
P15	0%	100%	0%	0%	0%
P16	0%	100%	0%	0%	0%

Nota. P1 …P16 son las preguntas que forman parte del cuestionario.

$$S_c = \frac{2+2+3+3+3+3+3+7+6+5+5+5+1}{16} \text{x}100$$

$$S_c = 3\%$$

El cálculo se realizó para cada indicador de satisfacción, de la tabla anterior se puede deducir que el 3% está totalmente insatisfecho, el 96% está insatisfecho y el 1% está algo satisfecho con la gestión de la seguridad de la información en la Municipalidad de la Victoria.

Resultados de Postest

Como se puede ver en la siguiente figura, el 59% del personal encuestado está satisfecho con la atención del área de TI ante fallas de equipos o sistemas y el 41% está totalmente satisfecho.

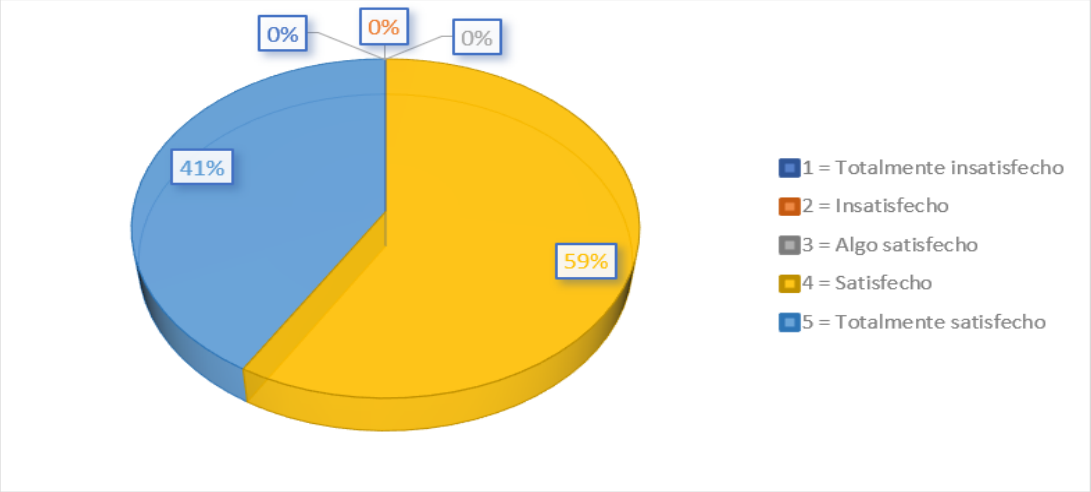


Fig. 23. P1 ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad? – Postest

Como se puede ver en la siguiente figura, el 78% del personal encuestado está satisfecho con los métodos actuales para protección ante robo de información en su espacio de trabajo, el 17% está totalmente satisfecho y sólo el 5% está algo satisfecho.

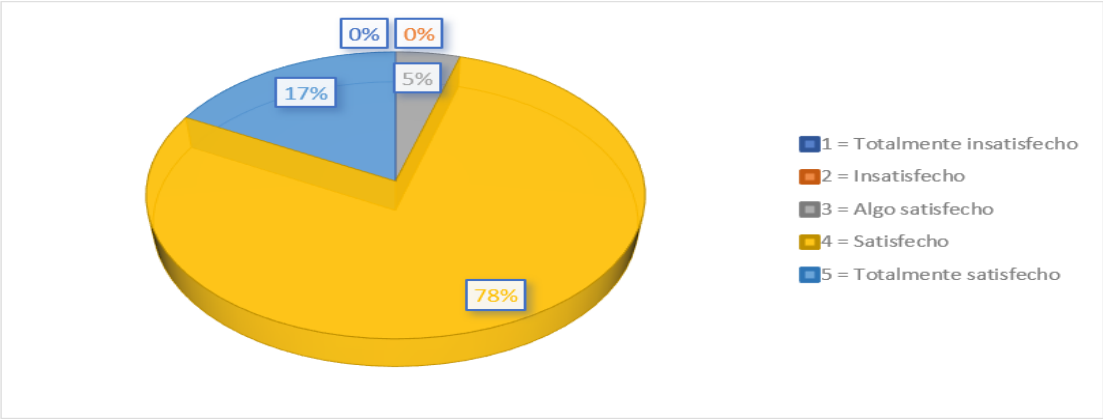


Fig. 24.P3 ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo? – Postest

Como se puede ver en la siguiente figura, el 66% del personal encuestado está satisfecho con el desempeño del área de informática con respecto al resguardo

de la información y el 34% está totalmente satisfecho.

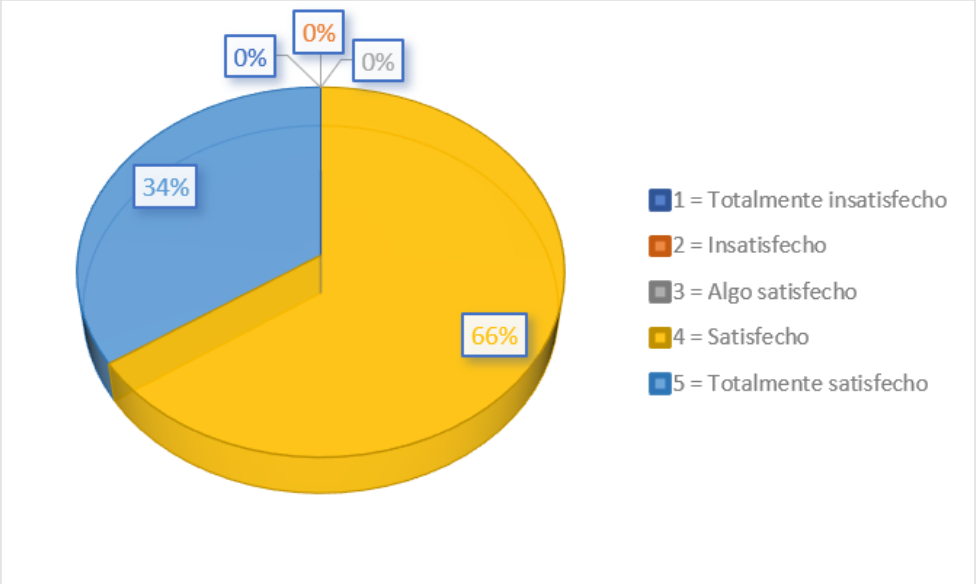


Fig. 25.P9 ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información? – Postest

Como se puede ver en la siguiente figura, el 83% del personal encuestado está satisfecho con la proporción de guías o políticas que les permita actuar ante robos, ataques o fallos y el 17% está totalmente satisfecho.

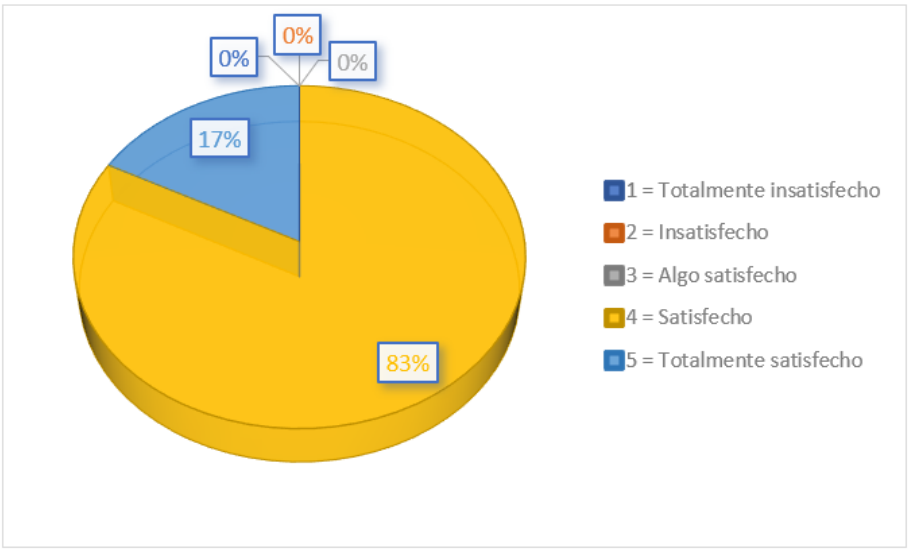


Fig. 26. P12 ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información? – Postest

Se puede deducir que el 23% está totalmente satisfecho, el 75% está satisfecho y el 2% está algo satisfecho en cómo se maneja la gestión de la seguridad en la Municipalidad de la Victoria como se muestra en la siguiente tabla:.

TABLA XXXVII.
RESULTADO DE LA ENCUESTA DE SATISFACCIÓN - POSTEST

	Totalmente insatisfecho	**Insatisfecho**	**Algo satisfecho**	**Satisfecho**	**Totalmente satisfecho**
P1	0%	0%	0%	59%	41%
P2	0%	0%	3%	77%	20%
P3	0%	0%	5%	78%	17%
P4	0%	0%	1%	82%	17%
P5	0%	0%	2%	79%	18%
P6	0%	0%	0%	78%	22%
P7	0%	0%	3%	79%	17%
P8	0%	0%	2%	82%	16%
P9	0%	0%	0%	66%	34%
P10	0%	0%	5%	68%	28%
P11	0%	0%	0%	82%	18%
P12	0%	0%	0%	83%	17%
P13	0%	0%	0%	69%	31%
P14	0%	0%	2%	69%	29%
P15	0%	0%	1%	74%	25%
P16	0%	0%	0%	83%	17%

Nota. P1 …P16 son las preguntas que forman parte del cuestionario.

$$S_c = \frac{41 + 20 + 17 + 17 + 18 + 22 + 17 + 16 + 34 + 28 + 18 + 17 + 31 + 29 + 25 + 17}{16} \text{x} 100$$

$$S_c = 23\%$$

Con esto se evidencia una mejora en cuanto a la apreciación que tienen los usuarios luego de la diseñar procesos de gobierno de TI basado en COBIT 2019 para la seguridad de la información en la municipalidad de la Victoria pasando de un 96% de insatisfacción a un 75% de satisfacción de los usuarios.

3.2 Discusión

Syaputra, M.; Kesuma, M.; Saputra, R.; Fitra, J. diseñaron un modelo de gobernanza de tecnología basado en el subdominio APO01 que les permitió analizar la relación del estado de los datos para poder medir la capacidad entre el nivel de objetivo actual y el esperado. Realizaron una evaluación mediante cuestionarios que tienen un valor de puntuación de 1 (Totalmente de acuerdo), 4 (de acuerdo), 3(duda), 2(en desacuerdo) y 1(en total desacuerdo). Para esto consideraron definir los problemas y oportunidades en relación con el proceso APO01 (Gestionar el marco de gestión de TI), posteriormente identificaron los objetivos de control para poder calcular la capacidad incluyeron un rango del valor de madurez de los objetivos en una escala de 7 niveles: Entre 4.51-5.00 (Optimizado), entre 3.51 - 4.50 (Gestionado), entre 2.51 – 3.50 (Definido), entre 1.51 – 2.50 (Repetible), entre 0.51 – 1.50 (Iniciado) y entre 0.00 – 0.50 (No). Obtuvieron como resultado que la empresa donde se realizó el estudio estaba en un nivel 1, es decir iniciado donde los objetivos y la implementación de las mismas se encuentran poco organizadas, mientras que su nivel esperado fue un nivel 3 donde los procesos son más organizados. Sin embargo en esta investigación, no sólo se consideró solo el APO01, sino que de acuerdo con la valoración inicial se midió la capacidad de 04 objetivos (DSS05, BAI09, APO12 y APO13) donde inicialmente se pudo identificar un nivel de madurez entre 1 y 2 para los objetivos, y en postest se pude mejorar y se pudo obtener in nivel de madurez entre 2 y 3 llegando al nivel definido donde al menos ya se tienen ordenados los procesos de la organización.

