FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Diseño de un Modelo de Auditoría de TI para el Cumplimiento de Normas y Políticas de una Empresa Retail Peruana

PARA OPTAR EL TÍTULO PROFESIONAL

DE INGENIERO(A) DE SISTEMAS

Autor(a) (es):
Bach. Rabanal Senmache Marry Cecy
ORCID: https://orcid.org/0000-0003-2847-7372

Bach. Sanchez Rubio Omar Alberto
ORCID: https://orcid.org/0000-0002-3797-551X

Asesor (a):
Mg. Ing. Aguinaga Tello Juan Adolfo
ORCID: https://orcid.org/0000-0003-2902-9264

Línea de Investigación:
Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú

2024

DISEÑO DE UN MODELO DE AUDITORÍA DE TI PARA EL CUMPLIMIENTO DE NORMAS Y POLITICAS DE UNA EMPRESA RETAIL PERUANA

Aprobación del jurado

MG. ASENJO CARRANZA ENRIQUE DAVID

Presidente del Jurado de Tesis

Mg. ARCILA DIAZ JUAN CARLOS

Secretario del Jurado de Tesis

Mg. ALVA ZAPATA JULIANA DEL PILAR

Vocal del Jurado de Tesis

DECLARACIÓN JURADA DE ORIGINALIDAD

Rabanal Senmache Marry Cecy y Sánchez Rubio Omar Alberto, suscriben la DECLARACIÓN JURADA, somos egresado (s) del Programa de Estudios de **Ingeniería de Sistemas** de la Universidad Señor de Sipán S.A.C, declaramos bajo juramento que somos autores del trabajo titulado:

DISEÑO DE UN MODELO DE AUDITORÍA DE TI PARA EL CUMPLIMIENTO DE NORMAS Y POLITICAS DE UNA EMPRESA RETAIL PERUANA

El texto de nuestro trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación 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:

Rabanal Senmache Marry Cecy	DNI: 47461274	
Omar Alberto Sánchez Rubio	DNI: 44621568	

Pimentel, 02 de Mayo del 2024.

Dedicatoria

Dedico esta tesis:

A mis padres Luis Alberto Sánchez Enríquez y a mi madre Blanca Zuzety Rubio por el apoyo brindado.

A mis hermanos por el constante apoyo para terminar mi carrera profesional.

A mi compañera Marry Cecy Rabanal Senmache por su apoyo y aliento para seguir adelante en esta etapa profesional.

Atte.: Sánchez Rubio Omar A.

Dedico esta tesis:

A mi esposo José Emiliano Cabrera Barboza, quien es mi compañero de vida y paradigma a seguir.

A mi madre María Senmache que es la inspiración de mi vida y por su inmenso apoyo en el proceso y desarrollo de mi etapa de formación profesional.

A mi padre y hermanos que son los que me impulsan a seguir adelante y ser ejemplo para ellos.

A Lenin y Karina que son mi gran motivación de vida, y a quienes siempre llevare presente en mi corazón.

Atte.: Rabanal Senmache Marry C.

Agradecimiento

Agradecemos a Dios, porque es nuestra fortaleza y guía, para seguir adelante con todos los objetivos propuestos.

Agradecemos a nuestros docentes de la USS, por su apoyo en nuestro proceso de formación profesional.

Agradecemos al Ingeniero Junior Cachay por sus enseñanzas y apoyo incondicional para el desarrollo de nuestra investigación.

Agradecemos al Ingeniero Jorge Arana, por ser participe y permitirnos poder desarrollar nuestra propuesta en su prestigiosa Organización.

Índice

Índice de tablas

Índice de figuras

Resumen

Las auditorías de Tecnologías de la Información logran la competitividad y sostenibilidad de las organizaciones, porque son parte esencial de la gestión empresarial y de la cadena de valor que les permite cumplir sus objetivos; Sin embargo, la calidad de las auditorías en los servicios de información de TI muchas veces se ve afectada cuando existen dificultades para identificar el diseño de un estándar óptimo para la organización. Frente a esto, se propone diseñar un modelo de auditoría informática que evalúe el cumplimiento de las políticas de las empresas retail peruanas. Se aplicó un marco y estándar internacional enfocado en auditorías de TI, que refleja las mejores prácticas de COBIT 2019 e ISO 19011, tomando como referencia la estructura, políticas y objetivos organizacionales. Como resultado el modelo de auditoría de TI logró cumplir con todos los objetivos estipulados, brindando un diseño riguroso que cumple con las expectativas de la organización, teniendo un resultado de 3.98 en juicio de expertos indicando que el modelo es bastante adecuado para su implementación. Se concluye que el modelo fue diseñado, validado y ejecutado obteniendo un 95.5% de cumplimiento de las normas y políticas de la organización. Hay que tener en cuenta que a la hora de implementar un determinado modelo de auditoría informática se debe realizar un buen diagnóstico para identificar qué cláusulas de los dominios ISO 19011 y COBIT 2019 son las más adecuadas. Se afirma que la norma internacional ISO 19011 y el marco COBIT 2019 están alineados y pueden cohesionarse para crear modelos de auditoría de TI eficientes que puedan aplicarse para minimizar los riesgos de Sistemas de Información de las empresas retail peruanas.

Palabras Clave: Auditoría de TI, ISO 19011, COBIT 2019, cumplimiento, políticas.

Abstract

Information Technology audits achieve the competitiveness and sustainability of organizations, because they are an essential part of business management and the value chain that allows them to meet their objectives; However, the quality of audits in IT information services is often affected when there are difficulties in identifying the design of an optimal standard for the organization. Faced with this, it is proposed to design a computer audit model that evaluates compliance with the policies of Peruvian retail companies. An international framework and standard focused on IT audits was applied, which reflects the best practices of COBIT 2019 and ISO 19011, taking as reference the structure, policies and organizational objectives. As a result, the IT audit model managed to meet all the stipulated objectives, providing a rigorous design that meets the expectations of the organization, having a result of 3.98 in expert judgment indicating that the model is quite suitable for its implementation. It is concluded that the model was designed, validated and executed, obtaining 90% compliance with the company's policies and standards. It must be taken into account that when implementing a certain computer audit model, a good diagnosis must be carried out to identify which clauses of the ISO 19011 and COBIT 2019 domains are the most appropriate. It is stated that the international standard ISO 19011 and the COBIT 2019 framework are aligned and can cohere to create efficient IT audit models that can be applied to minimize the IS risks of Peruvian retail companies.

Keywords: IT auditing, ISO 19011, COBIT 2019, compliance, policies.

I. INTRODUCCIÓN

1.1. Realidad problemática.

Las Tecnologías de Información (TI) logran la competitividad y sostenibilidad de las organizaciones, porque forman parte del corazón de la gestión empresarial y de la cadena de valor que les permite cumplir sus objetivos. A su vez, también posibilita un riesgo de impacto elevado, en cuanto a incidentes y amenazas en los Sistemas de Información (SI), por ello, es preocupante para las empresas resguardar sus activos de TI.

Así mismo, no solo les corresponde a las empresas velar por la defensa de la ciberseguridad, también es preocupación de las naciones que influyen en la gobernanza nacional, la cual vela por la seguridad de SI de los ciudadanos. Para ello, se han desarrollado centros de ciberdefensa a nivel mundial que se enfocan en el cumplimiento de normas, estándares o políticas de manera rigurosa. En Alemania, el centro nacional de Ciberdefensa, fue creado para proteger la infraestructura de los SI. España implementó el Centro Nacional de Infraestructura Crítica, para las mejoras de la ciberdefensa. En Francia se inauguró en el año 2011 la Agencia (ANSSI) dedicado a la creación de estrategias de Seguridad de SI. Colombia se dedica exclusivamente al análisis del ciberespacio y finalmente Perú cuenta con un grupo de coordinación de emergencia de redes teleinformáticas peCERT como una forma de estrategia para la ciberdefensa [1].

En cierto modo, a pesar que se han creado estrategias institucionales en entidades públicas o políticas gubernamentales, aún no existen criterios técnicos, en torno al marco de referencia adecuado, en los que se aplican procedimientos en el uso de las TI para gestionar de forma eficaz la ciberseguridad en el mundo [2].

Según un reporte de seguridad de ESET, refiere que, a nivel de Latinoamérica, un (60%) de entidades encuestadas, presentaron incidencias de acceso indebido en sus sistemas, complementado a un (56%) que han sido víctimas de robo de información y un (54%) tuvieron incidencias de infección con códigos maliciosos. El aumento y la exposición

de las amenazas en los SI, no solo afecta a las empresas internacionales, en el Perú, el (61%) de las empresas aplican y establecen políticas rigurosas en los SI. De igual modo, el (29%) tiene un plan en el aspecto de planificación ante incidentes y el (27%) de empresas considera incluir nuevas medidas de iniciativas empresariales [3]

Figura 1.Incidencia de seguridad en empresas en Latinoamérica en 2019.

Fuente*:* Tomado de [3].

En ese sentido, para maximizar el resguardo de los activos empresariales y recursos de TI, existen diversos tipos de auditorías de TI que nos permite evaluar y examinar de manera rigurosa los SI, ayudando a contrarrestar los riesgos en los sistemas, para conseguir la integridad de la información y lograr detectar las amenazas y a su vez las fortalezas sobresalientes de la empresa. Según [4], menciona que el sujeto más indispensable para

realizar una gestión eficiente de los SI, es el auditor, porque este debe poseer conocimientos adecuados en auditoría de TI, tener ciertas habilidades y competencias para poder realizar la aplicación de controles y procedimientos que se relacionan con los procesos de riesgo, permitiéndole dar valor agregado a la organización y minimizar las amenazas en servicios de TI.

No obstante, el desarrollo de una cultura de concientización por parte de los empleados en el aspecto de los riesgos en los SI, implica un factor crucial, dado que, los delincuentes informáticos se aprovechan del poco conocimiento digital y del exceso de confianza que tiene el ser humano, para engañar a sus víctimas y aprovecharse sigilosamente de estas debilidades, concretando sus objetivos de atacar las redes corporativas.

Por otra parte, Consulting Partner, EY Perú, indica que las empresas que realizan capacitaciones al personal de forma constante ante ataques maliciosos, tienen un riesgo reducido de (34%) y un (29%) en la detección de incidencias de seguridad. Sin embargo, las empresas que cuentan con encargados en la seguridad de los SI, tienen un porcentaje regular en seguridad con un valor de (61%), en comparación con las empresas que no tienen esta figura, cuentan con un (38%) de seguridad ante este tipo de riesgos [5]. Para contrarrestar lo antes mencionado, se implementa la auditoría de TI con un nuevo enfoque basada en el riesgo, la cual se centra en el logro de objetivos institucionales, realizar evaluaciones de riesgos, desarrollar y aplicar auditorías a medida que permita que el auditor sea capaz de evaluar y gestionar cualquier tipo de riesgo de TI [6].

Paralelamente, las organizaciones internacionales especializadas se han esforzado en crear nuevos modelos ingeniería que ayuden a enfrentar los delitos informáticos. Para ello se han apoyado con estándares certificados, como la norma ISO, con su estándar de seguridad de TI basadas en la normativa 27000, la cual propone la mejora en los SI de las entidades [7]. Consecuentemente existe la guía de ciberamenazas aplicadas a países en desarrollo ITU National Cybersecurity Strategy Guide, el cual es un modelo de referencia que se enfoca en salvaguardar los activos de las entidades [1].

Por otro lado, se han desarrollado nuevos modelos de auditorías de TI basados en un marco de trabajo internacional, que ayudan a mitigar y controlar riesgos en los sistemas de información las cuales son CSAM y CATRAM, donde se implementan varios marcos de trabajo internacionales, como son CSF NIST, COBIT 5, TOGAF, ISO27001, ISO 19011.

Tomando a [8] en su investigación, Methodology Based on the Nist Cybersecurity Framework as a Proposal for Cybersecurity Management in Government Organizations, desarrollado en Perú, indica que la mayoría de las entidades gestionan la ciberseguridad sin procesos definidos, obteniendo una gestión sin indicadores y muy deficiente. Frente a ello, proponen la implementación del marco NIST, para identificar y administrar el riesgo de ciberamenazas. Se utilizó el método de diseño de investigación experimental para manejar variables de tipo causa – efecto, por consiguiente, se aplicó una encuesta a 19 organizaciones gubernamentales, donde se plantearon preguntas sobre el estado actual de la gestión de la ciberseguridad con una escala a utilizar: Nivel 0 totalmente en desacuerdo, nivel 01 en desacuerdo, nivel 02 indeciso, nivel 3 de acuerdo, nivel 04 totalmente de acuerdo. Posteriormente se evalúa la dimensión del framework de NIST, se observa el plan para la gestión de ciberseguridad y finalmente se evalúa la dimensión del nivel de incidencia. Como resultado, se muestra que el 36,8% de los encuestados no están de acuerdo, el 31,6% (6) se encuentran en una posición indecisa, el 15,8% (3) están de acuerdo, y el 10,5% (2) totalmente de acuerdo. Consecuentemente, “el enfoque de la Ciberseguridad” muestra que un 36,8% (7) se encuentran en desacuerdo; 36,8% (7) un nivel indeciso, se puede decir que existe una influencia entre la ciberseguridad y el marco NIST. Se concluye que algunas empresas no han implementado estándares y políticas que ayuden a minimizar incidencias de ciberseguridad en la entidad, por ende, no cuentan con estadísticas de incidentes de riesgo; esto se debe a una mala gestión por parte del personal no capacitado. Se recomienda que las organizaciones gubernamentales adopten la metodología del framework de ciberseguridad de NIST para medir la mejora y la gestión de la seguridad cibernética.

Del mismo modo, [9] en su investigación, A Comprehensive Cybersecurity Audit Model

to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM) en Sevilla – España. Indica que el incremento en la complejidad y número de ataques cibernéticos, están retando a los modelos de auditoría aplicados a la ciberseguridad, producto que, se evidencia la necesidad crítica de modelos más rigurosos que ayuden a contrarrestar las amenazas y vulnerabilidades en el ciberespacio, pues se demuestra que no todos los marcos existentes ofrecen una solución única para planificar y realizar auditorías de seguridad cibernética. Por ende, se implementa un programa integral de ciberseguridad, utilizando el marco NIST de ISACA, el cual es propuesto a la organización como modelo de auditoría CSAM, este modelo aplica 18 dominios, de los cuales 1 es específico para las naciones unidas y los 17 pueden ser aplicados a cualquier organización. Se aplica la evaluación a los controles, sub-controles y guía, la cual es calculada asignando puntajes a un nivel de madurez específico: Nivel Inmaduro (0-30). En desarrollo (31-71). Maduro (71-90). Avanzado (90 - 100), luego se emplea un modelo de comparación de marcos (CSF, versión 1.1: NIST (2017) y la metodología Audist First). Como resultado se obtiene que CSAM se debe emplear para evaluar y planificar auditorías de ciberseguridad en todas partes de la organización, ya sea para un determinado dominio o para una auditoría integral de la organización. Se concluye que el modelo se probó, implementó y validó junto con el modelo (CATRAM) cabe decir que las auditorías de TI se están redefiniendo, porque no hay pautas claves sobre qué áreas dominios o subdominios deben incluir en las auditorías, por ello en trabajos futuros se fomenta una mayor investigación en las áreas de aseguramiento y auditorias de ciberseguridad.

Según [10] en el desarrollo de su investigación, Proposal of a framework for the internal audit to the service management of the department of information technologies, en Ecuador. Alude que la calidad de auditorías en los servicios de TI, suelen verse afectadas cuando existen dificultades para identificar las dimensiones en la creación de diseños de estándares en los servicios de TI. Por esta razón, plantea la implementación de un framework para auditorías internas que permitan identificar, analizar y evaluar los servicios de TI. Para ello se seleccionaron los modelos y estándares (COBIT5, ITIL v3, ISO/IEC 20000), donde se

aplica la metodología de análisis descriptivo entre ITIL e ISO, proponiendo un modelo comparativo a través de mapeo de normas, fundamentos teóricos y estándares de GSTI, donde se determinan los puntos más relevantes de las dimensiones, buscando la compatibilidad y combinación más eficaz de estándares y normas. Como resultado se obtuvo que la relación de procesos entre los tres marcos de referencia es fuerte y relevante, con respecto a las dimensiones planteadas, se logró identificar tres situaciones. 1) Existe una relación con el framework ITIL, 2) Las ISO aplicadas no aportaron mayor valor, por ende, su relación se toma como un valor referencial; y 3) Relevancia en la gestión y solución de problemas. Se concluye que se aplicó un diseño riguroso que aplica prácticas relacionadas a los servicios de TI e instrumentos relacionados al negocio.

Por otro lado, [11] en su investigación, A Proposed Cyber security framework for auditing in financial institutions, en Ciudad del Cabo – África. Menciona que producto del incremento de los delitos cibernéticos en las instituciones financieras, ha traído como consecuencia el cuestionamiento de la eficacia de las auditorias de TI por falta de auditores expertos que permitan garantizar la seguridad cibernética en las organizaciones. Al encontrar estas limitaciones en marcos existentes que ya han sido probados, se propone la implementación de un framework más completo para reforzar la credibilidad de las auditorías de TI en las entidades financieras. Para crear el modelo se identificaron las limitaciones del marco COBIT 5, el marco de seguridad cibernética NIST y las normas ISO colocándolas en una tabla denominada constructos, estas teorías y marcos se integraron en un modelo integrador que guía el desarrollo del modelo conceptual. El modelo integrador propuesto se alineó con el marco de seguridad cibernética de NIST, donde se evalúan los riesgos de TI como una construcción dependiente y los atributos individuales como los factores internos con construcciones independientes. Como resultado se obtuvo que los factores internos junto con los atributos individuales contribuyeron a una auditoría eficaz de la seguridad cibernética. Finalmente, esta investigación se centra en auditar la seguridad cibernética financiera, por lo que podría no ser generalizable a otros campos.

[12] manifiesta en su trabajo de investigación, Implementation of COBIT 5 Framework for Academic Information System Audit Perspective: Evaluate, Direct, and Monitor, en Indonesia. Las instituciones educativas enfrentan varios desafíos como proveedores de educación, porque las actividades principales están manejadas por el área administrativa ya respaldadas por los servicios de TI en la forma de sistemas de información académica. Por este motivo es que se propone realizar una auditoría de TI en la institución educativa Dinámica Bangsa Jambi, utilizando el estándar COBIT 5. Para ello se aplica un cuestionario de escala de medida de la capacidad, la cual se utiliza para obtener respuestas claras y firmes de los problemas específicos de los servicios de TI de la institución. Se determina e identifica al objeto (problemas existentes), luego se selecciona el marco a implementar y se ejecuta un análisis del nivel de capacidad y un análisis de brechas. Se realiza la identificación de diagramas RACI F, este ilustra los roles y prácticas en los procesos de dominio a evaluar, dirigir y monitorear. Como resultado tenemos que el nivel de capacidad actual conduce al proceso gestionado de nivel II, con un valor de 1.80, obteniendo resultados en base a las prácticas de gobierno. En el proceso EDM 01: con un valor de 2,28; En el proceso EDM02: El nivel de capacidad, con un valor de 2,55; En el proceso EDM03: El nivel de capacidad, con un valor de 2.06, En el proceso EDM04: El nivel de capacidad, con un valor de 1,61 y 5. El nivel actual de capacidad en el proceso EDM05 con un valor de 0,50. Se concluye que los procesos de TI, se han logrado, gestionado y llevado a cabo adecuadamente alcanzando los objetivos deseados.

Consecuentemente, [13] en su investigación, Audit sistem informasi menggunakan cobit 5 pada perusahaan penyedia layanan internet, en la Universitas Bunda Mulia de Indonesia. Manifiesta que existen complicaciones en la ejecución eficiente de la gobernanza de TI en las entidades y convirtiéndose en la principal causa de dificultad de las partes interesadas. Por esta razón se propone realizar una auditoría de sistemas enfocándose en el dominio DDS y en el subdominio DDS03 - COBIT 5. El resultado obtenido es que no se logró cumplir el nivel esperado por la organización en cuanto a la gestión de incidencias, Dos de

los 5 subdominios del marco de COBIT 5 se obtuvo 1 nivel de brecha (nivel actual 2, lo ideal 3). Por otro lado, de los 3 subdominios restantes se obtuvo una brecha de dos (nivel actual 1, lo ideal 3). En el aspecto del análisis de deficiencias se obtuvo un promedio de 1.4, dos de los 5 subdominios de obtuvo 1 de brecha (capacidad actual 2, esperado 3). Por otro lado, los 3 subdominios restantes obtuvieron 2 de brecha (actual 1, esperado 3). La conclusión que llegó esta investigación es que algunos procesos son hechos por la empresa y la mayoría están hechas de forma deficiente. Por ende, el autor recomienda lo siguiente: La empresa debería identificar, evaluar y procesar las mejoras que pueden emplearse para solucionar los problemas, la empresa debe organizarse para elaborar un diagrama para que los empleados conozcan los problemas y sobre todo conocer el tiempo que dura resolver esos problemas. Y finalmente realizar reuniones de directivos de la empresa para que discutan los problemas actuales que existen y hacer un plan de contingencia para minimizarlos.

En la investigación, Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company. En Indonesia. Existen pérdidas importantes de recursos financieros y sobre todo la inseguridad de los servicios de TI, producto del crecimiento de los sistemas tecnológicos. Por esta razón, se define la determinación del objeto de control correcto para la base de un programa de control de riesgos adecuado para respaldar los requisitos del estándar del SGSI ISO 27001. Los resultados se dieron de acuerdo a las cláusulas 11, 12, 7 ,8 y 9 de la norma ISO 270005:2011: a. Cláusula 11. Comunicación y consulta de riesgos: Como resultado se obtuvo que las organizaciones de telecomunicaciones necesitan llevar a cabo un gobierno de riesgos relacionados con la SI para respaldar los recursos de TI, de modo que permanezcan protegidos. b. Cláusula 12. Revisión y seguimiento de riesgos: Se llegó como resultados que requieren realizar un plan para mitigar y controlar los riesgos. c. Establecimiento del contexto: discute y concluye qué contextos se determinarán con base en la referencia a las etapas del gobierno de SI utilizado. d. Cláusula 8. Evaluación de riesgos. i. Identificación de riesgos: Se identificó que 26 activos tienen riesgos potenciales. Además, se hallaron 92 tipos de amenazas, 133 vulnerabilidades.

ii. Análisis de riesgos: Se establece que 38 escenarios de riesgos tienen un índice muy alto en las organizaciones. e. Cláusula 9. Tratamiento del riesgo: en este punto los investigadores se basan en recomendaciones para tener medidas de control de riesgos. Se concluye que, la investigación está centrada en la adecuada aplicación del control del gobierno de riesgos de la SI en las empresas de telecomunicaciones, ya que mediante el modelo obtenido se lograra identificar y clasificar de manera eficiente cada uno de los riesgos encontrados en la empresa, para efectuar un plan para su mitigación [14].

Según [15] en su investigación Evaluation model of computer audit methodologies based on inherent risk, en Sevilla – España. La selección incorrecta de herramientas en la implementación de modelos de auditoría de TI, han ocasionado resultados desastrosos, provocando pérdidas financieras a las organizaciones. Por esta razón se propone un tipo de exploración cuantitativa, que permite seleccionar las métricas relacionadas con los riesgos a metodologías de auditorías, involucradas a los recursos de TI, donde se implementa un método deductivo, así mismo la investigación es validada con el método Delphi. El método define cuatro pasos: Paso 01, se aplican mecanismos de recuperación para establecer metodologías de auditorías; Paso 02, se aplica un modelo comparativo de las diversas metodologías; Paso 3, se aplica la validación a través de del método Delphi, para comparar la objetividad del modelo; Paso 04, Evaluación donde se aplicó la Matriz de priorización Holmes, al cuadro comparativo del modelo actual y el estado inicial. En los resultados se obtiene que la metodología con mayor riesgo son las guías de auditoría interna AI ya que lograron un valor de 16.86 puntos de riesgo, por otro lado, la metodología ISSAI 5300 su nivel de riesgo asciende a 14, 93 puntos, clasificando este valor de riesgo alto. La metodología de auditoría ISAF ITAF ocupa el segundo lugar con 15 puntos, finalmente la técnica de auditoría TI obtiene un valor de 14,43. Se concluye que, para obtener el nivel de riesgo, se puede construir una matriz de priorización. Así mismo la metodología que obtuvo un menor nivel de riesgo es auditoria TI, considerando que esta metodología cumple con los parámetros y logra una completa gestión de riesgos en todas sus etapas.

Por otro lado, [16] en su investigación, IT management evaluation model based on COBIT, ITIL, ISO 27002 and its effect on the competitiveness of COAC in the area and segment 1, en Cuenca Ecuador. Menciona que no sé están implementando de manera oportuna las buenas prácticas de TI en las organizaciones financieras, producto que no incluye la normativa en sus planes de TI, ya que no contemplan en sus presupuestos de TI, la mejora del Gobierno de TI. Por ello, se implementa un método para la evaluación de Tecnologías de Información, donde se implementen los marcos ITIL v3 e ISO 27002 y COBIT 5, que ayuden a la competitividad de las organizaciones. Posteriormente se siguen los siguientes pasos: Paso 01, se aplica un enfoque cualitativo, para hacer que permite hacer una descripción de las empresas seleccionadas a las cuales se les denominará las COACs (estas son las dos empresas a las que se les aplica el modelo). Paso 02, se aplicarán las metodologías ITIL, COBIT e ISO para la gestión de procesos de TI. Paso 03: Se ejecuta un plan para el constructo del modelo de gestión de TI, que parte desde la planificación (diagnóstico de COAC-GR y MD son las cooperativas del caso de estudio), luego se determina un diagnóstico de las TI; Paso 04: Se realiza la elaboración del framework ITIL v3, COBIT 5 y ISO 27002 y se aplica un análisis comparativo estructurado en una matriz, con el fin de establecer la relación entre los modelos. Paso 5: Se diseña una matriz, a la cual se le aplicará el método del semáforo, según los criterios de evaluación establecidos, seguidamente se proponen indicadores según su dominio correspondiente. Como resultados se obtiene COAC-GR logra un 88% de cumplimiento de políticas y COAC-MD un 63% (COAC-GR) abarca un 77%. y la (COAC-MD) un 69%, como observamos en la entidad 2 se evidencia una estructura muy semejante a ITIL, por otro lado, la entidad 1 tiene semejanza a la estructura del modelo COBIT 5. Se concluye que hay un riesgo elevado en la cooperativa COAC-GR, reflejando el nivel de soluciones de tecnología, desarrollo y calidad del software. La cooperativa COAC-MD presenta un riesgo catalogado como informal, por ende, el modelo indica que ambas cooperativas deberían mejorar su gestión de TI.

Así mismo, en la investigación, Information Systems Audit Model for Savings and

Credit Cooperatives of segment 1, 2, and 3, in the city of Cuenca. A pesar que hoy en día las organizaciones ya han implementados modelos de auditoría que les permite minimizar los riesgos de los SI, sin embargo a pesar que se cuenta con áreas que aplican auditorías internas, no se cuenta con profesionales informáticos, que puedan llevar un planificación y organización de sus activos, dificultando realizar las auditorías de TI. Por esta razón se implementa la metodología propuesta por Becker, Knackstedt, y Pöppelbu. Cómo primer paso se realiza un estudio no experimental, dónde se aplican encuestas que ayudan a determinar información relevante para realizar una auditoría. Seguidamente se realiza la comparación de los modelos COSO, ISO 27001, COBIT e ISO 2230. Paso 3, se aplica la evaluación del modelo y se hace una revisión del modelo resultante Paso 04: Se verifica el que se cumplan la eliminación y reducción de riesgos. Se realiza el informe final de auditoría con los puntos críticos identificados y las soluciones correspondientes. Como resultado se obtuvo que el 89.47 de las organizaciones encuestadas tienen un área de auditoría interna; cabe decir que el 84.21% no tiene personal capacitado para aplicar una auditoría a los SI, por otro lado el 64.82% indican que lo más factible es contratar personal con experiencia en auditoría de seguridad, para que puedan aplicar los controles adecuados a los sistemas internos de la entidad, así mismo el 33,3% establecen que las herramientas automatizadas ayudarían a resguardar la seguridad de la información, mientras que un 55% no tiene confianza en que estas herramientas puedan medir métricas de seguridad de los sistemas. Se concluye que los estándares aplicados en el modelo necesitan profundizar en los riesgos y seguridad de los SI, que le permita construir un modelo híbrido para lograr un modelo de auditoría interno más completo [17].

En las investigaciones descritas, la metodología más aplicada es COBIT, este marco de gobierno y gestión de TI, nos permite examinar el grado de riesgo y aseguramiento en los SI de las entidades, fomentando la mejora continua, el respaldo de los recursos de TI que consumen las empresas, estableciendo políticas de seguridad y gestionando los incidentes informáticos de las organizaciones [12].

Así mismo, producto de la preocupación por la tecnología emergente y el creciente ataque de delitos informáticos en la actualidad, es que se busca entender cómo los auditores planean aplicar las auditorías de TI empleando técnicas adecuadas, que logren minimizar, gestionar y prevenir riesgos informáticos en las organizaciones, aprovechando cada uno de sus procesos desarrollados en la empresa, para realizar un seguimiento minucioso a las brechas identificadas y contrarrestarlas con un plan de contingencia que permita tener SI más seguros e íntegros.

Por consiguiente, al desarrollar auditorías de TI en las organizaciones, no solo deben enfocarse en los equipos computarizados, deben evaluar procedimientos y controles efectuados, con el objetivo de obtener mayor información de los servicios de TI de la empresa que será auditada. Frente a ello, nace el estándar internacional ISO 19011:2018, que posee directrices que permiten realizar auditoría de TI de calidad tanto interno o externo, así mismo imparte una estructura bien diseñada, donde permite plasmar los requerimientos de la organización. La ISO 19011, permite identificar y aplicar estrategias que se encargan de minimizar los riesgos informáticos, proporcionado un enfoque basado en auditoria de los SI, evaluando las capacidades y competencias de las personas involucradas, permite alinear las normas y estándares que se deben aplicar en los procesos de la organización [18].

Por ende, se diseñó un modelo de auditoría de TI, implementado en una pequeña empresa retail peruana, recalcando que la mayoría de marcos desarrollados, se han aplicado a grandes organizaciones, las cuales se encuentran formalmente definidas, no cabe duda que estos métodos han ayudado a las grandes empresas en la integración de técnicas de seguridad aplicadas a sus sistemas empresariales, sin embargo se requiere un modelo de auditoría de TI, que no exija muchos recursos económicos, permitiendo realizar la agrupación idónea de actividades para el control de riesgos, que ayude a reducir las incidencias en los SI de las pequeñas empresas, a su vez, el modelo debe adaptarse a otras entidades, para el funcionamiento adecuado y el buen desempeño de los procesos de los servicios de TI, proporcionando controles rigurosos que validan que los sistemas de gestión sean confiables

proporcionando una mejora continua en la empresa.

En consecuencia, esta investigación se enfoca en la verificación de cumplimiento de normas y políticas de una empresa retail, realizando un análisis exhaustivo, para finalmente brindar una recomendación eficiente que ayude a mitigar las incidencias encontradas y a su vez mejorar la seguridad de los servicios de TI de las organizaciones. La contribución social que proporciona esta investigación es que la empresa seleccionada, no asumirá ningún costo por medio de la auditoría de TI, así mismo podrá identificar los problemas que se vienen aconteciendo en sus servicios de TI y cómo puede hacer para mejorar sus protocolos de actuación para que no acontezca.

Así mismo la Universidad Señor de Sipán se beneficia, porque al tener este tipo de aportes por parte de los estudiantes, permite que la universidad cumpla su misión institucional, porque su principal objetivo es que los jóvenes estudiantes apliquen conocimientos de investigación rigurosa, contribuyendo al desarrollo económico social de la zona por parte de la gestión de la actividad. Consecuentemente los jóvenes universitarios que realizamos esta investigación, adquirimos experiencia en un campo laboral idóneo para nuestro desarrollo cognoscitivo, desarrollando habilidades que servirán para nuestro futuro profesional.

1.2. Formulación del problema

¿Cómo mejorar de forma eficiente el cumplimiento de normas y políticas de TI en una empresa retail peruana?

1.3. Hipótesis

Mediante el diseño de un modelo de auditoría de TI se podrá mejorar de forma eficiente el cumplimiento de normas y políticas de TI de una empresa retail peruana.

1.4. Objetivos

Objetivo general

Diseñar un modelo de auditoría de TI para asegurar de forma eficiente el cumplimiento de normas y políticas de TI en una empresa retail peruana.

Objetivos específicos

- Diagnosticar la situación actual de las políticas de TI de la empresa para la elaboración de un modelo de auditoría de TI.
- Seleccionar marcos y normas internacionales para la elaboración de un modelo de auditoría de TI.
- Diseñar el modelo de auditoría de TI apoyado en un marco y norma para la empresa en estudio.
- Validar el modelo de auditoría de TI por juicio de experto propuesto para la empresa en estudio.
- Ejecutar el modelo de auditoría de TI para determinar el cumplimiento de normas y políticas de la empresa en estudio.

1.5. Teorías relacionadas al tema

1.5.1. Tecnologías de Información

Con el avance tecnológico en el mundo, se ha creado una dependencia hacia los ordenadores y dispositivos electrónicos, dejando de lado los archivos de papel que se usaban de manera tradicional. Por consiguiente, las organizaciones al ser consumidoras de grandes volúmenes de información, no se escapan de estos cambios abruptos que trae la tecnología, en la organización el activo más indispensable es la información, por ello debe ser analizada y procesada en el menor tiempo posible, ya que es un componente clave y estratégico para

la organización [19].

Según [20] Cuando se habla de TI básicamente se refiere a los dispositivos, servicios y actividades por un equipo de cómputo basada en la transformación numérica, llamada también digital. Conocer este sistema es una forma de interactuar de manera exitosa con la tecnología. Cabe decir que no solo las organizaciones se han adaptado a esta transformación digital, en la actualidad las personas se han convertido en emisores y receptores de información, donde los usuarios de empresas, entidades, ciudadanos; utilizan la red como un medio insustituible para el traslado de información y medio para comunicarse [21].

Lo anterior conduce a que, las TI engloban de forma general todos los elementos y sistemas utilizados para el tratamiento de la información, y a medida que las redes prestan mayores servicios, también aumenta de forma sustancial la dependencia y vulnerabilidad de nuestros sistemas de información, por ende, tenemos muchas ventajas, pero estas vienen acompañadas de nuevos riesgos [22].

1.5.1.1. Riesgos de TI

Producto del avance tecnológico, y a la experticia de los ciberdelincuentes que han ido ganando experiencia para ser cada vez más audaces y vulnerar los sistemas de información. [21] en su libro amenazas criminales del ciberespacio indica que los riesgos a los sistemas de información pueden dividirse en dos grandes categorías:

a) *Amenazas sobre bienes jurídicos:* Estas son derivadas del empleo de las nuevas tecnologías. Riesgo latente en contra de la Protección contra la intimidad y riesgo en las infraestructuras electrónicas.

b) *Riesgos sobre infraestructuras electrónicas*: Estas son derivadas de los ataques producidos para alterar o impedir el funcionamiento de los SI. Ingreso a sistemas sin accesos autorizados y difusión de programas informáticos perjudiciales.

1.5.2. Auditoria de TI

La auditoría de TI adquiere un rol trascendental en el cumplimiento de estrategias y procedimientos que ayudan a controlar, prevenir y preservar la información de las

organizaciones empresariales [23].

Por otro lado, [24] manifiesta que la auditoría se basa en revisar que las actividades y operaciones sean ejecutadas según el plan creado por la organización, así mismo se encarga que las políticas y procedimientos sean respetados, para posteriormente ser evaluados de manera objetiva y ver la forma en que se puedan administrar y operar, para encontrar las áreas donde se requieren reforzar los controles ya existentes.

1.5.2.1. Esquema de la auditoría de TI

[25], recalca que la auditoría es para todo tipo de organizaciones, y su función principal es lograr el cumplimiento de sus objetivos, realizando un plan que les ayude a gestionar los riesgos.

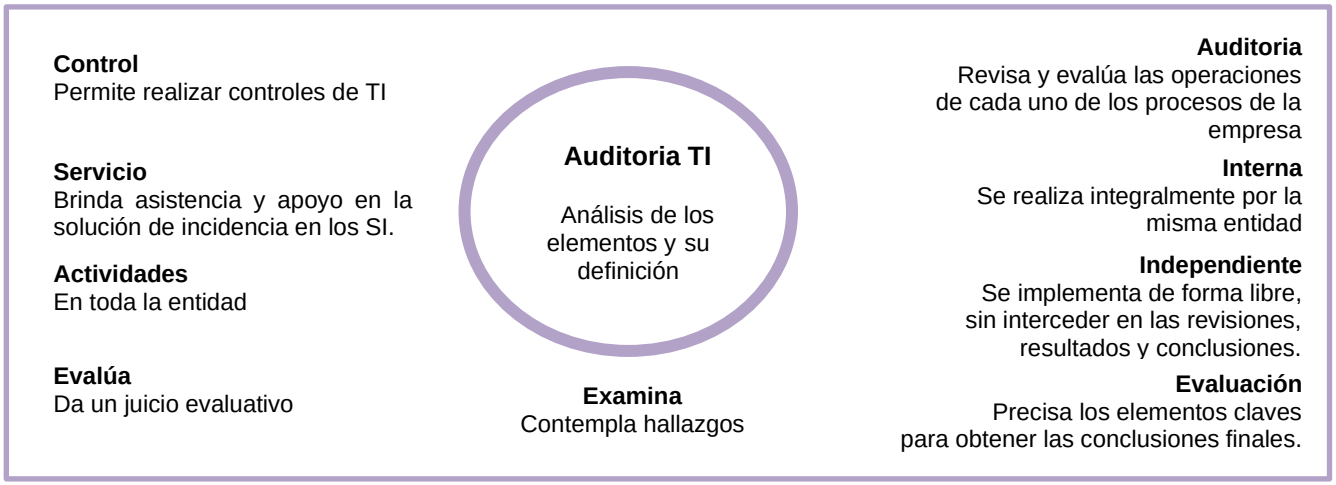


Figura 2.Elementos de la auditoría de TI.

Fuente: Tomado de [25]

1.5.2.2. Componentes de auditoría de TI que el auditor debe tener en cuenta

a) Plan de auditoria

Este plan debe proporcionar una herramienta en donde reúna de forma acertada, la información de todos los trabajos de revisión y de cada área de la organización relacionada con el proceso a realizar, documentándose en un informe. Por tanto, en la fase de planificación se considera muy importante, la correcta distribución de actividades y recursos para obtener un buen resultado de la auditoría. Posteriormente se prosigue con la ejecución del trabajo, comprendiéndose de diferentes actividades en donde se realizará pruebas y se

evaluará el trabajo que se ha realizado. Finalmente, terminada la ejecución del trabajo se recomienda realizar una primera reunión con las personas involucradas, tanto como de la empresa y el equipo de auditores con el objetivo de dar a conocer los resultados para conocer sus opiniones [26].

b) Ejecución de auditoria

En la etapa de evidencia, se debe considerar que el auditor debe recolectar información correcta y apta para concretar los objetivos de la auditoría. Así mismo, en la etapa de la documentación se deberá realizar un informe en donde se describirán los procesos y actividades de auditoría ejecutadas, como también las evidencias que se encontraron en el proceso de la auditoría, porque estas amparan las conclusiones del auditor. Finalmente, en la etapa de la supervisión se debe verificar que el personal de auditoría se haya cumplido las normas establecidas [26].

c) Informes de auditoria

Antes de realizar la redacción del informe el auditor debe tener los suficientes documentos de los resultados de las diferentes actividades de auditoría, ya que con ese material se podrá realizar el informe y hacer las recomendaciones pertinentes. Debido a los diferentes tipos de trabajo y los resultados, los veredictos se pueden clasificar de dos formas: efectiva o no efectiva [26].

d) Seguimiento de auditoria

[26] menciona que, al cierre de la auditoria, se deben tomar en cuenta y verificar el cumplimiento de acciones correctivas, donde la empresa auditada debe cumplir en un tiempo establecido. Por tanto, el equipo auditor, deberá verificar el cumplimiento de la mejora de incidencias encontradas, de esta manera se verifica mejora en los procedimientos de la empresa.