Alvarado D. y Andrade M. usaron el marco de trabajo COBIT 2019 como una herramienta para la gestión y gobierno de TI en su caso de estudio, partieron desde un análisis de la situación, levantaron procedimientos del área de TI y aplicaron COBIT 2019 con la finalidad de mejorar y revisar cómo se acoplan los objetivos de gobierno a los objetivos institucionales. Como parte de los hallazgos más importantes realizaron una caracterización del riesgo en un rango de 4 niveles donde: 1=riesgo bajo, 2=Riesgo normal, 3=riesgo alto y

4=Riesgo muy alto, entre los resultados encontraron que 12 riesgos equivalentes al 63.15% tienen un nivel de peligrosidad muy altos, el 21.05% son riesgos normales y sólo 1 fue considerado bajo. Además aplicaron y propusieron una lista de fórmulas basados en los objetivos EG01, EG08 y EG05. En comparación con este trabajo, debido a que los activos de la municipalidad de la Victoria eran cerca de 206, se pudo obtener un mayor rango de caracterización de riesgos donde para postest no había riesgos con el nivel muy alto, sólo el 27% tenía nivel alto, el 64% estaba en un nivel normal y el 10% tenía un nivel bajo de riesgo, con esto se evidencia una mejora considerable debido a que en comparación con la otra investigación que obtuvo un nivel de 63.15% de muy alta peligrosidad en este estudio se obtuvo 0% de peligrosidad muy alta.

Malca R. propuso un modelo de gobierno de TI basado en COBIT 2019, dentro de su modelo se consideró la cantidad de procesos, la cantidad de metas de TI en línea con las metas instruccionales, la implementación de los dominios y de los procesos COBIT y como parte de los indicadores consideró como parte importante considerar el porcentaje de dominios de COBIT 2019 en el cual obtuvo un total del 14.29% de dominios APO en consideración con el total de los 14 objetivos APO, esto le permitió analizar y priorizar la implementación de los procesos de acuerdo a los resultados obtenidos, donde se considera importante la participación de la alta dirección, tener cultura laboral, etc. En esta investigación se consideraron 2 APO, el APO12 y el APO13, ambos relacionados con el riesgo y la gestión de la seguridad que hacen un total del 14% con respecto al total de dominios. En comparación de amabas investigaciones ambas han coincidido con la elección de 2 APO, cabe mencionar que la numeración de las APO fue distinta para ambias investigaciones.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Se propuso diseñar procesos de gobierno de TI basado en COBIT 2019 para la gestión de la seguridad de la información en una municipalidad peruana. Lo más importante fue realizar la identificación de los riesgos y activos porque ayuda a manejar controles para mantener a los riesgos en un rango tolerable. Lo que más ayudó fue el análisis de la municipalidad porque se acoplan a los factores de diseño propuesto.

Se diagnosticaron las actividades que se relacionan de forma directa con la seguridad de la información, lo más importante fue detectar las vulnerabilidades a las cuales los activos de la municipalidad estaban expuestos. Lo más importante fue seguir los lineamientos de COBIT2019 para poder identificar las actividades que se realizan en la municipalidad que tienen relación con la seguridad de la información.

Se caracterizaron los procesos de TI de la municipalidad que se vinculan con la seguridad de la seguridad de la información. Lo más importante fue considerar los factores de diseño de COBIT2019 que se alinean a los objetivos y metas empresariales de la municipalidad de la Victoria lo cual nos ofrece un mejor entendimiento de las necesidades de la municipalidad para resguardar su información.

Se diseñaron los procesos de TI mediante gobierno que ayudaron a comprender los requerimientos necesarios para la seguridad de la información en base a COBIT2019. Lo más importante fue la guía que proporciona el marco de trabajo que muestra los pasos para poder aplicar y entender cómo se puede mejorar la gestión de la seguridad.

4.2 Recomendaciones

Organizar toda la información de la empresa previo al diseño de procesos basado en COBIT 2019, esto permitirá trabajar con mayor detalle y orden los objetivos y metas empresariales que servirá para que se acoplen de la mejor manera a los factores de diseño señalados en COBIT 2019.

Un indicador importante que se debe considerar es el porcentaje de riesgos, pues ayuda a identificar vulnerabilidades, riesgos o amenazas que puedan afectar de forma directa a la seguridad de la información, esto permitirá plantear de forma más certera los controles adecuados para gestionar de forma óptima la gestión de la seguridad de la información-

Para tener una mejor gestión de seguridad de la información, se recomienda trabajar siguiendo las herramientas de diseño que COBIT 2019 detalla, considerando los objetivos de gobierno que más se relacionen con la empresa.

Si se desea obtener una mejor visión, es importante la participación de la empresa o institución, pues para poder mejorar la gestión de la seguridad, se debe tener información importante con respecto a los objetivos, metas empresariales, activos de la empresa, riesgos, etc. que la empresa pueda tener identificados y que con la adecuada interpretación ayudará resguardar la información de robos, fallos, pérdidas, etc.

REFERENCIAS

[1] Banco Mundial, «La revolución digital: Promoción de un desarrollo inclusivo y resiliente,» 20 abril 2022. [En línea]. Available: https://envivo.bancomundial.org/evento/transformaciones-digitales. [Último acceso: 20 agosto 2023].

[2] M. Jiménez, «El Banco Mundial advierte del riesgo de una "década perdida" para la economía global,» elpais.com, 27 marzo 2023. [En línea]. Available: https://elpais.com/economia/2023-03-27/el-banco-mundial-advierte-del-riesgo-de-una-decada-perdida-para-la-economia-global.html. [Último acceso: 10 setiembre 2023].

[3] CEPAL, «Datos y hechos sobre la transformación digital,» Naciones Unidas, Santiago, 2022.

[4] Instituto Peruano de Economía, «Crecimiento de la economía será de apenas 0.8% en el 2023,» El Comercio, Lima, 2023.

[5] J. Lavado, «Diseño del sistema de Gobierno TI en una entidad pública de América Latina,» Isaca, Lima, 2021.

[6] M. Chocobar, «Política Nacional de transformación digital: Aspectos centrales para la equidad digital.,» Lima, 2022.

[7] OMPI, «Resumen índice Mundial de Innovación 2022,» OMPI, Suiza, 2022.

[8] Congreso de la República, *Undécima sesión ordinaria,* Lima: Congreso de la República, 2023.

[9] ACRONIS, «Informe mundial de la semana de Ciberprotección 2022,» Acronis, Singapur, 2022.

[10] IBM, «Informe de coste de la vulneración de datos 2023,» ibm.com, 2023. [En línea]. Available: https://www.ibm.com/es-es/reports/data-

breach#:~:text=El%20coste%20medio%20mundial%20de,del%2015%25%20en%203%20a%C3%B1os.. [Último acceso: 14 setiembre 2023].

[11] ESET, «Security Report Latinoamérica 2022,» 2022. [En línea]. Available: https://eset-la.com/Public_files/ESET-security-report-LATAM2022.pdf?utm_campaign=latam-es-online-esr_-5&utm_medium=email&utm_source=Eloqua&elqTrackId=206cc1fa7f41452f9dbe370fe144e462&elq=3a7e664b9a0b44a7aded4a8ece466dfb&elqaid=2832&elqat=1&elqCampaignId=. [Último acceso: 15 09 2023].

[12] CEPLAN, «Reporte 2023 Riesgos y oportunidades globales y nacionales para el Perú 2023-2033,» CEPLAN, Lima, 2022.

[13] Contraloría de la República, «Informe de visita de control N° 008-2023-OCI/2137-SVC,» Contraloría, Olmos, 2023.

[14] N. Miloslavskaya y S. Tolstaya, «Information Security Management Maturity Models,» *Procedia Computer Science,* pp. 49-57, 2022.

[15] S. Wulandari, A. Permata, M. Pohan, D. Sensuse y M. Syamsudin, «Risk assessment and recommendation strategy based on COBIT5 for Risk: Case study Sikn Jikn helpdesk service,» *Procedia Computer Science,* nº 161, pp. 168-177, 2019.

[16] A. Irsheid, A. Murad, M. AlNajdawi y A. Qusef, «Information security risk management models for cloud hosted systems: A comparative study,» *Procedia Computer Science,* nº 204, pp. 205-217, 2022.

[17] O. Plant, J. Hillegersberg y A. Aldea, «Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps envirnment,» *International Journal of Accounting Information Systems,* nº 45, pp. 1-17, 2022.

[18] D. Alvarado y M. Andrade, «Gestión de gobierno de Ti basado en COBIT2019, para el colegio de bachillerato Sara Serrano de Maridueña,» *Polo del Conocimiento,* vol. 6, nº 11, pp. 270-306, 2021.

[19] A. Cortés, «Propuesta de método basado en COBIT 2019 para la evaluación de procesos tecnológicos en la municipalidad de Carrillo,» *Revista Electrónica de las sedes regionales de la Universidad de Costa Rica,* vol. 24, nº 49, pp. 276-306, 2023.

[20] R. Malca, «Modelo de gobierno de tecnologías de la información: Diseño para una facultad de ingeniería de una universidad pública peruana.,» *Revista peruana de computación y sistemas,* vol. IV, nº 2, pp. 41-52, 2022.

[21] A. Morán, P. Jimbo, M. Jimbo y J. Franco, «Aplication of COBIT2019 to the government and management of information technologies in non-profit educational institutions,» *Sout Florida Journal,* vol. 4, nº 3, pp. 1388-1410, 2023.

[22] G. Nabeel, M. Rahmat y A. Widyatasya, «Transformasi digital InsurCo dengan merancang pengelolaan risiko teknologi informasi menggunakan framework COBIT2019 IT risk management focus area,» *Jurnal Ilmiah Teknologi Informasi Terapan,* vol. 9, nº 3, pp. 359-370, 2023.

[23] M. Syaputra, M. Kesuma, R. Saputra y J. Fitra, «Design of information technology (IT) gobernance using framework COBIT 2019 subdomain APO01 (Case study: Instidla),» *Jurnal Teknologi Komputer dan Sistem Informasi,* vol. 5, nº 3, pp. 157-162, 2022.

[24] J. Klucka y R. Grünbichler, «Enterprise risk management - approaches determining its application and relation to business performance,» *Quality Innovation Prosperity,* vol. 24, nº 2, pp. 51-58, 2020.

[25] C. Juiz, F. Duhamel, I. Gutiérrez y L. Luna, «IT managers´ framing of IT governance roles and responsibilities in Ibero-American Higher Education Institutions,» *Informatics,* vol. 9, nº 68, pp. 1-29, 2022.

[26] K. Kandasamy, S. Srinivas, K. Achuthan y V. Rangan, «IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process,» *EURASIP Journal on Information Security,* vol. 20, nº 8, pp. 1-18, 2020.

[27] N. Hakim, R. Fauzi y I. Santosa, «Analisis dan perancangan proses manajement risikó ti eggunakan kerangka kerja COBIT 2019 di PT iti (PERSERO),» *Proceedig og Egineering,* vol. 7, nº 3, pp. 9635-9642, 2020.

[28] A. Safitri, I. Syafii y K. Adi, «Measuring the performance of information system governance using framework COBIT 2019,» *International Journal of Computer Applications,* vol. 174, nº 31, pp. 23-30, 2021.

[29] N. Russo, L. Reis, C. Silveira y H. Mamede, «Towards a comprehensive framework for the multidisciplinary evaluation of organizational maturity on business continuity program manegement: A Systematic literature review,» *Information Security Journal: A Global Perspective,* vol. 20, nº 1, pp. 1-19, 2023.

ANEXOS

Anexo 1. Acta de revisión de similitud de la investigación.

ACTA DE REVISIÓN DE SIMILITUD DE LA INVESTIGACIÓN

Yo **Víctor Alexis Tuesta Monteza** docente del curso de **Investigación II**, del Programa de Estudios de **Ingeniería de Sistemas**, luego de revisar la investigación del (los) estudiante(s), **Karina Carolina De Los Santos Guerrero**, titulada:

DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACION EN UNA MUNICIPALIDAD PERUANA

Dejo constancia que la investigación antes indicada tiene un índice de similitud del porcentaje 13%, verificable en el reporte de originalidad mediante el software de similitud TURNITIN. Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre índice de similitud de los productos académicos y de investigación en la Universidad Señor de Sipán S.A.C. vigente.