1.5.2.3. Tipos de informe de auditoría de TI

Por otro lado [25] manifiesta que en la auditoria generalmente son aceptadas 4 opiniones básicas según los resultados del trabajo. Uno: Si el auditor determina que el

sistema está conforme, su veredicto sería favorable. Dos: Si se concluye que el sistema está inconforme, su veredicto sería desfavorable. Tres: En el caso que el sistema esté en buena condición, aunque con algunas fallas, su opinión sería salvedades. Cuatro: Si el auditor no tiene suficiente evidencia para calificar el estado del sistema, no podría opinar, por ende, se recomienda comunicar de inmediato si se detectan fallas mientras se está realizando la auditoría.

1.5.2.4. Tipos de auditorías de TI

Según [27] existen dos tipos de auditorías la interna y la externa.

a) Auditoría interna

La auditoría interna permite controlar, gestionar y evaluar el uso óptimo de los servicios de TI, ayudando a cumplir objetivos y creando valor a las operaciones de la organización. Así mismo la auditoría interna, ayuda a establecer los lineamientos que permiten aplicar buenas prácticas aplicadas al desempeño de la organización [27].

a) Auditoría externa

La Auditoría externa, expone una percepción sobre cómo se está ejecutando los controles, la evaluación y gestión de la organización por un sujeto que no pertenece a la empresa, la cual examina y evalúa sus operaciones, posteriormente emite una opinión veraz de los sistemas de control que se desarrolla en el área auditada. Cabe decir que la AE el auditor al no tener dependencia con la organización, es independiente y libre de las influencias por parte de los miembros de la organización [27].

1.5.2.5. Ciclo de mejora continua basado en la ISO 19011

El ciclo PDCA describe cuatro fases, que la organización realiza para efectuar la mejora continua y permitir alcanzar la calidad en sus procesos [28]. Inicia con el PLAN (Identificación del problema), DO (Obtener datos), Check (análisis y estudio) y ACT (Implementa programas de acción).

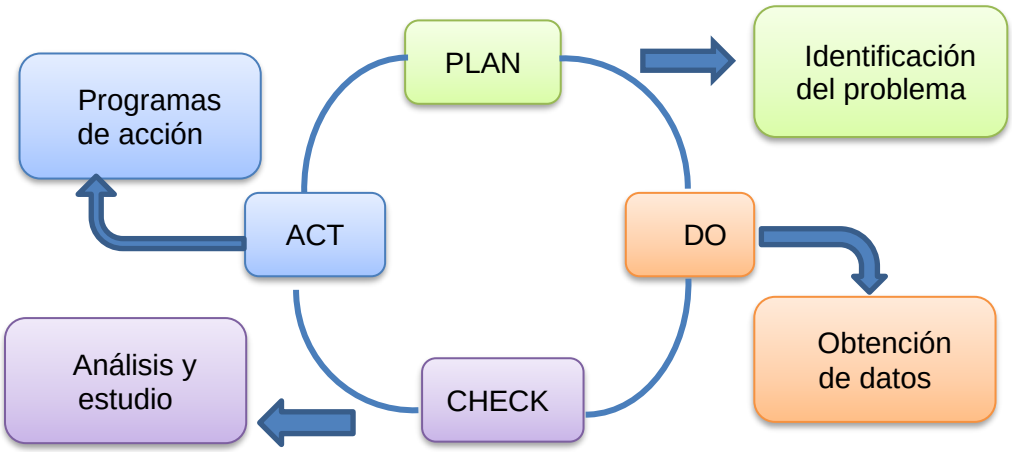


Figura 3.Ciclo de PDCA.

Fuente: Tomado de [28].

La primera fase está basada en la planeación (Plan), a partir de la identificación de problemas de la entidad, se determinan metas y objetivos que den solución a estas limitaciones, así mismo se plasman los mecanismos que se deben realizar para optimizar los procesos. Por otro lado, tenemos el hacer (Do) este paso se enfoca en proporcionar al personal estrategias de conocimiento que al llevar a la práctica, les ayude a lograr acciones que brindan satisfacción al cliente, consecuentemente verificar (check) es un paso que realiza el análisis y estudio de las actividades realizadas, para cerciorarnos que los planes se están efectuando y que serán alcanzados de manera eficiente, finalmente actuar (Act) permite a la organización realizar la ejecución de acciones que logren el cambio continuo de la organización [28].

Así mismo [28], menciona que la calidad y mejora continua permite que las empresas logren alcanzar sus objetivos a lo largo del desarrollo de cada proceso, por esta razón, el uso de la herramienta PDCA ayuda a la solución de limitaciones que presentan las organizaciones, de esta forma se mejoran los procesos y se obtienen resultados eficientes.

Por consiguiente, el cumplimiento del ciclo PDCA se debe asumir de forma exigente el compromiso de efectuar los procesos de mejora, de esta manera se inicia la aplicación del mejoramiento continuo de procedimientos y actividades de la empresa, posteriormente se podrá medir la calidad obteniendo datos exactos que permitirán dar solución a las diversas

dificultades encontradas.

Cabe decir, que una la cultura de mejora continua también es parte del personal de trabajo de la organización, por ello deben ser capacitados por la alta gerencia experta, buscando el mejoramiento de metas y prevención de defectos, obteniendo como resultado final procesos homogeneizados. [28].

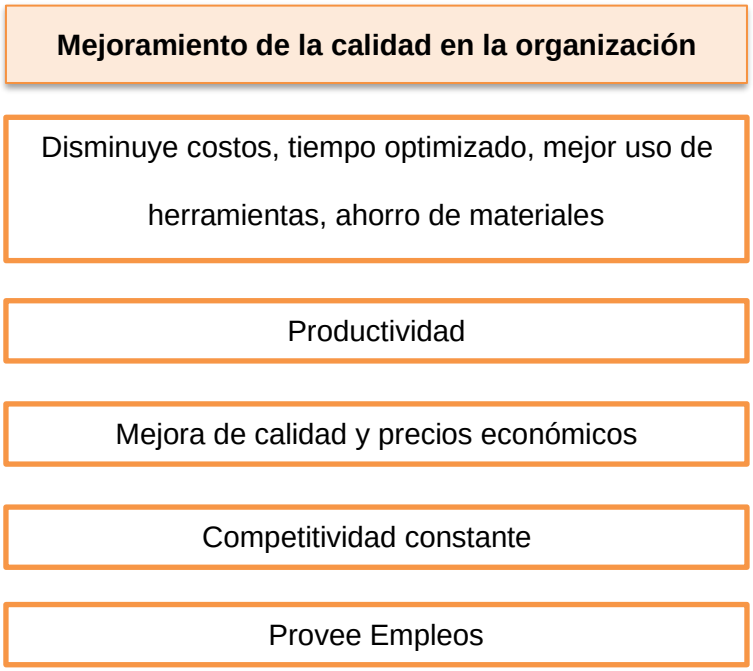


Figura 4.La reacción en cadena de calidad y productividad de Deming.

Fuente: Tomado de [28]

1.5.3. Modelos empresariales IT GRC

El GRC visualizado de forma integradora abarca cuatro perspectivas bien definidas con las cuales se puede concretar lo que se desea lograr en la organización, a su vez puede definir el nivel de madurez al que está dispuesto a escalar según el cumplimiento de objetivos; la primera perspectiva es el desempeño (donde se estipula el objetivo estratégico para el desarrollo de políticas y estándares que la empresa deberá cumplir para alcanzar su propósito), la segunda perspectiva es la arquitectura empresarial (representa los elementos que ayudan a materializar los resultados del desempeño realizado por la organización en cuanto a su estructura organizacional y resultado de las operaciones de los procesos basados en TI), la tercera se enfoca en el aseguramiento (el cual implica intervenir con el cumplimiento

de la gestión de normativas de la organización) finalmente la perspectiva del alcance (indica si lo propuesto puede implementarse en la organización o determinar el área donde será desarrollada de manera específica) [29].

a) Gobierno y gestión

El gobierno es el acto de supervisar, controlar una organización, así mismo puede evaluar procesos, recursos e información de la entidad, sin embargo, esta no administra ya que su intervención es de forma externa. Consecuentemente la gestión la cual es una intervención interna, es la inferencia de un acto de gobierno, que tiene por finalidad la ejecución y el logro de objetivos propuestos [29].

b) Riesgo

El riesgo hace referencia a un inadecuado manejo de estrategias en la entidad, donde la identificación de los riesgos y su control forman parte de la evaluación de la incertidumbre de las organizaciones, la cual enmarca las amenazas que se pueden producir y a su vez implementa la aplicación de estrategias que ayuden a mitigarlas. La proactividad con la que se busca un resultado eficiente, permite que la organización tome conciencia del riesgo que ha logrado asumir. En este contexto la empresa llega alcanzar un nivel aceptable de confianza, denotando productividad y eficacia en sus procesos, a la vez logra establecer con precisión las causas y efectos de los riesgos, ayudándole a conseguir los resultados de manera [29].

c) Cumplimiento

La organización busca el cumplimiento de la normativa de forma voluntaria, la cual está vinculada al código de ética y comportamiento cultural de la entidad, bajo esta premisa debe incorporarse el conjunto de normas y políticas que han sido establecidas por la empresa, las cuales serán acatadas y desarrolladas para gestionar los riesgos y aplicar controles que permitirán contrarrestar las incidencias de SI de la empresa. Así mismo se implementarán marcos de referencia que ayuden a efectuar su cumplimiento, en las que se establecerán

atributos y dimensiones que serán desarrolladas, al finalizar se realizan reportes sobre incidencias encontradas y el control que se ha establecido, los cuales deben estar alineados con los elementos y dominios de la arquitectura [29].

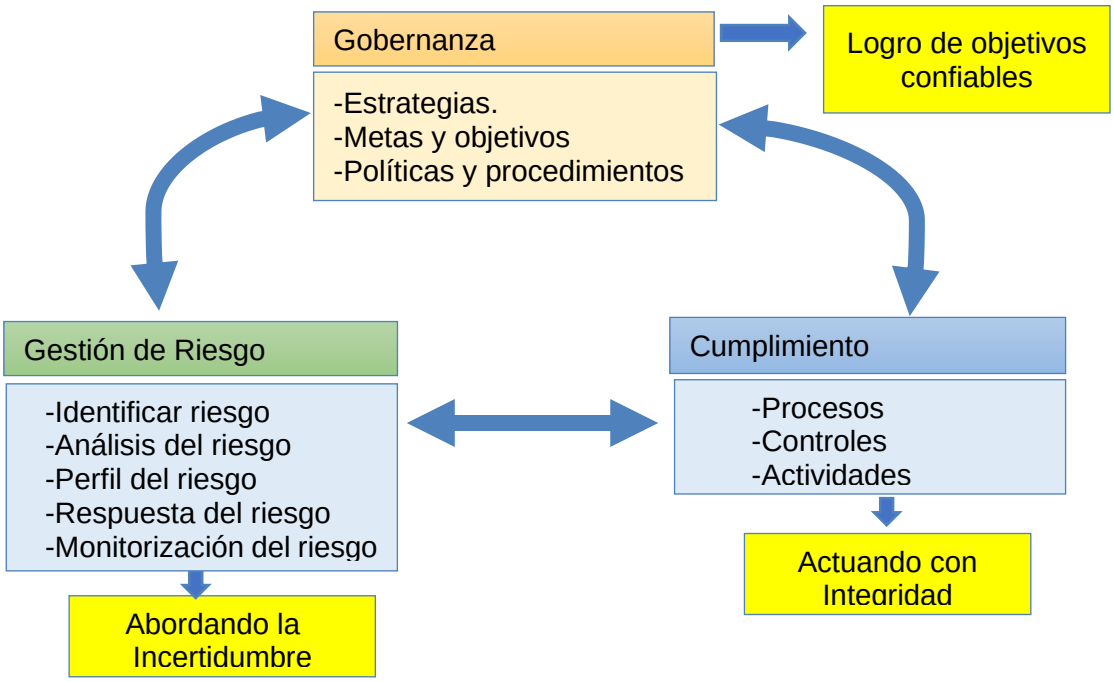


Figura 5.Ciclo de GRC.

Fuente: Tomado de [29].

1.5.4. COBIT 2019

COBIT 2019 ha sido implementado en base a principios definidos, el primero desarrolla los requerimientos de tecnología y gobierno, el segundo basado en desarrollar sistemas de gobiernos empresariales. COBIT 2019 está alineado a estándares, que le permiten consolidarse como un marco que permite la creación políticas, procesos, procedimientos, estructura organizacional, infraestructura y cultura de gestión [30]

1.5.4.1. Objetivos de COBIT

Según [30] Menciona que existen 5 dominios dentro de los objetivos de gestión y gobierno.

A. Objetivos de Gestión

Están agrupados en (EDM), Evaluate, Direct, Monitor, donde se determinan, evalúan

y monitorean las estrategias seleccionadas.

B. Objetivos de gobierno

Se agrupa en 4 dominios:

a) APO (Align, Plan, Organize) Actividades y estrategias para la gestión de TI.

b) BAI (Build, Acquire, Implement) Desarrollo de soluciones que permite que los procesos trabajen de forma integrada en la entidad.

c) DSS (Deliver, Service, Support) Desarrollo de la ejecución de procesos y a su vez da soporte a la seguridad, los servicios de la información y tecnología.

d) MEA (Monitor, Evaluate, Assess) Basado en cumplir los objetivos externos einternos de la entidad [30]

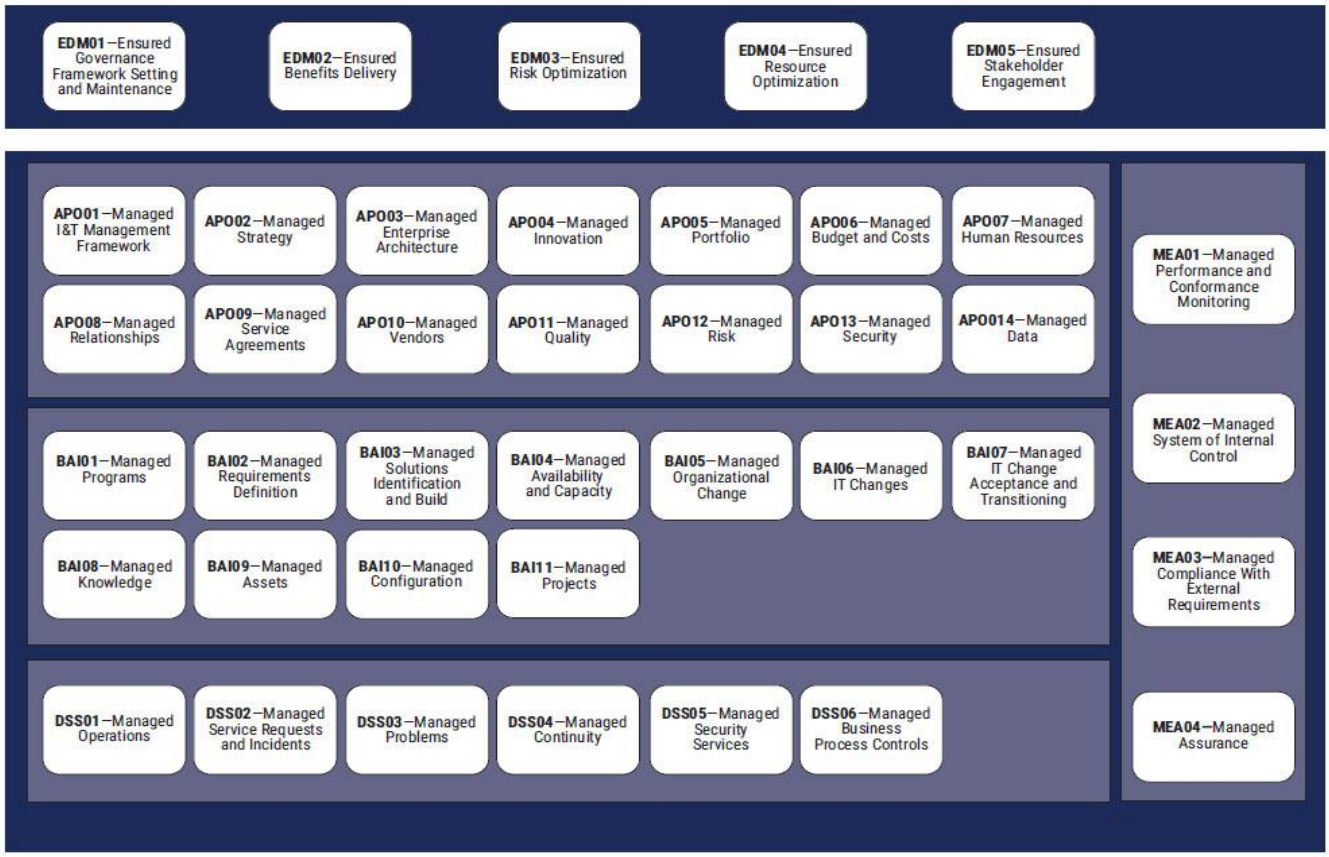


Figura 6.Modelo Core de COBIT.

Fuente: Tomado de [30].

1.5.4.2. Principios para la ejecución de un modelo de gobierno

a. Mantener el equilibrio que hay entre el riesgo, los recursos y los beneficios adquiridos. Por ende, la empresa necesita estrategias que permitan materializar este valor.

b. Se puede crear un SG implementando componentes de distinto tipo, pero que funcionen de forma holística.

c. Si hay cambios en el SG, se debe prever el impacto que estos cambios causarán, por ende, el sistema debe ser dinámico, ya que, al tener modificaciones futuras, este no pueda ser afectado, sino que debe adaptarse.

d. El SG debe conocer las diferencias entre la gestión, su estructura y las actividades de gobierno que serán establecidas en dicho sistema.

e. El SG debe diseñarse teniendo en cuenta los parámetros y funciones requeridas.

f. El SG permite que la empresa logre el cumplimiento de sus objetivos de principio a fin, así mismo no solo se enfoca en los servicios de TI, también cubre el funcionamiento de los procesos tecnológicos independientemente del área en que se encuentre (ISACA, 2018). [31]

Figura 7.Principios del Sistema de Gobierno.

Fuente: Tomado de [30].

1.5.4.3. Principios de COBIT 2019

a. Debe definirse sobre un marco que le permita identificar sus componentes, relaciones entre ellos, que le permita establecer la uniformidad de sus procesos y a la vez

implementar su automatización.

b. El marco de gobierno es flexible, a su vez permite la implementación o desarrollo de nuevo contenido, pero sin perder la uniformidad e integridad del sistema.

c. El marco debe cumplir los estándares, regulaciones y políticas empresariales [31]

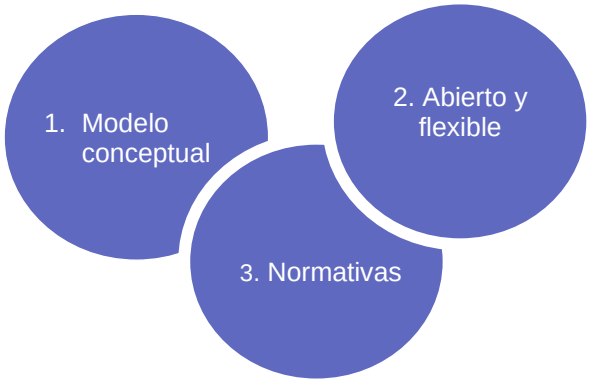


Figura 8.Principios del marco de Gobierno. [30]

Fuente: Tomado de [30].

1.5.4.4. Componentes de COBIT 2019

Según [31], menciona que las organizaciones que implementan un sistema de gobierno, deben establecer componentes que les ayude a tener un buen funcionamiento del sistema en la empresa son los siguientes:

a) Procesos

Estos son organizados para alcanzar el cumplimiento de objetivos de TI y que permitan producir resultados eficientes.

b) Estructura organizativa

La toma de decisiones más importantes las ejecuta la organización.

c) Marco de referencia y políticas

Permiten determinar el comportamiento del SG y verifica que se cumpla con el desarrollo de sus políticas empresariales y objetivos de gestión.

d) Información

COBIT se encarga de obtener la información pertinente para lograr una gestión eficaz de gobierno de la organización.

1.5.5. Cyberseguridad Nexus (CSX)

Es una estrategia alineada con los retos actuales a nivel global. Es un enfoque efectivo para poder afrontar los retos presentes y futuros en materia de seguridad digital o en ciberseguridad. Debido la escasa demanda de profesionales calificados en el rubro de la ciberseguridad, por ello se busca que los profesionales desarrollen capacidades idóneas que se requieren en los entornos reales a nivel internacional. Es así que la iniciativa se alinea con diferentes marcos de referencias internacionales y también se alinean con las estrategias de las diferentes naciones en cuanto a desarrollar estas competencias y capacidades [32].

A través del programa de entrenamiento y certificación en Cybersecurity Nexus (CSX), la asociación global de TI de ISACA brinda capacitación cibernética y certificaciones en todos los niveles de habilidades y especialidades, tales como: Certificado de Fundamentos en Seguridad Cibernética, practicante de CSX, especialista de CSX, experto en CSX, Certificado de Gerente de Seguridad de la Información [32].

1.5.6. Contraloría para gestionar y proteger los activos de sistemas de TI

El ente técnico regulador CGR (Contraloría General de la República) tiene como misión cautelar el desarrollo de los recursos económicos del gobierno. El objetivo de la política de la SI, es describir el marco general y los lineamientos que serán ejecutados por la Contraloría para gestionar y proteger los activos de los sistemas de TI. Este ente técnico de la contraloría provee bases tecnológicas como los equipos físicos y no físicos que se necesitan para poner en marcha el funcionamiento del sistema de Notificaciones y Casillas Electrónicas. En este sentido, el contenido y los procedimientos son de cumplimiento obligatorio para el personal involucrado en las operaciones críticas derivadas de la Prestación de Servicio de Valor Añadido del - CGR. Asimismo, es de carácter obligatorio el cumplimiento de los proveedores de servicios o terceros que suministren sus servicios al PSVAEP [33].

1.5.7. Norma Técnica Peruana 27001

[34], menciona que la NTP ISO/IEC 27001:2014 fue establecida mediante una resolución ministerial, reemplazando a la “NTP ISO/IEC 27001:2008, fue aprobada por la Resolución Nº 129-2014/DNB-INDECOPI. La norma ha sido implementada y adecuada de forma obligatoria con un mínimo de dos años, en entidades que son representantes del SI de la Nación. Por ende, si las entidades buscan certificarse con esta norma, deben realizar de manera opcional la inversión de recursos de la propia entidad para su desarrollo. Así mismo la empresa registrada debe estipular un comité de gestión de la SI (a. Titular de la organización, b. Administrador, c. jefe del área informática, d. jefe del área legal, e. jefe de seguridad), cada miembro tendrá funciones asignadas, las cuales serán establecidas por la organización de acuerdo a la norma implementada.

1.5.8. Norma Internacional ISO 19011

La norma ISO 19011:2018 es una asociación a nivel mundial de varios organismos nacionales de normalización. Está destinada a un gran número de usuarios los cuales pueden ser: a) auditores, b) organizaciones que deben realizar auditoría de TI [26].

1.5.8.1. Directrices para la auditoria de TI

Según [26], la ISO 19011, está enfocada en la gestión de auditorías de TI sobre:

a) Principios de auditoria

Los principios permiten que la auditoría que es realizada por los auditores se encuentre basada en buenas prácticas con el objetivo que la auditoría se efectúe de forma eficiente en la gestión y control proporcionando soluciones a la organización en acciones que ayuden a mejorar su desempeño. Los principios que se estipulan en la ISO 19011 son los siguientes: Imparcialidad, Integridad, Confidencialidad, Independencia, principios enfocados en la evidencia y en los riesgos, cuidado profesional [26],

b) Gestionar el programa de auditoria

Se desarrolla un plan, que establece estándares que permita gestionar la auditoría, del mismo modo se presenta el alcance de la auditoría el cual se enfoca en el tamaño y

naturaleza del auditor. Se deben tomar decisiones importantes y formar los equipos responsables para revisar la auditoría [26],

c) Auditorias basada en la gestión de riesgos

Para iniciar una auditoría, se sigue una secuencia de pasos, como primer punto se realiza un diagnóstico de la empresa que será auditada. El líder designado para la auditoría tiene como deber cuidar que se efectúe el cumplimiento de cada uno de los procesos ejecutados, hasta que la auditoría sea completada [26],

d) Lineamientos para la evaluación de personal competente

Las evaluaciones se realizan para medir las competencias de los auditores, deben planificarse, realizarse y a su vez realizar su documentación pertinente para garantizar resultados objetivos, consistentes, justos y confiables La evaluación debe incluir los siguientes cuatro procesos: Determinar la capacidad en cuanto a la satisfacción de necesidades establecidas para la implementación de la auditoría, seleccionar los criterios que deben ser evaluados y elegir un método de evaluación pertinente para evaluar el programa de auditoría [26],

1.5.9. Normativa SBS

La Superintendencia de Banca, Seguros y AFP (SBS), establecida por la resolución N° 504-2021, buscan que las entidades tengan un entorno confiable y optimizado para evitar incidentes de ciberseguridad, producto del avance tecnológico y la interconectividad empresarial. Las medidas que se tomaron son: Reforzamiento de la estructura organizacional, integradas por el directorio, gerencia y el comité enfocado en riesgos y ciberseguridad. Se establece que las entidades tengan un plan basado en Seguridad Informática y ciberseguridad, los cuales se encargaran del aseguramiento de controles de incidentes, para generar una respuesta inmediata ante incidencias de SI. Por otro lado, el reglamento establecer canales de autentificación de usuarios y evitar fuga de información producto del acceso de terceras personas a los sistemas de la entidad [35].

II. MATERIALES Y MÉTODO

1.1. Tipo y Diseño de Investigación

1.1.1. Tipo de Investigación

Se aplicará el método cuantitativo, producto que se utilizarán métricas para conocer el estado inicial de la empresa Retail, y exploratoria con el fin de adquirir información concisa sobre el caso de estudio.

1.1.2. Diseño de Investigación

Por su naturaleza, se empleará un diseño cuasi-experimental en la investigación, esto quiere decir que la variable independiente se diseñará con normas y marcos para mejorar eficientemente el cumplimiento de las políticas de TI de la empresa en estudio. Así mismo los métodos estadísticos permitirán validar los procedimientos empleados.

1.2. Variables, Operacionalización

Según [36], menciona que, en las hipótesis con predominancia causal, donde existe una vinculación de causa y efecto, se pueden identificar dos variables, las independientes que son aquellas consideradas como la “causa de” en la relación que existe frente a otra variable, y el dependiente considerado como el efecto que se produce por la acción de la variable independiente.

En la presente investigación tenemos:

a) ***Variable Independiente:*** Modelo de auditoría de TI.

b) ***Variable Dependiente:*** Cumplimiento de normas y políticas.

Tabla I.Operalización de la variable.

Variable de estudio	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos	Valores finales	Tipo de variable	Escala de medición
Modelo de auditoría de TI	Es el inicio para identificar las variables idóneas que evalúan las eficiencias de procesos empresariales transformando su servicio de TI, como un elemento de valor y mejora continua.	Basada en la selección e implementación de estándares y normas internacionales, que permiten planificar, ejecutar, evaluar y dar seguimiento a las políticas de TI de la organización.	Documentación para construcción del modelo de auditoría de TI	Porcentaje de documentación utilizada en selección de marcos y normas	$PDU = \sum_{i=1}^{i=n} \left(\frac{n * 100}{CDU}\right)$ En donde: CDU= Cantidad de Documentación Utilizada n= Sumatoria total de documentos utilizados.	Revisión documental/bitácora	(% porcentaje)	Variable independiente	Nominal
			Tiempo de ejecución del modelo de auditoría de TI	Tiempo de ejecución del modelo	$\sum_{i=1}^{i=n} (Hf - H\,i)$ En donde: Hf= Hora final Hi = Hora de inicio		(hrs horas hombre)		
			Procesos del marco de trabajo utilizado para la construcción del modelo de auditoría de TI	Porcentaje de procesos del marco y norma seleccionada	$PPM = \sum_{i=1}^{i=n} \left(\frac{CPMS * 100}{n}\right)$ En donde: CPMS = Cantidad procesos de marcos seleccionados N = Sumatoria total de procesos de marcos seleccionados	Revisión documental/ficha de revisión/ Juicio de experto/ficha de juicio de experto	(% porcentaje)		

			Juicio de experto para evaluación del modelo de auditoría de TI	Promedio de evaluación de expertos Se evalúa coherencia, pertinencia suficiencia objetividad claridad	$\sum_{k=1}^{j=p}\left(\frac{\sum_{j=1}^{i=n}\left(\frac{\sum_{i=1}^{i=n}\frac{ValorCriterio_{ij}}{n}}{m}\right)}{p}\right)$ En donde: n= Cantidad de actividades m= Cantidad de criterios p= Cantidad expertos	Juicio de experto/ficha de juicio de experto	(X̄ promedio)		
Cumplimiento de normas y políticas	Evaluación minuciosa del conjunto de actividades que permite identificar las incidencias en las políticas de TI de la organización.	Enfocado en cumplir con los objetivos, políticas y acuerdos de la entidad, implementando las buenas prácticas de los procesos de TI.	Cumplimiento de actividades notificadas a las partes interesadas	Porcentaje de cumplimiento de actividades	$PcA = \sum_{i=1}^{i=n}\left(\frac{AC * 100}{n}\right)$ En donde: AC= Actividades cumplidas n= Total de actividades de TI	Revisión documental/ficha de revisión/encuesta	(% porcentaje)	Variable dependiente	Razón
			Cumplimiento de políticas de TI	Porcentaje de cumplimiento de políticas de TI	$PCP = \sum_{i=1}^{i=n}\left(\frac{PC * 100}{n}\right)$ En donde: PC= Políticas cumplidas n= Total de actividades de TI	Revisión documental/ficha de revisión/encuesta	(% porcentaje)		

Fuente: Elaboración propia

1.3. Población de estudio, muestra, muestreo y criterios de selección

La población y muestra de la investigación desarrollada, hace énfasis a las políticas de TI de la empresa Conecta Retail S.A, del área de TI; la cual está situada en Lambayeque-Chiclayo, la razón por la que se ha seleccionado es porque cumple con los parámetros requeridos para aplicar el modelo de auditoría de TI.

1.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

1.4.1. Técnicas de Recolección de datos

A. Revisión documental

Permite la construcción de las ideas y la interpretación de los diferentes documentos que han identificado, así mismo se tiene ordenada la documentación, para el análisis de datos de la información recopilada.

B. Juicio de expertos

Se hará el contacto con expertos en el área de auditorías de TI mediante los diferentes medios para conocer la posición que adopten frente a la propuesta de los tesistas.

C. Encuesta

Se utiliza para conocer a la empresa CONECTA S.A.C en cuanto a marcos, estándares o metodologías que utilizan para desarrollar implementar políticas internas del área de TI, y en base a las respuestas diseñar un modelo de auditoría de TI que ayude al cumplimiento de las políticas.

1.4.2. Instrumentos de recolección de datos

A. Bitácora

Se realizará una bitácora para obtener la información indispensable, obteniendo un orden y fácil ubicación de cada uno de los documentos encontrados**.**

B. Ficha de revisión

Se elaborará una ficha de revisión de los documentos más relevantes de cada investigación, contendrán datos de las ideas más relevantes de los autores de como se hizo, para que se hizo y como se hizo.

C. Ficha de juicio de expertos

Se utilizará la ficha de experto para conocer la posición ante la propuesta final de la investigación, donde contendrán criterios evaluativos con su respectivo puntaje y así conocer la eficiencia de la propuesta.

D. Cuestionario

Instrumento que permite recolectar información de la empresa CONECTA RETAIL S.A., esta información obtenida posteriormente será analizada y se determinará que estándar o marco internacional calza de manera congruente con la construcción del modelo de auditoría de TI.

1.4.3. Validez y confiabilidad de los instrumentos

Se contó con 3 expertos con amplia experiencia en auditorías de TI, en Sistemas de Información, GRC, los cuales dan su criterio de calificación y aprobación mediante un instrumento de evaluación, donde evalúan con una escala de 0 al 4.

1.5. Procedimiento de análisis de datos

Se tomaron en cuenta los siguientes indicadores:

a) Porcentaje de documentación utilizada en selección de marcos

Se elaboró el cálculo del porcentaje de la cantidad de documentos utilizados entre el total de documentos, esto para obtener el *porcentaje de documentación relacionada para la construcción del modelo de auditoría de TI*.

Fórmula:

$$PDU = \sum_{i=1}^{i=n} \left(\frac{n * 100}{CDU}\right)$$

Donde:

CDU= cantidad de documentación utilizados

n= sumatoria total de documentos utilizados

b) Tiempo de ejecución del modelo

Se calculó el tiempo de diseño del modelo de auditoría de TI, aplicando la siguiente

Fórmula:

$$TEM = \sum_{i=1}^{i=n} Hf - Hi$$

Donde:

Hf= Hora final

Hi = Hora de inicio

c) Porcentaje de procesos del marco seleccionado

Se calculó el porcentaje de los procesos del marco de trabajo utilizado para la construcción del modelo de auditoría de TI.

Fórmula:

$$PPM = \sum_{i=1}^{i=n} \left(\frac{CPMS * 100}{n}\right)$$

Donde:

CPMS= cantidad procesos de marcos seleccionados

N = sumatoria total de procesos de marcos seleccionados

d) Promedio de evaluación de expertos

Se aplicó el juicio de experto para evaluación del modelo de auditoría de TI.

Fórmula:

$$PEX = \sum_{k=1}^{j=p} \left(\frac{\sum_{j=1}^{i=n} \left(\frac{\sum_{i=1}^{i=n} \frac{ValorCriterio_{ij}}{n}}{m} \right)}{p} \right)$$

Donde:

n= Cantidad de actividades

m= Cantidad de criterios

o= Cantidad expertos

e) Porcentaje de cumplimiento de actividades

Se calculó el porcentaje de cumplimiento de actividades notificadas a las partes interesadas.

Fórmula:

$$PCA = \sum_{i=1}^{i=n} \left(\frac{AC * 100}{n} \right)$$

Donde:

AC= Actividades con cumplimiento

n= Total de actividades de TI

f) Porcentaje de cumplimiento de políticas

Se calculó el porcentaje de cumplimiento de políticas de la empresa retail.

Fórmula:

$$PCP = \sum_{i=1}^{i=n} \left(\frac{PC * 100}{n} \right)$$

Donde:

PC= Políticas cumplidas

n= Total de políticas

2.6. Criterios éticos

a) Confidencialidad

Para respetar este estándar ético, los encuestados que apoyarán en la investigación permanecerán en el anonimato, con el fin que brinde información con honestidad y precisión,

para obtener datos fidedignos.

b) Derechos de autor

Los informes encontrados referentes a modelos de auditoría de TI serán citados y referenciados según corresponda, de esta manera se estaría respetando el derecho del autor.

c) Búsqueda del bien

Nuestra investigación va a brindar un beneficio empresarial y social, porque se busca que el caso de estudio, pueda mejorar de forma eficiente el cumplimiento de estándares y políticas, así mismo se buscará el beneficio social, porque la investigación quedará como ejemplo para posteriores investigaciones.

2.7. Criterios de Rigor Científico.

a) Originalidad: Se realizará el constructo de la investigación utilizando documentos sobre marcos y estándares internacionales de TI. Por otro lado, se respetarán los lineamientos establecidos por la propiedad intelectual de los diversos autores citados a lo largo de la investigación, finalmente se redactará con argumentación propia y para corroborar la originalidad de la tesis se aplicará el software antiplagio Turnitin.

*b) Confiabilidad**:** S*e empleará la herramienta Alfa de Cronbach, esta herramienta es utilizada para validación estadística de la encuesta, la cual contiene un conjunto de preguntas con alternativas, donde el valor mínimo aceptado es 0,60.

c) Validez: El modelo de auditoría de TI empleará el método Delphi que es valorado por el juicio de expertos para evaluar la consistencia. Inicia desde la fase de preparación, consulta y termina en el consenso, obteniendo como resultado las conformidades y el reporte final.

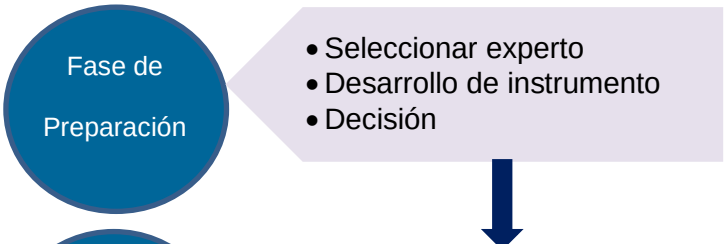


Figura 9.Procedimiento del método Delphi.

Fuente: Tomado de [37].

III. RESULTADOS Y DISCUSIÓN

3.1. Resultados

Se detallan los resultados según los indicadores de la variable dependiente e independiente, enfocados en el diseño de un modelo de auditoría de TI, tomando como norma la ISO 19011 que formará parte de la estructura del modelo de auditoría y el marco de COBIT 2019 que permitirá verificar el cumplimiento eficiente de las políticas de TI de una empresa Retail peruana:

3.1.1. Variable Dependiente

A. Porcentaje de documentación utilizada para la selección de marcos y normas aplicados al diseño del modelo de auditoría de TI.

Este indicador tiene como finalidad diseñar un modelo de auditoría de TI, adaptable a los requerimientos de la organización.

Desarrollo

Se realizó una bitácora de 100 documentos que hacen referencia a marcos y normas internacionales relacionadas a las auditorías de TI, tales como: *COBIT 2019, NIST, ISO*

19011, ITIL, RISK IT, *ISO 27001*, de ellos se seleccionaron 21 documentos destacados, ver anexo 5.1. Posteriormente, se elaboró una ficha para establecer cuatro criterios con su respectivo puntaje, donde se identificaron los documentos con marco y normas alineados a las auditorías de TI. Visualizar anexo 5.2, para observar la validación de los criterios de evaluación, mediante declaración jurada de experto, donde se validó el cuadro comparativo, criterios de selección y resultados.

Tabla II.Resultados finales de la evaluación de normas y marcos.

	ITIL	**COBIT 2019**	NIST	**ISO 19011**	ISO 27001	RISK IT
DIRIGIDO	5	5	5	5	5	1
ORIENTADO	1	5	2,5	5	5	2,5
CONSTITUIDO	2,5	5	2,5	5	5	5
FINALIDAD	2,5	5	2,5	5	2,5	2,5
PROMEDIO	2,8	5	3,1	5	4,4	2,8

Fuente: Elaboración propia.

En la tabla II se visualiza el puntaje obtenido de normas y marcos, donde se puede identificar que el marco COBIT 2019 y la norma ISO 19011 obtuvieron el más alto puntaje con un promedio de 5, indicando que han logrado el cumplimiento de cada uno de los criterios.

Tabla III.Porcentaje de documentos utilizados para el diseño del modelo de auditoría de TI.

ITEM	**total de documentos seleccionados**	**Total de documentos utilizados**
COBIT 2019	8	5
ISO 19011	2	2
TOTAL	**10**	**7**

Fuente: Elaboración propia.

En la tabla III, se observa el porcentaje de documentos oficiales de COBIT 2019 y del estándar ISO 19011, que se utilizaron para diseñar el modelo de auditoría de TI.