En virtud de lo antes mencionado, firma:

Mg. Víctor Alexis Tuesta Montesa	DNI: 42722929	

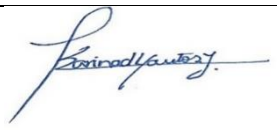
Pimentel, 27 de enero del 2025

Anexo 2. Acta de aprobación de asesor.

ACTA DE APROBACIÓN DEL ASESOR

Yo, **Heber Iván Mejía Cabrera** quien suscribe como asesor designado mediante Resolución de Facultad N° **0661-A-2023/FIAU-USS**, del proyecto de investigación titulado **DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACION EN UNA MUNICIPALIDAD PERUANA**, desarrollado por el(los) estudiante(s): **Karina carolina De Los Santos Guerrero**, del programa de estudios de **Ingeniería de Sistemas**, acredito haber revisado y declaro expedito para que continúe con el trámite pertinentes.

En virtud de lo antes mencionado, firman:

Mg. Heber Iván Mejía Cabrera (Asesor)	DNI: 41639565	
De Los Santos Guerrero Karina Carolina (Autor)	**DNI:** 43306449	

Pimentel, 27 de enero del 2025

Anexo 3. Tabla de operacionalización de variables.

OPERACIONALIZACIÓN DE LA VARIABLE

Variable de estudio	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítem	Instrumento	Valores finales	Tipo de variable	Escala de medición
Gobierno de TI basado en COBIT 2019	Es un marco de referencia asociado a gobierno de TI y gestión de la seguridad de la información [21]	Medición de procesos, dominios y capacidad que aporta COBIT 2019	Alineación a COBIT	Porcentaje procesos COBIT 2019	$PC = \frac{Objetivos}{N° \ Procesos} * 100\%$	Ficha resumen	11.4%	Numérica	Razón
				Porcentaje de dominios	$DOM = \frac{APO \ COBIT}{Total \ APO} * 100\%$	Ficha resumen	14%	Numérica	Razón
			Capacidad	Capacidad de cumplimiento	$KC = \frac{N° \ Objetivos}{Nivel \ Madurez} * 100\%$	Ficha resumen	20%	Numérica	Razón
Gestión de la seguridad de la información	Prácticas y políticas que mejoran el resguardo de la información en todos los ámbitos. [32]	Medición resultando de mejorar la gestión de la seguridad de la información	Operatividad	Porcentaje de incidentes	$KC = \frac{Inc.corporativos}{Total \ Incidentes} * 100\%$	Ficha resumen	9%	Numérica	Razón
				Porcentaje de activos	$AI = N° \ Activos * Cx100\%$	Ficha resumen	27%	Numérica	Razón
			Satisfacción	Nivel de satisfacción	$NS = \frac{\%Usuarios \ con \ alta \ satisfacción}{\% \ Usuarios \ con \ baja \ satisfacción}$	Cuestionario	75%	Numérica	Razón

Anexo 4. Matriz de consistencia.

MATRÍZ DE CONSISTENCIA LÓGICA DE PROYECTO DE INVESTIGACIÓN

Enfoque metodológico

Titulo	DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA

Tipo de investigación	Problema	Variables	Indicadores	Población	Muestra	Método de recolección de Datos	Técnicas de procesamiento de datos
Tecnologia aplicada tipo cuantitativa	¿Cómo mejorar la gestión de la seguridad de la información en una municipalidad peruana?	**VARIABLE INDEPENDIENTE:** Gobierno de TI basado en COBIT 2019 **VARIABLE DEPENDIENT:** Gestión de la seguridad de la información	**VARIABLE INDEPENDIENTE**:Porcentaje procesos COBIT 2019, Porcentaje de dominios y Capacidad de cumplimiento **VARIABLE DEPENDIENTE**:Porcentaje de incidentes, Porcentaje de activos y Nivel de satisfacción.	La población para el desarrollo del siguiente trabajo de investigación está presentado por un total de 38 municipalidades del departamento de Lambayeque	La municipalidad de la Victoria	Ficha resumen: Se realizó una recoleccion de datos actuales de la municipalidad para identificar y cacterizar los procesos y actividades que involucra con gobierno. Cuestionario: Se realizó una encuesta a los trabajadores de la municipalidad.	Ficha resumen y cuestionario

Diseño de investigación	Hipótesis	Objetivo General	Objetivos específicos	Método propuesto y desarrollado	Resultados preliminares
cuasi experimental	Mediante el diseño de gobierno de TI basado en COBIT 2019 se mejora la gestión de la seguridad de la información en una municipalidad peruana.	Diseñar procesos de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.	a) Diagnosticar las actividades relacionadas con seguridad de la información en la municipalidad peruana. b) Caracterizar los procesos de TI relacionados a la seguridad de la información. c) Diseñar mediante gobierno de TI los requerimientos necesarios para la seguridad de la información basado en COBIT 2019. d) Validar el diseño de gestión de la seguridad de la información con prueba empírica y por juicio de expertos.	OBJETIVO.1. DIAGNOSTICAR Se Identificaron actividades relacionadas a gobierno de TI, Identificaro roles y se realizó un cuadro para entender los problemas (contexto, metas y riesgos OBJETIVO.2. CARACTERIZAR Mapeo de procesos clave y con la Identificación de brechas. OBJETIVO.3.DISEÑAR Alineación entre requerimientos y procesos, asignación de Roles y Políticas OBJETIVO.4.VALIDAR Validación por juicio de expertos	

Anexo 5. Instrumentos de recolección de datos validados.

C01

Cuestionario de satisfacción a los

CUESTIONARIO DE SATISFACCIÓN A LOS USUARIOS SOBRE LA GESTIÓN DE LA SEGURIDAD DE LA

Área a la que pertenece: _____

Fecha: _____

Objetivo: Este cuestionario tiene como objetivo poder determinar el nivel de satisfacción que tienen los usuarios con respecto a la gestión de la seguridad de la información en La Municipalidad de la Victoria.

Indicaciones:

A continuación se muestra un rango de satisfacción, califique según su apreciación siguiendo la siguiente escala:

1 = Totalmente insatisfecho

2 = Insatisfecho

3 = Algo satisfecho

4 = Satisfecho

5 = Totalmente satisfecho

PREGUNTAS	ESCALA				
	1	2	3	4	5
1. ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad?					
2. ¿Se atendió oportunamente alguna interrupción de acceso de información ocasionado por un incidente de desastres naturales?					
3. ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo?					
4. ¿Alguna vez el área de TI atendió algún tipo de robo de datos mediante ciberataque?					
5. ¿Está satisfecho con la atención ante el fallo de infraestructura (Energía, transporte, agua, etc.) que afecte al acceso de la información?					
6. ¿Se siente seguro en el ambiente laboral ante ataques de fraude?					
7. ¿Se gestiona de forma correcta la interrupción de fallos en acceso a la información que puedan interrumpir la cadena de suministro?					
8. ¿Se atienden de forma segura eventos geopolíticos, o disturbios sociales que puedan afectar al acceso de la información?					

9. ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información?					
10. ¿Considera que los equipos de cómputo reciben las atenciones necesarias para que estén disponibles cuando se requiera acceder a la información?					
11. Considera que la Municipalidad cuenta con la infraestructura TI necesaria para proteger la información que maneja?					
12. ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información?					
13. ¿Siente que toda la información ya sea en documentación física o virtual está segura?					
14. ¿Se tienen capacitaciones constantes para proteger la información?					
15. ¿Se restringe de forma correcta el acceso a la información a personal extraño o externo a la Municipalidad?					
16. ¿Considera que la Ciberseguridad sea una solución que ayude al área de TI con el resguardo de la información?					

Validación del instrumento del cuestionario

Experto 1

V01

VALIDEZ DE INSTRUMENTO CUESTIONARIO

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Objetivo: Este cuestionario tiene como objetivo poder determinar el nivel de satisfacción que tienen los usuarios con respecto a la gestión de la seguridad de la información en una municipalidad peruana.

Indicaciones:

Señor especialista se le pide la colaboración, que luego de un riguroso análisis de los ítems del cuestionario, marque con un aspa (x) en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional.

PREGUNTAS	Es Esencial	Útil	No Necesaria
1. ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad?		Si	
2. ¿Se atendió oportunamente alguna interrupción de acceso de información ocasionado por un incidente de desastres naturales?	Si		
3. ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo?	Si		
4. ¿Alguna vez el área de TI atendió algún tipo de robo de datos mediante ciberataque?	Si		
5. ¿Está satisfecho con la atención ante el fallo de infraestructura (Energía, transporte, agua, etc.) que afecte al acceso de la información?		Si	
6. ¿Se siente seguro en el ambiente laboral ante ataques de fraude?		Si	
7. ¿Se gestiona de forma correcta la interrupción de fallos en acceso a la información que puedan interrumpir la cadena de suministro?	Si		
8. ¿Se atienden de forma segura eventos geopolíticos, o disturbios sociales que puedan afectar al acceso de la información?	Si		
9. ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información?		Si	
10. ¿Considera que los equipos de cómputo reciben las atenciones necesarias para que estén disponibles cuando se requiera acceder a la información?	Si		

11. Considera que la Municipalidad cuenta con la infraestructura TI necesaria para proteger la información que maneja?	Si		
12. ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información?		Si	
13. ¿Siente que toda la información ya sea en documentación física o virtual está segura?		Si	
14. ¿Se tienen capacitaciones constantes para proteger la información?		Si	
15. ¿Se restringe de forma correcta el acceso a la información a personal extraño o externo a la Municipalidad?	Si		
16. ¿Considera que la Ciberseguridad sea una solución que ayude al área de TI con el resguardo de la información?	Si		

FIRMA

Universidad Señor de Sipán

Escuela Profesional de Ingeniería de Sistemas

FICHA DE OPINIÓN DE EXPERTOS

Nombres y apellidos del experto: Ricardo Guanilo Gonzales

Grado Académico: Ingeniero Informático y de sistemas

Cargo: Docente del CIS

Institución: Universidad Señor de Sipán

Nombre del Instrumento a Validar: Validez de Contenido

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Aspectos de Validación:

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy Bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los ítems están formulados con el lenguaje apropiado y comprensible.				16
Organización	Existe una organización lógica en la redacción de los ítems.			13	
Suficiencia	Los ítems son suficientes para medir los indicadores de lasvariables.			13	
Valides	El instrumento es capaz de medir lo que se requiere.				16
Viabilidad	Es viable su aplicación				17

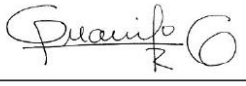
Valoración:

- ✓ Puntaje (0 a 20): 15
- ✓ Clasificación (Deficiente a Muy bueno): Bueno

Observaciones:

No se detalla alguna medición de la seguridad de la información en física, y si es digital algún software o antivirus usado.

Fecha: 16/03/2024



FIRMA

Experto 2:

V01

VALIDEZ DE INSTRUMENTO CUESTIONARIO

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Objetivo: Este cuestionario tiene como objetivo poder determinar el nivel de satisfacción que tienen los usuarios con respecto a la gestión de la seguridad de la información en una municipalidad peruana.

Indicaciones:

Señor especialista se le pide la colaboración, que luego de un riguroso análisis de los ítems del cuestionario, marque con un aspa (x) en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional.