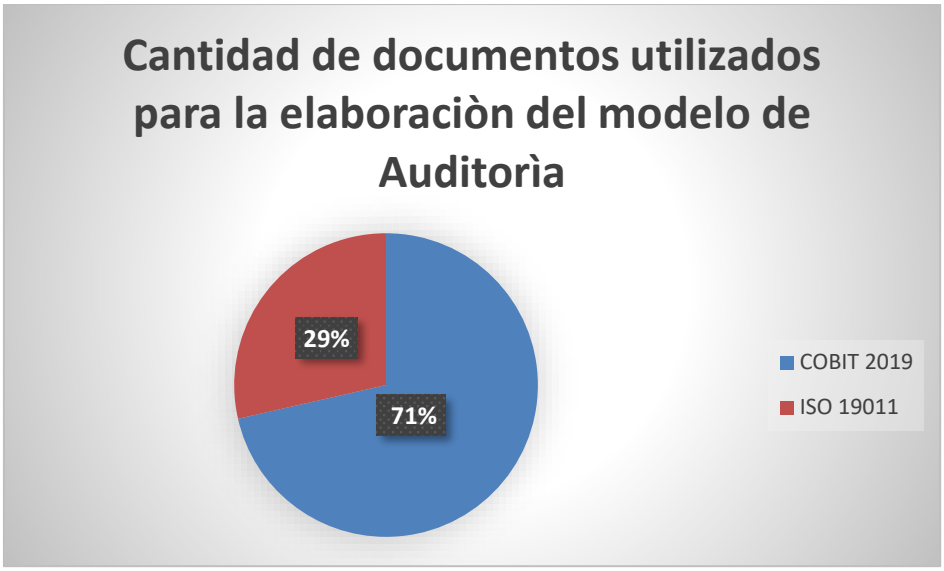


Figura 10.Porcentaje de documentación utilizada para el desarrollo del modelo de auditoría de TI.

Fuente: *Elaboración propia.*

B. Tiempo de ejecución del modelo de auditoría de TI

Este indicador nos permite establecer el tiempo que nos tomara ejecutar el modelo construido, esto con la finalidad de tener un modelo práctico y eficaz.

Desarrollo

Elaboramos una ficha que contempla el detalle de cada fase y el total de horas hombre utilizado. La estructuración del modelo contempla 4 fases que son las siguientes: *Fase 01-Planifiación, Fase 02-Ejecución, Fase 03-Verificación y Fase 04-Seguimiento y Mejora*. Ver anexo 5.3, para visualizar la ficha de tiempo de ejecución del modelo, firmada por el jefe del Área de TI de la Empresa Conecta Retail S.A. Posteriormente se calcula el total de las horas trabajadas, aplicando la siguiente operación: la hora final menos la hora de inicio y la sumatoria de todas las horas de las actividades de cada fase.

En la *tabla IV*, se muestra un resumen que evidencia el tiempo que se tomará el equipo auditor para ejecutar el modelo de auditoría de TI en la empresa CONECTA RETAIL S.A, tomando un valor total de 129 horas.

Tabla IV.Total de horas trabajadas para la ejecución del modelo de auditoría de TI.

	Actividades	Días útiles	DÍAS CALENDARIO		TOTAL DE HORAS HOMBRE
MARRY - OMAR	FASE 1 PLANIFICAR	6	DEL 03/10/2023	AL 09/10/2023	24
	FASE 2 EJECUTAR	5	DEL 10/10/2023	AL 14/10/2023	40
	FASE 3 VERIFICAR	8	DEL 16/10/2023	AL 24/10/2023	49
	FASE 4 MONITOREAR	2	DEL 25/10/2023	AL 08/11/2023	16
	TIEMPO DE EJECUCIÒN	21			**129**

Fuente: Elaboración propia

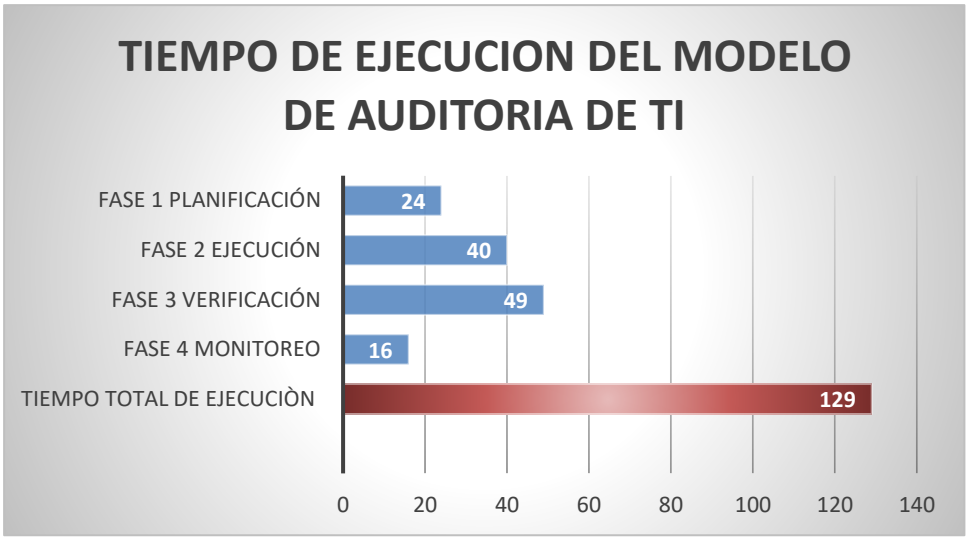


Figura 11.Cantidad de horas utilizadas para la ejecución del modelo de auditoría de TI.

Fuente: *Elaboración propia.*

C. Porcentaje de procesos de marcos y normas seleccionadas para el diseño del modelo de auditoría de TI

Este indicador nos permite evaluar los procesos adecuados que deben intervenir en el modelo de auditoría de TI, según la necesidad de la empresa.

Desarrollo

Para calcular el porcentaje de procesos del marco de COBIT 2019 y la norma ISO 19011, se realizó la selección de los procesos, para ello se realiza la Elaboración de la matriz de “Metas de negocio de la empresa CONECTA RETAIL S.A vs Metas Empresariales COBIT

2019.

Paso 01: ***Selección de Procesos COBIT 2019***

Realizamos la evaluación aplicando el procedimiento de Ingeniería Inversa, con el propósito de determinar los objetivos de gestión y gobierno de COBIT 2019 los cuales son: EDM, APO, BAI, DSS y MEA. Ver anexo 5.4.

Tabla V. Resultados del porcentaje de procesos obtenidos según la evaluación a los objetivos de COBIT 2019, mediante ingeniería inversa.

ABREV	DOMINIOS	Nº PROCESOS	%
APO07	Gestionar los Recursos Humanos	6	20%
BAI11	Gestión de Proyectos de Software	9	31%
DSS06	Gestión de Controles del Proceso del Negocio	6	21%
MEA02	Gestión del Control Interno	4	14%
MEA04	Gestión del Aseguramiento	4	14%
TOTAL PROCESOS		29	

Fuente: Elaboración propia.

En la tabla V, se aprecia los procesos de COBIT 2019 seleccionados a través de ingeniería inversa, considerándose fuertemente con lineamientos de gestión del desempeño de políticas de TI de la organización.

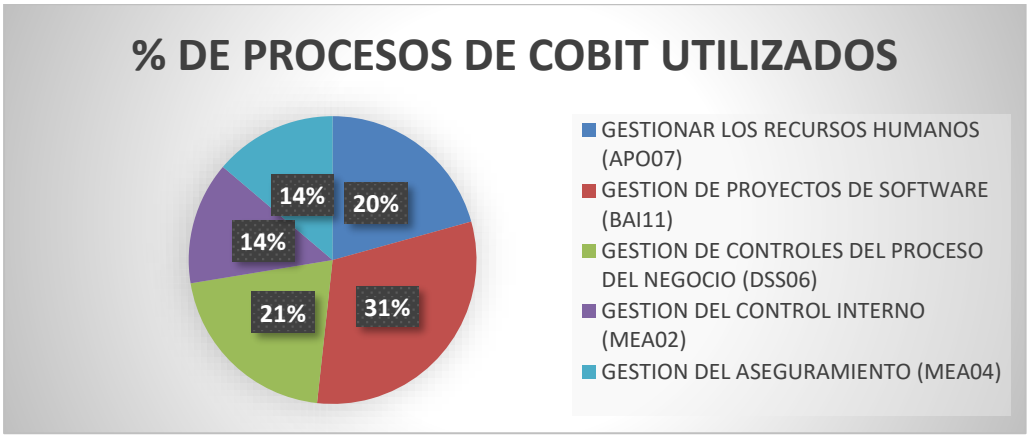


Figura 12.Porcentaje de la evaluación de los objetivos de gobierno de COBIT 2019.

Fuente: Elaboración propia

Paso 02: ***Selección de Procesos de la ISO 19011***

Realizamos la selección de una norma internacional que nos sirva como estructura para la construcción del modelo de auditoría de TI. Desarrollamos la evaluación de los procesos del estándar internacional ISO 19011 para seleccionar los más idóneos para la empresa retail. La ISO 19011 fue escogida porque es una norma que establece directrices para las auditorías de TI, implementando el ciclo de mejora continua, para una gestión de auditoria exitosa.

Tabla VI.Procesos de la ISO 19011 para la estructuración del modelo de auditoría de TI.

Gestionar un programa de auditoria	Realización de una Auditoria
- Establecer objetivos - Establecer programa de auditoría - Roles y responsabilidades - Establecer alcance de auditoría. - Determinar recursos para auditoria. - Implementar el esquema de la auditoría - Selección de métodos de auditoría. - Selección de equipo de auditoria. - Resultados. - Informe de auditoría y distribución - Seguimiento de auditoría	- Establecer contacto con partes interesadas de la empresa. - Preparar actividades Revisión de la información. - Planificación. - Asignar tareas. - Preparar documentación analizada. - Ejecución de actividades de auditoría. - Realizar reunión de apertura. Acceso a la información de auditoria. - Recolectar y verificar datos. - Hallazgos. - Conclusión de la auditoría. - Acta de cierre. - Revisar y mejorar el esquema de auditoria. - Seguimiento de una auditoría

Fuente: Elaboración propia basada en la ISO 19011

Paso 03: ***Cálculo del porcentaje de procesos utilizados***

*Finalmente calculamos el porcentaje de los procesos **COBIT 2019** y los procesos del estándar **ISO 19011**, que serán utilizados para la construcción del modelo de auditoria de TI.*

Tabla VII.Porcentaje de los procesos seleccionados de COBIT 2019 y la Norma ISO 19011.

Documento	Cantidad de Procesos de marco COBIT y la Norma ISO 19011	Porcentaje %
COBIT 2019	29	58%
ISO 19011	21	42%
TOTAL	**50**	**100%**

Fuente: Elaboración propia.

En la figura 13, se constata que la ISO 19011 se está tomando como estructura del modelo de auditoría de TI, en cuanto a COBIT 2019, tiene un porcentaje de 58%, utilizando los procesos de EDM, APO, BAI, DSS y MEA.

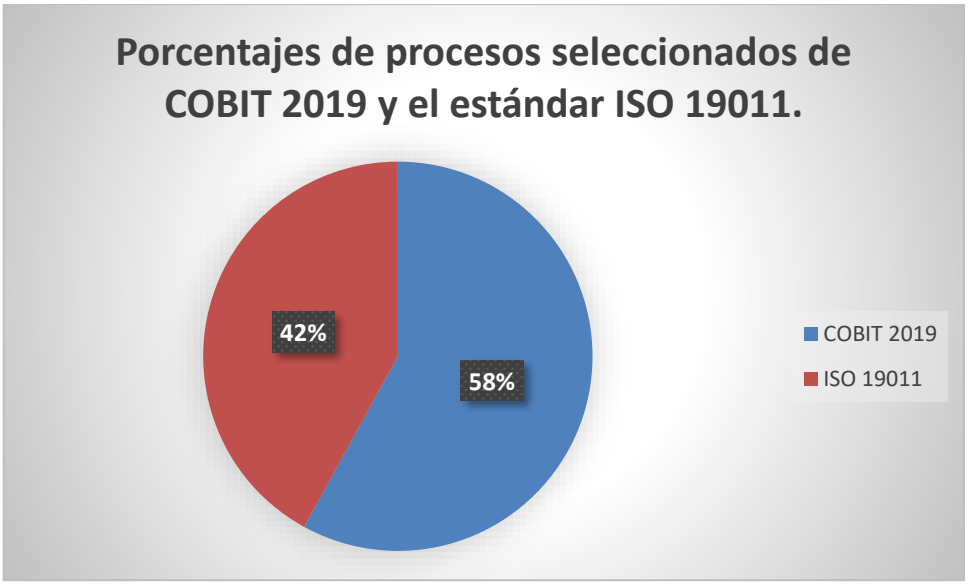


Figura 13.Porcentaje de procesos utilizados para desarrollar el modelo de auditoría.

Fuente: Elaboración propia

D. Evaluación del modelo de auditoría de TI por juicio de expertos

Este indicador Juicio de experto promueve un juicio objetivo para evaluar si el modelo es el adecuado y eficiente para ser aplicado a la empresa, para ello se ha conformado un grupo de expertos, en total 3 profesionales de TI, que tienen conocimientos y experiencias en auditorías, ciberseguridad, aseguramiento, etc.

Desarrollo

Los expertos realizaron su evaluación del modelo de auditorías frente a 5 criterios los cuales corresponden a: Claridad, objetividad, suficiencia, coherencia y pertinencia, la

evaluación en detalle se visualiza en el anexo 5.5

Tabla VIII.Resultados de la Evaluación del Modelo de Auditoria de TI por Juicio de Experto.

Criterio de calificación	Experto 01	Experto 02	Experto 03
claridad	4	4	4
Objetividad	4	4	4
Suficiencia	4	4	4
Coherencia	4	4	4
Pertinencia	3	4	4
Puntaje Promedio	3.93	4	4
TOTAL		**3.98**	

Fuente: Elaboración propia

Posteriormente al obtener el promedio final de evaluación de los expertos, se realiza la determinación de puntos de corte para determinar en qué escala se encuentra el modelo.

4	3.5	3	2.5	2	2.5	1	1.5	0
Muy adecuado		Bastante adecuado		Adecuado		Poco adecuado		Nada adecuado

Utilizando la escala de LICKER, se logra visualizar que el modelo es ***muy adecuado obteniendo un valor promedio de 3.98,*** lo que significa que se puede proceder en su ejecución.

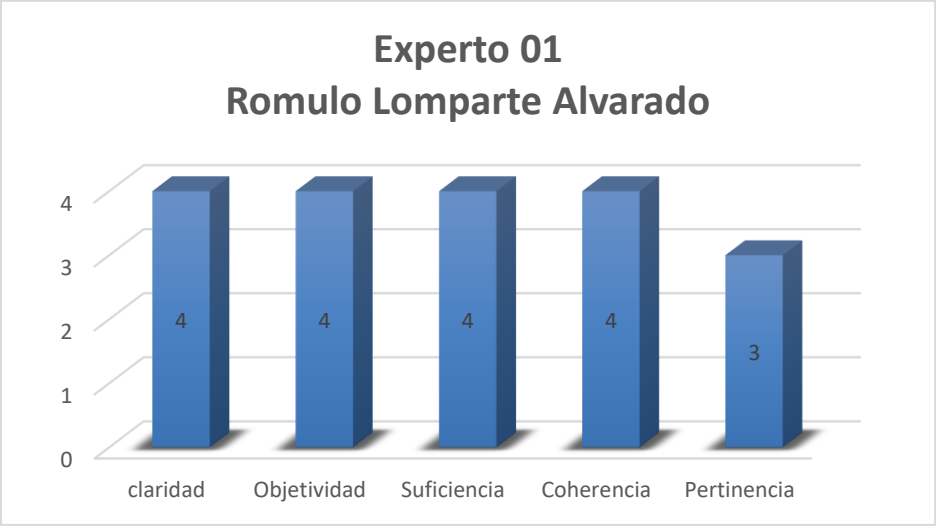


Figura 14.Resultado de evaluación del modelo de auditoría de TI por el Experto 01.

Fuente: Elaboración propia

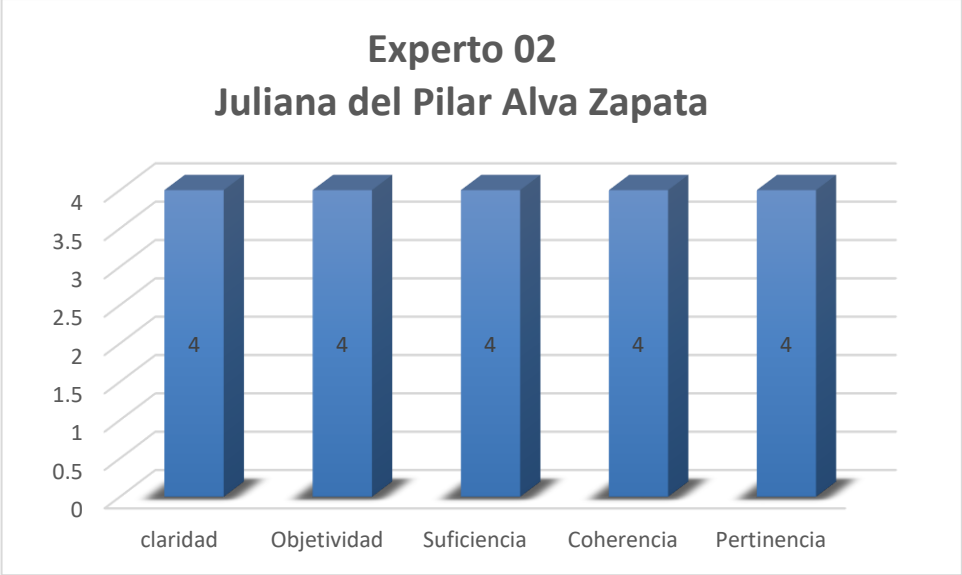


Figura 15.Resultado de evaluación del modelo de auditoría de TI por el Experto 02.

Fuente: Elaboración propia

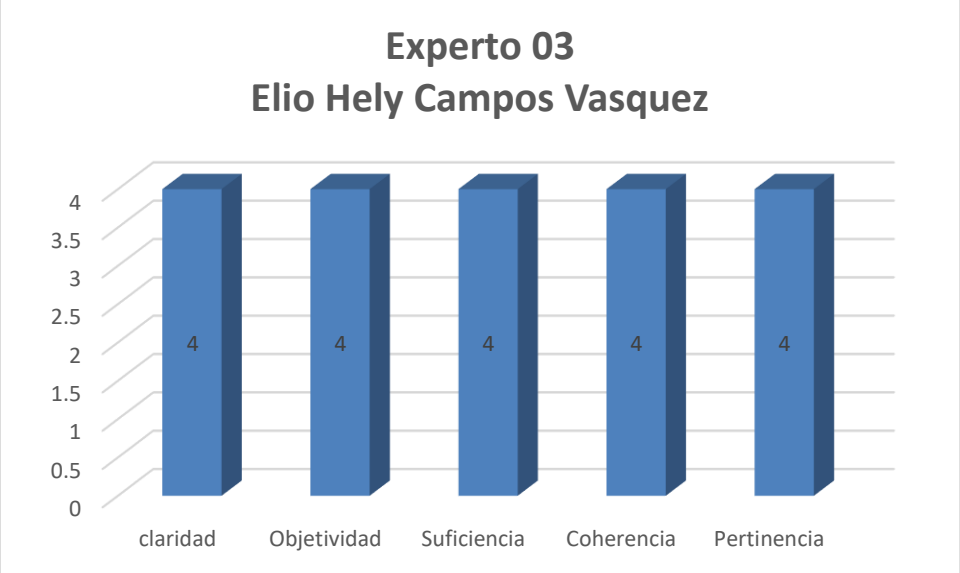


Figura 16.Resultado de evaluación del modelo de auditoría de TI por el Experto 03.

Fuente: Elaboración propia

3.1.2. Variable dependiente

A. Porcentaje de cumplimiento de actividades del marco COBIT 2019

Este indicador nos permite evaluar el porcentaje de cumplimiento de los dominios de gestión de COBIT los cuales son: DSS06, BAI11, APO07, MEA02, MEA04, para identificar que actividades son ejecutadas por la empresa.

Desarrollo

Se realizó una Bitácora de recopilación de información para identificar las actividades del área de TI enfocadas en las políticas de TI de la empresa y se compararon con los procesos del marco COBIT 2019. Ver anexo 5.6

Tabla IX.Resultado de Porcentaje de cumplimientos de las prácticas de gestión del marco de COBIT 2019 enfocados en políticas de TI de la empresa.

Marcos	Dominios	Actividades	%	Total %
COBIT 2019	DSS06	DSS06.01	100	91%
		DSS06.02	87	
		DSS06.03	100	
		DSS06.04	80	
		DSS06.05	80	
		DSS06.06	100	
	BAI11	BAI11.01	80	94%
		BAI11.02	90	
		BAI11.03	100	
		BAI11.04	90	
		BAI11.05	100	
		BAI11.06	100	
		BAI11.07	100	
		BAI11.08	90	
		BAI11.09	100	
	APO07	APO07.01	100	94%
		APO07.02	100	
		APO07.03	100	
		APO07.04	86	
		APO07.05	75	
		APO07.06	100	
	MEA04	MEA04.01	100	86%
		MEA04.02	85	
		MEA04.03	85	
		MEA04.04	75	
	MEA02	MEA02.01	100	85%
		MEA02.02	83	
		MEA02.03	86	
		MEA02.04	72	
% TOTAL				**90%**

Fuente: Elaboración propia basada en COBIT 2019.

Denotando que las actividades cumplidas tienen un porcentaje de 90% y la actividad

de menor cumplimiento abarca un 10% que puede disminuir aplicando el proceso de mejora continua, lo que indica que hay adecuado control para identificar e informar incidencias y solucionarlas de manera inmediata, indicando que el cumplimiento de controles en la empresa es eficiente. Cabe rescatar que al alto porcentaje de cumplimiento la empresa está alineada a una gran parte de las actividades de COBIT 2019.

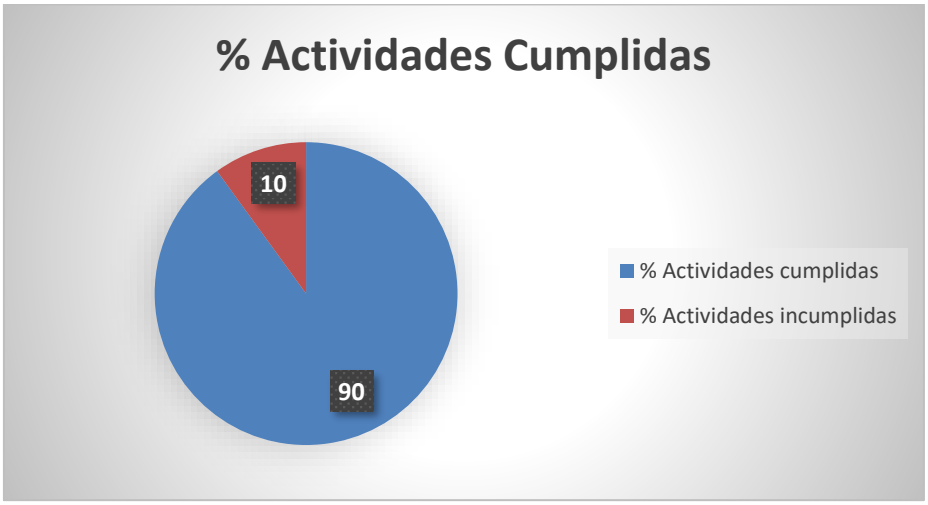


Figura 17.Evaluación de la cantidad de cumplimientos de actividades de COBIT 2019.

Fuente: Elaboración propia.

B. Porcentaje de cumplimiento de políticas

Para realizar la evaluación del cumplimiento de políticas de la empresa nos reunimos con el jefe Encargado del área de TI de la empresa CONECTA RETAIL S.A., posterior a la ejecución de modelo de auditoría de TI, se obtuvo un informe final de auditoría de TI, donde logramos identificar el porcentaje de cumplimiento de políticas establecidas en la empresa, obteniendo como resultado final una matriz de cumplimiento validado y firmado por el Ingeniero Jorge Cachay Arana, jefe encargado del área de TI de la empresa.

POLÍTICAS DE LA EMPRESA CONECTA S.A.C			
N°	Politicas	Observaciones	% Cumplimiento
1	Politicas de seguridad Lógica	Esta politica abarca todos los recursos informaticos de la empresa CONECTA RETAIL S.A.C. Y aquellos usuarios que son definidos implicitamente en los sistemas y que sirve para realizar	90%
2	Politicas de Seguridad Personal	El area de sistemas realiza periodicamente una revision de los equipos portatiles asignados a trabajadores , registrando los estados de estos y el motivo del cambio. El area de de riegos definira la	90%
3	Politica de seguridad fisica y ambiental	Esta politica se aplica a todas las areas de la empresa CONECTA RETAIL S.A.C que usa los servicios tecnologicos de la empresa. Esta politica abarca todos los centros de computo que cuentan con	100%
4	Politicas para el inventario de activos y classificación de la	Esta politica cuenta con escalas de clasificación de la información, según su nivel de criticidad. La gerencia de sistemas es la responsable de realizar el inventario de los activos de tecnologia de la	80%
5	Politicas para la administracion de operaciones y comunicaciones	Esta politica se enfoca en definir las reglas de seguirdad para el area de TI de la empresa CONECTA RETAIL S.A.C. El sistema core del negocio cuenta con mecanismos que les permite detectar	100%
6	Politica de adquisición, desarrollo	Esta politica controla el proceso de desarrollo, protege la informacion critica y apoya en el control de	

Figura 18.Porcentaje de cumplimiento de políticas de la empresa CONECTA RETAIL S.A.

Fuente: Elaboración propia

Tabla X. Porcentaje de cumplimientos de políticas de TI de la empresa

Políticas	%Cumplimiento
Nº 01	90
Nº 02	90
Nº 03	100
Nº 04	80
Nº 05	100
Nº 06	100
Nº 07	100
Nº 08	90
Nº 09	100
Nº 10	100
Nº 11	100
TOTAL	**93%**

Fuente: Elaboración propia.

Los resultados obtenidos de la evaluación arrojan que la empresa cumple con el 95.5% en cuanto a políticas de TI, lo que implica que la empresa está cumpliendo de forma congruente con cada una de las políticas estipuladas en su MPP (Manual de Políticas de Procesos)

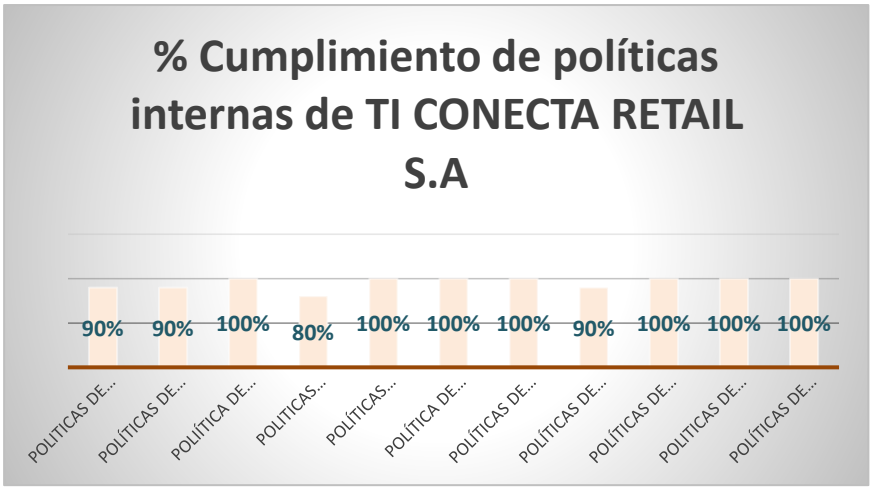


Figura 19. Porcentaje de cumplimientos de actividades de COBIT 2019.

Fuente: Elaboración propia.

3.2. Discusión

De forma general se identifica que la Empresa Conecta Retail S.A. se enfoca en el cuidado de la gestión y mejora de sus procesos de TI, y en el cumplimiento de normas y estándares que le permitan tener un desarrollo evolutivo, sin embargo, la empresa no cuenta un marco y estándar bien definido que le permita evaluar el cumplimiento las políticas de TI establecidas por la empresa. Para determinar la situación actual de las políticas de TI, se hizo una revisión del Manual de Políticas y Procesos de la empresa retail. Frente a estas políticas, se optó por construir una bitácora de documentos oficiales reconocidos internacionalmente, para conocer de manera exhaustiva que normas y estándares enfocados a las auditorias de TI, se encuentran alineados a las políticas, objetivos y procesos de la organización, con la finalidad de obtener un diseño de auditoría de TI bien estructurado. Según [38] indican que, para obtener un alineamiento eficaz de los objetivos y una óptima infraestructura de la organización, lo más eficiente es ejecutar políticas efectivas, que se puedan interpretar para ser gestionadas por los recursos adecuados, garantizando la retroinformación segura para la evaluación de su cumplimiento.

Consecuentemente, para determinar el marco y estándar más apropiado para ser aplicado, se ha realizado un estudio de variables y características comunes con la finalidad de obtener referencia del estándar y un marco que permita la comparación y análisis de su

estructura y aplicación en auditorias de TI. Determinando que la norma ISO 19011 y el marco COBIT 2019, son los más apropiados para ser aplicados, según los criterios de evaluación establecidos para diseñar un modelo de auditoría de TI con las directrices idóneas y efectivas, alineadas a las políticas de TI y objetivos de la organización. Según [15] utilizar mecanismos de recolección de documentos permite reconocer e identificar metodologías que estén alineados a la auditoría de TI como son: página oficial de ISACA, ISO, NIST, marco de gobierno COBIT 2019, así mismo permite realizar un análisis minucioso para visualizar las características y variables que ayuden a determinar parámetros de cada estándar o norma, realizando cuadros comparativos para definir la estructura más eficiente para la empresa.

Por otro lado, para el diseño del modelo de auditoría de TI, se ha designado un porcentaje de procesos de la Norma ISO 19011 y COBIT 2019, según las características de la empresa obtenidos después de la evaluación diagnostica realizada, se ha estructurado el modelo, combinando el estándar ISO 19011, la cual contempla 7 fases de procesos aplicados y el marco COBIT 2019, que consta de 40 objetivos de gestión, de los cuales han sido seleccionados los dominios de MEA02, MEA04, BAI11, APO07 y el DSS07

La estructura general está basada en el Ciclo de Mejora Continua implementado por la ISO 19011, aplicando sus cuatro etapas: PLANEAR () EJECUTAR () VERIFICAR () ACTUAR (), En la etapa de planear, establecimos 3 fases: Planear la auditoria, seleccionar el equipo de auditoría, principios de confidencialidad, todas basadas en la ISO 19011. En la etapa de ejecutar instauramos 6 objetivos de gestión de COBIT 2019 los cuales son: verificar la gestión del sistema del control, verificar la gestión del aseguramiento, verificar la gestión de los procesos, verificar la gestión de los proyectos, verificar la gestión de los recursos. En la etapa de verificación aplicamos nuevamente la ISO 19011 estableciendo la fase de hallazgos y observaciones y la fase del informe final. Posteriormente en la etapa de Actuar, se aplican las fases actividades de seguimiento y la fase final de revisión y mejora de la propuesta de auditoría. De esta manera se logró estructurar el modelo teniendo como resultado un modelo alineado a las políticas, procesos y objetivos de la empresa, obteniendo como resultado que la ISO 19011 y COBIT 2019, son congruentes para ser unidos y obtener

un constructo ideal para ser aplicado a la empresa CONECTA RETAIL S.A.

Consecuentemente al obtener el modelo de auditoría de TI, este pasa por una evaluación de juicio de experto, seleccionando profesionales expertos y capacitados, con experiencia en Auditoría de TI, cumplimiento, ciberseguridad, gestión de riesgos, etc. De esta manera los expertos podrán evaluar el nuevo modelo, basados en su experiencia a través de criterios evaluativos, puedan brindarnos una valoración del modelo, indicando la valides o no valides del modelo de auditoría de TI, para ser aplicado a la empresa. Tres expertos evaluaron el modelo, obteniendo un puntaje global de 3.93, lo que indica que nuestro modelo obtenido es Bastante adecuado, según la determinación de los puntos de corte, lo que significa que el modelo puede ser ejecutado en la empresa, y de esta forma determinar el cumplimiento de políticas de la organización.

Para la ejecución del modelo, se ha calculado el tiempo de ejecución del modelo de auditoría de TI, donde logramos determinar las horas requeridas, la cual asciende a 129 horas fueron aplicadas para efectuar las actividades que se desarrollan en la auditoría, según cada fase establecida las cuales son: Planear, Hacer, Verificar y Actuar, estas fases aplican las buenas prácticas implementadas en la ISO 19011 estipuladas en la ejecución de auditoría que se encuentra en la cláusula 6.

Los resultados conseguidos posteriores a la ejecución del Modelo de Auditoria de TI, en el contexto presente del área de TI de la organización CONECTA RETAIL S.A. evidencia algunas debilidades en cuanto al desarrollo de procedimientos de cumplimiento basados en auditorías de TI, dichos datos fueron el resultado del análisis de la documentación plasmada en los MPP de la organización, los cuales fueron contrastados con los estándares y políticas de la organización que se tomaron como referencia en la evaluación.

La aplicación del modelo de auditoría de TI nos ha permitido fortalecer debilidades y mejoras que ayudan al cumplimiento de objetivos y políticas empresariales de CONECTA RETAIL S.A., mediante las recomendaciones emitidas con el objeto de que las partes interesadas operen de manera productiva y efectiva en sus actividades diarias y sobre todo realice el cumplimiento general de la normativa establecida en los documentos del MPP. Así

mismo [2],menciona, que a pesar de existir propuestas de ingeniería y modelos que permiten establecer un cumplimiento de políticas y normas idóneos en las organizaciones, hasta la fecha no se ha logrado que los modelos se adapten a todas las entidades, el motivo fundamental es que cada país tiene diversas capacidades, infraestructura, gestión de políticas y, presupuesto para la gestión de activos, es por esta razón que los modelos no se adaptan de forma oportuna en la organización quedando como simples modelos referenciales no aplicables.

Las limitaciones que se evidenciaron en la investigación es el poco acceso a la información basados en modelos de auditorías de TI, sobre todo para pequeñas empresa, por ende antes de elegir un marco y estándar idóneo, lo más oportuno es realizar una evaluación de la empresa, que nos lleve a obtener un diagnóstico minucioso, para construir un modelo adecuado basados en las características de las políticas y objetivos de la organización, visualizando sus mecanismos aplicados, de esta manera nos enfocamos en que procesos son los más recomendados en ser implementados.

3.3. Aporte de la investigación

a) Diagnosticar la situación actual de las políticas de TI de la empresa para la elaboración de un modelo de auditoría de TI.

El diagnóstico inicial es necesario para identificar que políticas de TI existen en la organización, y en base a los resultados plantear un modelo de auditoría de TI, que se encuentre acorde con los requerimientos de la organización. Para ello, entrevistamos al jefe representante del área de TI, de la empresa CONECTA RETAIL S.A, para que nos brinde la información pertinente y de esta manera evaluar y diagnosticar la situación actual de la empresa. Se aplicó una matriz de diagnóstico, para evaluar el nivel de madurez de la empresa enfocada en la implementación de políticas y controles internos de la empresa, utilizando la herramienta DS5 de COBIT que garantiza la seguridad de los SI, aplicando el objetivo de gobierno MEA02, para visualizar como se ejecuta la gestión de los procesos y evaluar si la empresa se plantea políticas que permitan obtener sistemas seguros e íntegros y verificar la eficacia de los controles internos del negocio.

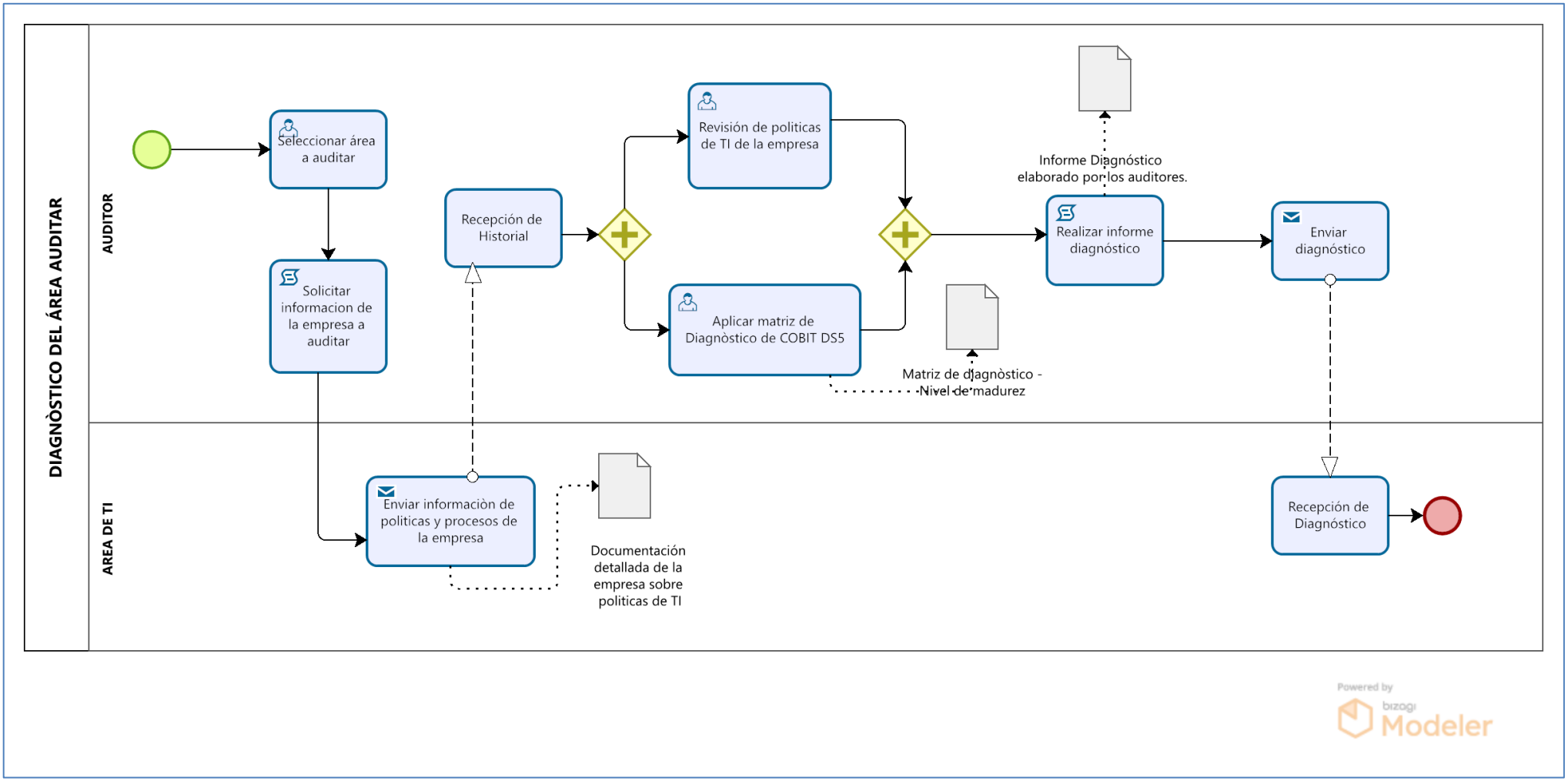


Figura 20. Diagrama de Diagnóstico de la empresa

Fuente: Elaboración propia.