PREGUNTAS	Es Esencial	Útil	No Necesaria
1. ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad?	x		
2. ¿Se atendió oportunamente alguna interrupción de acceso de información ocasionado por un incidente de desastres naturales?	x		
3. ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo?	x		
4. ¿Alguna vez el área de TI atendió algún tipo de robo de datos mediante ciberataque?	x		
5. ¿Está satisfecho con la atención ante el fallo de infraestructura (Energía, transporte, agua, etc.) que afecte al acceso de la información?		x	
6. ¿Se siente seguro en el ambiente laboral ante ataques de fraude?	x		
7. ¿Se gestiona de forma correcta la interrupción de fallos en acceso a la información que puedan interrumpir la cadena de suministro?	x		
8. ¿Se atienden de forma segura eventos geopolíticos, o disturbios sociales que puedan afectar al acceso de la información?	x		
9. ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información?	x		
10. ¿Considera que los equipos de cómputo reciben las atenciones necesarias para que estén disponibles cuando se requiera acceder a la información?		x	

11. Considera que la Municipalidad cuenta con la infraestructura TI necesaria para proteger la información que maneja?	x		
12. ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información?	x		
13. ¿Siente que toda la información ya sea en documentación física o virtual está segura?	x		
14. ¿Se tienen capacitaciones constantes para proteger la información?	x		
15. ¿Se restringe de forma correcta el acceso a la información a personal extraño o externo a la Municipalidad?	x		
16. ¿Considera que la Ciberseguridad sea una solución que ayude al área de TI con el resguardo de la información?		x	

FIRMA

Universidad Señor de Sipán

Escuela Profesional de Ingeniería de Sistemas

FICHA DE OPINIÓN DE EXPERTOS

Nombres y apellidos del experto: Anthony Walter Franco Rodriguez

Grado Académico: Ingeniero de Sistemas

Cargo: Gerente de TIC

Institución: Municipalidad de distrital de los olivos

Nombre del Instrumento a Validar: Cuestionario

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Aspectos de Validación:

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy Bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los ítems están formulados con el lenguaje apropiado y comprensible.				18
Organización	Existe una organización lógica en la redacción de los ítems.				16
Suficiencia	Los ítems son suficientes para medir los indicadores de lasvariables.				16
Valides	El instrumento es capaz de medir lo que se requiere.				20
Viabilidad	Es viable su aplicación				19

Valoración:

- ✓ Puntaje (0 a 20): 18
- ✓ Clasificación (Deficiente a Muy bueno): Muy Bueno

Observaciones:

Fecha: 14/03/ 2024

MUNICIPALIDAD DISTRITAL DE LOS OLIVOS
Ing. Anthony Walter Franco Rodriguez
OFICINA GENERAL DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

FIRMA

Experto 3

V01

VALIDEZ DE INSTRUMENTO CUESTIONARIO

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

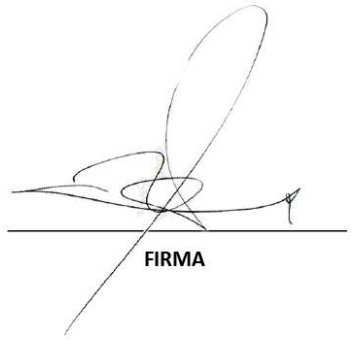
Objetivo: Este cuestionario tiene como objetivo poder determinar el nivel de satisfacción que tienen los usuarios con respecto a la gestión de la seguridad de la información en una municipalidad peruana.

Indicaciones:

Señor especialista se le pide la colaboración, que luego de un riguroso análisis de los ítems del cuestionario, marque con un aspa (x) en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional.

PREGUNTAS	Es Esencial	Útil	No Necesaria
1. ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad?		X	
2. ¿Se atendió oportunamente alguna interrupción de acceso de información ocasionado por un incidente de desastres naturales?		X	
3. ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo?		X	
4. ¿Alguna vez el área de TI atendió algún tipo de robo de datos mediante ciberataque?		X	
5. ¿Está satisfecho con la atención ante el fallo de infraestructura (Energía, transporte, agua, etc.) que afecte al acceso de la información?		X	
6. ¿Se siente seguro en el ambiente laboral ante ataques de fraude?		X	
7. ¿Se gestiona de forma correcta la interrupción de fallos en acceso a la información que puedan interrumpir la cadena de suministro?		X	
8. ¿Se atienden de forma segura eventos geopolíticos, o disturbios sociales que puedan afectar al acceso de la información?		X	
9. ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información?		X	
10. ¿Considera que los equipos de cómputo reciben las atenciones necesarias para que estén disponibles cuando se requiera acceder a la información?		X	

11. Considera que la Municipalidad cuenta con la infraestructura TI necesaria para proteger la información que maneja?		X	
12. ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información?		X	
13. ¿Siente que toda la información ya sea en documentación física o virtual está segura?		X	
14. ¿Se tienen capacitaciones constantes para proteger la información?		X	
15. ¿Se restringe de forma correcta el acceso a la información a personal extraño o externo a la Municipalidad?		X	
16. ¿Considera que la Ciberseguridad sea una solución que ayude al área de TI con el resguardo de la información?		X	



Universidad Señor de Sipán

Escuela Profesional de Ingeniería de Sistemas

FICHA DE OPINIÓN DE EXPERTOS

Nombres y apellidos del experto: ALBERTO ENRIQUE SAMILLAN AYALA

Grado Académico: DOCTOR

Cargo: DOCENTE PRINCIPAL

Institución: UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Nombre del Instrumento a Validar: Cuestionario de satisfacción a los usuarios sobre la gestión de la seguridad de la información en una municipalidad peruana

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Aspectos de Validación:

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy Bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los ítems están formulados con el lenguaje apropiado y comprensible.				18
Organización	Existe una organización lógica en la redacción de los ítems.				16
Suficiencia	Los ítems son suficientes para medir los indicadores de lasvariables.				17
Valides	El instrumento es capaz de medir lo que se requiere.				16
Viabilidad	Es viable su aplicación				18

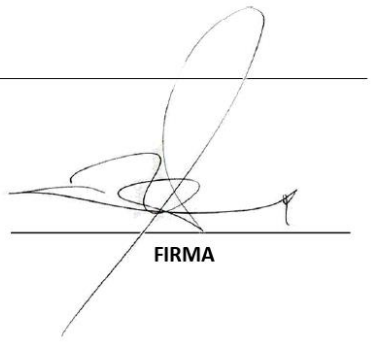
Valoración:

- ✓ Puntaje (0 a 20): 17
- ✓ Clasificación (Deficiente a Muy bueno): MUY BUENO

Observaciones:

NINGUNA

Fecha: 13 DE MARZO DEL 2024



FIRMA

Experto 4

V01

VALIDEZ DE INSTRUMENTO CUESTIONARIO

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Objetivo: Este cuestionario tiene como objetivo poder determinar el nivel de satisfacción que tienen los usuarios con respecto a la gestión de la seguridad de la información en una municipalidad peruana.

Indicaciones:

Señor especialista se le pide la colaboración, que luego de un riguroso análisis de los ítems del cuestionario, marque con un aspa (x) en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional.

PREGUNTAS	Es Esencial	Útil	No Necesaria
1. ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad?	x		
2. ¿Se atendió oportunamente alguna interrupción de acceso de información ocasionado por un incidente de desastres naturales?		x	
3. ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo?	x		
4. ¿Alguna vez el área de TI atendió algún tipo de robo de datos mediante ciberataque?	x		
5. ¿Está satisfecho con la atención ante el fallo de infraestructura (Energía, transporte, agua, etc.) que afecte al acceso de la información?		x	
6. ¿Se siente seguro en el ambiente laboral ante ataques de fraude?		x	
7. ¿Se gestiona de forma correcta la interrupción de fallos en acceso a la información que puedan interrumpir la cadena de suministro?	x		
8. ¿Se atienden de forma segura eventos geopolíticos, o disturbios sociales que puedan afectar al acceso de la información?		x	
9. ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información?			x
10. ¿Considera que los equipos de cómputo reciben las atenciones necesarias para que estén disponibles cuando se requiera acceder a la información?	x		

11. Considera que la Municipalidad cuenta con la infraestructura TI necesaria para proteger la información que maneja?	X		
12. ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información?	X		
13. ¿Siente que toda la información ya sea en documentación física o virtual está segura?	X		
14. ¿Se tienen capacitaciones constantes para proteger la información?	X		
15. ¿Se restringe de forma correcta el acceso a la información a personal extraño o externo a la Municipalidad?	X		
16. ¿Considera que la Ciberseguridad sea una solución que ayude al área de TI con el resguardo de la información?		x	

FIRMA

Universidad Señor de Sipán

Escuela Profesional de Ingeniería de Sistemas

FICHA DE OPINIÓN DE EXPERTOS

Nombres y apellidos del experto: Jessie Leila Bravo Jaico

Grado Académico: Doctora en Ciencias de la Computación y Sistemas

Cargo: Docente

Institución: Universidad Nacional Pedro Ruiz Gallo

Nombre del Instrumento a Validar: Cuestionario

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Aspectos de Validación:

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy Bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los ítems están formulados con el lenguaje apropiado y comprensible.			15	
Organización	Existe una organización lógica en la redacción de los ítems.				17
Suficiencia	Los ítems son suficientes para medir los indicadores de lasvariables.			15	
Valides	El instrumento es capaz de medir lo que se requiere.				17
Viabilidad	Es viable su aplicación				17

Valoración:

- ✓ Puntaje (0 a 20): 16
- ✓ Clasificación (Deficiente a Muy bueno): Bueno

Observaciones:

Debería mejorar la redacción de las preguntas planteadas y considerar algunas preguntas sobre temas de ciberseguridad

Fecha: 15/03/24

FIRMA

Experto 5

V01

VALIDEZ DE INSTRUMENTO CUESTIONARIO

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Objetivo: Este cuestionario tiene como objetivo poder determinar el nivel de satisfacción que tienen los usuarios con respecto a la gestión de la seguridad de la información en una municipalidad peruana.

Indicaciones:

Señor especialista se le pide la colaboración, que luego de un riguroso análisis de los ítems del cuestionario, marque con un aspa (x) en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional.

PREGUNTAS	Es Esencial	Útil	No Necesaria
1. ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad?	X		
2. ¿Se atendió oportunamente alguna interrupción de acceso de información ocasionado por un incidente de desastres naturales?	X		
3. ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo?	X		
4. ¿Alguna vez el área de TI atendió algún tipo de robo de datos mediante ciberataque?	X		
5. ¿Está satisfecho con la atención ante el fallo de infraestructura (Energía, transporte, agua, etc.) que afecte al acceso de la información?	X		
6. ¿Se siente seguro en el ambiente laboral ante ataques de fraude?	X		
7. ¿Se gestiona de forma correcta la interrupción de fallos en acceso a la información que puedan interrumpir la cadena de suministro?	X		
8. ¿Se atienden de forma segura eventos geopolíticos, o disturbios sociales que puedan afectar al acceso de la información?	X		
9. ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información?		X	
10. ¿Considera que los equipos de cómputo reciben las atenciones necesarias para que estén disponibles cuando se requiera acceder a la información?	X		

11. Considera que la Municipalidad cuenta con la infraestructura TI necesaria para proteger la información que maneja?	X		
12. ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información?	X		
13. ¿Siente que toda la información ya sea en documentación física o virtual está segura?	X		
14. ¿Se tienen capacitaciones constantes para proteger la información?	X		
15. ¿Se restringe de forma correcta el acceso a la información a personal extraño o externo a la Municipalidad?	X		
16. ¿Considera que la Ciberseguridad sea una solución que ayude al área de TI con el resguardo de la información?		x	

FIRMA

Universidad Señor de Sipán

Escuela Profesional de Ingeniería de Sistemas

FICHA DE OPINIÓN DE EXPERTOS

Nombres y apellidos del experto: SEGUNDO JOSE CASTILLO ZUMARAN

Grado Académico: MAGISTER

Cargo: DOCENTE

Institución: UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO

Nombre del Instrumento a Validar: Cuestionario

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Aspectos de Validación:

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy Bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los ítems están formulados con el lenguaje apropiado y comprensible.				17
Organización	Existe una organización lógica en la redacción de los ítems.				17
Suficiencia	Los ítems son suficientes para medir los indicadores de lasvariables.				17
Valides	El instrumento es capaz de medir lo que se requiere.				17
Viabilidad	Es viable su aplicación				17

Valoración:

- ✓ Puntaje (0 a 20): 17
- ✓ Clasificación (Deficiente a Muy bueno): Muy Bueno

Observaciones: NINGUNA

Fecha: 14-03-2024

FIRMA

V01

VALIDEZ DE INSTRUMENTO
CUESTIONARIO

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Objetivo: Este cuestionario tiene como objetivo poder determinar el nivel de satisfacción que tienen los usuarios con respecto a la gestión de la seguridad de la información en una municipalidad peruana.

Indicaciones:

Señor especialista se le pide la colaboración, que luego de un riguroso análisis de los ítems del cuestionario, marque con un aspa (x) en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional.