Tabla XI. Matriz de diagnóstico de la empresa CONECTA RETAL S.A – DS5 COBIT

			Evaluación			Porcentajes		
NIVEL	PROPÓSITO	MEA	No cumple	Cumple	Total	No cumple	Cumple	Total
Nivel 0	Políticas del negocio	¿La organización cuenta con políticas de TI?		1	5	0%	100%	100%
		¿Los recursos y actividades enfocadas en los sistemas de Información, se ajustan a los requerimientos de las políticas de TI la entidad?		1				
		¿Se estipulan los porcentajes de conformidades basadas en el cumplimiento de políticas de la empresa?		1				
		El área de TI asigna formalmente responsabilidades que permitan llevar el monitoreo efectivo de las políticas de TI?		1				
		El área de TI busca el cumplimiento de las políticas de TI manera continua.		1				
Nivel 1	MEA 02.01 Supervisar los controles internos	¿La empresa realiza acciones de seguimiento para evaluar de forma efectiva los procesos del negocio?		1	6	0%	100%	100%
		¿La organización aplica todas las iniciativas de aseguramiento que han sido planeadas, para posteriormente ser ejecutadas de manera pertinente?		1				
		Se gestiona de manera frecuente, la supervisión, de controles de TI para alcanzar el control y cumplimiento de políticas de la empresa.		1				
		Se realiza la inspección de controles, operaciones y pruebas, que evalúan que los controles aplicados a los SI, ¿funcionan de forma pertinente?		1				
		¿Se constata que n el desarrollo de las actividades de TI, se aplican mecanismos de evaluación constante de controles y supervisión de los centros de operación de red y centros de mando?		1				
		¿La entidad se preocupa por la aplicación de controles de los SI buscando la efectividad de los requisitos de las políticas del negocio?		1				
Nivel 2	MEA 02.02 Revisar la eficacia de los controles del proceso de negocio	¿Se obtienen porcentajes de los programas de aseguramiento que ejecuta la empresa que son probados, basados en estándares de planificación?		1	8	0%	100%	100%
		¿Se estimula a la alta dirección para que tomen medidas adecuadas enfocadas en el mejoramiento de los procedimientos aplicados a los CI?		1				
		¿Se ejecutan programas de evaluación que permitan obtener valores de la eficacia en cuanto la aplicación de políticas y contratos		1				

		del negocio?						
		¿Se plantean objetivos específicos a la función de TI?		1				
		¿Se logar reconocer de forma jerárquica de quien depende la unidad de TI?		1				
		¿Las función y responsabilidad de la unidad de TI es identificable?		1				
		¿La entidad cuenta con un plan de estrategias de TI?		1				
		La entidad logra identificar los riesgos que se encuentran asociados a las TI?		1				
Nivel 3	MEA 02.03 Realizar autoevaluaciones de control	¿El área de TI establece sus controles internos comunicando las deficiencias de manera oportuna?		1	6	14%	86%	86%
		¿Se tiene la trazabilidad del tiempo transcurrido cada vez que se efectúa una ocurrencia producto de las deficiencias de CI?		1				
		Se identifican las deficiencias de control del área de TI?		1				
		¿Se tiene un diseño documentado de alguna metodología de TI I?						
		¿Se conocen las normas y políticas aplicables a TI para la unidad?		1				
		¿Se han puesto de manifiesto los objetivos y funciones de TI al personal interesado?		1				
		¿El personal del área de TI cuenta con habilidades y conoce como debe establecer su función en cada uno de los procesos?		1				
Nivel 4	MEA 02.04 Identificar y reportar deficiencias de control	¿El proceso de TI es indispensable la lograr el éxito de la entidad?		1	11	36%	64%	64%
		¿Está definido y claro quién tiene la máxima responsabilidad en la instancia del resultado final de la verificación y supervisión de los CI y aplica las medidas correctivas?	1					
		¿Los procesos son realizados formalmente?		1				
		¿Los procesos son realizados correctamente?	1					
		¿Está definido de manera clara quien es el responsable del proceso?		1				
		¿Los procesos están bien definidos y tienen objetivos claros?		1				
		¿Se mide el desempeño de cada proceso?		1				
		¿Los procesos son auditados?		1				
		¿Se logra identificar las debilidades de los controles implementados en cada proceso?	1					
		¿La tecnología utilizada presenta vulnerabilidades?	1					
Nivel 5	MEA 02 Plan de continuidad y ejecución	¿Se ha establecido, un plan de seguridad y se ha comunicado a las partes interesadas?		1				
		¿Existen soluciones de seguridad de información que son implementadas	1					

	medidas correctivas	aplicando procedimientos de manera eficiente en toda el área de TI?						
		¿El alcance, políticas de los MPP son viables y están alineados a sus objetivos?		1				
		¿El personal relevante se compromete con los programas para minimizar la deficiencia del CI?	1					
		¿Los proyectos y las actividades son ejecutados de acuerdo al plan de acción establecido?		1				
		¿Los servicios críticos se adaptan con facilidad?	1					
		¿Al realizar pruebas de servicios se evidencia la eficiencia del plan de continuidad determinado?		1	9	44%	56%	56%
		¿El plan de continuidad muestra los requerimientos del área de TI?	1					
		¿El personal interesado tanto interno como externo son entrenados para ejecutar el plan de continuidad?		1				
		Validación Sumatoria de Totales de No Cumple Cumple	8	38	46			

Fuente: Elaboración propia, basada en COBIT- Herramienta de evaluación DS5

Tabla XI.Resultado de diagnóstico de la empresa CONECTA RETAL S.A

NIVEL ACTUAL	
Descripción	**Cumple**
Nivel 0	**100%**
Nivel 1	**100%**
Nivel 2	**100%**
Nivel 3	**86%**
Nivel 4	**64%**
Nivel 5	**56%**

Fuente: Elaboración propia

La empresa CONECTA RETAIL S.A se encuentra en un nivel de madurez de grado 3, a un 86% de cumplimiento, porque como es una empresa que brinda servicio a clientes y

cuenta con base de datos, estas deben ser resguardadas, velando para que los datos de usuario sean íntegros y confiables, así mismo debe existir conciencia de seguridad de la información, pues de no hacerlo puede provocar riesgos en la continuidad del negocio. Según los resultados de diagnóstico, se puede visualizar que se cuenta con políticas y controles internos, sin embargo, se recomienda que se implementen pruebas de seguridad que ayuden a cerciorarse que la información obtenida está bien protegida, así mismo es viable que se realicen capacitaciones constantes al personal en cuanto al manejo de credenciales de los sistemas utilizados.

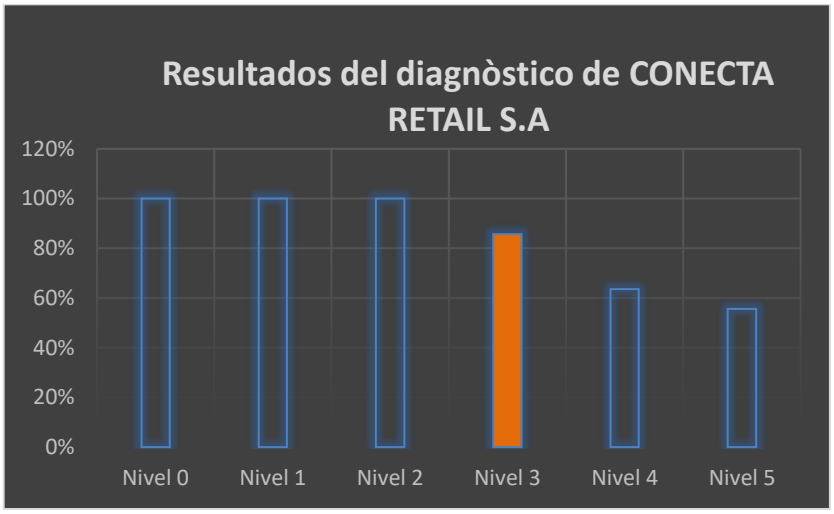


Figura 20.Resultado de diagnóstico de la empresa CONECTA RETAL S.A.

Fuente: Elaboración propia.

Posterior a realizar el diagnóstico, el equipo encargado de realizar la auditoría, identifica las políticas de la empresa extraídas del MPP, así mismo realiza un mapeo de los procesos del marco internacional COBIT 2019 y la norma ISO 19011 para diseñar un modelo que permita evaluar de manera minuciosa el cumplimiento eficiente de las políticas y normas según los criterios establecidos por la empresa.

Tabla XII.Identificación de Políticas de la Empresa CONECTA RETAIL S.A.

POLÍTICAS DE LA EMPRESA CONECTA S.A.C		
N°	**Políticas**	**Observaciones**
1	**Políticas de seguridad Lógica**	Esta política abarca todos los recursos informáticos de la empresa CONECTA RETAIL S.A. y aquellos usuarios que son definidos implícitamente en los sistemas y que sirve para realizar instalaciones de software, administrar sistemas, asignar roles, etc.
2	**Políticas de Seguridad Personal**	Se registra de manera periódica una revisión de los equipos portátiles asignados a trabajadores, registrando los estados de estos y el motivo del cambio. El área de riegos definirá si es factible realizar la capacitación del personal involucrado en SI.
3	**Política de seguridad física y ambiental**	Aplicada a todas las áreas de la empresa que usan los servicios tecnológicos de la empresa. Esta política abarca todos los centros de cómputo que cuentan con servidores y controladores de comunicaciones para el desarrollo de la información.
4	**Políticas de inventario y clasificación de datos**	Esta política cuenta con escalas de clasificación de la información, según su nivel de criticidad. La gerencia de sistemas es la responsable de realizar el inventario de los activos de tecnología de la información, y actualización.
5	**Políticas para la administración de operaciones y comunicaciones**	Esta política se enfoca en definir las reglas de seguridad para el área de TI de la empresa CONECTA RETAIL S.A. El sistema Core del negocio cuenta con mecanismos que les permite detectar anomalías que avisan al administrador todo tipo de eventos realizados.
6	**Política de adquisición, desarrollo y mantenimiento de sistemas informáticos**	Esta política controla el proceso de desarrollo, protege la información crítica y apoya en el control de la ejecución y mejora del proceso. El área de sistemas lleva el control responsable de los sistemas, software, licencias, etc.
7	**Políticas de respaldo**	Esta política define las reglas que norman el manejo de los respaldos del sistema del área de TI de la empresa CONECTA RETAL S.A.
8	**Políticas de SI**	Se involucran políticas que logren asegurar la información que se considera como crítica y que se apliquen los controles necesarios ante su acceso no autorizado.
9	**Políticas de cumplimiento normativo**	Involucra políticas que aseguran que los requerimientos legales o de regulaciones sean cumplidos cuando corresponda, incorporado a una lógica interna de aplicaciones informáticas.
10	**Políticas de gestión de Incidencias de seguridad**	Involucra que, a través de notificaciones de eventos y puntos débiles de seguridad, se mejore los procedimientos y responsabilidades que se siguen para la mejora de la SI de la empresa.
11	**Políticas de subcontratación definitiva**	Esta política involucra que en caso haya suspensión del servicio, se realice subcontrataciones para no afectar los ingresos, solvencia o continuidad operativa del negocio.

a)

Fuente: Elaboración propia basado en el MPP de la empresa CONECTA RETAIL S.A

b) Seleccionar marcos y normas internacionales para la elaboración de un modelo de auditoría de TI.

Para la selección del marco y la norma para elaborar el modelo de auditoría de TI, se ha realizado previamente una revisión documental, basada en GRC, gestión, riesgo y cumplimiento, auditorias, etc. Para ello se aplican preguntas y se van seleccionando los documentos más congruentes y que indican los marcos y normas que se están aplicando hasta la fecha. RQ1. ¿Cuáles son los marcos y normas más utilizados para auditorias de TI en grandes, medianas y pequeñas empresas? RQ2. ¿Cuáles son los marcos y normas orientados para aplicar buenas prácticas en auditorías de TI?, RQ3. ¿Cuáles son los marcos y normas que aplican objetivos de gobierno y/o directrices para realizar auditorías de TI?, RQ4. ¿Cuáles son los marcos que aplican metas empresariales de TI y normas para realizar auditorías eficaces?

Con la documentación obtenida, el auditor tendrá los conocimientos necesarios para realizar auditorías de TI tanto externas como internas, con el fin que tenga las condiciones idóneas para identificar los marcos y normas aplicados en las áreas involucradas dentro de la entidad para evaluar y analizar las posibles carencias del área de TI.

Posteriormente se efectúa el estudio y la selección de marcos y normas internacionales mediante un cuadro comparativo, basado en criterios selectivos, el cual es revisado por juicio de experto, determinando si el marco seleccionado es el más idóneo para diseñar el modelo de auditoría de TI.

Tabla XIII.Cuadro comparativo de marcos y normas.

Ítem	ITIL	COBIT 2019	ISO 19011	NIST	ISO 27001	RISK IT
Dirigido a	Empresa pequeña, mediana y grande	Empresa Grande, mediana y pequeña	Empresa pequeña, mediana y grande	Empresa medianas y grandes	Empresa pequeña, mediana y grande	Empresa mediana y grande
Orientado a	Buenas prácticas en el beneficio a los servicios de TI	Aplicar buenas prácticas en los recursos de TI	Auditoria a los sistemas de gestión organizacional	Orientado al análisis de los riesgos empresariales	Requisitos que establecen la documentación y evaluación de SGS en las organizaciones	Buenas practicas aplicadas a la gestión de riesgos
Constituido por	Compuesto por Ciclo de vida del servicio	Objetivos de gobierno, gestión y cumplimiento. Compuesto por proceso de control organizacional.	Compuesto en principios, gestión en competencia y evaluación de auditores	Compuestos por elementos, eventos y procesos	Compuesto por cláusulas y controles de los SI	Está constituido por áreas para el control interno
Finalidad	Evaluación de calidad de prestación regular	Cumplimiento de metas organizacionales	Finalidad de una planeación y realización de las auditorías.	Proporcionar principios básicos y requisitos para la protección de datos.	Tiene la finalidad de definir un control para garantizar la integridad y confidencialidad de información.	Mide el grado de riesgos de las empresas

Fuente: Elaboración propia.

Se evidencia los resultados obtenidos de los marcos seleccionados más adecuados para el diseño del modelo de auditoría de TI, para visualizar los criterios de evaluación donde se obtuvieron los resultados finales ir al anexo 5.2.

Tabla XIV.Resultado de la evaluación de los marcos internacionales más adecuados para la construcción del modelo de auditoría de TI.

CRITERIOS	ITIL	**COBIT 2019**	NIST	**ISO 19011**	ISO 27001	RISK IT
DIRIGIDO	5	5	5	5	5	1
ORIENTADO	1	5	2,5	5	5	2,5
CONSTITUIDO	2,5	5	2,5	5	5	5
FINALIDAD	2,5	5	2,5	5	2,5	2,5
PROMEDIO	2,8	5	3,1	5	4,4	2,8

Fuente: Elaboración propia

En la tabla se visualiza el resultado final obtenido, se logra evidenciar que el marco con mayor puntaje es COBIT 2019 y la norma ISO 19011, indicando que son las más adecuadas para construir el modelo de auditoría de TI de la empresa.

c) Diseñar el modelo de auditoría de TI apoyado en un marco y una norma para la empresa en estudio.

El diseño del modelo de auditoría de TI, está distribuido en cuatro fases, las cuales están basadas en la norma ISO 19011 y el marco COBIT 2019, posteriormente se puntualizan cada una de las fases: FASE 01: Se realiza la planificación, donde se montará el plan de auditoría, se desarrolla el objetivo y alcance de auditoría. Así mismo se realiza la selección del equipo auditor y se establecen los principios de confidencialidad de la auditoría de TI. FASE 02: Se efectúa la elaboración de la auditoría donde se establece el contacto inicial con los representantes de la empresa CONECTA RETAIL S.A, para que nos facilite los datos requeridos para la construcción del diseño del modelo e auditoria de TI. Así mismo en esta fase se desarrollan cada una de las actividades establecidas como son: Gestionar el sistema de control interno del área de TI de la organización, gestionar el aseguramiento, gestionar los proyectos y gestionar los recursos humanos. FASE TRES: En este apartado se comprueba los efectos de la auditoría y se demuestran los hallazgos que se han identificado en la auditoría y las observaciones. Posteriormente se realiza la elaboración del informe final. FASE

CUATRO: En esta fase tenemos el seguimiento y mejora del proceso de auditoría, en este apartado se ha llegado a la etapa final de la auditoría, y según los resultados obtenidos, se proponen mejoras y recomendación para la organización, las cuales van a tener un seguimiento adecuado que verifique su cumplimiento.

El diseño del modelo de auditoría de TI, se realiza con la finalidad de tener una visión holística de cada una de las etapas del modelo y de cómo se efectuará el desarrollo de las actividades de auditoría. Así mismo se realiza el diseño previo, para que la empresa pueda estar alineada con los objetivos del marco implementado y pueda tener una mejor estructuración en cuanto al cumplimiento eficiente de las políticas y normas requeridas a implementar.

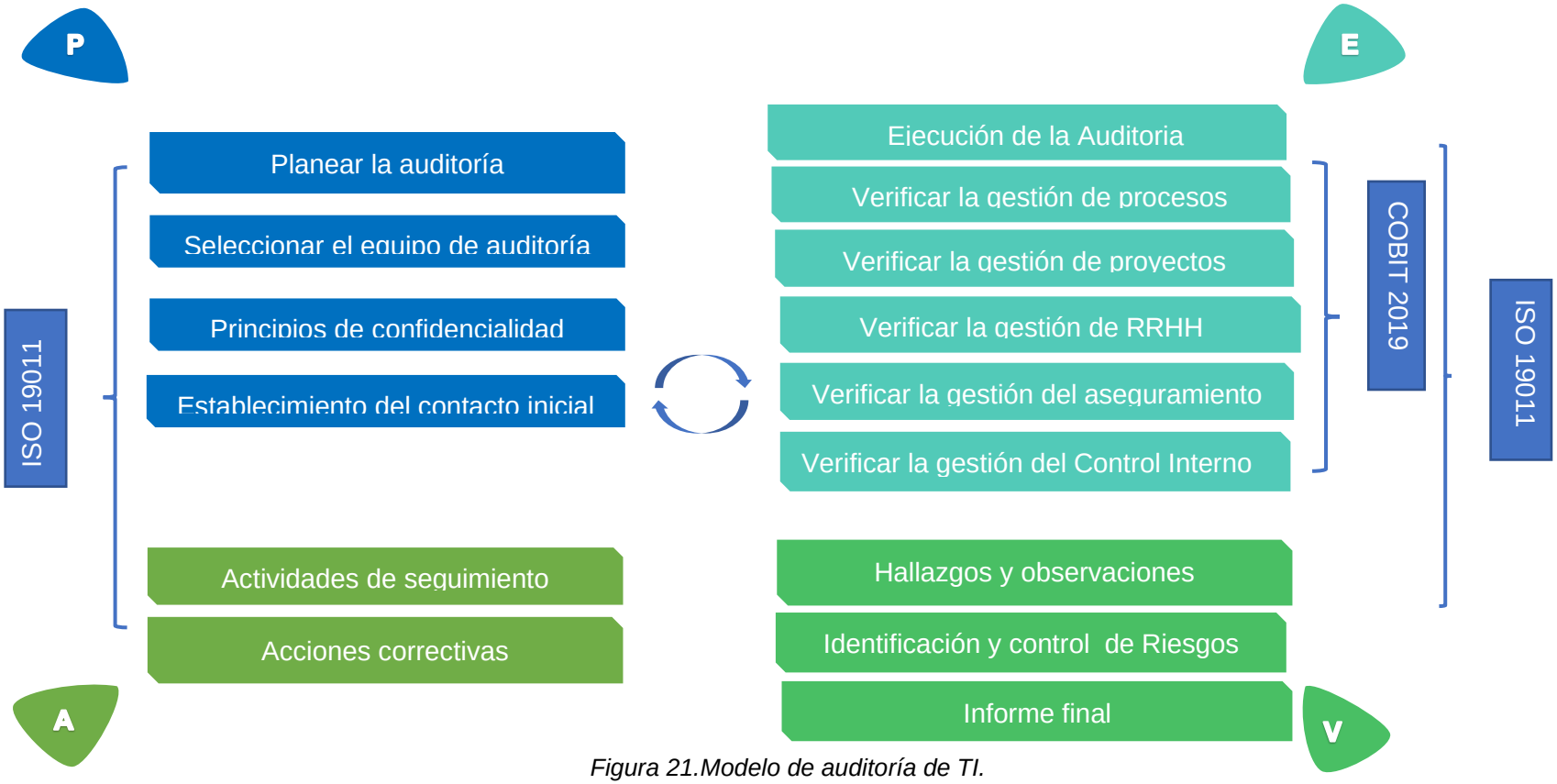


Figura 21.Modelo de auditoría de TI.

Fuente: Elaboración propia

Etapas del Modelo de Auditoría de TI

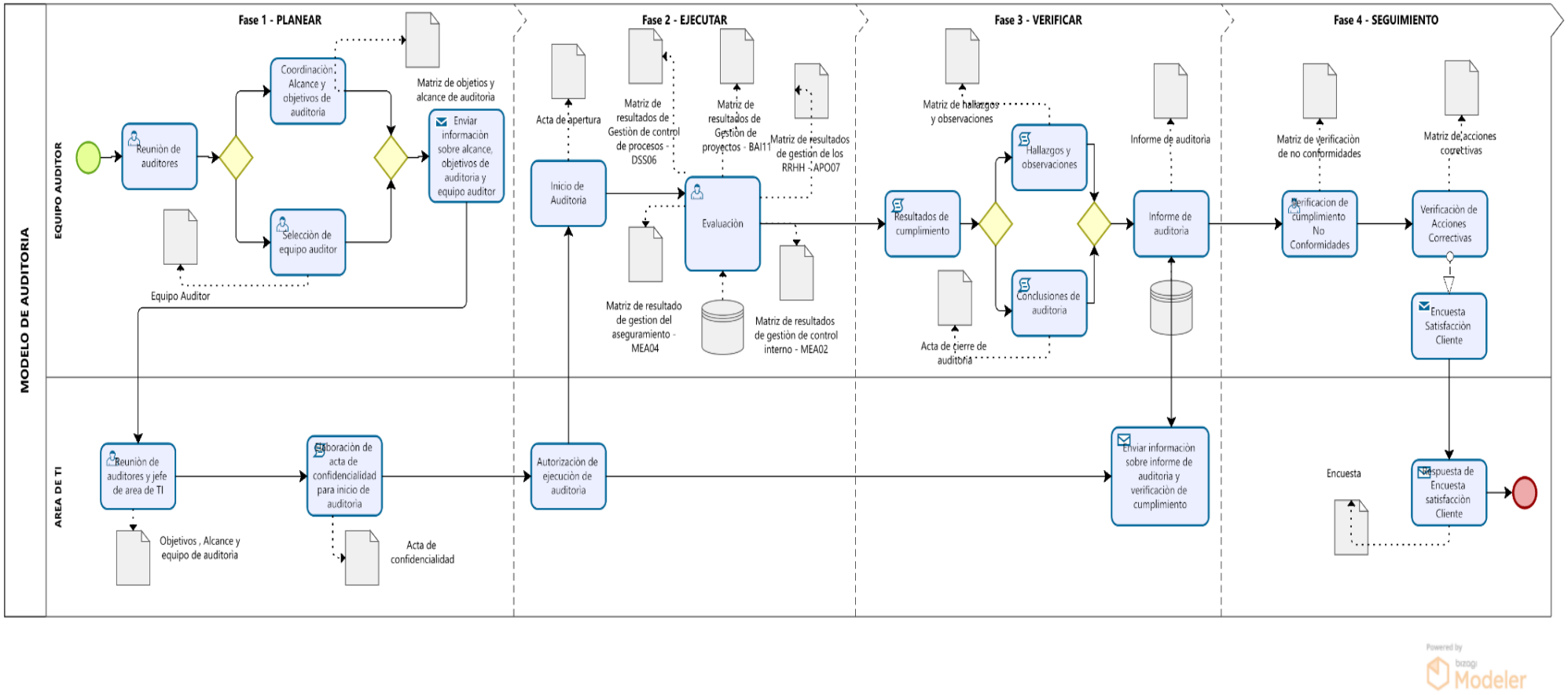


Figura 22.22Diagrama del Modelo de Auditoria de TI

Fuente: Elaboración propia

Diagrama de Actividades de Auditoría de TI

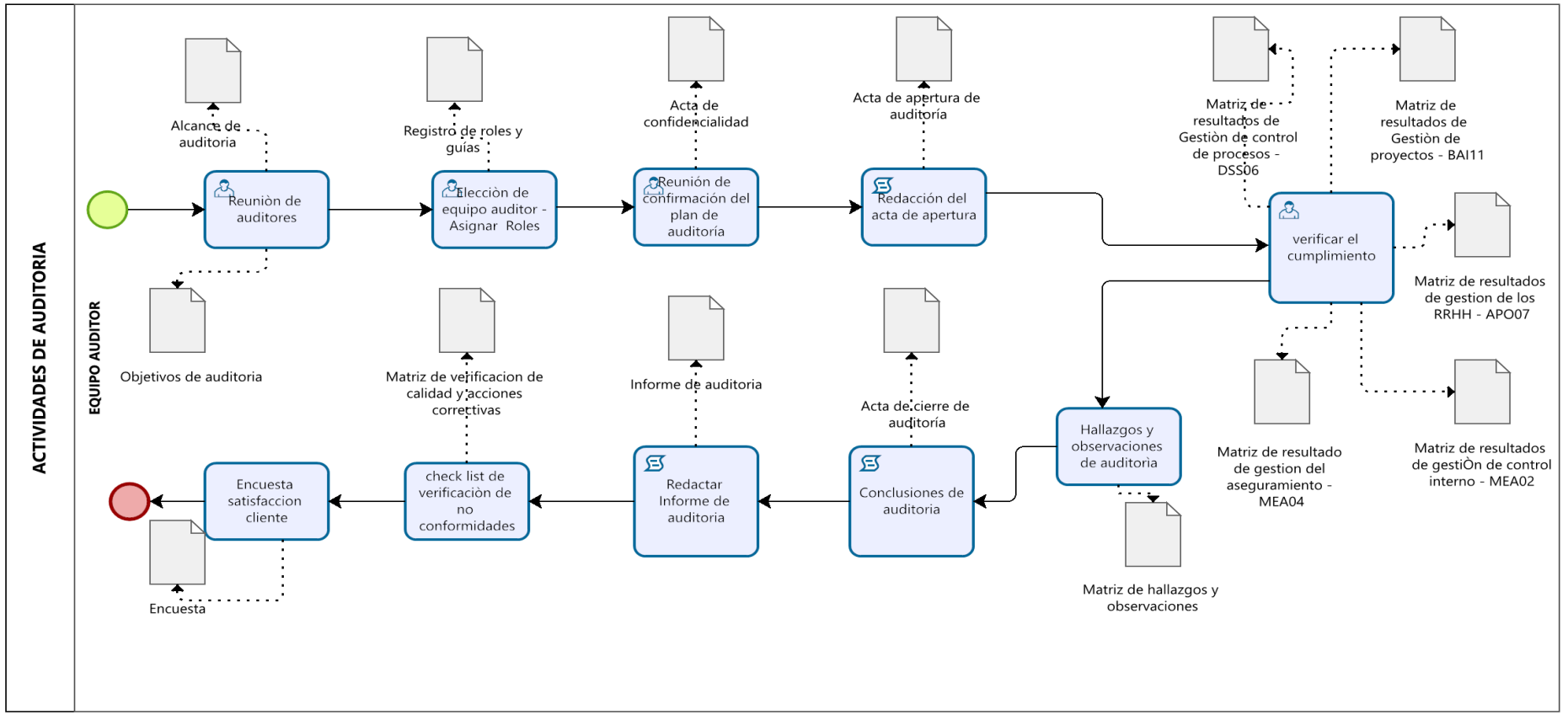


Figura 23.23Diagrama de actividades de Auditoria de TI

Fuente: Elaboración propia

Descripción del modelo diseñado

Para la elaboración del modelo de auditoría de TI propuesto, se está utilizando la Norma Internacional ISO 19011 y el marco COBIT 2019. Para el diseño del modelo, se realizó la alineación de metas empresariales de la empresa (ver anexo 5.4), de esta manera se busca tener un modelo coherente que permita realizar auditorías de TI en la empresa CONECTA S.A. que ayude al cumplimiento del programa de auditoría de manera eficiente. Para lograr una secuencia lógica que permita visualizar de una manera organizada, se utilizó diagramas SIPOC, en donde se identifican los elementos clave y el dominio de cada proceso.

1. Planear de la auditoria – Clausula 6.2.2 (ISO 19011)

La planificación se realiza por el equipo de auditoria, el cual busca que las actividades tengan un orden establecido y una secuencia lógica para alcanzar el cumplimiento de los objetivos de manera eficaz, así mismo esta etapa es importante, porque se realiza el contacto inicial con las partes involucradas de la organización, como establece la norma internacional ISO 19011 en esta etapa se presentan los objetivos de auditoria y se pactan las fechas en que se realizara cada actividad. El plan final debe contener cada una de las fases que serán desarrolladas en el programa de auditoría las cuales deben ser presentadas a las partes interesadas (Empresa auditada) para que pueda tener un alcance de la auditoria.

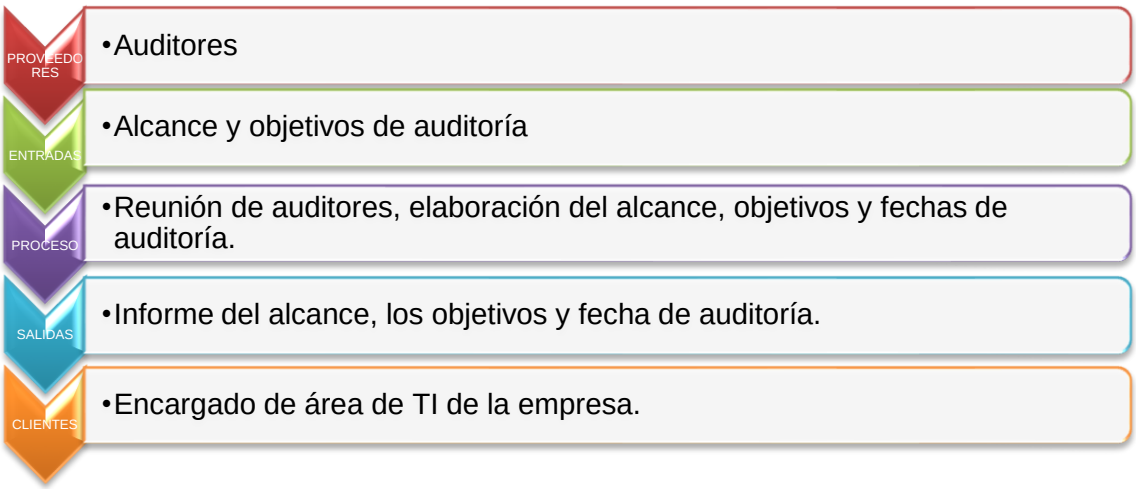


Figura 244.Diagrama SIPOC - Planificación de la auditoría

Fuente: Elaboración propia

1.1.Elección del equipo auditor (Clausula 5.5.4 - ISO 19011)

La selección de auditores es indispensable, porque se debe considerar un personal responsable y con experiencia en auditorías de Tecnologías de Información que cumpla las necesidades del esquema, como la norma ISO 19011 lo establece, determina para la selección del equipo auditor se debe efectuar una evaluación de competencias de cada unidad auditor, para ello se deben constituir criterios de evaluación (Comportamiento personal, competencias, experiencia de auditoría).

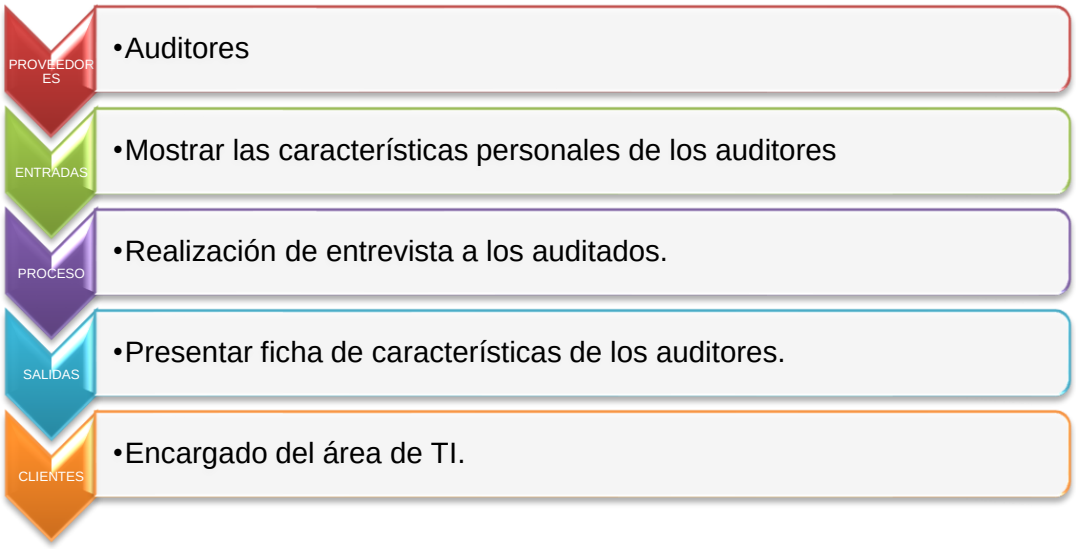


Figura 255.Diagrama SIPOC - Caracterización personal del equipo auditor.

Fuente: Elaboración propia

1.2. Principios de confidencialidad (Clausula 4 – ISO 19011)

La auditoría que se ejecuta en la empresa CONECTA S.A. se realiza bajo principios éticos fundamentales con el equipo auditor y la organización, según la ISO 19011, el auditor debe ser capaz de desarrollar un trabajo ético durante la auditoría, por ende, es indispensable que el material obtenido en el proceso de auditoria se mantenga de manera confidencial por cada miembro del equipo auditor.

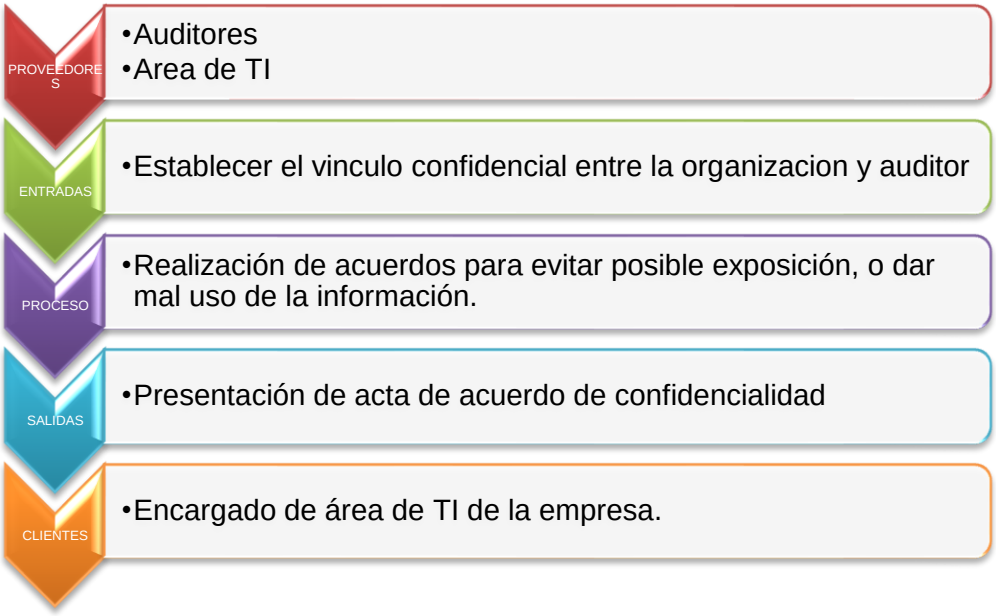


Figura 266.Diagrama SIPOC – Principios de confidencialidad.

Fuente: Elaboración propia

1.3. Establecimiento del contacto inicial

En este punto el auditor encargado hace su presentación de manera formal a las partes interesadas para contemplar los propósitos más sobresalientes de la auditoría como lo de certificar las vías de comunicación con el encargado del área de sistemas, presentar los auditores que realizarán la auditoría, manifestar el alcance, los objetivos, requerir el acceso a la información que sea conveniente entre otros.

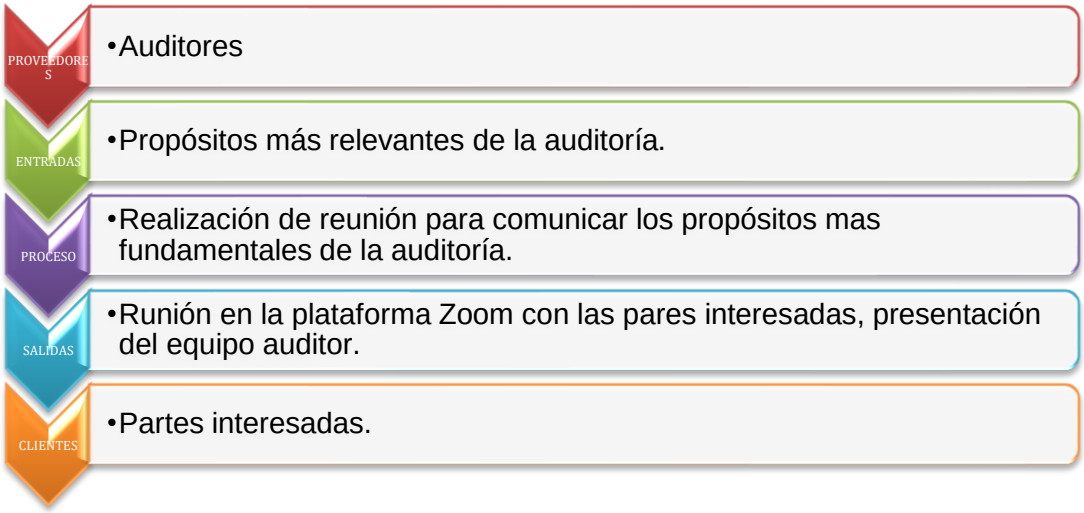


Figura 277.Diagrama SIPOC – Establecimiento del contacto inicial.

Fuente: Elaboración propia

2. Ejecución de la auditoria

Al inicio de la ejecución, se procede con el acta de apertura de la auditoria, donde se informan las pautas que se deben seguir a las partes interesadas, los objetivos y el propósito de la auditoria y posteriormente se procede a evaluar si la empresa cumple con los procedimientos establecidos por el área de TI de control interno.

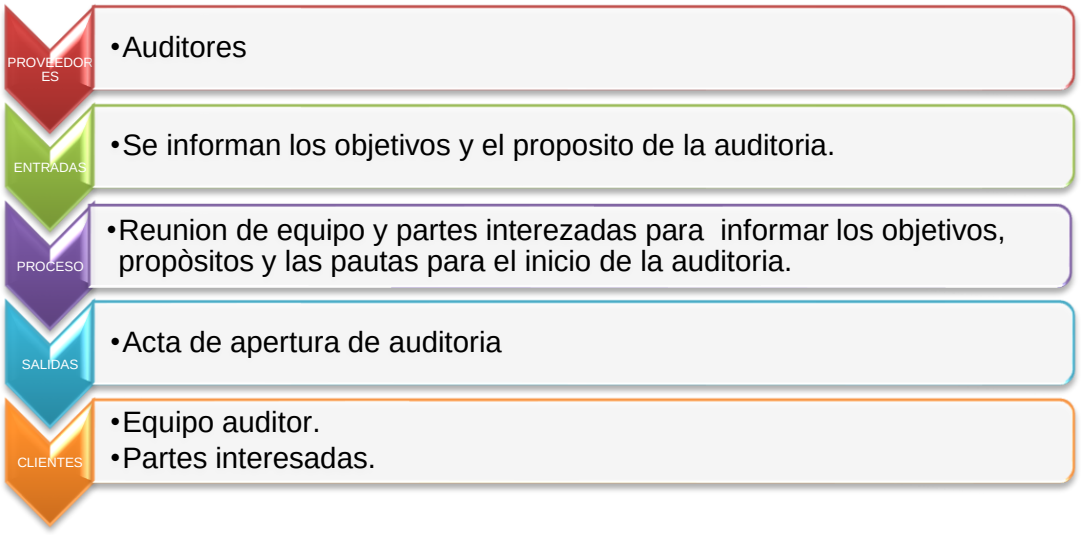


Figura 288.Diagrama SIPOC – Ejecución de la auditoria.