PREGUNTAS	Es Esencial	Útil	No Necesaria
1. ¿El área de Ti atiende oportunamente incidentes de falla de equipos o sistemas informáticos donde aloja información importante para la municipalidad?	X		
2. ¿Se atendió oportunamente alguna interrupción de acceso de información ocasionado por un incidente de desastres naturales?	X		
3. ¿Cuenta con la protección necesaria para evitar algún tipo de robo de información en su espacio de trabajo?	X		
4. ¿Alguna vez el área de TI atendió algún tipo de robo de datos mediante ciberataque?	X		
5. ¿Está satisfecho con la atención ante el fallo de infraestructura (Energía, transporte, agua, etc.) que afecte al acceso de la información?	X		
6. ¿Se siente seguro en el ambiente laboral ante ataques de fraude?	X		
7. ¿Se gestiona de forma correcta la interrupción de fallos en acceso a la información que puedan interrumpir la cadena de suministro?	X		
8. ¿Se atienden de forma segura eventos geopolíticos, o disturbios sociales que puedan afectar al acceso de la información?	X		
9. ¿Está satisfecho con el desempeño del área de Informática con respecto al resguardo de la información?		X	
10. ¿Considera que los equipos de cómputo reciben las atenciones necesarias para que estén disponibles cuando se requiera acceder a la información?	X		

11. Considera que la Municipalidad cuenta con la infraestructura TI necesaria para proteger la información que maneja?	X		
12. ¿Cuenta con alguna guía o política para actuar ante algún tipo de robo, ataque o fallo que puedan afectar al acceso a la información?	X		
13. ¿Siente que toda la información ya sea en documentación física o virtual está segura?	X		
14. ¿Se tienen capacitaciones constantes para proteger la información?	X		
15. ¿Se restringe de forma correcta el acceso a la información a personal extraño o externo a la Municipalidad?	X		
16. ¿Considera que la Ciberseguridad sea una solución que ayude al área de TI con el resguardo de la información?		x	

FIRMA

Universidad Señor de Sipán

Escuela Profesional de Ingeniería de Sistemas

FICHA DE OPINIÓN DE EXPERTOS

Nombres y apellidos del experto: SEGUNDO JOSE CASTILLO ZUMARAN

Grado Académico: MAGISTER

Cargo: DOCENTE

Institución: UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO

Nombre del Instrumento a Validar: Cuestionario

Título de la Tesis: Diseño de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

Aspectos de Validación:

Indicadores	Criterios	Calificación			
		Deficiente	Regular	Bueno	Muy Bueno
		De 0 a 5	De 6 a 10	De 11 a 15	De 16 a 20
Claridad	Los ítems están formulados con el lenguaje apropiado y comprensible.				17
Organización	Existe una organización lógica en la redacción de los ítems.				17
Suficiencia	Los ítems son suficientes para medir los indicadores de lasvariables.				17
Valides	El instrumento es capaz de medir lo que se requiere.				17
Viabilidad	Es viable su aplicación				17

Valoración:

- ✓ Puntaje (0 a 20): 17
- ✓ Clasificación (Deficiente a Muy bueno): Muy Bueno

Observaciones: NINGUNA

Fecha: 14-03-2024

FIRMA

Anexo 6. Ficha resumen de porcentaje de procesos COBIT2019

FI-01

DO. PROCESOS COBIT

FICHA RESUMEN DE REVISIÓN DOCUMENTAL

Documentos vinculados a procesos COBIT 2019

Datos Generales	
N° Ficha	01
Fecha de revisión de documento	2019
Persona a cargo	Carolina De Los Santos Guerrero.
Tiempo de revisión	120 minutos
Datos del Documento	
Título	COBIT 2019 Objetivos de gobierno y gestión
Fecha del documento	2018
Título del proyecto	Sistema de gestión de la seguridad basado en COBIT 2019
Autor	Grupo ISACA
Información relevante de los documentos	
Objetivo	Considerar los objetivos de gestión relacionados a la seguridad de la información.
Justificación	Este documento sirve de apoyo para conocer los objetivos de COBIT relacionado a la gestión de seguridad.
Fundamentación	**DSS05** Gestionar los servicios de seguridad.
Referencias	Grupo ISACA
Observaciones	

Anexo 7**.** Ficha resumen de porcentaje de dominios

FI-02

DO. Dominios de gestión

FICHA RESUMEN DE REVISIÓN DOCUMENTAL

Documentos vinculados a procesos COBIT 2019

Datos Generales		
N° Ficha	03	
Fecha de revisión de documento	2019	
Persona a cargo	Carolina De Los Santos Guerrero.	
Tiempo de revisión	120 minutos	
Datos del Documento		
Título	COBIT 2019 Objetivos de gobierno y gestión	
Fecha del documento	2018	
Título del proyecto	Sistema de gestión de la seguridad basado en COBIT2019	
Autor	Grupo ISACA	
Información relevante de los documentos		
Objetivo	Considerar los objetivos de gestión relacionados a la seguridad de la información.	
Justificación	Este documento sirve de apoyo para conocer los objetivos de COBIT relacionado a la gestión de seguridad.	
Fundamentación	**N° APO Considerados**	Gestionar el riesgo.
	Total APO COBIT 2019	Gestionar la seguridad. 13
Referencias	Grupo ISACA	
Observaciones		

Anexo 8. Ficha resumen de capacidad de cumplimiento

FI-03

DO. Capacidad de cumplimiento

FICHA RESUMEN DE REVISIÓN DOCUMENTAL

Documentos vinculados a procesos COBIT 2019

Datos Generales	
N° Ficha	02
Fecha de revisión de documento	2021
Persona a cargo	Carolina De Los Santos Guerrero.
Tiempo de revisión	120 minutos
Datos del Documento	
Título	Plan Operativo Institucional – POI Multianual 2022-2024
Fecha del documento	29 de abril 2021
Título del proyecto	Sistema de gestión de la seguridad basado en COBIT 2019
Autor	Municipalidad Distrital de la Victoria - Chiclayo
Información relevante de los documentos	
Objetivo	Considerar los objetivos estratégicos institucionales relacionados a la gestión de la seguridad de la información en la Municipalidad de La Victoria.
Justificación	Este documento sirve de apoyo para conocer tanto los objetivos como metas institucionales
Fundamentación	**Objetivos Estratégicos** - Promover los niveles de competitividad económica en el distrito de la victoria **Metas** - Ferias económicas de la formalización de manera integral a la población

- Asistencia técnica a los emprendedores del distrito de La Victoria
- Asistencia técnica en la formalización de los establecimientos de manera oportuna a los comerciantes informales
- Plataforma de defensa civil fortalecida en beneficio del distrito

Referencias Municipalidad distrital de La Victoria

Observaciones

Anexo 9. Ficha resumen de porcentaje de incidentes

FI-04

DO. Porcentaje de incidencias

FICHA RESUMEN DE REVISIÓN DOCUMENTAL

Documentos vinculados a procesos COBIT 2019

Datos Generales	
N° Ficha	03
Fecha de revisión de documento	2021
Persona a cargo	Carolina De Los Santos Guerrero.
Tiempo de revisión	120 minutos

Datos del Documento	
Título	PLAN OPERATIVO INSTITUCIONAL POI 2021
Fecha del documento	2 de abril 2021
Título del proyecto	Sistema de gestión de la seguridad basado en COBIT 2019
Autor	Municipalidad Distrital de la Victoria - Chiclayo

Información relevante de los documentos		
Objetivo	Revisar la cantidad de incidencias relacionadas a la seguridad de la información en 1 mes.	
Justificación	Este documento sirve de apoyo para conocer las vulnerabilidades y amenazas.	
Fundamentación	**Incidencias**	- Actualización diaria del portal institucional
	Total	154
	Inc. Corp	134
Referencias	Municipalidad distrital de La Victoria	
Observaciones		

Anexo 10. Ficha resumen de porcentaje de activos

FI-05

DO. Porcentaje de activos

FICHA RESUMEN DE REVISIÓN DOCUMENTAL

Documentos vinculados a procesos COBIT 2019

Datos Generales

N° Ficha	02
Fecha de revisión de documento	2021
Persona a cargo	Carolina De Los Santos Guerrero.
Tiempo de revisión	120 minutos

Datos del Documento

Título	PLAN OPERATIVO INSTITUCIONAL POI 2021
Fecha del documento	29 de abril 2021
Título del proyecto	Sistema de gestión de la seguridad basado en COBIT 2019
Autor	Municipalidad Distrital de la Victoria - Chiclayo

Información relevante de los documentos

Objetivo	Considerar los activos de infraestructura que tiene la Municipalidad	
Justificación	Este documento sirve de apoyo para conocer la cantidad de activos que pueden ser considerados vulnerables a sufrir algún tipo de ataque.	
Fundamentación	**Nombre de activo**	Impresoras (55)
	Total de activos	206
Referencias	Municipalidad distrital de La Victoria	
Observaciones		

Anexo 11. Resumen de los factores de diseño DF5-DF11

A6-DF5

Identificador		Alto	Normal
EDM01	Garantizar el establecimiento y el mantenimiento del marco de gobierno.	3	1
EDM02	Asegurar la realización de beneficios.	2	1
EDM03	Asegurar la optimización del riesgo.	4	1
EDM04	Asegurar la optimización de los recursos.	3	1
EDM05	Asegurar la transparencia de las partes interesadas.	2	1
APO01	Gestionar el marco de gestión de TI.	4	1
APO02	Gestionar la estrategia.	2	1
APO03	Gestionar la arquitectura de la empresa.	3	1
APO04	Gestionar la innovación.	3	1
APO05	Gestionar el portafolio.	2	1
APO06	Gestionar el presupuesto y los costes.	1	1
APO07	Gestionar los recursos humanos.	3	1
APO08	Gestionar las relaciones.	1	1
APO09	Gestionar los acuerdos de servicio.	2	1
APO10	Gestionar los proveedores.	1	1
APO11	Gestionar la calidad.	3	1
APO12	Gestionar el riesgo.	4	1
APO13	Gestionar la seguridad.	4	1
APO14	Gestionar los datos.	2	1
BAI01	Gestionar los programas.	3	1
BAI02	Gestionar la definición de los requisitos.	2	1
BAI03	Gestionar la identificación y construcción de soluciones.	2	1
BAI04	Gestionar la disponibilidad y capacidad.	3	1
BAI05	Gestionar los cambios organizativos.	2	1
BAI06	Gestionar los cambios de TI.	1	1
BAI07	Gestionar la aceptación y la transición de los cambios de TI.	3	1
BAI08	Gestionar el conocimiento.	1	1
BAI09	Gestionar los activos.	4	1
BAI10	Gestionar la configuración.	1	1
BAI11	Gestionar los proyectos.	3	1
DSS01	Gestionar las operaciones.	1	1
DSS02	Gestionar las solicitudes e incidentes de servicio.	1	1
DSS03	Gestionar los problemas.	2	1
DSS04	Gestionar la continuidad.	2	1
DSS05	Gestionar los servicios de seguridad.	4	1

DSS06	Gestionar los controles de procesos de negocio.	3	1
MEA01	Gestionar la monitorización del rendimiento y la conformidad.	1	1
MEA02	Gestionar el sistema de control interno.	3	1
MEA03	Gestionar el cumplimiento de los requisitos externos.	3	1
MEA04	Gestionar el aseguramiento.	1	1