Fuente: Elaboración propia

2.1. Gestionar el sistema del control interno (MEA02)

La empresa CONECTA RETAIL S.A. usa procedimientos que son realizados por el área competente de la organización, que garantiza la seguridad, orientado a lograr cumplir los objetivos en diferentes aspectos con la medida de llevar las operaciones de forma eficiente y efectiva. Verificar si cuenta con un sistema de control, verificar la necesidad por parte de la organización en la gestión de controles de TI. Verificar su formalidad, si tienen definidos sus roles responsabilidades para monitorear y hacer el seguimiento efectivo de los controles internos.

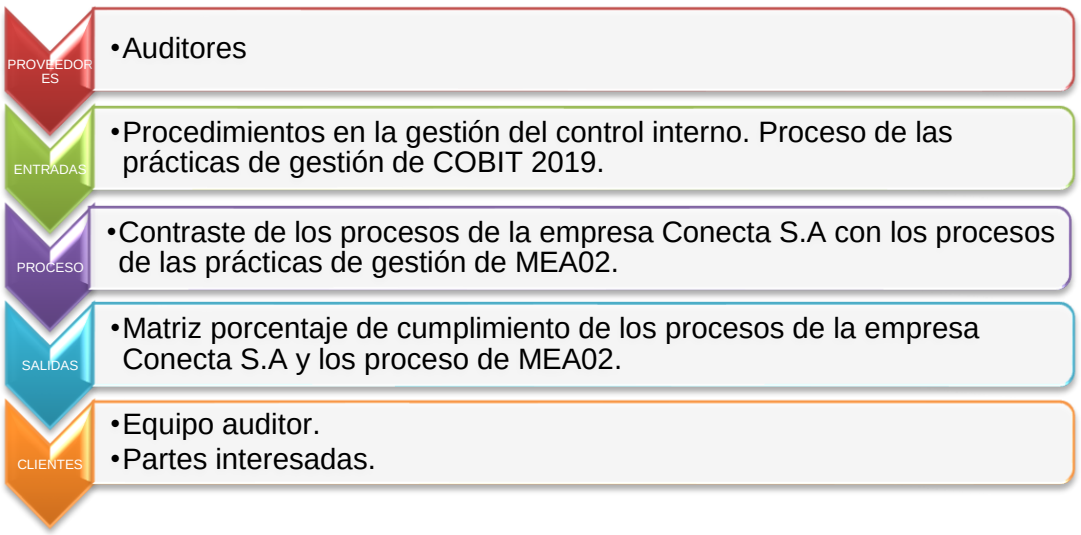


Figura 299.Diagrama SIPOC – Gestionar el control interno.

Fuente: Elaboración propia

*2.2.*Gestionar el aseguramiento (MEA04)

Se debe verificar si la organización cuenta con actividades enfocadas en planificar, delimitar y ejecutar el aseguramiento de la entidad, con el objetivo de lograr el cumplimiento de sus requerimientos internos, objetivos y políticas de la organización.

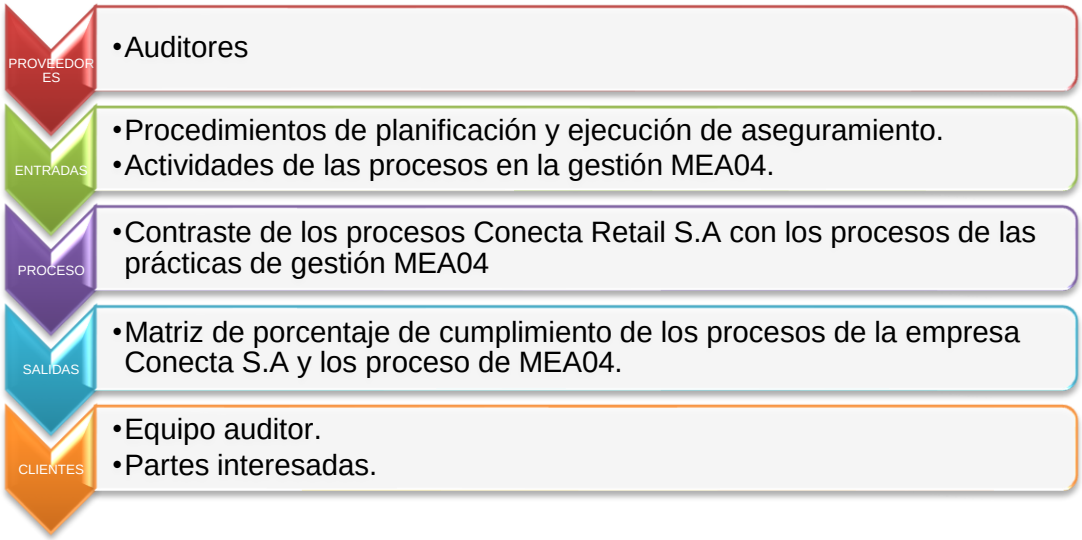


Figura 30.Diagrama SIPOC – Gestionar el aseguramiento.

Fuente: Elaboración propia

*2.3.*Gestión de controles del proceso del negocio (DSS06)

El control de los procesos del negocio es primordial, porque la empresa mediante la Gerencia de riesgos y la gerencia de sistemas, establece un conjunto de políticas necesarias para garantizar y salvaguardar la integridad del activo principal de los sistemas de la información, contra su uso no acreditado, modificaciones, daño o pérdida. La empresa hace posible mediante controles de aseguramiento para el acceso a sistemas, datos y programas que se restrinjan a usuarios no autorizados.

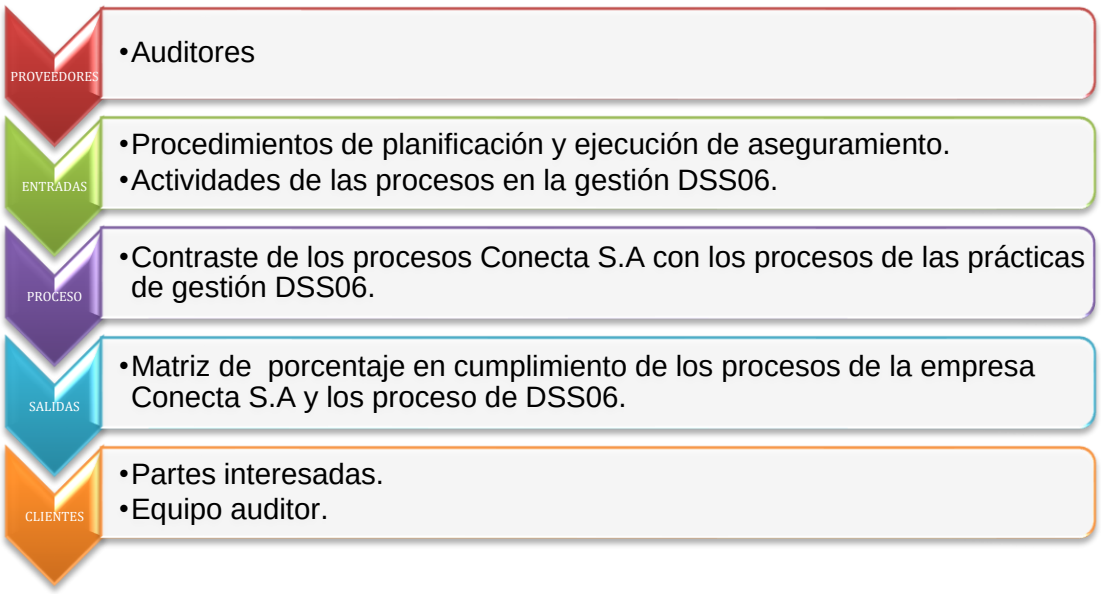


Figura31.Diagrama SIPOC – Gestionar el control de los procesos.

Fuente: Elaboración propia

2.4. Gestionar los proyectos (BAI11)

Realizar evaluaciones continuadas para mejorar y gestionar de forma eficiente los proyectos de software de la organización, para determinar el cumplimiento de los proyectos que son realizados de manera exitosa. Verificar si se mantiene un estándar idóneo para gestionar los proyectos de software, verificar si se desarrollan de forma adecuada los planes de proyectos y si se cumple con la normativa que estipula la empresa, verificar si se gestionan los riesgos en los proyectos y si estos son supervisados y controlados, a través de normas internas que buscan el mejoramiento continuo de la empresa CONECTA RETAIL S.A.

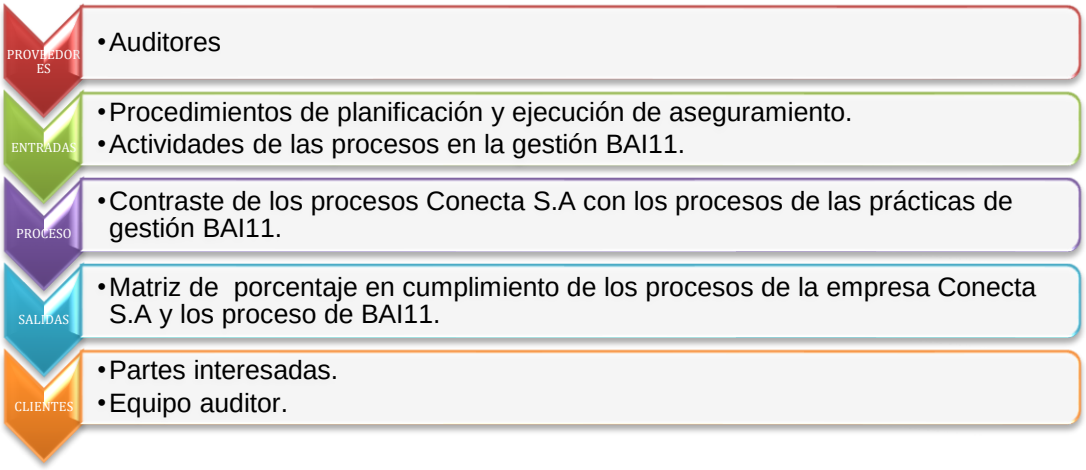


Figura 32..Diagrama SIPOC – Gestionar los proyectos.

Fuente: Elaboración propia

2.5. Gestionar los recursos humanos (APO 07)

En la organización CONECTA RETAIL S.A. la gestión de recursos humanos les permite proporcionar un enfoque que se encuentre estructurado y que permita asegurar la contratación, evaluación y asignación de recursos humanos más idóneos tanto internos como externos, se verificara la evaluación que se realiza para identificar al personal adecuado y se verificara el cumplimiento de la gestión para identificar a las personas indispensables, para de esta manera poder aplicar una filosofía de compartir conocimientos y que esas personas se conviertan en no indispensables ya que es un riesgo para la empresa.

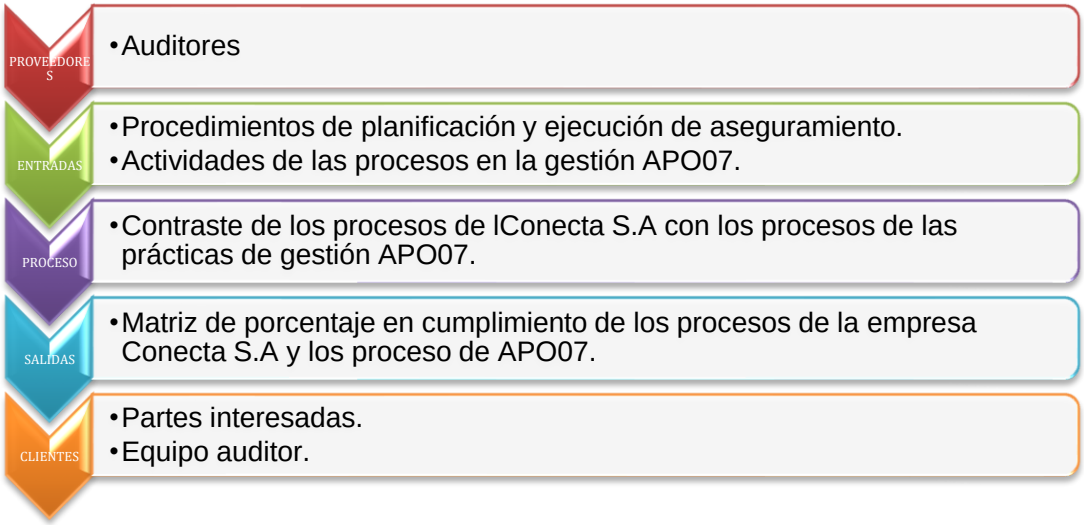


Figura 303.Diagrama SIPOC – Gestionar los recursos Humanos.

Fuente: Elaboración propia

3. Hallazgos y observaciones de la auditoría (clausula 6.4.8 - ISO 19011)

En este paso el auditor encargado de la auditoría, puede narrar y de forma lógica explicar los hechos detectados durante la realización de la auditoría, con el fin de comunicar las carencias, desviaciones, irregularidades, deficiencias, fortalezas y los posibles cambios que sean necesarios para la organización.

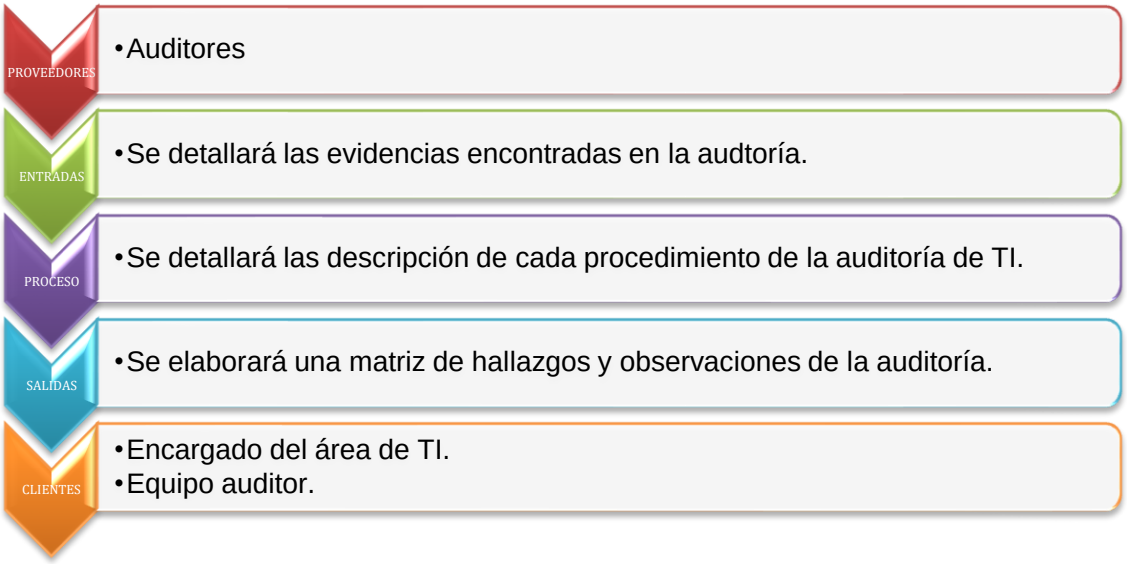


Figura 314.Diagrama SIPOC – Generación de hallazgos de la auditoría.

Fuente: Elaboración propia.

*3.1.*Realizar informe final de la auditoría (clausula 6.5.1 – ISO 19011)

Luego de conseguir la conformidad de los hallazgos por parte de los auditores y las partes interesadas, en este punto se busca documentar las conclusiones y recomendaciones en un informe, para su posterior revisión y ejecución por parte de la organización. Sin embargo lo que nos recomienda la ISO 19011 en su cláusula 6.5.1, el informe de auditoría debe ser claro y preciso, y también hacer referencia al desarrollar un síntesis del proceso de la auditoría, como también mencionar las dificultades que se hayan producido durante la ejecución de la auditoría, seguidamente de la confirmación del desempeño de los objetivos que se han planteado en el alcance de la auditoría, se debe elaborar un síntesis que abarque las conclusiones y principales evidencias encontradas en la auditoría.

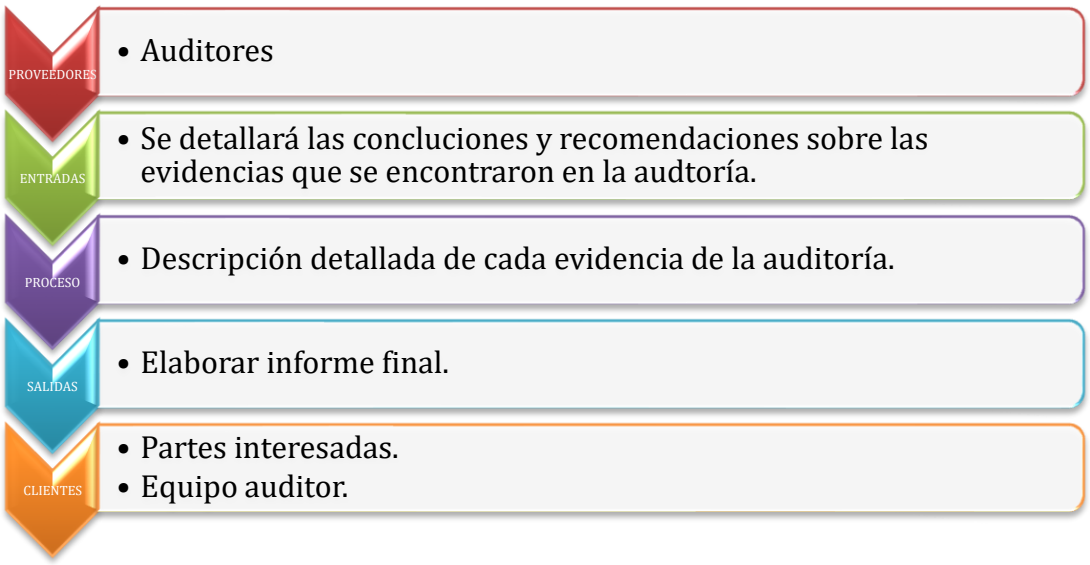


Figura 325.Diagrama SIPOC - Realización del informe final de la auditoría.

Fuente: Elaboración propia

4. Actividades de seguimiento y verificación de acciones correctivas

En este paso lo que se busca es verificar el progreso del cumplimiento correcto de las métricas establecidas para minimizar los riesgos identificados. La cláusula 6.7 de la ISO 19011 nos recomienda que el seguimiento implica corregir o tomar acciones de mejoras en los resultados de la auditoría dependiendo de lo que se ha planteado en los objetivos iniciales de la auditoría, así mismo se recomienda que el auditado debe estar en constante comunicación con los elementos representantes de la auditoría, con el objetivo de conocer el estado de dichas acciones.

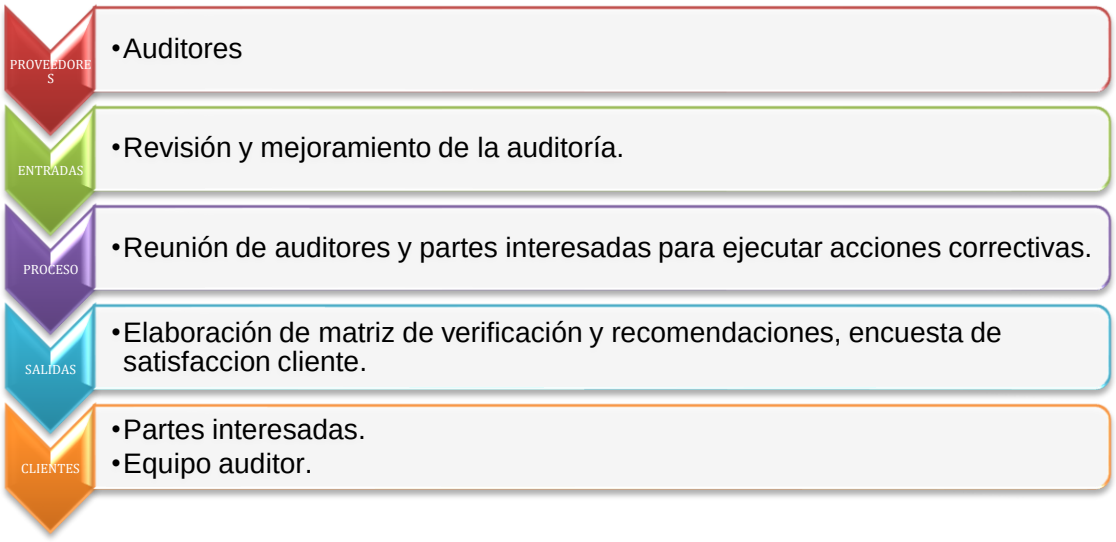


Figura 336.Diagrama SIPOC – Revisión y optimización de la auditoría.

Fuente: Elaboración propia

c) Validación del modelo de auditoría de TI por juicio de experto.

Una vez planteado el modelo de auditoría, y comparada su eficacia, se procede a validarlo a través de juicio de experto, para ello se conformó un grupo de 3 expertos en auditoría de TI, para que evalúen los instrumentos de recolección y para que realicen la evaluación del diseño del modelo de auditoría de TI, que será aplicado en la empresa CONECTA RETAIL S.A.

Tabla XV.Conjunto de expertos en auditoría de TI que participaron en la evaluación del modelo de auditoría de TI.

Nombre y Apellido	Profesión	Especialidad/ Conocimiento	Cargo	Ubicación
Rómulo Lomparte Alvarado	Lic. Computación/ Ciencias de la computación. Mg. En Administración de Negocios/MBA	Consultoría, auditoría, seguridad, ciberseguridad y ejecución de proyectos de SI. Representante ISACA GROUP	Líder de la Comunidad de Práctica de TI	Lima, Perú
Juliana Alva zapata	Mg. Ing. Computación e Informática	Área de TI, Riesgos, Auditoría y cumplimiento. Representante ISACA GROUP	Auditoría y cumplimiento de	Chiclayo, Lambayeque, Perú
Eloy Hely Campos Vásquez	Ing. Informático y de Sistemas	Oficina de Tecnología de Información y Comunicación	Líder en Prácticas de Gestión y Cumplimiento	Jaén, Cajamarca

Fuente: Elaboración propia.

En la tabla XVI, se visualiza el registro de los expertos que evaluaron dando su perspectiva frente al modelo propuesto por los tesistas, ante la claridad, objetividad, suficiencia, coherencia, pertinencia del modelo diseñado propuesto, con correlación a los procesos del marco de trabajo internacional COBIT 2019 y de la norma ISO 19011, en ese sentido comprobar su grado de alineación a lo que se instituye.

Se realizó el acercamiento con los expertos por medio del correo electrónico, para brindarles el contexto sobre el modelo de auditoría de TI y sus fases, para luego proceder a enviarle un resumen del informe con la teoría relacionada al marco COBIT 2019 y la norma ISO 19011, descripción de las fases y sus actividades que involucra el proceso del modelo

de auditoría de TI, para a continuación ser relacionada con el resultado de la escala de Likert. Para visualizar la evaluación detallada por cada experto verificar el anexo 5.5

Tabla XVI. Escala utilizada para la valoración de los criterios.

Valoración Nominal	Asignación Ordinal
Muy adecuado	4
Bastante adecuado	3
Adecuado	2
Poco adecuado	1
Nada adecuado	0

Fuente: Elaboración propia

Este resultante es registrado para el estudio concerniente, la evaluación obtenida se evidencia en la siguiente tabla:

Tabla XVII.Puntuación de expertos según los criterios establecidos para evaluar el modelo de auditoria propuesto.

Criterio de calificación	Experto 01	Experto 02	Experto 03
Claridad	4	4	4
Objetividad	4	4	4
Suficiencia	4	4	4
Coherencia	4	4	4
Pertinencia	3	4	4
Puntaje Promedio	3.8	4	4
TOTAL		**3.93**	

Fuente: Elaboración propia

De acuerdo del resultado arrojado se obtiene un puntaje total de 3.93, si medimos en el punto de corte podemos determinar que nuestro modelo se encuentra en muy adecuado.

4	3.5	3	2.5	2	1.5	1	0.5	0
Muy adecuado		Bastante adecuado		Adecuado		Poco adecuado		Nada adecuado

Se concluye que el modelo es ***muy adecuado,*** lo que significa que se puede proceder en su ejecución.

d) Ejecución del modelo de auditoría de TI.

Se procedió a elaborar el siguiente documento:

CONECTA RETAIL S.A.

MODELO DE AUDITORIA DE TI PARA EL CUMPLIMIENTO DE NORMAS Y POLITICAS DE LA EMPRESA CONECTA RETAIL S.A.

Código: MATI-001

Creado por: Rabanal Senmache Marry Cecy
Sánchez Rubio Omar Alberto

Aprobado por: Jorge Eugenio Cachay Arana

Historial de Modificación

Fecha	Versión	Creado	Descripción	Aprobado	Nivel confidencial
20/10/2023	01	Rabanal Senmache Marry C. Sánchez Rubio Omar A.	Versión Inicial	Jorge E. Cachay Arana	Uso Interno

Documentos Referidos

Norma 19011 – Capítulos
Marco COBIT 2019
MPP de Seguridad de la Información
MPP de Políticas
Manual de Metas de alineamiento y empresariales
Guía de Implementación
COBIT 2019 Governance and Management Objectives
Design of an Information and Technology Government solution

1. **PLANEACIÒN DE LA AUDITORIA**

Objetivos de la Auditoría de TI

General

Realizar de manera oportuna el cumplimiento de las acciones de auditoría de TI en la organización.

Específicos

a. Informar al área de TI acerca de las normas que se están aplicando de forma real en cada uno de los procesos de TI de la organización.

b. Evaluar si se cumple con las pautas establecidas por el área de TI referentes al control interno.

c. Evaluar si se cumple con cada uno de los requerimientos establecidos por el área de TI de acuerdo a sus características prioritarias.

d. Determinar si se han producido desvíos en la gestión de auditorías de TI y recomendar medidas de acción para minimizar dichas incidencias.

1.1. Reunión con el jefe del área de TI

Presentamos el alcance y objetivos de auditoria de la empresa, para que sea aprobado.

PLANTILLA DE OBJETIVOS DE AUDITORÍA DE TI					
Nombre del Proyecto	**Desarrollo de un modelo de auditoría para el cumplimiento de normas y políticas de la empresa CONECTA RETAIL S.A.**				
ACCIÓN	**RESPONSABLE**	**PRIORIDAD**	**ESTADO**	**INICIO**	**FIN**
Objetivo N°01					
Informar al área de TI acerca de las normas que se están aplicando de forma real en cada uno de los procesos de TI de la organización.	Rabanal Senmache Marry Cecy Sánchez Rubio Omar Alberto	Alta	En proceso	03/10/2023	09/10/2023
Objetivo N°02					
Evaluar si se cumple con las pautas establecidas por el área de TI referentes al control interno.	Rabanal Senmache Marry Cecy Sánchez Rubio Omar Alberto	Alta	En proceso	03/10/2023	09/10/2023
Objetivo N°03	Rabanal Senmache Marry Cecy Sánchez Rubio Omar Alberto	Alta	En proceso	03/10/2023	09/10/2023
Evaluar si se cumple con cada uno de los requerimientos establecidos por el área de TI de acuerdo a sus características prioritarias.					
Objetivo N°04	Rabanal Senmache Marry Cecy Sánchez Rubio Omar Alberto	Alta	En proceso	03/10/2023	09/10/2023
Determinar si se han producido desvíos en la gestión de auditorías de TI y recomendar medidas de acción para minimizar dichas incidencias.					

Fuente: Elaboración propia.

Alcance de la Auditoria.

En este proceso se define cuáles son los pasos a seguir, de manera detallada, brindando un alcance real de las actividades a realizar.

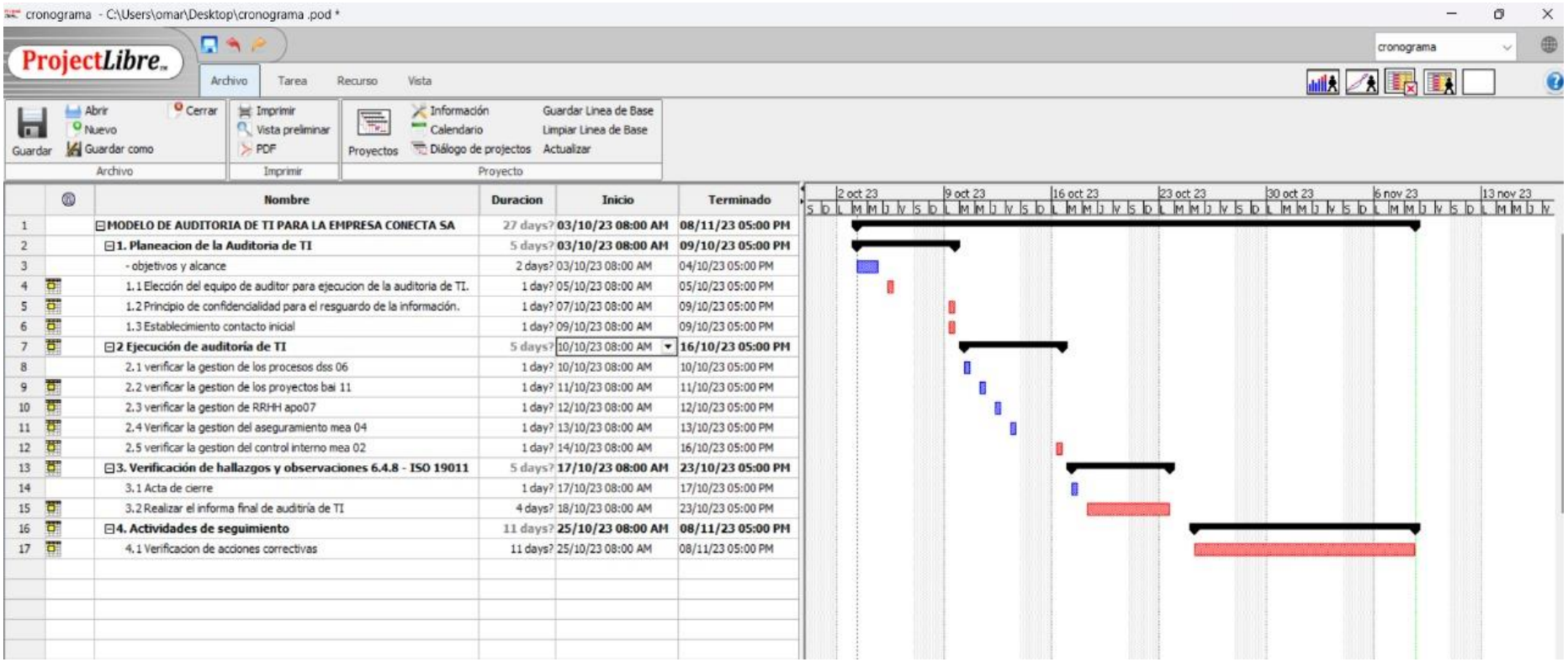


Figura 347. Alcance de auditoría de TI.

Fuente: Elaboración propia.

1.2. Equipo Auditor para Ejecución de la Auditoria

Se designa a los auditores y el personal responsable para ejecutar el programa de auditoría.

Tabla XVIII.Descripción del equipo auditoría

EQUIPO AUDITOR PARA AUDITORIA DE TI			
CARGO	**PROFESIÓN**	**ESPECIALIDAD**	**DATOS**
Supervisor del área de TI.	Ing. Sistemas	Supervisor	Jorge, A Cachay Arana
Auditor Líder	Ing. Sistemas	Auditor	Omar A. Sánchez Rubio
Auditor de Apoyo	Ing. Sistemas	Auditor	Marry C. Rabanal Senmache
Auditor Supervisor	Mg.Ing. Sistemas	Supervisor	Junior Cachay Maco

Fuente: Elaboración propia

1.3. Principio de confidencialidad para el resguardo de la información con respecto al equipo auditor

Se establecen los principios que serán desarrollados en la auditoría.

a. Principio de Integridad.

- El equipo auditor desarrolla un estándar ético, basado en la honestidad y responsabilidad.
- Desarrolla su trabajo de forma parcial, evita el sesgo en el desarrollo de sus actividades.
- Es sensible ante influencia que puedan incurrir en su ejercicio de auditoría.

b. Principio de Imparcialidad

-Los hallazgos en la auditoria proporcionan la exactitud y veracidad del desarrollo de actividades realizadas en la empresa.

-El auditor reportar las dificultades más significativas encontradas durante la auditoria.

c. Principio de evidencia y juicio al auditar

-El auditor debe trabajar con cuidado su tarea, validándose en la confianza, que se le ha brindado.

- El auditor tiene la habilidad de realizar juicios eficientes y racionales.

d. Principio de confidencialidad

-El auditor debe realizar el desarrollo de auditoria con reserva, conservando y resguardando la información que es confidencial en la empresa.

-El auditor no debe utilizar la información de manera apropiada.

e. Principio de Independencia

-El auditor debe velar que la auditoria logre ser objetiva e imparcial.

-La independencia del auditor del área que será auditada es ideal, para mostrar

f. Principio de enfoques racionales para obtener evidencias

-El auditor debe lograr obtener conclusiones de auditoria confiables.

-Las evidencias recolectadas, deben ser verificables.

g. Principios basado en riesgos

-El auditor determina los riesgos que pueden afectar la planificación y el reporte de las auditorias.

-El auditor debe verificar el complimiento global de cada uno de los objetivos del inicio de la agricultura

1.4. Establecimiento del contacto inicial

Después de contar con el plan de auditoría de TI, los auditores pactan una reunión con el encargado del área TI de la organización CONECTA RETAIL S.A, en donde se hace conocer los diferentes puntos de la auditoría. A continuación, desarrollamos los pasos que debe realizar el equipo encargado de la auditoría.

Se establecerán lo siguiente:

a) Las vías de comunicación durante el desarrollo de la auditoría: Se acordó utilizar la plataforma Zoom para reuniones que se realicen en el proceso de auditoría.

b) Presentación del equipo encargado de realizar la auditoría: Se presentó al equipo auditor, en este caso son: Rabanal Senmache, Marry Cecy; Sánchez Rubio Omar Alberto. El supervisor del equipo: Cachay Maco, Junior.

c) Informe sobre los objetivos de la auditoría: Se presentan los objetivos y se concluye con el acuerdo de los objetivos planteados por los auditores.

d) Presentación del alcance de auditoría: Se concluyó con el acuerdo del alcance de la auditoría.

e) Presentación de solicitud al acceso a la información: Se elaboró y se firmó una carta de confidencialidad para el acceso de la información

1.4.1. Acta de Confidencialidad

CONECTA RETAIL S.A. efe la curacao	FORMATO DE LA EMPRESA CONECTA RETAIL S.A PARA COMPROMISO DE CONFIDENCIALIDAD DE AUDITORES	**Formato** N°1 - CC	**Versión** 1
		Fecha 15/10/2023	

Marry Cecy Rabanal Senmache, identificado con DNI N° 47461274 y Omar Alberto Sánchez Rubio, identificado con DNI Nº 44621568; en desarrollo de Auditores externos a los servicios de TI de la empresa CONECTA RETAIL S.A., producto de ejercer el ejercicio de auditor tendremos acceso a la información escrita, oral, digital o de cualquier índole que esté relacionada con el proceso de auditoría a cargo de la oficina de TI basada en el control interno, (documentos, informes, registros, listas de chequeo) gestión y resultados de los servicios de Tecnología de Información que han sido auditados.

Teniendo previsto lo anterior, declaramos voluntariamente que nos comprometemos a:

1. Proceder con reserva en el uso y protección de la información adquirida durante el curso de mis deberes.
2. No usar la información de auditoría de manera inapropiada para beneficio personal, lo cual pueda perjudicar los intereses legítimos de la empresa CONECTA RETAIL S.A.
3. No acceder mediante unidades removibles a los servicios de TI para extraer información sin previa autorización.
4. No remitir archivos que contengan información confidencial de la empresa a terceros que puedan usar esa información en contra de la empresa CONECTA RETAIL S.A.

Asimismo, nos comprometemos a cumplir: normas y políticas de seguridad de la información contenidas en la Ley de Acceso a la Información Pública, la Ley de Protección de Datos Personales y el Decreto Legislativo N° 1128.; la Normatividad que regula mi profesión; el Código de Ética de la Entidad y el Estatuto de Auditoría Interna y Código de Ética de Auditoría; la normativa técnica y administrativa establecida por la Oficina de Control Interno para el desarrollo auditorías internas, y todas aquellas directrices que regulen el desempeño profesional de mis actividades en la NTC ISO 19011:2018 y el Marco Internacional para la Práctica Profesional de la Auditoría Interna, así como las leyes y regulaciones relevantes del Perú.

En caso de tener dudas sobre lo que está o no permitido divulgar conforme a este Compromiso de Confidencialidad me comprometo a consultar al Líder de Auditoría.

En caso de incumplimiento de lo establecido en el presente documento, la Oficina de Control Interno lo comunicará a las instancias competentes a las que haya lugar, con el fin que inicien las actuaciones pertinentes.

Dejo expresa constancia que este Compromiso de Confidencialidad lo he suscrito a los 15 de octubre del año 2023.

Marry Cecy Rabanal Senmache
DNI: 47461274

Omar Alberto Sánchez Rubio
DNI: 44621568

Figura 40. Acta de confidencialidad de la empresa CONECTA RETAIL S.A.

Fuente: Elaboración propia.

2. Ejecución de la auditoria

Acta de Apertura De Auditoria

ACTA DE REUNIÓN DE APERTURA DE AUDITORÍA

PROCESO: AUDITORIA DE TI	DEPENDENCIA AUDITADA: AREA DE TI
FECHA: 10-10-23 - 14-10-23	HORA DE INICIO:8:00 a.m.
LUGAR: CONECTA RETAIL S.A.	HORA DE TERMINACIÓN: 5:00 p.m

ASISTENCIA

La reunión de apertura contó con los siguientes servidores:

Por parte del proceso o dependencia auditada: **Jorge A, Cachay Arana**

Por parte de la Unidad de Auditoria:
Omar Sánchez Rubio
Marry Rabanal Senmache
Junior Cachay Maco

PRESENTACIÓN

A la hora señalada se inició la reunión de apertura de la auditoria al proceso o dependencia procediendo a hacer la presentación formal del Equipo Auditor indicando las funciones de cada uno. De igual forma se llevó a cabo la presentación de cada uno de los servidores que participarán o atenderán como designados las visitas de auditoría, como facilitadores y articuladores de la información requerida para su desarrollo. Designando a **Jorge A, Cachay Arana** como enlace entre el equipo auditor y el equipo auditado.

Luego se explicó por parte del equipo auditor el contenido del plan de auditoría, en cuanto a metodología de seguimiento y el término previsto para la ejecución.

Se dieron a conocer los objetivos, el alcance, los criterios y el cronograma de auditoría plasmados en el plan de auditoría que se entregó a **Jorge A, Cachay Arana**, Jefe del Área de TI de la empresa CONECTA RETAIL S.A. Así mismo, se dio a conocer la programación de la ejecución de las actividades de auditoría, se confirma la fecha y hora del cierre de la auditoría.

Se confirmaron los canales de comunicación a ser empleados durante el proceso auditor.

Se confirmaron asuntos relacionados con la confidencialidad y reserva de la información.

Se confirmó las personas que eventualmente atenderán la auditoría, acorde a las actividades del proceso que desarrolle cada uno.

Se aclaró que la labor de auditoría en ningún momento afecta o entorpece el normal desarrollo de las actividades propias del proceso auditado.

Se aclaró que es responsabilidad de la dependencia o proceso auditado el contenido en calidad y cantidad de la información suministrada, así como con el cumplimiento de las normas que le son aplicables a sus actividades en relación con el asunto auditado; señalando que es obligación de la Unidad de Auditoría expresar con independencia una conclusión sobre el cumplimiento de las disposiciones aplicables en el asunto auditado, la cual estará fundamentada en los resultados obtenidos en la auditoría realizada.

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 10/10/2023	FECHA 10/10/2023	FECHA 14/10/2023

Pág. 1 | 2

Figura 41.Acta de apertura de Auditoria de TI de la empresa CONECTA RETAIL S.A.

Fuente: Elaboración propia.

ACTA DE REUNIÓN DE APERTURA DE AUDITORIA

PROPOSITO Y OBJETIVOS DE LA AUDITORIA
El equipo auditor explicó a los asistentes el propósito general de la auditoria a realizar consistente en Realizar de manera oportuna el cumplimiento de las acciones de auditoría de TI en la organización, que involucra los siguientes objetivos específicos: Informar al área de TI acerca de las normas que se están aplicando de forma real en cada uno de los procesos de TI de la organización. Evaluar si se cumple con las pautas establecidas por el área de TI referentes al control interno. Evaluar si se cumple con cada uno de los requerimientos establecidos por el área de TI de acuerdo a sus características prioritarias. Determinar si se han producido desvíos en la gestión de auditorías de TI y recomendar medidas de acción para minimizar dichas incidencias.

CONTROL DE REGISTRO DE LA ASISTENCIA A LA REUNIÓN DE APERTURA			
Nombres y Apellidos	**Dependencia**	**Cargo**	**Firma**
Jorge A, Cachay Arana	**Área de TI**	**Supervisor**	
Omar Sánchez Rubio	**Área de TI**	**Auditor**	
Marry Rabanal Senmache	**Área de TI**	**Auditor**	
Junio E, Cachay Maco	**Área de TI**	**Supervisor**	

Fuente: Elaboración propia.

2.1. Evaluar la gestión del control interno de los procesos del negocio

Gestionar los procesos de TI, es prioritario para el buen funcionamiento de la empresa CONECTA RETAIL S.A, se estableció la verificación y control de procesos de la entidad buscando proteger los SI y al mismo tiempo establecer metodologías para evaluar los riesgos para poder aplicar los controles idóneos y de esta manera minimizar las incidencias de los SI de la empresa. Ver la evaluación ir anexo 5.7

Tabla XIX.Resultado de la evaluación de la Gestión de control interno de los procesos del negocio.

DSS06 – Gestión en los controles de procedimientos de la organización		
DOMINIOS	**CUMPLIMIENTO**	**%**
DSS06.01	La jefatura de riesgo operacional se encarga de desarrollar el cumplimiento idóneo de políticas de SI de los contratos, estableciendo fórmulas que estén alineadas a las metas empresariales y lo establecido en las normas de CONECTA RETAIL S.A.	100%
DSS06.02	Se desarrollan políticas para asegurar que la información considerada como crítica y que tenga los controles ante un acceso no autorizado.	87%
DSS06.03	CONECTA RETAIL S.A implementa políticas de desarrollo y mantenimiento de sistemas informáticos. Tiene por objetivo controlar el proceso de desarrollo, proteger la información crítica, apoyar en el control del proceso de puesta a producción y contar con un adecuado control de cambios.	100%
DSS06.04	Las incidencias registradas y su tratamiento se reportan de manera periódica. La empresa CONECTA RETAIL S.A, cuenta con una escala de clasificación de la información de los procesos según su nivel de criticidad. Se gestionan los controles necesarios para la gestión de excepciones	80%
DSS06.05	En la empresa CONECTA RETAIL S.A., se aplican controles respectivos que aseguran la privacidad de la información del cliente.	100%
DSS06.06	Las áreas que tengan acceso los activos de TI, deberán tener los cuidados respectivos para que esta información tenga carácter restringido solo para nivel de acceso respectivo.	100%

Fuente: Elaboración propia basada en COBIT 2019

Después de evaluar cada una de las actividades del objetivo de gestión DSS06 aplicado a la empresa CONECTA RETAIL S.A, se determina que se tiene un cumplimiento acertado de **94.5%** en cuanto al desarrollo de actividades de control en función del negocio y

de sus objetivos empresariales. Así mismo se evidencia que en la gestión de roles y responsabilidades, cuentan con privilegios de accesos en función a su nivel rango de responsabilidad del usuario, también se evidencia que aplican de manera rigurosa la gestión de errores y excepciones y están en constante mejora continua, aplicando la trazabilidad de eventos de información que se puedan suscitar, velando por salvaguardar los activos de la información, ya que son parte primordial de la empresa. Por otro lado se observó que en cuanto al control de procesamiento de la información, si se presenta incumplimiento en actividades como listar él envió de datos que se han enviado o se han introducido de manera errónea y se debe realizar un listado de evidencias de acciones correctivas.

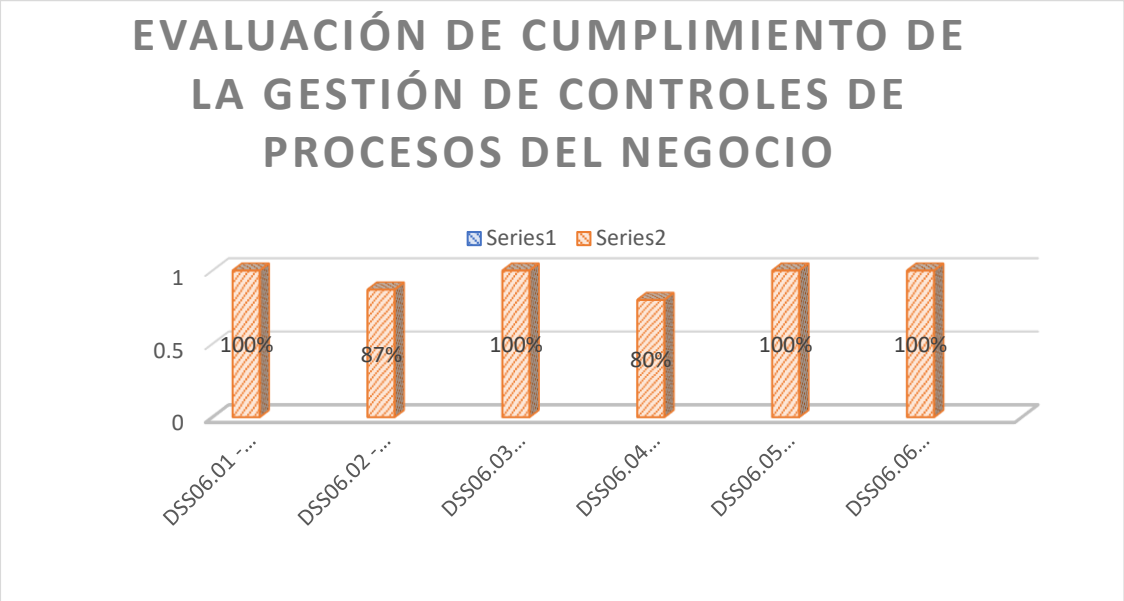


Figura 35.Verificación de cumplimiento de gestión de controles de procesos del negocio.

Fuente: Elaboración propia

En la figura 40, se puede visualizar el porcentaje de cumplimiento enfocados en gestionar los procesos de la empresa CONECTA RETAIL S.A, donde se evidencia que el nivel promedio es de 94.5%, estableciendo un nivel de cumplimiento bueno, aunque hay dos controles que se le debe dar un poco más de prioridad como son el **DSS06.02** y el **DSS06.04,** tomando en cuenta estos lineamiento y efectuando su cumplimiento se podría decir que la

empresa está orientada a ejecutar resultados óptimos debido a que es una empresa muy rigurosa en cuento al cumplimiento de sus políticas y controles .

2.2. Evaluar la gestión de los proyectos

La empresa CONECTA RETAIL S.A, busca el mejoramiento continuo de sus proyectos, busca que los proyectos estén alineados a las políticas establecidas, por ende, se verificara el cumplimiento de los proyectos basados en el desarrollo del software.

Tabla XX.Resultado de la gestión de los proyectos de software de la empresa CONECTA RETAIL S.A.

Objetivo de gestión: BAI11 — Gestionar los proyectos		
DOMINIOS	**CUMPLIMIENTO**	**%**
BAI11.01	Se realiza una gestión estándar de forma parcial en cuanto a la gestión de proyectos. Se evidencia que se proporciona capacitaciones a los gestores de los proyectos, para posteriormente certificarlos en base a los aprendizajes obtenidos en cuanto a gestión de proyectos.	80%
BAI11.02	La empresa cuenta con un SGSI la cual busca que los activos estén siempre protegidos de los riesgos que los afecten y establecen metodologías donde se evalúan los riesgos con técnicas de control idóneas para minimizarlos.	90%
BAI11.03	Cada parte interesada contempla un rol dentro y fuera de la organización, los cuales tienen asignada un área y una función.	100%
BAI11.04	La empresa conecta define política y define las reglas, centradas en el tema de seguridad, que deben ser consideradas en la ejecución, Continuidad y Término de los proyectos CONECTA RETAIL S.A.	90%
BAI11.05	La jefatura de riesgo operacional hace cumplir las políticas de seguridad en los contratos, documentos de proyectos. Así mismo los proyectos deben contar con procedimientos operativos y de control necesarios para los requerimientos legales que sean cumplidos según lo establecido.	100%
BAI11.06	La empresa CONECTA RETAIL S.A cuenta con un plan para identificación de riesgos e incidencias, el personal a cargo gestiona cada uno de los procesos de acuerdo al área asignada.	100%
BAI11.07	Los sistemas core de la empresa CONECTA RETAIL S.A, cuentan con mecanismos de detección de anomalías que avisen al administrador responsable cuando ocurra cualquier evento.	100%
BAI11.08	Cada empleado se le asigna un rol y un área en el cual implementan varias actividades a su cargo. De acuerdo a su rol cumple funciones y elabora su plan de actividades.	90%
BAI11.09		100%

	Al finalizar el proyecto, se realiza la recopilación de lecciones aprendidas de los participantes del proyecto. Se analizan los datos y se realizan las recomendaciones pertinentes para mejorar el proyecto actual y futuros.

Fuente: Elaboración propia basada en COBIT 2019

En la figura 41, se visualiza el nivel de cumplimiento de los dominios de COBIT 2019, los cuales tienen un porcentaje general de **94.4%** de cumplimiento, lo que establece que la empresa CONECTA RETAIL S.A, es muy estricta en cuanto a la aplicación de normas y políticas que le ayuden a efectuar la gestión de sus recursos de manera eficiente. Cabe decir que se debe priorizar el domino BAI01.01, para cumplir de manera más oportuna cada una de las actividades establecidas por el área de TI de la empresa.

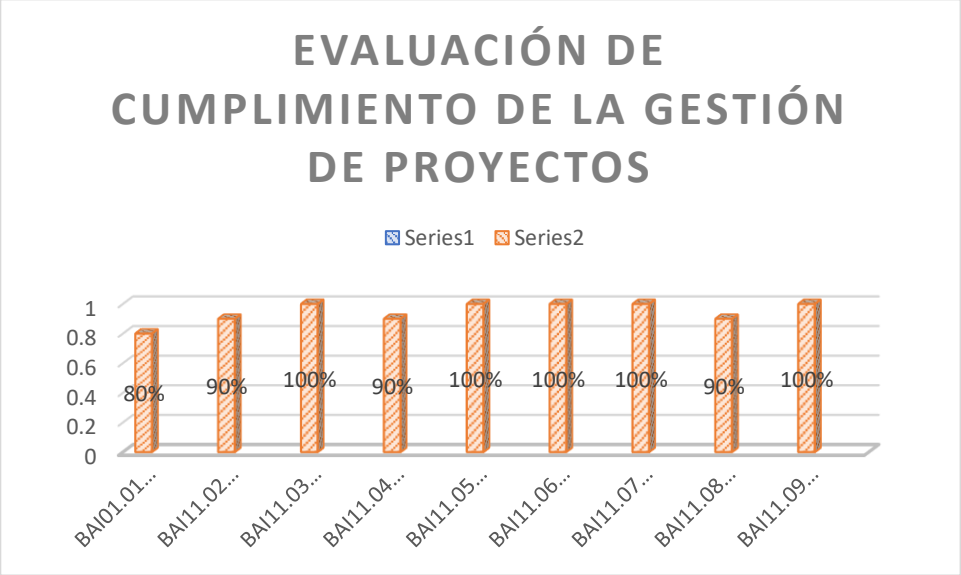


Figura 362. Resultado de la evaluación de la gestión de proyectos de software.

Fuente: Elaboración propia

2.3. Evaluar la gestión los recursos humanos

Es indispensable en la empresa CONECTA RETAIL S.A, porque un personal eficiente y capacitado logra el cumplimiento de objetivos empresariales de manera efectiva, por ende, la empresa realiza capacitaciones progresivas, para que el personal, logre el cumplimiento de metas en plazos específicos. Se observa que la empresa logra un porcentaje de 100% en 4 dominios, indicando que se está estableciendo el cumplimiento adecuado de sus actividades, sin embargo en los dominios de evaluación y rendimiento de los empleados

obtuvo un valor de 86% y en el dominio de planificar y hacer seguimiento del uso de recursos humanos se evidencia un cumplimiento de 75%, lo que implica que se deben priorizar estos dominios y efectuar mejoras ya sé que están implementando de forma parcial, para tener mejores resultados. Cabe decir que el personal si es capacitado para que cumpla una determinada actividad y conozca lo indispensable que es conocer que roles tiene en la protección de la información de los datos de la empresa.

Tabla XXI.Evaluación de la gestión de los recursos humanos de la empresa CONECTA RETAIL S.A.

Objetivo en la gestión: APO07 - Gestión de los recursos del personal		
DOMINIOS	**CUMPLIMIENTO**	**%**
APO07.01	Todos los nuevos empleados pasan por un período de evaluación**,** y luego son entrenados según sus competencias más relevantes.	100%
APO07.02	Periódicamente realiza un análisis y determinan cual es el personal indispensable y luego definen un plan de capacitación para convertirlo en no indispensable, compartiendo la filosofía compartir conocimientos.	100%
APO07.03	Realizan la identificación del personal clave, en base a ello se crean grupos de intercambio de conocimientos, para mantener habilidades y ampliar el campo de conocimiento en todos los empleados que son claves.	100%
APO07.04	Se establecen metas, que incentivan al personal a ser más productivo y a cambio se le otorgan incentivos monetarios y certificaciones que acreditan sus habilidades.	86%
APO07.05	Todos los empleados se comprometen a conocer y realizar el cumplimiento de las políticas de TI de seguridad genérica de la empresa CONECTA RETAIL S.A, así mismo asisten a charlas y capacitaciones de entrenamiento en materias de seguridad.	75%
APO07.06	El jefe directo del área de TI informa y capacita a todos los empleados sobre los riesgos que se presentan según su cargo que desempeña y está expuesto, así mismo debe entrenarlo, para hacer frente a estos riesgos y lograr minimizarlo de la manera más oportuna.	100%

Fuente: Elaboración propia

En la figura 42, se evidencia que el nivel de cumplimiento de recursos humanos enfocados en el dominio de COBIT 2019, tiene un porcentaje de **93.5%**, lo que establece que la empresa CONECTA RETAIL S.A, es muy estricta en cuanto a la aplicación de normas y políticas que le ayuden a efectuar la gestión de sus recursos de manera eficiente, sin

embargo, hay dos dominios que deben ser priorizados para efectuar su cumplimiento de manera efectiva.

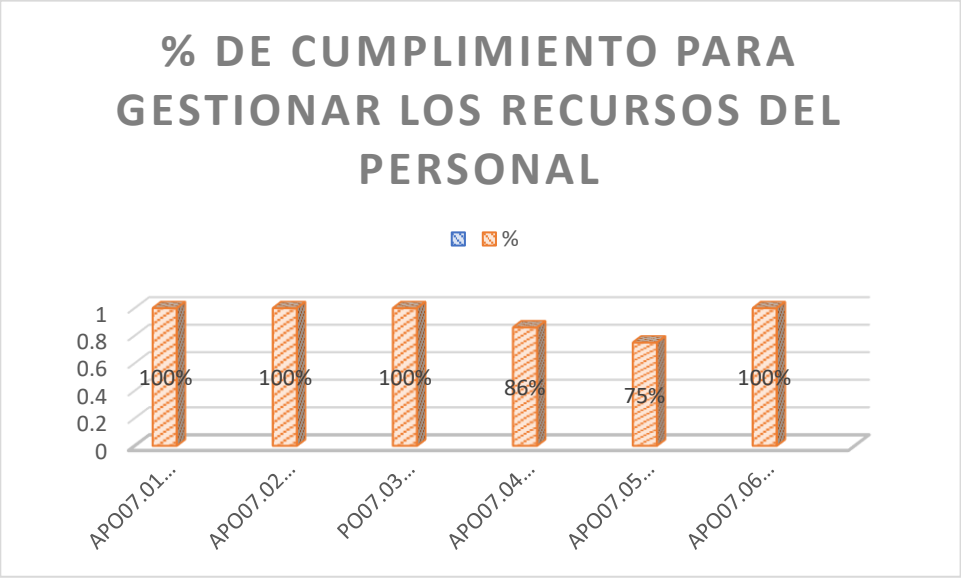


Figura 373.Verificación de cumplimiento para gestionar los recursos del personal del área de TI de la empresa CONECTA RETAIL S.A.

Fuente: Elaboración propia.

2.4. Evaluar la gestión del aseguramiento

La empresa realiza actividades de evaluación para el cumplimiento o no con los requisitos internos, leyes, regulaciones y estándares, con el objetivo de tener claro la dirección de ofrecer garantía adecuada y sostenibilidad a la empresa.

Tabla XXII.Evaluación de la gestión del aseguramiento de la empresa CONECTA

MEA04 — Gestionar el aseguramiento		
DOMINIOS	**CUMPLIMIENTO**	**%**
MEA04.01	Asegurar que la organización CONECTA S.A. realice evaluaciones autónomas de cada una de las funciones de los interesados incluidos en el alcance de auditoría.	100%
MEA04.02	Determinar objetivos de aseguramiento de la empresa CONECTA RETAIL S.A. establecidos en apreciaciones del entorno para lograr que las metas estratégicas de la empresa se cumplan a cabalidad.	85%
MEA04.03	Definir con las partes interesadas de la empresa CONECTA RETAIL S.A. el aseguramiento de los objetivos definidos.	85%

MEA04.04	Precisar con todas las partes interesadas de la empresa CONECTA RETAIL S.A, el alcance de aseguramiento, basados en sus objetivos.	75%

Fuente: Elaboración propia

En la figura 43, se visualiza el nivel de cumplimiento de los dominios MEA04 de COBIT 2019, para gestionar el aseguramiento, se evidencia que el nivel de cumplimiento general es de 75 %, lo que establece que la empresa CONECTA RETAIL S.A, toman acciones con rigor a los procedimientos que implican en la gestión del aseguramiento del cumplimiento de políticas, regulaciones y normativas, sin embargo, existen 3 objetivos que deben tomarse en cuenta para su cumplimiento efectivo.

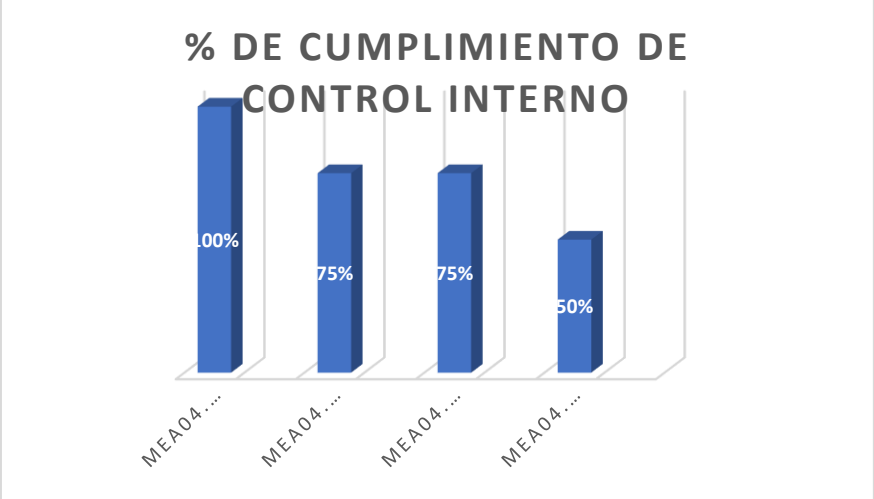


Figura 384.Gestión del aseguramiento – MEA04 CONECTA RETAIL S.A.

Fuente: Elaboración propia.

2.5. Evaluar la gestión del sistema de control interno

CONECTA RETAIL S.A. busca supervisar y la evaluación constante referente a su entorno de control, con el objetivo de efectuar la entrega de información clara y precisa a las partes interesadas, enfocada en la importancia y la rigurosidad del sistema del control interno que maneja la empresa.

Tabla XXIII. Valoración de cumplimiento para gestionar el sistema de control interno de la empresa CONECTA RETAIL S.A.

MEA02 — Gestionar el sistema de control interno		
DOMINIOS	**CUMPLIMIENTO**	**%**
MEA02.01	Mejorar el control de los procesos de TI de la empresa CONECTA RETAIL S.A.	100%
MEA02.02	Inspeccionar la eficiencia del control de procesos del área de desarrollo de software en la empresa CONECTA RETAIL S.A. Se revisan los procedimientos y evalúan los controles del negocio para asegurar su cumplimiento.	83%
MEA02.03	Incitar a la gerencia y a alta dirección de los procesos de la empresa CONECTA RETAIL S.A. para que corrijan los controles de forma proactiva, de esta manera se pueda evaluar la integridad de los controles, basados en la gestión de los procesos y políticas de la entidad.	86%
MEA02.04	Equilibrar las carencias de control y analizar e identificar sus procedencias raíces	72%

Fuente: Elaboración propia

En la figura 44, se visualiza el nivel de cumplimiento de los dominios MEA02 de COBIT 2019, para la gestión del sistema del control interno, se evidencia que el nivel de cumplimiento general es de 80 %, lo que establece que la empresa CONECTA RETAIL S.A, es muy estricta en cuanto a la aplicación de normas y políticas que le ayuden a efectuar la gestión de sus recursos de manera eficiente, sin embargo, hay tres dominios que deben ser priorizados para efectuar su cumplimiento de manera efectiva.

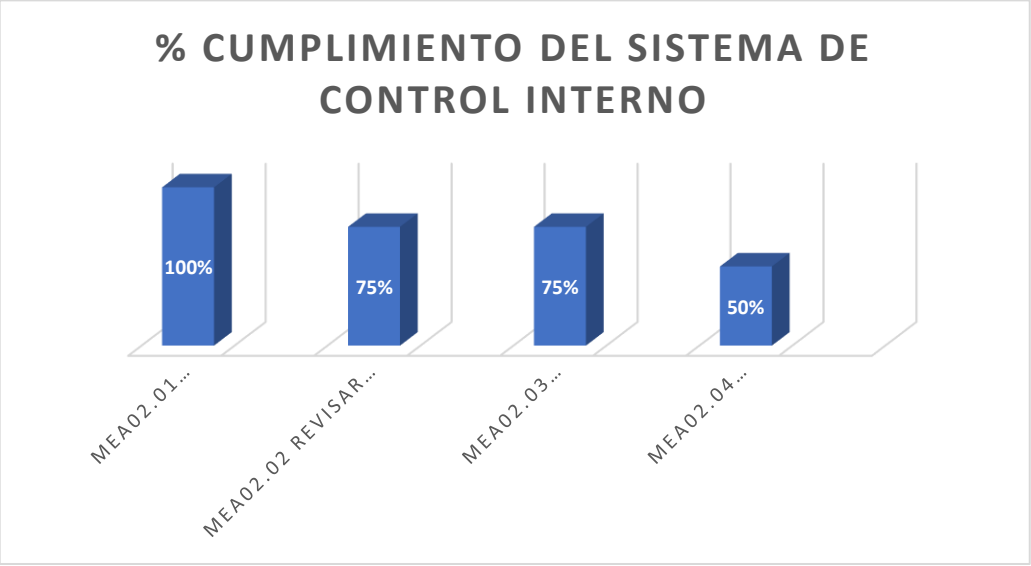


Figura 395.Gestión del sistema del control interno – MEA04 CONECTA RETAIL S.A.

Fuente: Elaboración propia.

3. Hallazgos y observaciones

MATRIZ DE HALLAZGOS Y OBSERVACIONES

PROCESO: AUDITORIA DE TI				DEPENDENCIA AUDITADA: AREA DE TI		
FECHA: 17-10-23 - 24-10-23				HORA DE INICIO:8:00 a.m.		
LUGAR: CONECTA RETAIL S.A.				HORA DE TERMINACIÓN: 5:00 p.m		
N°	**HALLAZGO**	**NIVEL DE OCURRENCIA**	**ÁREA DE IMPACTO**	**EFECTO**	**RESPONSABLE**	**RECOMENDACIONES**
1	Deficiencias en el control de excepciones.	Ocasionalmente	Área de TI	*No se logra definir cuáles son las deficiencias de excepciones más consecutivas.	Jefe del área de TI	Se recomienda que se analicen y se ponga en marcha las acciones correctivas para la gestión de riesgos e identificar si es un riesgo clave o no clave.
2	No existe un plan de evaluación de criterios para llevar a cabo las evaluaciones de actividades.	Ocasionalmente	Área de auditoría interna	*No se logra determinar el nivel de cumplimiento de actividades.	Jefe del área de auditoría interna de TI	Se recomienda que se realice la Planificación de resultados del proceso de autoevaluación de la empresa CONECTA RETAIL S.A y que estas autoevaluaciones sean informadas a la dirección general y al jefe encargado del área de TI de la empresa
3	No se establecen autoevaluaciones periódicas para verificar si los procesos se realizan de manera eficaz	Ocasionalmente	Área de TI	*No se puede medir la eficiencia de los procesos efectuados	Jefe del área de auditoría interna de TI	Se recomienda determinar con qué frecuencia se realizan las evaluaciones de manera periódica.
4	No se tiene un informe sobre los resultados evaluativos que se realizaron con anterioridad, que permita poner en marcha las acciones correctivas en incidencias encontradas en el área de TI.	Ocasionalmente	Área de auditoría interna		Jefe del área de auditoría interna de TI	Se recomienda realizar informes e historial de autoevaluaciones que indiquen desarrollar acciones correctivas en las incidencias encontradas en el área de TI

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 17/10/2023	FECHA 24/10/2023	FECHA 24/10/2023

Figura 406.Matriz de Hallazgos y observaciones de la empresa CONECTA RETAIL S.A.

Fuente: Elaboración propia.

MATRIZ DE HALLAZGOS Y OBSERVACIONES

5	No existe un plan anual donde se establezcan iniciativas de aseguramiento de objetivos que han sido consolidados	Ocasionalmente	Área de TI	*No se logra establecer las metas que permita el cumplimiento de los objetivos consolidados.	Jefe del área de TI	S e recomienda elaborar un plan anual donde se manifieste el consolidadas de iniciativas que ayuden al aseguramiento de objetivos planteados por la empresa en el área de TI
6	No se realiza un listado de datos que se introducen de manera errónea al sistema	Ocasionalmente	Área de TI		Jefe del área de auditoría interna de TI	Se recomienda la construcción y conservación de los documentos originales en un periodo de tiempo prudente, cuando se ingresen datos de manera errónea, de esta manera se puede filtrar el origen de estos datos.
7	No existe un historial de acciones correctivas	Ocasionalmente	Área de auditoría interna	*No se puede conocer las acciones correctivas que han sido efectuadas.	Jefe del área de TI	Se recomienda crear un historial de acciones correctivas, que pueda quedar como evidencia antes posibles incidencias.
8	No se establece un historial de lecciones aprendidas sobre estrategias para gestionar los proyectos de software de la empresa.	Ocasionalmente	Área de auditoría interna		Jefe del área de auditoría interna de TI	Se recomienda realizar una bitácora de las buenas prácticas, conforme sea necesario.
9	El control de cambios se realiza de forma parcial	Ocasionalmente	Área de auditoría interna	*No se puede conocer el tiempo en que se efectúa un determinado cambio.	Jefe del área de auditoría interna de TI	Se recomienda revisar e incorporar un plan integrado de proyectos, para efectuar de manera constante el control de cambios.
10	No se mide el rendimiento de los proyectos de desarrollo de software, con respecto a criterios de rendimiento	Ocasionalmente	Área de TI		Jefe del área de TI	Se recomienda realizar el análisis de los proyectos, para evaluar los aspectos positivos y negativos, de esta manera determinar el rendimiento de los proyectos.

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 17/10/2023	FECHA 24/10/2023	FECHA 24/10/2023

Fuente: Elaboración propia

MATRIZ DE HALLAZGOS Y OBSERVACIONES

11	No se realizan evaluaciones continuas del personal para medir su rendimiento	Ocasionalmente	Área de TI	*No se puede determinar si un personal está efectuando su cargo de forma efectiva.	Jefe del área de TI	Se recomienda crear un plan para evaluar resultados de rendimiento de personal
12	No existe un plan enfocado en la contratación del personal de TI, que permita realizar un seguimiento	Ocasionalmente	Área de auditoría interna	*No se puede identificar el personal clave del área de TI.	Jefe del área de auditoría interna de TI	Se recomienda crear un plan del personal, mediante un seguimiento oportuno, para verificar el cumplimiento de sus funciones.

CONTROL DE REGISTRO DE VERIFICACION DE HALLAZGOS Y OBSERVACIONES			
Nombres y Apellidos	**Dependencia**	**Cargo**	**Firma**
Jorge A, Cachay Arana	**Área de TI**	**Supervisor**	
Omar Sánchez Rubio	**Área de TI**	**Auditor**	
Marry Rabanal Senmache	**Área de TI**	**Auditor**	
Junio E, Cachay Maco	**Área de TI**	**Supervisor**	

Fuente: Elaboración propia

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 17/10/2023	FECHA 24/10/2023	FECHA 24/10/2023

Fuente: Elaboración propia

PROCESOS DE CIERRE DE AUDITORIA DE TI

ACTA DE CIERRE DE AUDITORÍA DE TI	FECHA DE VIGENCIA: 18/10/2023
	VERSIÓN: Nº01
	CODIGO: MATI-1

PROCESO:AUDITORIA DE TI	DEPENDENCIA AUDITADA: AREA DE TI
FECHA:08/11/2023	HORA DE INICIO:8:00 a.m.
LUGAR:CONECTA RETAIL S.A	HORA DE TERMINACIÓN:10:00 a.m.

1.ASISTENCIA

La reunión de apertura contó con los siguientes servidores:
Por parte del proceso o dependencia auditada: Jorge A, Cachay Arana
Por parte de la Unidad de Auditoria:
Omar Sánchez Rubio (Auditor 1)
Marry Rabanal Senmache (Auditor 2)

2. AGRADECIMIENTO

Se agradeció al líder del proceso al ingeniero Jorge A, Cachay Arana y a los funcionarios de las dependencias auditadas, por la disponibilidad de los recursos físicos y logísticos que fueron solicitados para realizar el trabajo y por disposición del personal que fue requerido en las evaluaciones, fueron realizadas.

3. CONCLUSIONES DE AUDITORIA

FORTALEZAS

El auditor presenta los hechos más relevantes encontrados en desarrollo de la auditoria:

- Se obtuvo un apoyo y guía constante por parte del equipo de la empresa CONECTA RETAIL S.A.
- Se evidencia que la empresa cumple con la mayoría de actividades plasmadas en su MPP basadas en el cumplimiento de normas y políticas.
- Se logró cumplir con los objetivos de la auditoria.
- El jefe del Área de TI, mediante la auditoria, podrá medir si se han producido desvíos en la gestión de auditoria de TI.
- Cumplimiento en los diferentes roles de control interno.

DEBILIDADES

-No se pudo evidenciar total formatos de auditorías anteriores.
-No se pudo evidenciar el total del historial de auditorías anteriores.

ASPECTOS DE MEJORA

-Se verifica que se está adelantando en el cumplimiento de acciones correctivas en cuanto a no conformidades.
-Se verifica la intención de mejora continua por parte de los encargados del proceso.

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 19/10/2023	FECHA 19/10/2023	FECHA 19/10/2023

Figura 417. Procesos de cierre de la Auditoria.

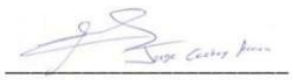
Fuente: Elaboración propia

PROCESOS DE CIERRE DE AUDITORIA DE TI

4. PLAN DE MEJORAMIENTO
Los responsables del proceso, presenta el plan de mejoramiento de acuerdo a los hallazgos registrados en el informe final de auditoría según el formato establecido por la entidad.
5. INFORME FINAL
Finalmente se informó que se procede a la entrega del informe final de la auditoría, el día 20/10/2024.

Auditor 1

Auditor 2



Jefe encargado área de TI

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 19/10/2023	FECHA 19/10/2023	FECHA 19/10/2023

Fuente: Elaboración propia

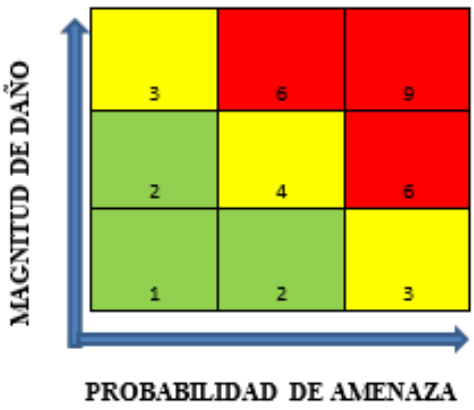
REPRESENTACION GRAFICA DE LOS RIESGOS

Se ha diseñado una matriz de riesgos que nos permite el grado de probabilidad e impacto de la magnitud de daño y amenaza que puede causar el no cumplimiento de las observaciones encontradas, sino se toman las medidas idóneas para lograr su mitigación.

RIESGO CONTROLABLE: 1 – 2 (VERDE)

RIESGO INTERMEDIO: 3 – 4 (AMARILLO)

RIESGO CRÍTICO: 6 - 9 (ROJO)



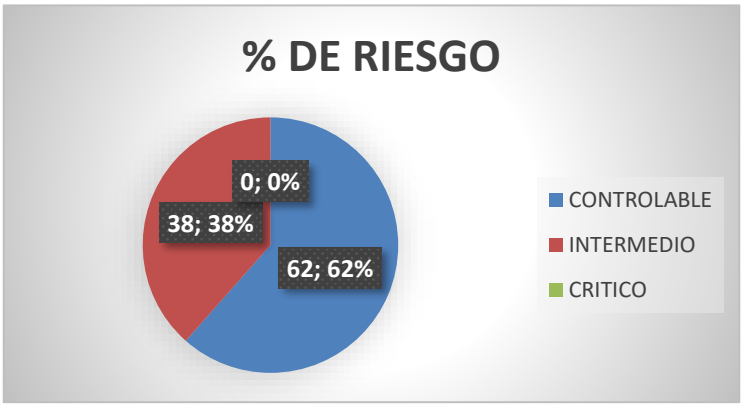
MATRIZ DE RIESGOS				
RIESGOS	PROBABILIDAD (1 - 3)	IMPACTO (1 - 3)	EXPOSICION	IVEL DEL RIESGO
Deficiencias en el control de excepciones	1	1	2	**RIESGOS CONTROLABLES**
No existe un plan de evaluación de criterios para llevar a cabo las evaluaciones de actividades	2	2	4	**RIESGO INTERMEDIO**
No se establecen autoevaluaciones periódicas para verificar si los procesos se realizan de manera eficaz	1	2	2	**RIESGOS CONTROLABLES**
No existen restricciones en la operación de comunicaciones y manejo de programas.	2	2	4	**RIESGO INTERMEDIO**

No se tiene un informe sobre los resultados evaluativos que se realizaron con anterioridad, que permita poner en marcha las acciones correctivas en incidencias encontradas en el área de TI.	2	2	4	**RIESGO INTERMEDIO**
No existe un plan anual donde se establezcan iniciativas de aseguramiento de objetivos que han sido consolidados	1	2	2	**RIESGOS CONTROLABLES**
No se realiza un listado de datos que se introducen de manera errónea en el sistema.	2	2	4	**RIESGO INTERMEDIO**
No existe un historial de acciones correctivas	2	2	4	**RIESGO INTERMEDIO**
No se realiza un historial de lecciones aprendidas sobre estrategias para gestionar los proyectos de software de la empresa	1	2	2	**RIESGOS CONTROLABLES**
el control de cambios se realiza de forma parcial	1	2	2	**RIESGOS CONTROLABLES**
No se mide el rendimiento de los proyectos de desarrollo de software, con respecto a criterios de rendimiento	1	2	2	**RIESGOS CONTROLABLES**
No se realizan evaluaciones continuas al personal para medir su rendimiento	1	2	2	**RIESGOS CONTROLABLES**
No existe un plan enfocado en la contratación del personal de TI, que permita realizar un seguimiento idóneo.	1	2	2	**RIESGOS CONTROLABLES**

Como se visualiza en la evaluación realizada, se concluye que el 62% de riesgos son controlables de probabilidad de ocurrencia y el 38 % de probabilidad de ocurrencia son riesgos intermedios, a los cuales se les debe aplicar un plan de mitigación para evitar que se materialicen dentro de la empresa.

TIPO DE RIESGO	TOTAL	PORCENTAJE
CONTROLABLE	8	62%
INTERMEDIO	5	38%
CRITICO	0	0%

En la imagen se puede visualizar el porcentaje de riesgos encontrados los cuales en su mayoría abordan a ser controlables, pues existe un gran cumplimiento de sus políticas de TI empresariales.



A continuación se presenta de matriz de riesgos con su respectivo plan de mitigación y contingencia para hacer frente a los riesgos controlables e intermedios que se han observado durante la auditoria de TI, permitiendo de esta manera minimizar las incidencias de seguridad en el Area de TI de la empresa en estudio.

MATRIZ DE RIESGOS

[16-10-23]-[24-10-23]

RIESGOS INMEDIATOS								
ID	**Descripción**	**Probabilidad (1-3)**	**Impacto (1-3)**	**Exposición (PxI)**	**Planes de Mitigación/Contingencia**	**Responsable**	**Estatus**	**Criticidad**
1	Deficiencias en el control de excepciones	2	1	2	**Mitigación:** Implementar un plan para la gestión de los incidentes de fuga de información. Desarrollar y actualizar políticas de acceso a la información.	Área responsable de TI - Área de aseguramiento y control de ciberseguridad y auditorias.	[Pendiente]	
2	No existe un plan de evaluación de criterios para llevar a cabo las evaluaciones de actividades	2	2	4	**Mitigación:** Desarrollar un plan con criterios minuciosos que permitan llevar acabo las evaluaciones oportunas de cada una de las actividades de TI.	Áreas responsables del manejo del sistema - Área De tecnología.	[Pendiente]	
3	No se establecen autoevaluaciones periódicas para verificar si los procesos se realizan de manera eficaz	2	1	2	**Mitigación:** Realizar evaluaciones continuas, para verificar el cumplimiento de los procesos.	Área responsable de TI - Área de aseguramiento y control de ciberseguridad y auditorias.	[Pendiente]	

LEYENDA (Criticidad)		
 Serios riesgos críticos o de alta prioridad	 Riesgo intermedio, problemas menores	 Riesgos bajos controlables, no hay problemas hasta el momento

RIESGOS INMEDIATOS								
ID	**Descripción**	**Probabilidad (1-3)**	**Impacto (1-3)**	**Exposición (PxI)**	**Planes de Mitigación/Contingencia**	**Responsable**	**Estatus**	**Criticidad**
4	No existen restricciones en la operación de comunicaciones y manejo de programas.	2	2	4	**Mitigación:** Implementar criterios de restricciones para el manejo de programas internos.	Área responsable de TI - Área de aseguramiento y control de ciberseguridad y auditorias.	[Pendiente]	
5	No se tiene un informe sobre los resultados evaluativos que se realizaron con anterioridad, que permita poner en marcha las acciones correctivas en incidencias encontradas en el área de TI.	2	2	4	**Mitigación:** Realizar la planificación y trazabilidad de los informes basados en resultados, que promuevan la mejora continua e incidencias de seguridad encontradas.	Áreas responsables del manejo del sistema - Área De tecnología.	[Pendiente]	
6	Falta de inducción, capacitación y sensibilización sobre riesgos	1	2	2	**Mitigación:** Desarrollar un plan de riesgo para la identificación de amenazas y vulnerabilidades de los activos, o posibles escenarios de riesgo.	Área responsable de TI - Área de aseguramiento y control de ciberseguridad y auditorias.	[Pendiente]	

LEYENDA (Criticidad)		
 Serios riesgos críticos o de alta prioridad	Riesgo intermedio, problemas menores	 Riesgos bajos controlables, no hay problemas hasta el momento

RIESGOS INMEDIATOS								
ID	Descripción	Probabilidad (1-3)	Impacto (1-3)	Exposición (PxI)	Planes de Mitigación/Contingencia	Responsable	Estatus	Criticidad
7	No se realiza un listado de datos que se introducen de manera errónea en el sistema.	2	2	4	**Mitigación:** Implementar un plan para la gestión de los incidentes de fuga de información. Desarrollar y actualizar políticas de acceso a la información.	Área responsable de TI - Área de aseguramiento y control de ciberseguridad y auditorias.	[Pendiente]	
8	No existe un historial de acciones correctivas	2	2	4	**Mitigación:** Desarrollar una bitácora de acciones correctivas y a su vez un check list para la revisión de oportunidades de mejora y su respectiva ejecución.	Áreas responsables del manejo del sistema - Área De tecnología.	[Pendiente]	
9	No se realiza un historial de lecciones aprendidas sobre estrategias para gestionar los proyectos de software de la empresa	1	2	2	**Mitigación:** Implementar una bitácora de lecciones aprendidas, para gestionar de forma eficiente el desarrollo de los proyectos de software de la empresa.	Área responsable de TI - Área de aseguramiento y control de ciberseguridad y auditorias.	[Pendiente]	
10	el control de cambios se realiza de forma parcial	1	2	2	**Mitigación:** Desarrollar una matriz que permita conocer la fecha de cambio y a su vez conocer la fecha de implementación del control.	Área responsable de TI - Área de aseguramiento y control de ciberseguridad y auditorias.		