A7-DF6

Identificador		Alto	Normal	Baja
EDM01	Garantizar el establecimiento y el mantenimiento del marco de gobierno.	2	1	1
EDM02	Asegurar la realización de beneficios.	2	1	1
EDM03	Asegurar la optimización del riesgo.	4	2	1
EDM04	Asegurar la optimización de los recursos.	3	1	1
EDM05	Asegurar la transparencia de las partes interesadas.	1	1	1
APO01	Gestionar el marco de gestión de TI.	4	2	1
APO02	Gestionar la estrategia.	1	1	1
APO03	Gestionar la arquitectura de la empresa.	2	1	1
APO04	Gestionar la innovación.	2	1	1
APO05	Gestionar el portafolio.	2	1	1
APO06	Gestionar el presupuesto y los costes.	1	1	1
APO07	Gestionar los recursos humanos.	1	1	1
APO08	Gestionar las relaciones.	1	1	1
APO09	Gestionar los acuerdos de servicio.	1	1	1
APO10	Gestionar los proveedores.	1	1	1
APO11	Gestionar la calidad.	2	1	1
APO12	Gestionar el riesgo.	4	2	1
APO13	Gestionar la seguridad.	4	2	1
APO14	Gestionar los datos.	2	1	1
BAI01	Gestionar los programas.	1	1	1
BAI02	Gestionar la definición de los requisitos.	1	1	1
BAI03	Gestionar la identificación y construcción de soluciones.	1	1	1
BAI04	Gestionar la disponibilidad y capacidad.	2	1	1
BAI05	Gestionar los cambios organizativos.	1	1	1
BAI06	Gestionar los cambios de TI.	1	1	1
BAI07	Gestionar la aceptación y la transición de los cambios de TI.	1	1	1
BAI08	Gestionar el conocimiento.	1	1	1
BAI09	Gestionar los activos.	4	2	1
BAI10	Gestionar la configuración.	1	1	1

BAI11	Gestionar los proyectos.	1	1	1
DSS01	Gestionar las operaciones.	1	1	1
DSS02	Gestionar las solicitudes e incidentes de servicio.	1	1	1
DSS03	Gestionar los problemas.	2	1	1
DSS04	Gestionar la continuidad.	2	1	1
DSS05	Gestionar los servicios de seguridad.	4	2	1
DSS06	Gestionar los controles de procesos de negocio.	1	1	1
MEA01	Gestionar la monitorización del rendimiento y la conformidad.	1	1	1
MEA02	Gestionar el sistema de control interno.	1	1	1
MEA03	Gestionar el cumplimiento de los requisitos externos.	1	1	1
MEA04	Gestionar el aseguramiento.	1	1	1

A8-DF7

Identificador		Soporte	Fábrica	Cambio	Estratégica
EDM01	Garantizar el establecimiento y el mantenimiento del marco de gobierno.	1	1	1	1
EDM02	Asegurar la realización de beneficios.	1	1	1	2
EDM03	Asegurar la optimización del riesgo.	2	1	4	4
EDM04	Asegurar la optimización de los recursos.	1	1	2	2
EDM05	Asegurar la transparencia de las partes interesadas.	1	1	2	1
APO01	Gestionar el marco de gestión de TI.	3	1	3	4
APO02	Gestionar la estrategia.	1	1	1	3
APO03	Gestionar la arquitectura de la empresa.	1	1	1	2
APO04	Gestionar la innovación.	1	1	1	1
APO05	Gestionar el portafolio.	1	1	1	1
APO06	Gestionar el presupuesto y los costes.	1	1	1	2
APO07	Gestionar los recursos humanos.	1	1	1	2
APO08	Gestionar las relaciones.	1	1	2	1
APO09	Gestionar los acuerdos de servicio.	1	1	1	1
APO10	Gestionar los proveedores.	1	1	1	1
APO11	Gestionar la calidad.	1	1	1	2
APO12	Gestionar el riesgo.	3	1	3	5
APO13	Gestionar la seguridad.	3	1	4	5
APO14	Gestionar los datos.	1	1	2	2
BAI01	Gestionar los programas.	1	1	1	1
BAI02	Gestionar la definición de los requisitos.	1	1	1	1
BAI03	Gestionar la identificación y construcción de soluciones.	1	1	2	1
BAI04	Gestionar la disponibilidad y capacidad.	1	1	1	1

BAI05	Gestionar los cambios organizativos.	1	1	1	2
BAI06	Gestionar los cambios de TI.	1	1	2	2
BAI07	Gestionar la aceptación y la transición de los cambios de TI.	1	1	1	1
BAI08	Gestionar el conocimiento.	1	1	1	1
BAI09	Gestionar los activos.	5	1	4	3
BAI10	Gestionar la configuración.	1	1	1	1
BAI11	Gestionar los proyectos.	1	1	2	2
DSS01	Gestionar las operaciones.	1	1	1	1
DSS02	Gestionar las solicitudes e incidentes de servicio.	1	1	1	2
DSS03	Gestionar los problemas.	1	1	2	2
DSS04	Gestionar la continuidad.	1	1	1	1
DSS05	Gestionar los servicios de seguridad.	3	1	4	4
DSS06	Gestionar los controles de procesos de negocio.	1	1	1	1
MEA01	Gestionar la monitorización del rendimiento y la conformidad.	1	1	2	1
MEA02	Gestionar el sistema de control interno.	1	1	1	2
MEA03	Gestionar el cumplimiento de los requisitos externos.	1	1	1	2
MEA04	Gestionar el aseguramiento.	1	1	1	1

A9-DF8

Identificador		Externalización (Outsourcing)	Nube	Personal Interno (Insoursing)
EDM01	Garantizar el establecimiento y el mantenimiento del marco de gobierno.	1	1	1
EDM02	Asegurar la realización de beneficios.	1	1	1
EDM03	Asegurar la optimización del riesgo.	1	1	3
EDM04	Asegurar la optimización de los recursos.	1	1	2
EDM05	Asegurar la transparencia de las partes interesadas.	1	1	1
APO01	Gestionar el marco de gestión de TI.	1	1	3
APO02	Gestionar la estrategia.	1	1	2
APO03	Gestionar la arquitectura de la empresa.	1	2	1
APO04	Gestionar la innovación.	1	1	2
APO05	Gestionar el portafolio.	1	1	1
APO06	Gestionar el presupuesto y los costes.	1	1	2
APO07	Gestionar los recursos humanos.	1	1	3
APO08	Gestionar las relaciones.	1	1	3
APO09	Gestionar los acuerdos de servicio.	1	1	2
APO10	Gestionar los proveedores.	1	1	1
APO11	Gestionar la calidad.	1	1	2

APO12	Gestionar el riesgo.	1	1	3
APO13	Gestionar la seguridad.	1	2	4
APO14	Gestionar los datos.	1	1	2
BAI01	Gestionar los programas.	1	1	1
BAI02	Gestionar la definición de los requisitos.	1	1	2
BAI03	Gestionar la identificación y construcción de soluciones.	1	1	2
BAI04	Gestionar la disponibilidad y capacidad.	1	1	1
BAI05	Gestionar los cambios organizativos.	1	1	2
BAI06	Gestionar los cambios de TI.	1	1	1
BAI07	Gestionar la aceptación y la transición de los cambios de TI.	1	1	1
BAI08	Gestionar el conocimiento.	1	1	2
BAI09	Gestionar los activos.	1	1	3
BAI10	Gestionar la configuración.	1	1	1
BAI11	Gestionar los proyectos.	1	1	1
DSS01	Gestionar las operaciones.	1	1	1
DSS02	Gestionar las solicitudes e incidentes de servicio.	1	1	2
DSS03	Gestionar los problemas.	1	1	1
DSS04	Gestionar la continuidad.	1	1	1
DSS05	Gestionar los servicios de seguridad.	1	2	3
DSS06	Gestionar los controles de procesos de negocio.	1	1	1
MEA01	Gestionar la monitorización del rendimiento y la conformidad.	1	1	1
MEA02	Gestionar el sistema de control interno.	1	1	1
MEA03	Gestionar el cumplimiento de los requisitos externos.	1	1	1
MEA04	Gestionar el aseguramiento.	1	1	1

A10-DF09

Identificador		Agile	DevOps	Tradicional
EDM01	Garantizar el establecimiento y el mantenimiento del marco de gobierno.	2	1	1
EDM02	Asegurar la realización de beneficios.	1	1	1
EDM03	Asegurar la optimización del riesgo.	1	1	1
EDM04	Asegurar la optimización de los recursos.	2	1	1
EDM05	Asegurar la transparencia de las partes interesadas.	1	1	1
APO01	Gestionar el marco de gestión de TI.	1	1	1
APO02	Gestionar la estrategia.	2	1	1
APO03	Gestionar la arquitectura de la empresa.	1	1	1

APO04	Gestionar la innovación.	1	1	1
APO05	Gestionar el portafolio.	2	1	1
APO06	Gestionar el presupuesto y los costes.	1	1	1
APO07	Gestionar los recursos humanos.	1	1	1
APO08	Gestionar las relaciones.	1	1	1
APO09	Gestionar los acuerdos de servicio.	2	2	1
APO10	Gestionar los proveedores.	1	2	1
APO11	Gestionar la calidad.	1	1	1
APO12	Gestionar el riesgo.	3	1	1
APO13	Gestionar la seguridad.	3	1	1
APO14	Gestionar los datos.	1	1	1
BAI01	Gestionar los programas.	1	1	1
BAI02	Gestionar la definición de los requisitos.	1	1	1
BAI03	Gestionar la identificación y construcción de soluciones.	1	1	1
BAI04	Gestionar la disponibilidad y capacidad.	1	1	1
BAI05	Gestionar los cambios organizativos.	1	1	1
BAI06	Gestionar los cambios de TI.	2	1	1
BAI07	Gestionar la aceptación y la transición de los cambios de TI.	1	1	1
BAI08	Gestionar el conocimiento.	1	1	1
BAI09	Gestionar los activos.	3	2	1
BAI10	Gestionar la configuración.	1	1	1
BAI11	Gestionar los proyectos.	3	1	1
DSS01	Gestionar las operaciones.	1	1	1
DSS02	Gestionar las solicitudes e incidentes de servicio.	1	1	1
DSS03	Gestionar los problemas.	1	1	1
DSS04	Gestionar la continuidad.	1	1	1
DSS05	Gestionar los servicios de seguridad.	3	1	1
DSS06	Gestionar los controles de procesos de negocio.	1	1	1
MEA01	Gestionar la monitorización del rendimiento y la conformidad.	1	2	1
MEA02	Gestionar el sistema de control interno.	1	1	1
MEA03	Gestionar el cumplimiento de los requisitos externos.	1	1	1
MEA04	Gestionar el aseguramiento.	1	1	1

A11-DF10

Identificador		First mover (Primero en reaccionar)	Follower (Segidor)	Slow adopter (Adoptador lento)
EDM01	Garantizar el establecimiento y el mantenimiento del marco de gobierno.	1	1	1

EDM02	Asegurar la realización de beneficios.	1	1	1
EDM03	Asegurar la optimización del riesgo.	4	2	1
EDM04	Asegurar la optimización de los recursos.	1	1	1
EDM05	Asegurar la transparencia de las partes interesadas.	1	1	1
APO01	Gestionar el marco de gestión de TI.	4	3	1
APO02	Gestionar la estrategia.	1	1	1
APO03	Gestionar la arquitectura de la empresa.	1	1	1
APO04	Gestionar la innovación.	1	1	1
APO05	Gestionar el portafolio.	1	1	1
APO06	Gestionar el presupuesto y los costes.	1	1	1
APO07	Gestionar los recursos humanos.	1	1	1
APO08	Gestionar las relaciones.	1	1	1
APO09	Gestionar los acuerdos de servicio.	1	1	1
APO10	Gestionar los proveedores.	1	1	1
APO11	Gestionar la calidad.	1	1	1
APO12	Gestionar el riesgo.	4	3	1
APO13	Gestionar la seguridad.	5	2	1
APO14	Gestionar los datos.	1	1	1
BAI01	Gestionar los programas.	1	1	1
BAI02	Gestionar la definición de los requisitos.	1	1	1
BAI03	Gestionar la identificación y construcción de soluciones.	1	1	1
BAI04	Gestionar la disponibilidad y capacidad.	1	1	1
BAI05	Gestionar los cambios organizativos.	1	1	1
BAI06	Gestionar los cambios de TI.	1	1	1
BAI07	Gestionar la aceptación y la transición de los cambios de TI.	1	1	1
BAI08	Gestionar el conocimiento.	1	1	1

BAI09	Gestionar los activos.	5	2	1
BAI10	Gestionar la configuración.	1	1	1
BAI11	Gestionar los proyectos.	1	1	1
DSS01	Gestionar las operaciones.	1	1	1
DSS02	Gestionar las solicitudes e incidentes de servicio.	1	1	1
DSS03	Gestionar los problemas.	1	1	1
DSS04	Gestionar la continuidad.	1	1	1
DSS05	Gestionar los servicios de seguridad.	5	2	1
DSS06	Gestionar los controles de procesos de negocio.	1	1	1
MEA01	Gestionar la monitorización del rendimiento y la conformidad.	1	1	1
MEA02	Gestionar el sistema de control interno.	1	1	1
MEA03	Gestionar el cumplimiento de los requisitos externos.	1	1	1
MEA04	Gestionar el aseguramiento.	1	1	1

Anexo 12. Ficha de evaluación de expertos.

VALIDACION DE EXPERTO

Estimado Ingeniero:
A través de la presente me dirijo a usted con la finalidad de solicitarle su apoyo en la validación de la propuesta realizada en la investigación que lleva como título **DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA.**

Agradecemos su colaboración.

I. DATOS GENERALES DEL EXPERTO	
Nombres y apellidos:	
Grado académico y profesión:	
Áreas de experiencia laboral:	
Cargo Actual:	
Empresa donde labora:	
Tiempo de experiencia:	

II. OBJETIVOS:

2.1. Objetivo general:

- ✓ Diseñar proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

2.2. Objetivos específicos:

- ✓ Seleccionar una municipalidad peruana como caso de estudio.
- ✓ Diagnosticar las actividades relacionadas con seguridad de la información en la municipalidad peruana.
- ✓ Caracterizar los procesos de TI relacionados a la seguridad de la información alineados a COBIT 2019.
- ✓ Diseñar mediante gobierno de TI los requerimientos necesarios para la seguridad de la información basado en COBIT 2019.

- ✓ Validar el diseño de gestión de la seguridad de la información con prueba empírica y por juicio de expertos.

2.3. Objetivo del juicio de expertos: Verificar la validez del Diseño proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

2.4. Objetivo de la prueba: Determinar el Diseño proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

- De acuerdo son los siguientes indicadores califique cada uno de los ítems según corresponda.

III. CRITERIOS DE VALIDACIÓN DEL MODELO		
Indicador	**Criterio**	**Valoración**
CLARIDAD	El contenido del diseño de gestión de la seguridad es legibles y comprensibles.	Rango del 1 al 5 donde: 1=Muy Malo 2=Malo 3=Medio 4=Bueno 5=Muy Bueno
OBJETIVIDAD	El contenido del diseño de gestión de la seguridad cumple con la finalidad de sus actividades involucrados.	
COHERENCIA	El diseño de gestión de la seguridad respeta las normas internacionales y el contexto de la Municipalidad.	
PERTINENCIA	El diseño de gestión de la seguridad refleja los elementos del contexto de la Municipalidad y refleja la realidad.	
SUFICIENCIA	El diseño de gestión de la seguridad satisface el ámbito de Gobierno de TI dentro de la Municipalidad.	
RELEVANCIA	El diseño de gestión de la seguridad manifiesta importancia y prioridad según el contexto de la Municipalidad.	

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA.

PROCESOS	Factores de diseño según COBIT 2019	CRITERIOS						Comentarios / Observaciones
		CLARIDAD	OBJETIVIDAD	COHERENCIA	PERTENENCIA	SUFICIENCIA	RELEVANCIA	
Extender y Contextualizar	**Entender el contexto y la estrategia empresarial** ✓ Entender la estrategia empresarial ✓ Entender las metas empresariales ✓ Comprender el perfil de riesgo							
Determinar el Alcance	**Determinar el alcance inicial del sistema de gobierno** ✓ Considerar la estrategia empresarial.							

	✓ Considerar las metas de la empresa y aplicar la cascada de metas de COBIT 2019. ✓ Considerar el perfil de riesgo de la empresa. ✓ Considerar temas abiertos relacionados a TI.							
Afinar el Alcance	**Afinar el alcance del sistema de gobierno** ✓ Considerar el panorama de amenazas. ✓ Considerar los requerimientos regulatorios. ✓ Considerar el rol de las TI. ✓ Considerar el modelo de aprovisionamiento. ✓ Considerar los métodos de implementación para las TI. ✓ Considerar la estrategia de adopción de las TI. ✓ Considerar el tamaño de la empresa.							
Concluir el Sistema	**Concluir el diseño del sistema de gobierno** ✓ Valoración de los objetivos de gobierno y gestión							

ACEPTACIÓN	
OBSERVADO	
DISCONFORMIDAD	

Firma del Experto

Anexo 13. Juicio de expertos para la validación del diseño de procesos basado en COBIT 2019 para la gestión de la seguridad.

Experto 1: Dr. Ing. Ernesto Karlo Celi Arévalo

VALIDACION DE EXPERTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitarle su apoyo en la validación de la propuesta realizada en la investigación que lleva como título **DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA,** cuya finalidad es comprobar los criterios de consistencia, validez, fiabilidad, transferibilidad y neutralidad de los ítems considerados.

Agradecemos su colaboración.

I. DATOS GENERALES DEL EXPERTO	
Nombres y apellidos:	Ernesto Karlo Celi Arévalo
Grado académico y profesión:	Doctor
Áreas de experiencia laboral:	Seguridad de la información, Gestión de riesgos de TI, Auditoría de TI, Gestión por procesos
Cargo Actual:	Director del Instituto de Investigación de la Universidad Nacional Pedro Ruiz Gallo
Empresa donde labora:	Universidad Nacional Pedro Ruiz Gallo
Tiempo de experiencia:	30 años

II. OBJETIVOS:

2.1. Objetivo general:

- ✓ Diseñar proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

2.2. Objetivos específicos:

- ✓ Seleccionar una municipalidad peruana como caso de estudio.
- ✓ Diagnosticar las actividades relacionadas con seguridad de la información en la municipalidad peruana.
- ✓ Caracterizar los procesos de TI relacionados a la seguridad de la información alineados a COBIT 2019.
- ✓ Diseñar mediante gobierno de TI los requerimientos necesarios para la seguridad de la información basado en COBIT 2019.
- ✓ Validar el diseño de gestión de la seguridad de la información con prueba empírica y por juicio de expertos.

2.3. Objetivo del juicio de expertos: Verificar la validez del Diseño proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

2.4. Objetivo de la prueba: Determinar el Diseño Diseño proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

- De acuerdo son los siguientes indicadores califique cada uno de los ítems según corresponda.

III. CRITERIOS DE VALIDACIÓN DEL MODELO		
Indicador	**Criterio**	**Valoración**
CLARIDAD	El contenido del diseño de gestión de la seguridad son legibles y comprensibles.	Rango del 1 al 5 donde: 1=Muy Malo 2=Malo 3=Medio 4=Bueno 5=Muy Bueno
OBJETIVIDAD	El contenido del diseño de gestión de la seguridad cumplen con la finalidad de sus actividades involucrados.	
COHERENCIA	El diseño de gestión de la seguridad respetan las normas internacionales y el contexto de la Municipalidad.	
PERTINENCIA	El diseño de gestión de la seguridad refleja los elementos del contexto de la Municipalidad y refleja la realidad.	
SUFICIENCIA	El diseño de gestión de la seguridad satisface el ámbito de Gobierno de TI dentro de la Municipalidad.	
RELEVANCIA	El diseño de gestión de la seguridad manifiestan importancia y prioridad según el contexto de la Municipalidad.	

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA.

PROCESOS	Factores de diseño según COBIT 2019	CRITERIOS						Comentarios / Observaciones
		CLARIDAD	OBJETIVIDAD	COHERENCIA	PERTENENCIA	SUFICIENCIA	RELEVANCIA	
Extender y Contextualizar	**Entender el contexto y la estrategia empresarial** ✓ Entender la estrategia empresarial ✓ Entender las metas empresariales ✓ Comprender el perfil de riesgo	5	5	4	5	4	4	
Determinar el Alcance	**Determinar el alcance inicial del sistema de gobierno** ✓ Considerar la estrategia empresarial. ✓ Considerar las metas de la empresa y aplicar la cascada de metas de COBIT 2019. ✓ Considerar el perfil de riesgo de la empresa. ✓ Considerar temas abiertos relacionados a TI.	5	5	4	5	4	4	
Afinar el Alcance	**Afinar el alcance del sistema de gobierno** ✓ Considerar el panorama de amenazas. ✓ Considerar los requerimientos regulatorios. ✓ Considerar el rol de las TI. ✓ Considerar el modelo de aprovisionamiento. ✓ Considerar los métodos de implementación para las TI. ✓ Considerar la estrategia de adopción de las TI. ✓ Considerar el tamaño de la empresa.	5	5	5	5	4	4	
Concluir el Sistema	**Concluir el diseño del sistema de gobierno** ✓ Valoración de los objetivos de gobierno y gestión	5	4	4	5	4	4	

ACEPTACIÓN	X
OBSERVADO	
DISCONFORMIDAD	

Dr. Ing. Ernesto Karlo Celi Arévalo

Experto 2: Dr. Ing. Carlos Alberto Chirinos Mundaca

VALIDACION DE EXPERTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitarle su apoyo en la validación de la propuesta realizada en la investigación que lleva como título **DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA,** cuya finalidad es comprobar los criterios de consistencia, validez, fiabilidad, transferibilidad y neutralidad de los ítems considerados.

Agradecemos su colaboración.

I. DATOS GENERALES DEL EXPERTO	
Nombres y apellidos:	CARLOS ALBERTO CHIRINOS MUNDACA
Grado académico y profesión:	Doctor en Educación, Maestro en Ciencias con mención en Informática y Sistemas, Ingeniero Informático y de Sistemas
Áreas de experiencia laboral:	Auditoria de Sistemas de Información, Sistemas Inteligentes, Programación Lógica
Cargo Actual:	Consultor TI - Peritajes en sistemas
Empresa donde labora:	Poder Judicial
Tiempo de experiencia:	23 Años

II. OBJETIVOS:

2.1. Objetivo general:

- ✓ Diseñar proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

2.2. Objetivos específicos:

- ✓ Seleccionar una municipalidad peruana como caso de estudio.
- ✓ Diagnosticar las actividades relacionadas con seguridad de la información en la municipalidad peruana.
- ✓ Caracterizar los procesos de TI relacionados a la seguridad de la información alineados a COBIT 2019.
- ✓ Diseñar mediante gobierno de TI los requerimientos necesarios para la seguridad de la información basado en COBIT 2019.
- ✓ Validar el diseño de gestión de la seguridad de la información con prueba empírica y por juicio de expertos.

2.3. Objetivo del juicio de expertos: Verificar la validez del Diseño proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

2.4. Objetivo de la prueba: Determinar el Diseño del proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

- De acuerdo son los siguientes indicadores califique cada uno de los ítems según corresponda.

III. CRITERIOS DE VALIDACIÓN DEL MODELO		
Indicador	**Criterio**	**Valoración**
CLARIDAD	El contenido del diseño de gestión de la seguridad son legibles y comprensibles.	Rango del 1 al 5 donde: 1=Muy Malo 2=Malo 3=Medio 4=Bueno 5=Muy Bueno
OBJETIVIDAD	El contenido del diseño de gestión de la seguridad cumplen con la finalidad de sus actividades involucrados.	
COHERENCIA	El diseño de gestión de la seguridad respetan las normas internacionales y el contexto de la Municipalidad.	
PERTINENCIA	El diseño de gestión de la seguridad refleja los elementos del contexto de la Municipalidad y refleja la realidad.	
SUFICIENCIA	El diseño de gestión de la seguridad satisface el ámbito de Gobierno de TI dentro de la Municipalidad.	
RELEVANCIA	El diseño de gestión de la seguridad manifiestan importancia y prioridad según el contexto de la Municipalidad.	

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA.