LEYENDA (Criticidad)		
 Serios riesgos críticos o de alta prioridad	 Riesgo intermedio, problemas menores	 Riesgos bajos controlables, no hay problemas hasta el momento

RIESGOS INMEDIATOS								
ID	**Descripción**	**Probabilidad (1-3)**	**Impacto (1-3)**	**Exposición (PxI)**	**Planes de Mitigación/Contingencia**	**Responsable**	**Estatus**	**Criticidad**
11	No se mide el rendimiento de los proyectos de desarrollo de software, con respecto a criterios de rendimiento	1	2	2	**Mitigación:** Desarrollar y actualizar políticas de TI, enfocadas en la gestión de los proyectos de software.	Área responsable de TI - Área de aseguramiento y control de ciberseguridad y auditorias.	[Pendiente]	
12	No se realizan evaluaciones continuas al personal para medir su rendimiento	1	2	2	**Mitigación:** Uso de técnicas y herramientas que permita medir el rendimiento del personal.	Áreas responsables del manejo del sistema - Área De tecnología.	[Pendiente]	
13	No existe un plan enfocado en la contratación del personal de TI, que permita realizar un seguimiento idóneo.	1	2	2	**Mitigación:** Realizar procedimientos de selección, capacitación, inducción y evaluación del personal y así mismo evaluar aptitudes mediante un examen psicológico.	Área responsable de TI - Área de aseguramiento y control de ciberseguridad y auditorias.	[Pendiente]	

LEYENDA (Criticidad)					
	Serios riesgos críticos o de alta prioridad		Riesgo intermedio, problemas menores		Riesgos bajos controlables, no hay problemas hasta el momento

INFORME FINAL DE AUDITORIA DE TI

PROCESO: AUDITORIA DE TI	DEPENDENCIA AUDITADA: AREA DE TI
FECHA: 17-10-23 - 20-10-23	HORA DE INICIO:8:00 a.m.
EMPRESA: CONECTA RETAIL S.A.	HORA DE TERMINACIÓN: 5:00 p.m
NORMA: ISO 19011	MARCO: COBIT 2019

EQUIPO

Por parte del proceso o dependencia auditada: **Jorge A, Cachay Arana**

Por parte de la Unidad de Auditoria:

Omar Sánchez Rubio
Marry Rabanal Senmache
Junior Cachay Maco (Supervisor)

ALCANCE

Verificación del cumplimiento de políticas internas del área de TI (Gestión del sistema de control, gestión del aseguramiento, gestión del control del proceso del negocio, gestión de los programas y gestión de los recursos humanos).

RESULTADOS DE AUDITORIA

- No conformidades: 12
- Observaciones: 4
- Oportunidades de mejora: 8

NO CONFORMIDADES

1. Deficiencias en el control de excepciones.
2. No existe un plan evaluativo que permita identificar los criterios y alcance para llevar a cabo las evaluaciones de actividades.
3. No se establecen autoevaluaciones periódicas para verificar si los procesos se realizan de manera eficaz
4. No se tienen un informe sobre los resultados anteriores, que permitan verificar si se llegó a realizar acciones correctivas en incidencias encontradas en el área de TI.
5. No existe un plan anual donde se establezcan iniciativas de aseguramiento de objetivos que han sido consolidados.
6. No se realiza un listado de datos que se introducen de manera errónea al sistema
7. No existe un historial de acciones correctivas

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 17/10/2023	FECHA 19/10/2023	FECHA 20/10/2023

Figura 428.Informe de Auditoría de TI de la empresa CONECTA RETAIL S.A.

Fuente: Elaboración propia

8. No se establece un historial de lecciones aprendidas sobre estrategias para gestionar los proyectos de software.

9. El control de cambios se realiza de forma parcial.

10. No se mide el rendimiento de los proyectos de desarrollo de software, con respecto a criterios de rendimiento.

11. No se realizan evaluaciones continuas del personal para medir su rendimiento

12. No existe un plan enfocado en la contratación del personal de TI, que permita realizar un seguimiento eficaz.

OBSERVACIONES

1. Se deben realizar controles internos oportunos para evitar que se efectúen los riesgos.
2. Considerar estándares para realizar autoevaluaciones.
3. Se considera que se realice la corrección de los sistemas que permiten ingresar datos de forma errónea.
4. Se considera que se realice una matriz que permita medir el rendimiento de los proyectos basados en desarrollo de software.

OPORTUNIDADES DE MEJORA

1. Se recomienda hacer correcciones a la deficiencia del control de mejoras, considerando un historial que permita visualizar la comparación entre la deficiencia encontrada y la corrección efectuada.

2. Se recomienda crear un plan de evaluación de actividades para verificar su cumplimiento.

3. Se recomienda mencionar en el procedimiento de selección, capacitación, inducción y evaluación del personal, que cuando se apruebe el documento, desde ese momento recién se evaluara el cumplimiento con las actitudes, las cuales serán evaluadas por medio de un examen psicológico realizado en el reclutamiento.

Fuente: Elaboración propia

4. Se recomienda considerar en la evaluación del desempeño, la evaluación de responsabilidades no solo las habilidades, con el fin de clarificar que la acción plasmada en el programa de capacitación van a permitir mejorar el desempeño al realizar las funciones que se han observado con deficiencias.

5. Se recomienda definir el responsable de gestionar el ambiente de trabajo en el manual de políticas y procesos.

6. Registrar el método para el control de registros, considerando el responsable de la actualización de todos los registros de la empresa sean estos los MPP manuales de políticas y procesos, detallando el responsable de controlar cada uno de ellos.

7. Considerar que los registros deben contemplar solo el nombre del registro, mas no la lista de todos los casos en los que se reporta dicho registro, ya que este último es parte del control operativo, mas no del control del registro como tal.

8. Se recomienda elaborar un documento que describa nuevas prácticas enfocadas en la gestión de proyectos de software.

CONTROL DE REGISTRO DE LA ASISTENCIA A LA REUNIÓN DE APERTURA

Nombres y Apellidos	Dependencia	Cargo	Firma
Jorge A, Cachay Arana	Área de TI	Supervisor	
Omar Sánchez Rubio	Área de TI	Auditor	
Marry Rabanal Senmache	Área de TI	Auditor	
Junio E, Cachay Maco	Área de TI	Supervisor	

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 17/10/2023	FECHA 19/10/2023	FECHA 20/10/2023

Fuente: Elaboración propia

4. Actividades de seguimiento y acciones correctivas

LISTADO DE VERIFICACIÒN DE CALIDAD Y ACCIONES CORRECTIVAS

PROCESO: AUDITORIA DE TI	DEPENDENCIA AUDITADA: AREA DE TI
FECHA: 25-10-23 - 08-11-23	HORA DE INICIO:8:00 a.m.
LUGAR: CONECTA RETAIL S.A.	HORA DE TERMINACIÓN: 5:00 p.m

ASISTENCIA

Se contó con los siguientes servidores:
Por parte del proceso o dependencia auditada: **Jorge A, Cachay Arana**
Por parte de la Unidad de Auditoria:
Omar Sánchez Rubio
Marry Rabanal Senmache
Junior Cachay Maco

LISTADO DE VERIFICACION DE CALIDAD Y ACCIONES CORRECTIVAS

Nº	Procesos	Fecha de Inicio	Fecha de termino	Encargado	Código
1	Determinación de Objetivos y alcance de la auditoria	03/10/2023	04/10/2023	Líder del proceso	MATI-01
2	Elección del equipo auditor	05/10/2023	05/10/2023	Líder del proceso	MATI-01
3	Principios de confidencialidad	07/10/2023	09/10/2023	Líder del proceso	MATI-01
4	Establecimiento del contacto inicial	09/10/2023	09/10/2023	Líder del proceso	MATI-01
5	Ejecución de la auditoria	10/10/2023	16/10/2023	Líder del proceso	MATI-01
6	Reunión y acta de apertura de la auditoria de TI	10/10/2023	10/10/2023	Líder del proceso	MATI-01
7	Formato para la verificación de la gestión de los procesos	11/10/2023	11/10/2023	Líder del proceso	MATI-01
8	Formato para la verificación de la gestión de proyectos	12/10/2023	12/10/2023	Líder del proceso	MATI-01
9	Formato para la verificación de la gestión de recursos humanos	13/10/2023	13/10/2023	Líder del proceso	MATI-01
10	Formato para la verificación de la gestión del aseguramiento	14/10/2023	16/10/2023	Líder del proceso	MATI-01
11	Formato para la verificación de la gestión de control interno	16/10/2023	16/10/2023	Líder del proceso	MATI-01
12	Hallazgos y observaciones	17/10/2023	20/10/2023	Líder del proceso	MATI-01
13	Informe Final	17/10/2023	20/10/2023	Líder del proceso	MATI-01
14	Cierre del proyecto	20/10/2023	20/10/2023	Líder del proceso	MATI-01

CÓDIGO MATII-01	ELABORÓ Lider del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 25/10/2023	FECHA 08/11/2023	FECHA 08/11/2023

Pág. 1 | 3

Figura 439. Listado de verificación y acciones correctivas.

Fuente: Elaboración propia

LISTADO DE VERIFICACIÒN DE CALIDAD Y ACCIONES CORRECTIVAS

ACCIONES CORRECTIVAS				
Nº	**No Conformidades**	**Verificación**	**Fecha**	**Acciones correctivas**
1	Deficiencia en el control de excepciones	Conforme	25/10/2023	Se verifica que se ha creado un historial de comparación entre la deficiencia encontrada y la corrección efectuada
2	No existe un plan evaluativo que permita identificar los criterios y alcance para llevar a cabo las evaluaciones de actividades.	Conforme	26/10/2023	Se verifica que existe un plan de evaluación para el control de actividades
3	No se establecen autoevaluaciones periódicas para verificar si los procesos se realizan de manera eficaz.	Conforme	27/10/2023	Se verifica una ficha para verificar si los procesos son efectuados de manera conforme
4	No se tiene un informe sobre los resultados anteriores, que permita verificar si se llegó a realizar acciones correctivas en incidencias encontradas en el área de TI.	Conforme	28/10/2023	Se verifica que ya se lleva un control de acciones correctivas encontradas en el área de TI.
5	No existe un plan anual donde se establezcan iniciativas de aseguramiento de objetivos que han sido consolidados.	Conforme	30/10/2023	Se verifica una plantilla de objetivos, donde se puede evaluar la fecha de inicio y culminación del objetivo de aseguramiento
6	No se realiza un listado de datos que se introducen de manera errónea al sistema	Conforme	31/10/2023	Se verifica un check list de datos que se insertan de forma errónea al sistema
7	No existe un historial de acciones correctivas	Conforme	01/11/2023	Se verifica una matriz de evaluación de acciones correctivas
8	No se establece un historial de lecciones aprendidas sobre estrategias para gestionar los proyectos de software	Conforme	02/11/2023	Se verifica un cuadro de lecciones aprendidas, donde se plasman nuevas estrategias para el control del proyectos de software
9	El control de cambios se realiza de forma parcial	Conforme	03/11/2023	Se verifica un control en la política de control de cambios, donde se identifican al responsables del cambio efectuado
10	No se mide el rendimiento de los proyectos de desarrollo de software, con respecto a criterios de rendimiento	Conforme	04/11/2023	Se verifica control en la política de gestión de proyectos de software, que ayudan a medir el rendimiento de los proyectos.

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 25/10/2023	FECHA 08/11/2023	FECHA 08/11/2023

Pág. 2 | 3

Fuente: Elaboración propia

LISTADO DE VERIFICACIÒN DE CALIDAD Y ACCIONES CORRECTIVAS

11	No se realiza evaluaciones continuas del personal para medir su rendimiento	Conforme	06/11/2023	Se verifica controles de rendimiento del personal mediante exámenes psicológicos
12	No existe un plan enfocado en la contratación del personal de TI, que permita realizar un seguimiento eficaz.	Conforme	07/11/2023	Se verifica un control en la política de recursos humanos, basadas en las contrataciones del personal

CONCLUSION

Se ha revisado el listado de verificación de calidad de auditoria de TI y ha determinado que se ha completado de manera apropiada y precisa.

CONTROL DE REGISTRO DE LA ASISTENCIA A LA REUNIÓN DE APERTURA

Nombres y Apellidos	Dependencia	Cargo	Firma
Jorge A, Cachay Arana	Área de TI	Supervisor	
Omar Sánchez Rubio	Área de TI	Auditor	
Marry Rabanal Senmache	Área de TI	Auditor	
Junio E, Cachay Maco	Área de TI	Supervisor	

CÓDIGO MATII-01	ELABORÓ Líder del Proceso	REVISÓ	APROBÓ
VERSIÓN 1.0	FECHA 25/10/2023	FECHA 08/11/2023	FECHA 08/11/2023

Pág. 3 | 3

Fuente: Elaboración propia

SATISFACIÓN CLIENTES FORMULARIO DE ENCUESTA

Fecha: 08/11/2023

Cliente (Nombre o Razón Social): CONECTA RETAIL S.A

Nombre de la persona de contacto:

JORGE CACHAY ARANA

Cargo: JEFE DEL AREA DE TI

¿Cuál es su opinión sobre los siguientes aspectos de nuestra gestión de auditoría de TI?

	Malo	Regular	Bueno	Muy Bueno	Excelente
¿Cómo evalúa nuestro servicio de auditoría?					X
Nivel con el cual nuestros servicios satisfacen sus necesidades.					X
Tiempo de respuesta a las sugerencias brindadas.					X
Cumplimiento de plazos de entrega de resultados.					X
Calidad de atención y asesoramiento en auditorías de TI.					X
Calidad de respuesta ante inconvenientes.					X

	1	2	3	4	5
En una escala del 1-5, que tan importante crees que sea el trabajo de auditoría de TI que se realiza en la empresa.	○	○	○	○	X

¿Tiene alguna propuesta de mejora para sugerirnos?

Tener un plan de acción, infunde confianza en los empleados. Por ello es bueno que se realicen auditorias de forma continua y que se realicen los seguimientos correspondientes, para verificar si la empresa está realizando los cambios recomendados.

Figura 50. Formulario de la encuesta de satisfacción cliente.

Fuente: Elaboración propia.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

La forma más eficiente para mejorar el cumplimiento de políticas de TI de las empresas retail en el Perú, es diseñar modelos de auditoría de TI, aplicando una norma y un marco que se adecue a las políticas y objetivos de la empresa, frente a ello se debe evaluar de manera minuciosa las actividades y procesos que realiza la organización y bajo ese enfoque, construir un modelo orientado a las características de la organización, para evaluar el cumplimiento de las políticas de TI. Por ende, el modelo de auditoría de TI diseñado está enfocado en verificar el funcionamiento correcto de las políticas de TI de la empresa auditada, utilizando como norma de estructura la ISO 19011 y como marco de referencia a COBIT 2019.

En el diagnóstico inicial de la empresa retail, se utilizó la matriz de COBIT DS5, implementando preguntas basadas en políticas de TI de la empresa y en el objetivo de gestión MEA02, alineados a auditorias de TI. En el resultado diagnostico se verifica que la empresa se encuentra en un nivel de madurez de grado 3, con un 86% de cumplimiento en cuanto a políticas de TI y las métricas de COBIT 2019, se puede visualizar que se cuenta con políticas y controles internos, sin embargo se recomienda que se implementen pruebas de seguridad que ayuden a cerciorarse que la información obtenida está bien protegida, así mismo es viable que se realicen capacitaciones constantes al personal en cuanto al manejo de credenciales de los sistemas utilizados.

Para la selección de la norma ISO 19011 y el marco de COBIT 2019, se establecieron criterios específicos enfocados en el control interno y las auditorias de TI, evaluados posteriormente por Juicio de experto, obteniendo como resultado que el marco y la norma seleccionados, son aplicables para la empresa en estudio, indicando que ambos parámetros seleccionados son óptimos para la construcción del diseño del modelo de auditoría de TI.

Con este enfoque, la propuesta de este diseño de modelo de auditoría de TI, está enfocado en pequeñas empresas, este criterio se enfatiza porque según la revisión documental realizada, se analizó que la mayoría de modelos de auditoría creados, están enfocados para grandes y medianas empresas, la razón es que las pequeñas empresas tienen escasos recursos económicos, sin embargo nuestro modelo está diseñado para empresas retail y se adapta para gestionar de forma eficiente los procesos del área de TI, dirigido a sus políticas de TI.

Se concluye que la validación de juicio de experto en nuestra investigación, nos permite comprender las dimensiones adecuadas, para la construcción de un modelo óptimo, y nos orienta en que partes del diseño se puede mejorar o si el modelo es convincente y puede ser ejecutado, cabe decir que el modelo obtuvo como puntaje promedio 3.9, indicando que el modelo de auditoria es bastante adecuado para ser ejecutado en la organización.

En la ejecución de la propuesta del modelo de auditoría de TI, que se diseñó para la empresa en estudio obtuvo un 93% de cumplimiento en sus políticas de TI, indicando que la empresa ha reforzado la gestión de los controles internos, referentes a sus políticas de TI. Cabe decir que, al ejecutar el modelo de la auditoria, se aprecia que existe una cohesión entre el uso de la norma Internacional ISO 19011 y el marco COBIT 2019, porque ambos brindan soluciones y métricas para realizar auditoría de TI, basadas en cumplir las políticas y llevar una gestión idónea del área de TI de la empresa.

Finalmente podemos indicar que cada modelo de auditoría de TI desarrollado debe ser único, porque cada empresa es un universo que cuenta con características diferenciadas según sus procesos y actividades a las que se dedica. Si bien el modelo de auditoría de TI desarrollado tiene en cuenta el enfoque de análisis de cumplimiento de políticas que documenta los tipos de incumplimientos, se recomienda crear un sistema de incidencias, que recopile notificaciones constantes de los usuarios e identifique nuevas amenazas y vulnerabilidades de los servicios de TI de la empresa que vulneran el cumplimiento de las políticas de la organización. A su vez se requiere que las empresas promuevan presupuestos adicionales en aporte a la concienciación del personal

en cuanto a gestión de SI e implementación de marcos y normas internacionales que ayuden a minimizar las incidencias y promover la mejora continua de la empresa.

4.2. Recomendaciones

El modelo de auditoría de TI fue diseñado para que la empresa en estudio, cuente con un modelo de auditoría que sea eficiente, sin embargo, es recomendable que apliquen controles adecuados, para generar el cumplimiento efectivo de las auditorías.

Se recomienda a la empresa retail considerar la presente investigación que le ayudará a mejorar el cumplimiento de sus políticas y estándares de manera efectiva, debido que se desarrolló un modelo de auditoría de TI basado en el marco COBIT 2019 y la norma internacional ISO 19011.

Se recomienda que las organizaciones antes de aplicar el modelo de auditoría de TI, evalué de manera minuciosas sus políticas y objetivos y en torno a ello, pueda evaluar si los objetivos de COBIT 2019 son los más idóneos, caso contario se puede realizar una restructuración del modelo, que se adapte a las necesidades más puntuales de la entidad.

Es recomendable entender cómo los auditores planean asegurar de forma eficiente el cumplimiento de normas y políticas de las empresas retail peruanas, de esta manera se podrá identificar, evaluar y controlar el uso óptimo de los servicios de TI, ayudando a cumplir objetivos y creando valor en las operaciones de la organización.

REFERENCIAS

[1] Vargas B., R., Recalde H., L., & Reyes Ch., R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO*. doi:http://dx.doi.org/10.17141/urvio.20.2017.2571

[2] COMEXPERU (2021) Agenda Digital para el Perú 2021 – 2026. Informe Final. Perú. Lima. pp. 1 – 193. Recuperado de: https://www.comexperu.org.pe/upload/articles/publicaciones/agenda_digital_2021_2026.pdf

[3] ESET. (2020). Security Report - Latinoamérica. ESET. pp. 1-30. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf.

[4] Arcentales F., D., & Caycedo C., X. (2017). Computer audit: an effective approach. Ecuador. Cuenca. Doi:http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173

[5] Cama, E. (2020). El 51% de las compañías en el Perú sostienen que la relación entre ciberseguridad y sus líneas de negocio es inexistente o neutral. *EY Perú*. Obtenido de https://www.ey.com/es_pe/news/2020/06/ciberseguridad-lineas-negocio-neutral

[6]. ISACA (2018) Basic IS audit: Innovation in the IT audit process. *ISACA Journal*, vol. 2, 2018. Recuperado de:https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-2/is-audit-basics-innovation-in-the-it-audit-process

[7] Viguri Cordero JA (2021) The use of Certification Mechanisms as an efficient guarantee of personal data protection. Revista Catalana de Dret Públic. 2021;(62):160-176. doi:10.2436/rcdp.i62.2021.3571

[8] Frayssinet Delgado, M., Esenarro, D., Juárez Regalado, F. F., & Díaz Reátegui, M. (2021). Methodology Based on the Nist Cybersecurity Framework as a Proposal for Cybersecurity Management in Government Organizations. 3C TIC, 10(2), 123–141. https://doi.org/10.17993/3ctic.2021.102.123-141

[9] Sabillon, Regner; Serra-Ruiz, Jordi; Cavaller, Victor; Cano, Jeimy (2017). [IEEE 2017 International Conference on Information Systems and Computer Science (INCISCOS) - Quito, Ecuador (2017.11.23-2017.11.25)] 2017 International Conference on Information Systems and Computer Science (INCISCOS) - A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). , (), 253–259. doi:10.1109/INCISCOS.2017.20

[10] Zumba-Vasquez, Carlos; Garcia-Pelaez, Diana; Bolanos-Burgos, Francisco (2018). [IEEE 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) - Cáceres, Spain (2018.6.13-2018.6.16)] 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) - Proposal of a framework for the internal audit to the service management of the department of information technologies. , (), 1–5. doi:10.23919/CISTI.2018.8399441

[11] H. Matsikidze and M. Kyobe, "A Proposed Cyber security framework for auditing in financial institutions," *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada, 2020, pp. 0276-0281, doi: 10.1109/IEMCON51383.2020.9284861.

[12] Murad, D., Fernando, E., Irsan, M., Kosala, R., Ranti, B., & Supangkat, S. (2018). *Implementation of COBIT 5 Framework for Academic Information System Audit Perspective: Evaluate, Direct, and Monitor.* International Conference on Applied Information Technology and Innovation (ICAITI). doi:10.1109/ICAITI.2018.8686700

[13] Andry, Johanes & Lee, Francka & Darma, William & Pr, Paramita & Ekklesia, Reynaldi & Studi, Program & Informasi, Sistem & Teknologi, Fakultas & Desain, Dan. (2022). AUDIT SISTEM INFORMASI MENGGUNAKAN COBIT 5 PADA PERUSAHAAN PENYEDIA LAYANAN INTERNET. Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi. 8. 17-22. 10.24014/rmsi.v8i1.14761.

[14] S. Jaya Putra, M. Nur Gunawan, A. Falach Sobri, J. Muslimin, Amilin y D. Saepudin (2021)"Análisis de gestión de riesgos de seguridad de la información utilizando ISO 27005: 2011 para la empresa de telecomunicaciones", *2020 Octava Conferencia Internacional sobre Cibernética y TI Gestión de Servicios (CITSM)* , Pangkal, Indonesia, 2020, págs. 1-5, doi: 10.1109/CITSM50537.2020.9268845.

[15] Esparza, FJ Díaz, MBR Egas, FAC Sinchiguano y RAL Misacango (2020) Evaluation model of computer audit methodologies based on inherent risk.15° Iberian Congress of Information Systems and Technologies (CISTI) , Sevilla, España, 2020, pp. 1 -7, doi: 10.23919/CISTI49556.2020.9140877.

[16] Cando E & González V (2019) IT management evaluation model based on COBIT, ITIL, ISO 27002 and its effect on the competitiveness of COAC in the area and segment 1. Ecuador. Cuenca. Recuperado de: http://repositorio.uees.edu.ec/bitstream/123456789/3056/1/CANDO%20SALAS%20EDUARDO%20PATRICIO.pdf

[17] Zhañay Soliz, O., Erazo Álvarez, J., & Narváez Zurita, C. (2019). Modelo de Auditoria de Sistemas de Información para las Cooperativas de ahorro y crédito del segmento 1, 2, y 3, de la ciudad de Cuenca. CIENCIAMATRIA, 5(1), 361-393. https://doi.org/10.35381/cm.v5i1.271

[18] Clayman, K., & Lehner, K. (2023). Synergy between Iso 45001 & 19011. Professional Safety, 68(7), 33–34. Recuperado de: https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=164732332&lang=es&site=ehost-live

[19] Cruz, Y., & Pinto, M. (2018). Uso de información para la toma de decisiones en las organizaciones y servicios. Alfagrama Ediciones.pp.52

[20]Universidad Nacional de Salta Argentina (2019) Introducción a la informática Hardware y software. Seminario de informática. Facultad de ciencias económicas, Jurídicas y Sociales. Recuperado de: https://economicas.unsa.edu.ar/sigeco/archivos/semi_material/U1-DT-IntroduccionalaInformatica.pdf.pp1

[21] Barrio, A. (2018). *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos.* Madrid, España: Wolters Kluwer España. Obtenido de https://elibro.net/es/ereader/bibsipan/56038?page=19

[22] Moisés, A. (2017). *CIBERDELITOS: AMENAZAS CRIMINALES DEL CIBERESPACIO.* Madrid, España: REUS EDITORIAL. Obtenido de https://elibro.net/es/ereader/bibsipan/46673?. pp.20

[23] Fonseca, Á. (2015). *Auditoría Forence.* Bogotá, Colombia: Ediciones de la U. Obtenido de https://elibro.net/es/ereader/bibsipan/70254?. pp.199

[24] Tapia, K., Contreras, R., & Silva, R. (2017). *AUDITORÍA INTERNA* (1a ed.). México, México: IMCP. Obtenido de https://books.google.com.pe/books?id=JCFHDwAAQBAJ&lpg=PA1&hl=es&pg=PA1#v=onepage&q&f=false

[25] Piattini, M., Navarro, E., & Ruiz, M. (2015). AUDITORÍA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN. Madrid, España: RAMA Editorial. ¿Obtenido de https://elibro.net/es/ereader/bibsipan/106490?

[26] NORMA ISO 19011 (2018). *Directrices para la auditoría de los sístemas de gestión.* Obtenido de https://uadeo.mx/wp-content/uploads/2020/11/NORMA-ISO-19011-2018.pdf

[27] Serrano, C., Cruz, R., Salcedo, J., & Malagón, A. (2022). *Knowledge management in internal audits: a theoretical-relational model for business growth.*

doi:http://dx.doi.org/10.4067/S0718-07642022000100003
[28] Zapata, A. (2020). *Ciclo de la calida PHVA* (1a, 2015 ed.). Editorial Universidad Nacional de Colombia. Obtenido de https://elibro.net/es/ereader/bibsipan/129837. pp.64
[29] Vasquez, R. (2015). FUNDAMENTOS DE GRC. *Baker Tilly Colombia*. Obtenido de https://studylib.es/doc/7128401/fundamentos-de-grc---baker-tilly-colombia
[30] ISACA (2021) COBIT 2019 Framework: Governance and Management Objectives. Recuperado de: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko5aEAC
[31] ISACA. (2018). *COBIT 2019 Framework: Introduction & Methodology Recuperado de:*https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9cEAC
[32] Aracil, A. (2015). Cybersecurity Nexus [CSX]. Valencia, España. Obtenido de http://www.isacavalencia.org/docs/Eventos/2015/2015.06.25%20-%20Evento%20itSMF-ISACA%20VLC%202015%20-%20Programa%20CSX.pdf
[33] La Contraloría. (2020). *La Contraloría General de la República del Perú.* Obtenido de https://doc.contraloria.gob.pe/ecasilla/docs/acreditacion/15.PO-TI-03.Politica_de_Seguridad_del_PSVAEP.pdf
[34] La NTP ISO/IEC 27001:2014
[35] Superintendencia de banca y seguros AFP (2022) Normativa SBS. Republica del Peru. Recuperado de: https://www.sbs.gob.pe/regulacion/compendio-de-normas-reglamentarias-del-spp
[36] Monroy Mejía, M. D. L. Á. y Nava Sanchezllanes, N. (2018). Metodología de la investigación: (ed.). México, D.F, Grupo Editorial Éxodo. Recuperado de https://elibro.net/es/ereader/bibsipan/172512?page=86.
[37] García, M., & Suarez, M. (2013). Delphi method for the expert consultation in the scientific. Revista Cubana de Salud Pública. Obtenido de https://www.scielosp.org/pdf/rcsp/2013.v39n2/253-267/es
[38] Peña Casanova, M., & Anías Calderón, C. (2019). Sistema para ejecutar políticas sobre infraestructuras de Tecnologías de la Información. INGENIARE - Revista Chilena de Ingeniería, 27(3), 479–494.
[39] Quezada-Sarmiento, P. A., Alvarado-Camacho, P.-E., & Chango-Cañaveral, P. M. (2017). Development of an Information System Audit in a Data Center: Implementation of web application to the management of Audited elements . CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 1, 132–136. Recuperado de: https://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=127420924&lang=es&site=ehost-live

ANEXOS

Anexo1. **Resolución de aprobación del proyecto de investigación**

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0443-2022/FIAU-USS

Pimentel, 06 de julio de 2022

VISTO:
El Acta de reunión N° 00407 - 2022 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante Oficio N°0157-2022/FIAU-IS-USS de fecha 06 de Julio de 2022, y;

CONSIDERANDO:
Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y *tesis* son *aprobados por el Comité de Investigación* y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, mediante documentos de vistos, el Comité de investigación de la referida Escuela profesional acordó aprobar los títulos de los proyectos de investigación que se detallan en el Acta de reunión N° 0407 - 2022, de la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y AMBIENTE, a cargo de los estudiantes del Programa de estudios INGENIERÍA DE SISTEMAS, que indica en el anexo de la presente resolución.
Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO ÚNICO: APROBACION DE TITULOS DE PROYECTO DE INVESTIGACION, a cargo de los estudiantes del Programa de estudios de **INGENIERÍA DE SISTEMAS** que se detallan en el anexo de la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Mg. Victor Alexci Tuesta Monteza
Decano (e) / Facultad De Ingeniería, Arquitectura Y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

DR. HALYN ALVAREZ VÁSQUEZ
SECRETARIO ACADÉMICO | FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
UNIVERSIDAD SEÑOR DE SIPÁN SAC.
CHICLAYO

Cc: Interesado, Archivo

Anexo 1.1. Resolución de aprobación de tema de Tesis.

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N° 0758-2022/FIAU-USS

Pimentel, 05 de diciembre de 2022

VISTOS:

El Acta de reunión N° 01711 – 2022 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante oficio N° 0261-2022/FIAU-II-USS de fecha 30 de noviembre de 2022, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y tesis son *aprobados por el Comité de Investigación* y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, según documentos de vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerda aprobar el tema tesis en el extremo de la tesis a cargo de los estudiantes oegresados que se detallan en el anexo de la presente Resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR, el tema tesis en el extremo de la tesis perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de los estudiantes o egresados del Programa de estudios de INGENIERÍA DE SISTEMAS según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N° 0758-2022/FIAU-USS

Pimentel, 05 de diciembre de 2022

ANEXO

APROBACION DE TEMA DE TESIS

SECCION A

	APELLIDOS	TESIS
1	TAPIA FUENTES MARIANO HERNANDO	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE SERVICIOS DE TI PARA UNA PEQUEÑA EMPRESA PERUANA BASADA EN ITIL V4
2	RIVAS PLATA CASAS CARLOS GUALBERTO	CLASIFICACIÓN DE CÁNCER DE PULMÓN EN IMÁGENES DE TOMOGRAFÍAS MEDIANTE PROCESAMIENTO DE IMÁGENES Y APRENDIZAJE AUTOMÁTICO
3	FARROÑAN TERAN NIXON PAUL	APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO
4	LUNA BECERRA JHERSON ISAC	MÉTODO DE CLASIFICACIÓN AUTOMÁTICA DE DEFICIENCIAS NUTRICIONALES EN HOJAS DE CAFETO MEDIANTE PROCESAMIENTO DE IMÁGENES DIGITALES Y APRENDIZAJE PROFUNDO
5	CABREJOS SEVERINO LUZ ANTONELLA	DESARROLLO DE UN MÉTODO DE LECTURA AUDIBLE DE LIBROS DE TEXTO BASADO EN PROCESAMIENTO DIGITAL DE IMÁGENES Y DEEP LEARNING
6	RABANAL SENMACHE MARRY CECY SÁNCHEZ RUBIO OMAR ALBERTO	DISEÑO DE UN MODELO DE AUDITORÍA DE TI PARA EL CUMPLIMIENTO DE NORMAS Y POLÍTICAS DE UNA EMPRESA RETAIL PERUANA
7	JULCA BRUNO HOLVER KABIR VILCHEZ BAILA ERICKSON YOVANI	EVALUACIÓN DE LA CALIDAD EN USO DE UN SISTEMA DE GESTIÓN EDUCATIVA PARTICULAR BASADO EN LA NORMA ISO/IEC 25022
8	FIESTAS TELLO, TATIANA MERCEDES TEJADA PAREDES, JORGE LUIS	IMPLEMENTACIÓN DE UN MODELO BASADO EN ITIL 4, PARA MEJORAR LA EFICIENCIA DE ITSM EN UNA INSTITUCIÓN REGIONAL DEL ESTADO.
9	AYALA SÁNCHEZ MARIO FRANKLIN TEPE LEON EDWIN ANTONIO	MÉTODO DE DETECCIÓN DE ATAQUES A UNA RED DEFINIDA POR SOFTWARE DE UNA EMPRESA PERUANA BASADO EN MACHINE LEARNING

SECCION B

	APELLIDOS	TESIS
1	SANCHEZ PARDO SAMUEL MORE VILLEGAS FIORELLA JHAJAIRA	DESARROLLO DE MÉTODO PARA LA CLASIFICACIÓN POR MADUREZ DE LA FRESA UTILIZANDO PROCESAMIENTO DE IMÁGENES DIGITALES Y MACHINE LEARNING
2	LOPEZ VALLEJOS ROBER YUBELDER	IMPLEMENTACIÓN DE TECNOLOGÍA BLOCKCHAIN ASOCIANDO USUARIO Y DISPOSITIVO PARA MEJORAR LA SEGURIDAD EN LA AUTENTICACIÓN DE CREDENCIALES DE ACCESO
3	LOZANO DELGADO KELEIN HEIMINN GUERRERO VEGA ERICKS TITO	IMPLEMENTACIÓN DE ALGORITMOS CRIPTOGRÁFICOS PARA MEJORAR LA SEGURIDAD EN EL ENVIO DE TEXTO PLANO POR INTERNET
4	GARCIA CHOZO DIANA KATHERINE MACHUEN MUJICA MIGUEL ANGEL	DESARROLLO DE APLICATIVO MOVIL DE REALIDAD AUMENTADA PARA MEJORAR EL APRENDIZAJE DE INGLES EN ESTUDIANTES DE PRIMERO DE SECUNDARIA

	[illegible]	MACHINE LEARNING
2	LOPEZ VALLEJOS ROBER YUBELDER	IMPLEMENTACIÓN DE TECNOLOGÍA BLOCKCHAIN ASOCIANDO USUARIO Y DISPOSITIVO PARA MEJORAR LA SEGURIDAD EN LA AUTENTICACIÓN DE CREDENCIALES DE ACCESO
3	LOZANO DELGADO KELEIN HEIMINN GUERRERO VEGA ERICKS TITO	IMPLEMENTACIÓN DE ALGORITMOS CRIPTOGRÁFICOS PARA MEJORAR LA SEGURIDAD EN EL ENVIO DE TEXTO PLANO POR INTERNET
4	GARCIA CHOZO DIANA KATHERINE MACHUEN MUJICA MIGUEL ANGEL	DESARROLLO DE APLICATIVO MOVIL DE REALIDAD AUMENTADA PARA MEJORAR EL APRENDIZAJE DE INGLES EN ESTUDIANTES DE PRIMERO DE SECUNDARIA

Anexo 2. Carta de autorización para la recolección de la información.

''Año del Fortalecimiento de la Soberanía Nacional''

CARTA DE ACEPTACIÓN

PROYECTO DE INVESTIGACIÓN

Lima, 11 de julio de 2022

Señor(a): Mg. Ing. Heber Ivan Mejía Cabrera

Director (a) de la Escuela Profesional de Ingeniería de Sistemas

Presente. -

ASUNTO: ACEPTACIÓN DE PROYECTO DE INVESTIGACIÓN

Es grato dirigirme a usted para comunicarle que los estudiantes RABANAL SENMACHE MARRY CECY, identificada con código universitario N°2181802045, con DNI N°47461274 y SÁNCHEZ RUBIO OMAR ALBERTO, identificado con código universitario N°2172801296, con DNI N°44621568, estudiantes del IX ciclo, de la Escuela Profesional de Ingeniería de Sistemas, han sido aceptados para realizar su PROYECTO DE INVESTIGACIÓN, cuyo tema es ''Implementación de un modelo de auditoría basado en un marco de ciberseguridad para el cumplimiento de las normas y estándares de los servicios de TI de una empresa retail peruana'', aprobado con resolución N°0443-2022/FIAU-USS, este será realizado en la Oficina de Informática y Sistemas de la empresa retail CONECTA RETAIL S.A., de acuerdo con los recursos y el asesoramiento requerido para el cumplimiento de las actividades que le sean asignadas.

Esperamos que nuestro aporte sea de gran utilidad para la institución y para la mejora de nuestro país, aprovecho la oportunidad para expresarle mi consideración y estima personal, me suscribo de Ud.

Sin más por el momento reciba un cordial saludo de nuestra parte.

Atentamente,

Mg. Ing. Jorge Andrés Cachay Arana

Sub. Gerente de Desarrollo Sistemas

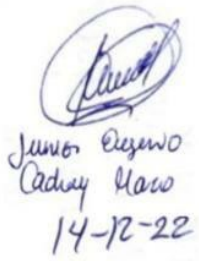
Conecta Retail.

Anexo 3.Instrumentos de recolección de datos.