PROCESOS	Factores de diseño según COBIT 2019	CRITERIOS						Comentarios / Observaciones
		CLARIDAD	OBJETIVIDAD	COHERENCIA	PERTENENCIA	SUFICIENCIA	RELEVANCIA	
Extender y Contextualizar	**Entender el contexto y la estrategia empresarial** ✓ Entender la estrategia empresarial ✓ Entender las metas empresariales ✓ Comprender el perfil de riesgo	4	4	5	4	5	4	
Determinar el Alcance	**Determinar el alcance inicial del sistema de gobierno** ✓ Considerar la estrategia empresarial. ✓ Considerar las metas de la empresa y aplicar la cascada de metas de COBIT 2019. ✓ Considerar el perfil de riesgo de la empresa. ✓ Considerar temas abiertos relacionados a TI.	4	4	5	4	5	4	
Afinar el Alcance	**Afinar el alcance del sistema de gobierno** ✓ Considerar el panorama de amenazas. ✓ Considerar los requerimientos regulatorios. ✓ Considerar el rol de las TI. ✓ Considerar el modelo de aprovisionamiento. ✓ Considerar los métodos de implementación para las TI. ✓ Considerar la estrategia de adopción de las TI. ✓ Considerar el tamaño de la empresa.	4	4	5	4	5	5	
Concluir el Sistema	**Concluir el diseño del sistema de gobierno** ✓ Valoración de los objetivos de gobierno y gestión	4	4	5	4	5	5	

ACEPTACIÓN	X
OBSERVADO	
DISCONFORMIDAD	

Dr. Ing. Carlos Alberto Chirinos Mundaca
DNI° 16721607
CIP N° 82847

Experto 3: Dr. Ing. Alberto Enrique Samillan Ayala

2.3. Objetivo del juicio de expertos: Verificar la validez del Diseño proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

2.4. Objetivo de la prueba: Determinar el Diseño Diseño proceso de gobierno de TI basado en COBIT 2019 para gestionar la seguridad de la información en una municipalidad peruana.

- De acuerdo son los siguientes indicadores califique cada uno de los ítems según corresponda.

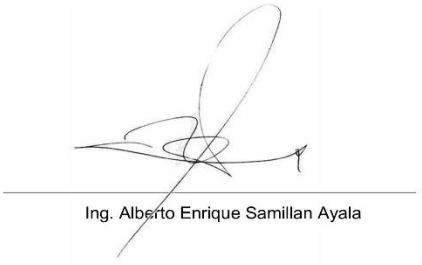
III. CRITERIOS DE VALIDACIÓN DEL MODELO		
Indicador	**Criterio**	**Valoración**
CLARIDAD	El contenido del diseño de gestión de la seguridad son legibles y comprensibles.	Rango del 1 al 5 donde: 1=Muy Malo 2=Malo 3=Medio 4=Bueno 5=Muy Bueno
OBJETIVIDAD	El contenido del diseño de gestión de la seguridad cumplen con la finalidad de sus actividades involucrados.	
COHERENCIA	El diseño de gestión de la seguridad respetan las normas internacionales y el contexto de la Municipalidad.	
PERTINENCIA	El diseño de gestión de la seguridad refleja los elementos del contexto de la Municipalidad y refleja la realidad.	
SUFICIENCIA	El diseño de gestión de la seguridad satisface el ámbito de Gobierno de TI dentro de la Municipalidad.	
RELEVANCIA	El diseño de gestión de la seguridad manifiestan importancia y prioridad según el contexto de la Municipalidad.	

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

DISEÑO DE GOBIERNO DE TI BASADO EN COBIT 2019 PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA MUNICIPALIDAD PERUANA.

PROCESOS	Factores de diseño según COBIT 2019	CRITERIOS						Comentarios / Observaciones
		CLARIDAD	OBJETIVIDAD	COHERENCIA	PERTENENCIA	SUFICIENCIA	RELEVANCIA	
Extender y Contextualizar	**Entender el contexto y la estrategia empresarial** ✓ Entender la estrategia empresarial ✓ Entender las metas empresariales ✓ Comprender el perfil de riesgo	5	5	5	5	5	5	
Determinar el Alcance	**Determinar el alcance inicial del sistema de gobierno** ✓ Considerar la estrategia empresarial. ✓ Considerar las metas de la empresa y aplicar la cascada de metas de COBIT 2019. ✓ Considerar el perfil de riesgo de la empresa. ✓ Considerar temas abiertos relacionados a TI.	5	5	5	5	5	5	
Afinar el Alcance	**Afinar el alcance del sistema de gobierno** ✓ Considerar el panorama de amenazas. ✓ Considerar los requerimientos regulatorios. ✓ Considerar el rol de las TI. ✓ Considerar el modelo de aprovisionamiento. ✓ Considerar los métodos de implementación para las TI. ✓ Considerar la estrategia de adopción de las TI. ✓ Considerar el tamaño de la empresa.	5	5	5	5	5	5	
Concluir el Sistema	**Concluir el diseño del sistema de gobierno** ✓ Valoración de los objetivos de gobierno y gestión	5	5	5	5	5	5	

ACEPTACIÓN	Aceptado
OBSERVADO	
DISCONFORMIDAD	



Ing. Alberto Enrique Samillan Ayala

Anexo 14. Perfil profesional de los expertos

Dr. Ing. Ernesto Karlo Celi Arévalo

Contactar

www.linkedin.com/in/ernesto-karlo-celi-arévalo-0b6a0277 (LinkedIn)

Aptitudes principales

Linux

AutoCAD

Java

Publications

Aplicación de la plataforma Moodle para mejorar el proceso enseñanza-aprendizaje en los estudiantes

Application of Dashboards and Scorecards for Learning Models IT Risk Management: A User Experience

Information Security Policies Based on the Behavior of IT Users in the Microfinance Sector of Lambayeque-Peru

Evaluación del nivel de capacidad de los procesos de TI, mediante el marco de referencia COBIT PAM

La gestión de riesgos de TI y la efectividad de los sistemas de seguridad de la información: Caso procesos críticos en las pequeñas entidades financieras de Lambayeque, Perú

Ernesto Karlo Celi Arévalo

Auditoría de TI, gestión de riesgos de TI, Gestión de la continuidad del negocio

Perú

Experiencia

Universidad Nacional Pedro Ruíz Gallo

8 años

Director de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional Pedro Ru

2016 - Present (8 años)

Coordinador de la Maestría en Ingeniería de Sistemas con mención en Gerencia de tecnologías de l

2018 - 2020 (2 años)

Independiente

Ingeniero en Computación y Sistemas

octubre de 1994 - Present (30 años 1 mes)

Auditoría de TI

Evaluación de Sistemas de gestión de riesgos y controles de TI

Evaluación de continuidad de procesos

Evaluación de seguridad de TI

Consultoria en TI

Elaboración de expedientes técnicos TI

Universidad Nacional Pedro Ruiz Gallo

Docente universitario

octubre de 1994 - Present (30 años 1 mes)

Director de la Escuela Profesional de Ingeniería de Sistemas

Decano de la Facultad de Ingeniería Civil, Sistemas y Arquitectura

Diversas entidades financieras

Auditor externo de TI, con especialidad en SGSI, Gestión de riesgos y Gestion Continuidad del negoci

enero de 2001 - Present (23 años 10 meses)

Auditoria de seguridad de TI, gestión de riesgos, continuidad de negocio

Consorcio ATA KUKOVA

Proyectista

Page 1 of 3

mayo de 2008 - agosto de 2012 (4 años 4 meses)
Lima

Proyectista en la especialidad de Sistemas de Información, en diversos proyectos de construcción de hospitales Categoría III. Incluye los expedientes técnicos del Sistema de Información Hospitalario (HIS), Sistema RIS/PACs para la administración de imágenes médicas y Sistema para la gestión de colas

Universidad Nacional Pedro Ruíz Gallo
Decano de la Facultad de Ingeniería Civil, de Sistemas y Arquitectura
2008 - 2011 (3 años)

Colegio de Ingenieros del Perú - Consejo departamental de Lambayeque
Presidente del Capítulo de Ingeniería Industrial y de Sistemas del Colegio de Ingenieros del Perú
2006 - 2007 (1 año)

Asociación de Universidades del Sur del Ecuador y Norte del Perú
Secretario Ejecutivo por Perú en la Asociación de Universidades del Sur del Ecuador y Norte del P
2004 - 2006 (2 años)

Universidad Nacional Pedro Ruíz Gallo
Director de la Escuela Profesional de Ingeniería de Sistemas
2001 - 2006 (5 años)

Educación

Universidad Privada Antenor Orrego
Ingeniero de Computación y Sistemas, Control, Seguridad, Riesgos, Auditoria de TI · (1988 - 1993)

Universidad Nacional Pedro Ruíz Gallo
Doctorado en Administración · (2014 - 2016)

SCRUMstudy
SCRUM Fundamentals Certified, Ingeniería de software · (2019 - 2019)

Colegio de Ingenieros del Perú

Especialización en Gestión de Servicios de Tecnologías de Información con ITIL 2011 · (2015 - 2015)

Universidad Católica Santo Toribio de Mogrovejo
Especialización en Auditoría de Tecnologías de Información y Seguridad Informática · (2013 - 2013)

Dr. Ing. Carlos Alberto Chirinos Mundaca

Contactar

www.linkedin.com/in/carlos-chirinosmundaca (LinkedIn)

Certifications

Academia Ágil®. Curso "La Semilla Ágil: Contexto de Scrum"

Academia Ágil®. Curso "La Semilla Ágil: Contexto de Scrum"

Carlos Alberto Chirinos Mundaca

Consultor TI - Seguridad de la Información

Área metropolitana de Lima

Experiencia

InfoConsulting ICSAC

Perito Informático, de Sistemas de Información y Comunicaciones

enero de 2010 - Present (14 años 10 meses)

Perú

Educación

Universidad Privada Antenor Orrego

Ingeniería de Computación y Sistemas

Escuela de Posgrado de la Universidad Nacional Pedro Ruiz Gallo

Maestría en Informática y Sistemas

Universidad César Vallejo

Doctorado en Educación

Universidad Privada Antenor Orrego

Maestría en Ingeniería de Sistemas con mención en Sistemas de Información (c), Escuela de Posgrado

Universidad Nacional de Piura

Doctorado en Tecnologías de la Información y Comunicaciones (t), Escuela de Posgrado

Ing. Alberto Enrique Samillan Ayala

Contactar

www.linkedin.com/in/kikesamillan (LinkedIn)

Aptitudes principales

Liderazgo
Microsoft Office
Microsoft Excel

Alberto Enrique Samillan Ayala

Ex Director General de TI en MIDAGRI, Consultor Gerencia de Proyectos, MBA, PMP®, Cred. 2864844, Espec. en Gestión Pública. Docente Universitario, Investigador RENACYT P0063355
Perú

Extracto

Hola, me apasiona los proyectos informáticos de innovación que buscan mejorar la calidad de vida de las personas y la forma como estas crean oportunidades de negocios. Mi experiencia en el campo universitario y en el sector público busca crear espacios de innovación en los jóvenes

Experiencia

MIDAGRI
Director General de Tecnologias de la Informacion
octubre de 2022 - Present (2 años 1 mes)

CONCYTEC
Investigador RENACYT
octubre de 2022 - Present (2 años 1 mes)

Profesional independiente
Consultor Gerencia de Proyectos, PMP-PMI
noviembre de 2020 - Present (4 años)
Chiclayo, Lambayeque, Perú

Universidad Nacional Pedro Ruiz Gallo
Catedratico Universitario
abril de 1998 - Present (26 años 7 meses)
Director de Escuela
Jefe de Departamento
Jefe Centro de Produccion
Jefe Oficina de Asuntos Pedagogicos

Municipalidad Provincial de Chiclayo
Gerente de Tecnologias de la Informacion
diciembre de 2018 - octubre de 2022 (3 años 11 meses)

Provincia de Chiclayo, Peru

Universidad Nacional Pedro Ruz Gallo
Magister en Adminitracion de Empresas
marzo de 2001 - marzo de 2003 (2 años 1 mes)

Educación

Project Management Institute
Project Management Professional · (2020 - 2023)

ESAN Graduate School of Business
Gestion Publica, Gestión Publica · (marzo de 2021 - julio de 2021)

ESAN Graduate School of Business
Gestion Publica · (marzo de 2021 - julio de 2021)

Universidad Nacional Pedro Ruíz Gallo
Doctorado, Ciencias Ambientales · (2014 - 2016)

New Horizons Computer Learning Center of Raleigh-Durham-Chapel Hill
ITIL, ITIL · (2014 - 2014)