A. Ficha para recolectar datos de diagnóstico de la empresa en estudio.

NIVEL	PROPÓSITO	MEA	o cumple	Cumple
Nivel 0	Políticas del negocio	La organización cuenta con políticas de TI?		
		Los recursos y actividades enfocadas en los sistemas de Información, se ajustan a los requerimientos de las políticas de TI la entidad?		
		Se estipulan los porcentajes de conformidades basadas en el cumplimiento de políticas de la empresa?		
		El área de TI asigna formalmente responsabilidades que permitan llevar el monitoreo efectivo de las políticas de TI?		
		El área de TI busca el cumplimiento de las políticas de TI manera continua.		
Nivel 1	MEA 02.01 Supervisar los controles internos	La empresa realiza acciones de seguimiento para evaluar de forma efectiva los procesos del negocio?		
		La organización aplica todas las iniciativas de aseguramiento que han sido planeadas, para posteriormente ser ejecutadas de manera pertinente?		
		Se gestiona de manera frecuente, la supervisión, los análisis comparativos y la mejora de los controles de TI para alcanzar el control y cumplimiento de políticas de la empresa.		
		Se realiza la verificación de controles, operaciones y pruebas, que evalúan que los controles aplicados a los SI, funcionan de forma pertinente?		
		Se constata que n el desarrollo de las actividades de TI, se aplican mecanismos de evaluación constante de controles y supervisión de los centros de operación de red y centros de mando?		
		La entidad se preocupa por la aplicación de controles de los SI buscando la efectividad de los requisitos de las políticas del negocio?		
Nivel 2	MEA 02.02 Revisar la eficacia de los controles del proceso de negocio	Se obtienen porcentajes de los programas de aseguramiento que ejecuta la empresa que son probados, basados en estándares de planificación?		
		Se estimula a la alta dirección para que tomen medidas adecuadas enfocadas en el mejoramiento de los procedimientos aplicados a los CI?		
		Se ejecutan programas de evaluación que permitan obtener valores de la eficacia en cuanto la aplicación de políticas y contratos del negocio?		
		Se plantean objetivos específicos a la función de TI?		
		Se logar reconocer de forma jerárquica de quien depende la unidad de TI?		
		La función y la responsabilidad de la unidad de TI son identificable? La entidad cuenta con un plan de estrategias de TI?		
		La entidad logra identificar los riesgos que se encuentran asociados a las TI?		
Nivel 3	MEA 02.03 Realizar autoevaluaciones de control	El área de TI establece sus controles internos comunicando las deficiencias de manera oportuna? Se tiene la trazabilidad del tiempo transcurrido cada vez que se efectúa una ocurrencia producto de las deficiencias de CI?		
		Se identifican las deficiencias de control y se realiza el análisis de las causas raíz subyacente.		
		Se tiene un diseño documentado de alguna metodología de TI I? Se conocen las normas y políticas aplicables a TI para la unidad?		
		Se han puesto de manifiesto los objetivos y funciones de TI al personal interesado?		
		El personal del área de TI cuenta con habilidades y conoce como debe establecer su función en cada uno de los procesos?		
Nivel 4		El proceso de TI es indispensable la lograr el éxito de la entidad?		

	MEA 02.04 Identificar y reportar deficiencias de control	¿Está definido y claro quién tiene la máxima responsabilidad en la instancia del resultado final de la verificación y supervisión de los CI y aplica las medidas correctivas?		
		¿Los procesos son realizados formalmente?		
		¿Los procesos son realizados correctamente?		
		¿Está definido de manera clara quien es el responsable del proceso?		
		¿Los procesos están bien definidos y tienen objetivos claros?		
		Se mide el desempeño de cada proceso?		
		¿Los procesos son auditados?		
		¿Se logra identificar las debilidades de los controles implementados en cada proceso?		
		¿La tecnología utilizada presenta vulnerabilidades?		
Nivel 5	MEA 02 Plan de continuidad y ejecución medidas correctivas	Se ha establecido, un plan de seguridad y se ha comunicado a las partes interesadas?		
		Existen soluciones de seguridad de información que son implementadas aplicando procedimientos de manera eficiente en toda el área de TI?		
		El alcance, políticas de los MPP son viables y están alineados a sus objetivos?		
		El personal relevante se compromete con los programas para minimizar la deficiencia del CI?		
		Los proyectos y las actividades son ejecutados de acuerdo al plan de acción establecido?		
		Los servicios críticos se adaptan con facilidad?		
		Al realizar pruebas de servicios se evidencia la eficiencia del plan de continuidad determinado?		
		El plan de continuidad muestra los requerimientos del área de TI?		
		El personal interesado tanto interno como externo es entrenados para ejecutar el plan de continuidad?		



B. Cuadro comparativo de marco y norma seleccionado para el modelo de auditoria

Cuadro comparativo de marcos y estándares

Ítem	ITIL	COBIT 2019	ISO 19011	NIST	ISO 27001	RISK IT
Dirigido a	Empresas pequeñas, medianas y grandes	Empresas Grandes, medianas y pequeñas	Empresas pequeñas, medianas y grandes	Empresas medianas y grandes	Empresas pequeñas, medianas y grandes	Empresas medianas y grandes
Orientado a	Buenas prácticas en el beneficio a los servicios de TI	Aplicar buenas prácticas en los recursos de TI	Auditoria a los sistemas de gestión organizacional	Orientado al análisis de los riesgos empresariales	Requisitos que establecen la documentación y evaluación de SGS en las organizaciones	Buenas practicas aplicadas a la gestión de riesgos
Constituido por	Compuesto por Ciclo de vida del servicio	Objetivos de gobierno, gestión y cumplimiento. Compuesto por proceso de control organizacional.	Compuesto en principios, gestión en competencia y evaluación de auditores	Compuestos por elementos, eventos y procesos	Compuesto por cláusulas y controles de los SI	Está constituido por áreas para el control interno
Finalidad	Evaluación de calidad de prestación regular	Cumplimiento de metas organizacionales	Finalidad de una planeación y realización de las auditorías.	Proporcionar principios básicos y requisitos para la protección de la información.	Tiene la final de definir los controles ineludibles para garantizar la integridad y disponibilidad de la información	Mide el grado de riesgos de las empresas

	ITIL	COBIT 2019	NIST	ISO 19011	ISO 27001	RISK IT
DIRIGIDO	5	5	5	5	5	1
ORIENTADO	1	5	2,5	5	5	2,5
CONSTITUIDO	2,5	5	2,5	5	5	5
FINALIDAD	2,5	5	2,5	5	2,5	2,5
PROMEDIO	2,8	5	3,1	5	4,4	2,8

Fuente: Elaboración propia.

C. Ficha de selección de procesos de ISO 19011 y del marco de COBIT 2019

Ficha de criterios de selección de objetivos de Gestión de COBIT

OBJETIVOS DE COBIT 2019	Ficha de Criterios para selección de objetivos de Gestión			
	Procesos dirigidos al control interno	Proceso para realizar autoevaluaciones de control interno	Proceso para el seguimiento y monitoreo del control interno	Total
EDM01	1	1	4	6
EDM02	1	1	4	6
EDM03	1	1	4	6
EDMO4	1	1	4	6
EDMO5	1	1	4	6
APO01	1	4	1	6
APO02	1	4	1	6
APO03	1	4	1	6
APO04	1	4	1	6
APO05	1	4	1	6
APO06	1	4	1	6
APO07	2	4	4	10
APO08	1	4	1	6
APO09	1	4	1	6
APO10	1	4	1	6
APO11	1	4	1	6
APO12	1	4	1	6
APO13	1	4	1	6
APO14	1	4	1	6
BAI01	1	2	1	4
BAI02	1	2	1	4
BAI03	1	2	1	4
BAI04	1	2	1	4
BAI05	1	2	1	4
BAI06	1	2	1	4
BAI07	1	2	1	4
BAI08	1	2	1	4
BAI09	1	2	1	4
BAI10	1	2	1	4
BAI11	4	2	4	10
DSS01	1	1	2	4
DSS02	1	1	2	4
DSS03	1	1	2	4
DSS04	1	1	2	4
DSS05	1	1	2	4
DSS06	2	4	4	10
MEA01	2	4	2	8
MEA02	4	4	4	12
MEA03	2	2	4	8
MEA04	4	4	4	12

OBJETIVOS DE COBIT 2019	Resultados de selección			
	Procesos dirigidos al control interno	Proceso para realizar autoevaluaciones de control interno	Proceso para el seguimiento y monitoreo del control interno	Total
APO07	2	4	4	10
BAI11	4	2	4	10
DSS06	2	4	4	10
MEA02	4	4	4	12
MEA04	4	4	4	12

Junior Orozco
Cadray Marco
14-12-22

D. Propuesta del diseño para modelo de auditoria de TI

DISEÑO DE UN MODELO DE AUDITORÍA DE TI PARA EL CUMPLIMIENTO DE NORMAS Y POLITICAS DE UNA EMPRESA RETAIL PERUANA

Alumnos: Rabanal Senmache Marry Cecy.

Sánchez Rubio Omar Alberto.

La presente investigación desarrolla un modelo de auditoría de TI, para el cumplimiento de normas y políticas de la empresa CONECTA RETAIL S.A, basada en la estructura del estándar internacional ISO/IEC 19011 alineados al ciclo de mejora continua PDCA (Plan, Do, Check, Act) y COBIT 2019, con sus dominios DSS06, BAI11, APO07, MEA04 y MEA02.

FASE PRELIMINAR: En esta fase se realiza una reunión con el jefe encargado del área de TI de la empresa CONECTA S.A, para tener un alcance documental y verbal de los procesos involucrados en el área de TI, con la finalidad que el auditor tenga los conocimientos necesarios de los procesos y de auditorías de TI tanto externas como internas de la empresa y que tenga las condiciones idóneas para identificar las políticas de TI de las áreas involucradas dentro de la entidad y analizar las posibles deficiencias del área de Tecnología de Información, para establecer los objetivos de la auditoría.

Diagnóstico: Se realiza un diagnóstico inicial, para ello se ha diseñado una matriz basada en COBIT 2019, estableciendo preguntas que nos ayuden a determinar el estado actual de cumplimiento de auditoría del área de TI de la empresa, para realizar el análisis y selección de normas y estándares a aplicar.

En base a los resultados obtuvimos el siguiente diseño del modelo de auditoria de TI basada en las buenas prácticas de COBIT 2019 y el estándar internacional ISO 19011.

Figura1: Modelo de Auditoria de TI basada en la ISO/IEC 19011 y dominios de COBIT 2019

ESTRUCTURA DEL MODELO DE AUDITORIA DE TI

FASE I – PLANIFICACION

En etapa se desarrolla el cronograma de actividades de auditoria de TI, se realiza la selección del equipo auditor, desarrollamos los objetivos, se procede a firmar el acta de los principios de confidencialidad, se establece el contacto inicial entre el equipo auditor y el equipo del área de TI de la empresa.

FASE II – EJECUCIÒN DE ACTIVIDADES DE AUDITORÍA

En la etapa de ejecución, se aplican 5 dominios de COBIT 2019, los cuales son:

1. *DSS06:* Enfocado en gestionar los controles de procesos del negocio, con la finalidad de verificar si existen controles de aseguramiento para el acceso a sistemas, datos y programas que se restrinjan a usuarios no autorizados.

2. BAI11: Basado en la gestión de proyectos, para evaluar si se gestionan los riesgos en los proyectos y si estos son supervisados y controlados, a través de normas internas que buscan el mejoramiento continuo de la empresa.

3. APO07: Apoya en gestionar los recursos humanos, donde evaluamos la asignación de recursos humanos más idóneos para el desempeño de las actividades de TI.

4. MEA04: Sustentado en gestionar el aseguramiento, para verificar si la organización cuenta con actividades en cuanto a la planificación, delimitación y la ejecución de iniciativas de aseguramiento, con el propósito de alcanzar el cumplimiento de sus requerimientos internos y de los objetivos estratégicos de la organización

5. MEA02: Basado en la gestión del sistema de control interno, donde nos encargaremos de verificar si en la empresa se encuentran definidos de manera formal los roles y responsabilidades para el monitoreo y seguimiento de la efectividad de los controles internos.

FASE III – EVALUACIÓN DE AUDITORÍA DE TI

En esta fase se desarrollan dos actividades:

Hallazgos y Observaciones: Se explican los hechos detectados durante la realización de la auditoría, con el fin de comunicar las carencias, desviaciones, irregularidades, deficiencias, fortalezas y los posibles cambios que sean necesarios para la organización.

Informe de auditoría: La finalidad del informe de auditoría es determinar si la empresa está realizando el cumplimiento eficaz de las normas y políticas, establecidas por la organización, así mismo en el informe se presentan las evidencias objetivas y se evalúa el grado en que se cumplen los criterios de auditoría.

Evaluación de resultados: Se realiza con la finalidad de medir el nivel de satisfacción de la empresa, este proceso se efectúa mediante una encuesta satisfacción cliente.

FASE IV - REVISIÓN Y SEGUIMIENTO: Se realiza una revisión para determinar si se han cumplido los objetivos planteados en la fase 01. Consecuentemente se efectúa el seguimiento de auditoría, para verificar si se están realizando las acciones correctivas estipuladas en el informe de auditoría. Estas acciones son realizadas por la empresa auditada, porque de esta manera la organización logra oportunidades de mejora continua.

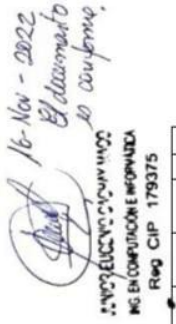


Tabla 1.*Descripción de las fases de ISO/IEC 19011 y dominios de COBIT 2019 utilizados*

	COBIT 2019					ISO 190011
	DSS06	BAI11	APO07	MEA02	MEA04	
FASE I - PLANIFICACION						X
FASE II - EJECUCION	X	X	X	X	X	X
FASE III - VERIFICACION						X
FASE IV - SEGUIMIENTO Y MEJORA						X

Nota: Fases determinadas en ISO/IEC 19011 (2018) y dominios de COBIT 2018

INFORME DE OPINION DE EXPERTO

Este informe tiene como objetivo someter a evaluación el modelo de auditoría de TI basado en un marco de ciberseguridad para el cumplimiento de política y normas, cuya finalidad es comprobar los criterios de claridad, objetividad, suficiencia, coherencia, pertinencia del modelo diseñado.

1. **Datos del Experto**

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

2. **Criterios de validación**

CRITERIOS DE VALIDACIÓN DEL MODELO DE AUDITORÍA DE TI		
Indicador	**Criterio**	**Valoración**
CLARIDAD	El contenido de las fases y de las actividades son legibles y comprensibles.	Rango del 0 al 4 Donde: 0=Nada adecuado 1=Poco Adecuado 2=Adecuado 3=Bastante adecuado 4=Muy Adecuado
OBJETIVIDAD	El contenido de las fases cumple con la finalidad de sus actividades involucradas.	
COHERENCIA	Las fases y actividades respetan las normas internacionales y el contexto de la empresa retail CONECTA S. A	
PERTINENCIA	Las fases y actividades consideran los elementos del contexto de la empresa CONECTA S.A y refleja la realidad.	
SUFICIENCIA	Las fases y actividades satisfacen el ámbito de Auditoría de TI dentro de la empresa retail CONECTA S. A	
RELEVANCIA	El proceso y sub procesos manifiestan importancia y prioridad según el contexto de la empresa.	

16-Nov - 2022
El documento
lo conforme.

ING. EN COMPUTACIÓN E INFORMÁTICA
Reg CIP 179375

3. Instrucciones: Asigne una valoración del 0 al 4 que corresponda para cada criterio en cada actividad de acuerdo al cuadro de valoración presentado en el ítem anterior y finalmente coloque su calificación según los criterios establecidos.

FASE	ACTIVIDAD	CRITERIOS EVALUADOR 1					OBSERVACIONES
		Claridad	Objetividad	Suficiencia	Coherencia	Pertinencia	
FASE PRELIMINAR	A1-Diagnóstico para conocer el estado actual de cumplimiento de la empresa.						
	A2- Selección de Normas, marcos y estándares según diagnóstico						
	A3- Diseño de modelo de auditoría de TI						
FASE 1 PLANIFICACIÓN	A4-Cronograma de actividades de alcance de auditoria						
	A5-Selección del equipo auditor						
	A6-Principio de confidencialidad de la auditoria						
	A7-Establecimiento del contacto inicial						
FASE 02 EJECUCION	A8-Verificar el cumplimiento de la gestión de los procesos						
	A9- Verificar el cumplimiento de la gestión de los proyectos						
	A10- Verificar el cumplimiento de la gestión de los recursos humanos						
	A11- Verificar el cumplimiento de la gestión del aseguramiento						
	A12- Verificar el cumplimiento de la gestión del sistema de control interno						
FASE 3 EVALUACIÓN	A13-Hallazgos y observaciones						
	A14- Informe Final						
	A15 - Evaluación de resultados de auditoria						
FASE 4 REVISIÓN Y SEGUIMIENTO	A16- Actividades de seguimiento						
	A17- Verificación de acciones correctivas						
TOTAL, CRITERIO							
TOTAL, MODELO							

16-Nov-2022
El documento
se conforme

Reg. CIP 179375

E. Matriz de Operalizacion de la variable

Variable de estudio	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos	Valores finales	Tipo de variable	Escala de medición
Modelo de auditoría de TI	Es el inicio para identificar las variables idóneas para evaluar la eficacia y eficiencia de los procesos empresariales transformando su servicio de TI, como un elemento de valor y mejora continua.	Basada en la selección e implementación de estándares y normas internacionales, que permiten planificar, ejecutar, evaluar y dar seguimiento a las políticas de TI de la organización.	Documentación para construcción del modelo de auditoría de TI	Porcentaje de documentación utilizada en selección de marcos	$PDU = \sum_{i=1}^{i=n} \left(\frac{n * 100}{CDU}\right)$ En donde: CDU= Cantidad de Documentación Utilizada n= Sumatoria total de documentos utilizados.	Revisión documental/bitácora	(% porcentaje)	Variable independiente	Nominal
			Tiempo de ejecución del modelo de auditoría de TI	Tiempo de ejecución del modelo	$\sum_{i=1}^{i=n} (Hf - H\,i)$ En donde: Hf= Hora final Hi = Hora de inicio		(hrs horas hombre)		
			Procesos del marco de trabajo utilizado para la construcción del modelo de auditoría de TI	Porcentaje de procesos del marco seleccionado	$PPM = \sum_{i=1}^{i=n} \left(\frac{CPMS * 100}{n}\right)$ En donde: CPMS = Cantidad procesos de marcos seleccionados N = Sumatoria total de procesos de marcos seleccionados	Revisión documental/ficha de revisión/ Juicio de experto/ficha de juicio de experto	(% porcentaje)		

16-Nov-2022
El documento
es conforme

ING EN COMPUTACIÓN E INFORMÁTICA
Reg CIP 179375

			Juicio de experto para evaluación del modelo de auditoría de TI	Promedio de evaluación de expertos Se evalúa coherencia, pertinencia suficiencia objetividad claridad	$\sum_{k=1}^{j=p}\left(\frac{\sum_{j=1}^{i=n}\left(\frac{\sum_{i=1}^{i=n}\frac{ValorCriterio_{ij}}{n}}{m}\right)}{p}\right)$ En donde: n= Cantidad de actividades m= Cantidad de criterios p= Cantidad expertos	Juicio de experto/ficha de juicio de experto	($\bar{X}$ promedio)		
Cumplimiento de normas y políticas	Evaluación minuciosa del conjunto de actividades que permite identificar las incidencias en los servicios de TI de la empresa.	Enfocado en el cumplimiento de objetivos, políticas y acuerdos de la organización, implementando las buenas prácticas de los procesos de TI.	Cumplimiento de actividades notificadas a las partes interesadas	Porcentaje de cumplimiento de actividades	$PcA = \sum_{i=1}^{i=n}\left(\frac{AC * 100}{n}\right)$ En donde: AC= Actividades cumplidas n= Total de actividades de TI	Revisión documental/ficha de revisión/encuesta	(% porcentaje)	Variable dependiente	Razón
			Cumplimiento de políticas de TI	Porcentaje de cumplimiento de políticas de TI	$PCP = \sum_{i=1}^{i=n}\left(\frac{PC * 100}{n}\right)$ En donde: PC= Políticas cumplidas n= Total de actividades de TI	Revisión documental/ficha de revisión/encuesta	(% porcentaje)		

Fuente: Elaboración propia

16-Nov-2020
El documento
se conforma

ING EN COMPUTACIÓN E INFORMÁTICA
Reg CIP 179375

Anexo 3.1 Validación de Instrumentos por el Experto 1 – Rómulo Lomparte Alvarado.

"Año del Fortalecimiento de la Soberanía Nacional"

Chiclayo, miércoles, 20 de Noviembre de 2022

Señor (a):
MG.ING. ROMULO LOMPARTE ALVARADO
SUB GERENTE DE TI
ITG CONSULTING
Ciudad.-

Asunto: VALIDACION DE INSTRUMENTOS A TRAVES DE JUICIO DE EXPERTO

Estimado Señor (a):

Quienes suscriben **RABANAL SENMACHE MARRY CECY** identificado con DNI: 47461274 **y SANCHEZ RUBIO OMAR ALBERTO identificado con DNI:** 44621568 nos es grato dirigirnos a usted para expresarle el saludo cordial y así mismo hacer de conocimiento que siendo estudiante de la Universidad Señor de Sipán, FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO de la Escuela Académico Profesional de **INGENIERÍA DE SISTEMAS**, requiero validar el instrumento de recolección de datos, con el que me permitirá obtener la información requerida para realizar mi investigación.

El título de la investigación es: **DISEÑO DE UN MODELO DE AUDITORIA DE TI PARA EL CUMPLIMIENTO DE NORMAS Y POLITICAS DE UNA EMPRESA RETAIL PERUANA.**

Siendo indispensable que ingenieros calificados y con especialidad en el área de investigación puedan validar los instrumentos, es que recurro a su despacho con la finalidad que usted pueda evaluar dicho instrumento de recolección de datos que aplicare posteriormente.

El expediente de validación contiene lo siguiente:
- Carta de presentación
- Matriz de Operalizacion de la variable
- Certificado de validez de contenido de los instrumentos

En espera de su atención a la presente, aprovecho la oportunidad para expresarle mi consideración y estimapersonal.

Cordialmente,

RABANAL SENMACHE MARRY CECY **SANCHEZ RUBIO OMAR ALBERTO**

CERTIFICADO DE VALIDEZ DE FICHA DIAGNÒSTICO, MARCO, NORMA Y PROCESOS SELECCIONADOS POR MEDIO DE JUICIO DE EXPERTO												
DATOS DEL VALIDADOR			MG.ING. ROMULO LOMPARTE ALVARADO						FECHA: 20/11/2022			
Nº	VARIABLE	DIMENSION	CLARIDAD		OBJETIVIDAD		SUFICIENCIA		COHERENCIA		PERTINENCIA	
			SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
1	DIAGNOSTICO	La ficha diagnostico está bien diseñada y cuenta con los parámetros requeridos	x		x		x		x		x	
2	SELECCIÓN DE NORMA Y MARCO	El marco y la norma están enfocado para empresas pequeñas.	x		x		x		x		x	
3		El marco y norma aplican buenas practicas orientas a los recursos de TI	x		x		x		x		x	
4		El marco y la norma están constituidos por objetivos de gobierno y principios de gestión.	x		x		x		x		x	
5		El marco y la norma tienen por finalidad el cumplimiento de metas organizaciones y la planeación y realización de auditorías de TI.	x		x		x		x		x	
6	SELECCIÓN DE PROCESOS DE NORMA Y MARCO	Los procesos seleccionados están dirigidos al control interno de las políticas de TI de la empresa.	x		x		x		x		x	
7		Los procesos están enfocados en realizar autoevaluaciones de control interno de las políticas de TI de la empresa.	x		x		x		x		x	
8		Los procesos están enfocados en el monitoreo y seguimiento del control interno de políticas de empresa	x		x		x		x		x	

OPINIÒN: APLICABLE (x) NO APLICABLE ( )

CLARIDAD: El indicador es preciso, conciso y exacto
OBJETIVIDAD: El indicador desarrolla procedimientos aceptados
SUFICIENCIA: El indicador es apto para representar la dimensión
COHERENCIA: El indicador se entiende de forma explícita
PERTINENCIA: El indicador es coherente al concepto teórico

FIRMA DIGITAL
Firmado digitalmente por: LOMPARTE ALVARADO ROMULO FERNANDO FIR 32100189 hard
Motivo: Doy V° B°
Fecha: 28/11/2022 01:22:40-0500

CERTIFICADO DE VALIDEZ DEL INSTRUMENTO DE RECOLECCION DE DATOS POR JUICIO DE EXPERTO

DATOS DEL VALIDADOR ROMULO LOMPARTE ALVARADO — **FECHA: 20/11/2022**

Nº	VARIABLE	DIMENSION	INDICADOR	CLARIDAD		OBJETIVIDAD		SUFICIENCIA		COHERENCIA		PERTINENCIA	
				SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
1	**VARIABLE INDEPENDIENTE:** MODELO DE AUDITORIA DE TECNOLOGIAS DE INFORMACIÒN	Documentación para construcción del modelo de auditoria de TI	Porcentaje de documentación utilizada en selección de marcos	X		X		X		X		X	
2		Tiempo de ejecución del modelo de auditoria de TI	Tiempo de ejecución del modelo	X		X		X		X		X	
3		Procesos del marco de trabajo utilizado para la construcción del modelo de auditoria de TI	Porcentaje de procesos del marco seleccionado	X		X		X		X		X	
4		Juicio de experto para evaluación del modelo de auditoria de TI	Promedio de evaluación de expertos	X		X		X		X		X	
5	**VARIABLE DEPENDIENTE:** CUMPLIMIENTO DE NORMAS Y POLITICAS	Cumplimiento de actividades notificadas a las partes interesadas	Porcentaje de cumplimiento de actividades	X		X		X		X		X	
6		Cumplimiento de políticas de TI	Porcentaje de cumplimiento de políticas de TI	X		X		X		X		X	

OPINIÒN: Excelente

APLICABLE (x)

NO APLICABLE ( )

FIRMA DIGITAL

Firmado digitalmente por LOMPARTE ALVARADO ROMULO FERNANDO FIR 32180188 hard
Motivo: Doy V° B°
Fecha: 20/11/2022 01:22:40-0500

CLARIDAD: El indicador es preciso, conciso y exacto.
OBJETIVIDAD: El indicador desarrolla procedimientos aceptados.
SUFICIENCIA: El indicador es apto para representar la dimensión.
COHERENCIA: El indicador se entiende de forma explícita.
PERTINENCIA: El indicador es coherente al concepto teórico.

Anexo 3.2 Validación de Instrumentos por el Experto 2 – Juliana del Pilar Alba Zapata.

"Año del Fortalecimiento de la Soberanía Nacional"

Chiclayo, miércoles, 20 de Noviembre de 2022

Señor (a) (ita):
MG.ING. JULIANA DEL PILAR ALVA ZAPATA
LIDER DEL AREA DE TI, RIESGOS AUDITORIA Y CUMPLIMIENTO
EDYPIME ALTERNATIVA
Ciudad.-

Asunto: VALIDACION DE INSTRUMENTOS A TRAVES DE JUICIO DE EXPERTO

Estimado Señor (a):

Quienes suscriben **RABANAL SENMACHE MARRY CECY** identificado con DNI: 47461274 **y SANCHEZ RUBIO OMAR ALBERTO identificado con DNI:** 44621568 nos es grato dirigirnos a usted para expresarle el saludo cordial y así mismo hacer de conocimiento que siendo estudiante de la Universidad Señor de Sipán, FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO de la Escuela Académico Profesional de **INGENIERÍA DE SISTEMAS**, requiero validar el instrumento de recolección de datos, con el que me permitirá obtener la información requerida para realizar mi investigación.

El título de la investigación es: **DISEÑO DE UN MODELO DE AUDITORIA DE TI PARA EL CUMPLIMIENTO DE NORMAS Y POLITICAS DE UNA EMPRESA RETAIL PERUANA.**

Siendo indispensable que ingenieros calificados y con especialidad en el área de investigación puedan validar los instrumentos, es que recurro a su despacho con la finalidad que usted pueda evaluar dicho instrumento de recolección de datos que aplicare posteriormente.

El expediente de validación contiene lo siguiente:
- Carta de presentación
- Matriz de Operalizacion de la variable
- Certificado de validez de contenido de los instrumentos

En espera de su atención a la presente, aprovecho la oportunidad para expresarle mi consideración y estimapersonal.

Cordialmente,

RABANAL SENMACHE MARRY CECY **SANCHEZ RUBIO OMAR ALBERTO**

CERTIFICADO DE VALIDEZ DE FICHA DIAGNÒSTICO, MARCO, NORMA Y PROCESOS SELECCIONADOS POR MEDIO DE JUICIO DE EXPERTO												
DATOS DEL VALIDADOR			Juliana del Pilar Alva Zapata						FECHA: 20/11/2022			
Nº	VARIABLE	DIMENSION	CLARIDAD		OBJETIVIDAD		SUFICIENCIA		COHERENCIA		PERTINENCIA	
			SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
1	DIAGNOSTICO	La ficha diagnostico está bien diseñada y cuenta con los parámetros requeridos	X		X		X		X		X	
2	SELECCIÓN DE NORMA Y MARCO	El marco y la norma están enfocado para empresas pequeñas.	X		X		X		X		X	
3		El marco y norma aplican buenas practicas orientas a los recursos de TI	X		X		X		X		X	
4		El marco y la norma están constituidos por objetivos de gobierno y principios de gestión.	X		X		X		X		X	
5		El marco y la norma tienen por finalidad el cumplimiento de metas organizaciones y la planeación y realización de auditorías de TI.	X		X		X		X		X	
6	SELECCIÓN DE PROCESOS DE NORMA Y MARCO	Los procesos seleccionados están dirigidos al control interno de las políticas de TI de la empresa.	X		X		X		X		X	
7		Los procesos están enfocados en realizar autoevaluaciones de control interno de las políticas de TI de la empresa.	X		X		X		X		X	
8		Los procesos están enfocados en el monitoreo y seguimiento del control interno de políticas de empresa	X		X		X		X		X	

OPINIÒN: APLICABLE (x) NO APLICABLE ( )

JULIANA DEL PILAR ALVA ZAPATA
ING. EN COMPUTACION E INFORMATICA
REG. CIP. 200951
Firma del Evaluador

CLARIDAD: El indicador es preciso, conciso y exacto
OBJETIVIDAD: El indicador desarrolla procedimientos aceptados
SUFICIENCIA: El indicador es apto para representar la dimensión
COHERENCIA: El indicador se entiende de forma explicita
PERTINENCIA: El indicador es coherente al concepto teórico

CERTIFICADO DE VALIDEZ DEL INSTRUMENTO DE RECOLECCION DE DATOS POR JUICIO DE EXPERTO

DATOS DEL VALIDADOR Juliana del Pilar Alva Zapata **FECHA: 20/11/2022**

Nº	VARIABLE	DIMENSION	INDICADOR	CLARIDAD		OBJETIVIDAD		SUFICIENCIA		COHERENCIA		PERTINENCIA	
				SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
1	VARIABLE INDEPENDIENTE: MODELO DE AUDITORIA DE TECNOLOGIAS DE INFORMACIÓN	Documentación para construcción del modelo de auditoría de TI	Porcentaje de documentación utilizada en selección de marcos	X		X		X		X		X	
2		Tiempo de ejecución del modelo de auditoría de TI	Tiempo de ejecución del modelo	X		X		X		X		X	
3		Procesos del marco de trabajo utilizado para la construcción del modelo de auditoría de TI	Porcentaje de procesos del marco seleccionado	X		X		X		X		X	
4		Juicio de experto para evaluación del modelo de auditoría de TI	Promedio de evaluación de expertos	X		X		X		X		X	
5	VARIABLE DEPENDIENTE: CUMPLIMIENTO DE NORMAS Y POLITICAS	Cumplimiento de actividades notificadas a las partes interesadas	Porcentaje de cumplimiento de actividades	X		X		X		X		X	
6		Cumplimiento de políticas de TI	Porcentaje de cumplimiento de políticas de TI	X		X		X		X		X	

OPINIÒN: Excelente APLICABLE (X) NO APLICABLE ( )

Conforme

JULIANA DEL PILAR ALVA ZAPATA
ING. EN COMPUTACION E INFORMATICA
REG. CIP. 200951

Firma del Evaluador

CLARIDAD: El indicador es preciso, conciso y exacto.
OBJETIVIDAD: El indicador desarrolla procedimientos aceptados.
SUFICIENCIA: El indicador es apto para representar la dimensión.
COHERENCIA: El indicador se entiende de forma explícita.
PERTINENCIA: El indicador es coherente al concepto teorico.

Anexo 3.3 Validación de Instrumentos por el Experto 3 – Elio Hely Campos Vásquez

"Año de la Unidad Paz y Desarrollo"

Chiclayo, miércoles, 08 de Febrero del 2024

Señor (a):
ING. ELIO HELY CAMPOS VASQUEZ
OFICINA DE TECNOLOGIAS DE LA INFORMACION Y TELECOMUNICACIONES
MUNICIPALIDAD NACIONAL DE JAEN
Ciudad.-

Asunto: VALIDACION DE INSTRUMENTOS A TRAVES DE JUICIO DE EXPERTO

Estimado Señor (a):

Quienes suscriben **RABANAL SENMACHE MARRY CECY** identificado con DNI: 47461274 **y SANCHEZ RUBIO OMAR ALBERTO identificado con DNI:** 44621568 nos es grato dirigirnos a usted para expresarle el saludo cordial y así mismo hacer de conocimiento que siendo estudiante de la Universidad Señor de Sipán, FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO de la Escuela Académico Profesional de **INGENIERÍA DE SISTEMAS**, requiero validar el instrumento de recolección de datos, con el que me permitirá obtener la información requerida para realizar mi investigación.

El título de la investigación es: **DISEÑO DE UN MODELO DE AUDITORIA DE TI PARA EL CUMPLIMIENTO DE NORMAS Y POLITICAS DE UNA EMPRESA RETAIL PERUANA.**

Siendo indispensable que ingenieros calificados y con especialidad en el área de investigación puedan validar los instrumentos, es que recurro a su despacho con la finalidad que usted pueda evaluar dicho instrumento de recolección de datos que aplicare posteriormente.

El expediente de validación contiene lo siguiente:
- Carta de presentación
- Matriz de Operalizacion de la variable
- Certificado de validez de contenido de los instrumentos

En espera de su atención a la presente, aprovecho la oportunidad para expresarle mi consideración y estimapersonal.

Cordialmente,

RABANAL SENMACHE MARRY CECY **SANCHEZ RUBIO OMAR ALBERTO**

CERTIFICADO DE VALIDEZ DE FICHA DIAGNÒSTICO, MARCO, NORMA Y PROCESOS SELECCIONADOS POR MEDIO DE JUICIO DE EXPERTO												
		DATOS DEL VALIDADOR	ING. ELIO HELY CAMPOS VASQUEZ						FECHA: 20/11/2023			
Nº	VARIABLE	DIMENSION	CLARIDAD		OBJETIVIDAD		SUFICIENCIA		COHERENCIA		PERTINENCIA	
			SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
1	DIAGNOSTICO	La ficha diagnostico está bien diseñada y cuenta con los parámetros requeridos	x		x		x		x		x	
2	SELECCIÓN DE NORMA Y MARCO	El marco y la norma están enfocado para empresas pequeñas.	x		x		x		x		x	
3		El marco y norma aplican buenas practicas orientas a los recursos de TI	x		x		x		x		x	
4		El marco y la norma están constituidos por objetivos de gobierno y principios de gestión.	x		x		x		x		x	
5		El marco y la norma tienen por finalidad el cumplimiento de metas organizaciones y la planeación y realización de auditorías de TI.	x		x		x		x		x	
6	SELECCIÓN DE PROCESOS DE NORMA Y MARCO	Los procesos seleccionados están dirigidos al control interno de las políticas de TI de la empresa.	x		x		x		x		x	
7		Los procesos están enfocados en realizar autoevaluaciones de control interno de las políticas de TI de la empresa.	x		x		x		x		x	
8		Los procesos están enfocados en el monitoreo y seguimiento del control interno de políticas de empresa	x		x		x		x		x	

OPINIÒN: APLICABLE (x) NO APLICABLE ( )

CLARIDAD: El indicador es preciso, conciso y exacto
OBJETIVIDAD: El indicador desarrolla procedimientos aceptados
SUFICIENCIA: El indicador es apto para representar la dimensión
COHERENCIA: El indicador se entiende de forma explícita
PERTINENCIA: El indicador es coherente al concepto teórico

Cip: 130773

CERTIFICADO DE VALIDEZ DEL INSTRUMENTO DE RECOLECCION DE DATOS POR JUICIO DE EXPERTO

DATOS DEL VALIDADOR ELIO ELOY CAMPOS VASQUEZ **FECHA: 20/11/2023**

Nº	VARIABLE	DIMENSION	INDICADOR	CLARIDAD		OBJETIVIDAD		SUFICIENCIA		COHERENCIA		PERTINENCIA	
				SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
1	**VARIABLE INDEPENDIENTE:** MODELO DE AUDITORIA DE TECNOLOGIAS DE INFORMACIÒN	Documentación para construcción del modelo de auditoría de TI	Porcentaje de documentación utilizada en selección de marcos	X		X		X		X		X	
2		Tiempo de ejecución del modelo de auditoría de TI	Tiempo de ejecución del modelo	X		X		X		X		X	
3		Procesos del marco de trabajo utilizado para la construcción del modelo de auditoría de TI	Porcentaje de procesos del marco seleccionado	X		X		X		X		X	
4		Juicio de experto para evaluación del modelo de auditoría de TI	Promedio de evaluación de expertos	X		X		X		X		X	
5	**VARIABLE DEPENDIENTE:** CUMPLIMIENTO DE NORMAS Y POLITICAS	Cumplimiento de actividades notificadas a las partes interesadas	Porcentaje de cumplimiento de actividades	X		X		X		X		X	
6		Cumplimiento de políticas de TI	Porcentaje de cumplimiento de políticas de TI	X		X		X		X		X	

OPINIÒN: Excelente APLICABLE (x) NO APLICABLE ( )

CLARIDAD: El indicador es preciso, conciso y exacto.
OBJETIVIDAD: El indicador desarrolla procedimientos aceptados.
SUFICIENCIA: El indicador es apto para representar la dimensión.
COHERENCIA: El indicador se entiende de forma explícita.
PERTINENCIA: El indicador es coherente al concepto teórico.

Cip: 130773

Anexo 3.4. Instrumento de recolección de datos con su respectiva evaluación por Experto 1

INFORME DE OPINION DE EXPERTO

Este informe tiene como objetivo someter a evaluación el modelo de auditoría de TI basado en un marco de ciberseguridad para el cumplimiento de política y normas, cuya finalidad es comprobar los criterios de claridad, objetividad, suficiencia, coherencia, pertinencia del modelo diseñado.

1. **Datos del Experto**

DATOS GENERALES DEL EXPERTO	
Nombres y apellidos:	Rómulo Lomparte Alvarado
Grado académico y profesión:	Licenciado en Computación/ Ciencias de la Computación Magister en Administración de Negocios/MBA
Áreas de experiencia laboral:	Consultoría, auditoria, seguridad, ciberseguridad y desarrollo de proyectos de sistemas de información. Experiencia en uso de COSO, COBIT y procesos de certificación Sarbanes-Oxley
Empresa donde labora:	ITG Consulting
Tiempo de experiencia:	35 años

2. **Criterios de validación**

CRITERIOS DE VALIDACIÓN DEL MODELO DE AUDITORÍA DE TI		
Indicador	**Criterio**	**Valoración**
CLARIDAD	El contenido de las fases y de las actividades son legibles y comprensibles.	Rango del 0 al 4 Donde: 0=Nada adecuado 1=Poco Adecuado 2=Adecuado 3=Bastante adecuado 4=Muy Adecuado
OBJETIVIDAD	El contenido de las fases cumple con la finalidad de sus actividades involucradas.	
COHERENCIA	Las fases y actividades respetan las normas internacionales y el contexto de la empresa retail CONECTA S. A	
PERTINENCIA	Las fases y actividades consideran los elementos del contexto de la empresa CONECTA S.A y refleja la realidad.	
SUFICIENCIA	Las fases y actividades satisfacen el ámbito de Auditoría de TI dentro de la empresa retail CONECTA S. A	

4

3. Instrucciones: Asigne una valoración del 0 al 4 que corresponda para cada criterio en cada actividad de acuerdo al cuadro de valoración presentado en el ítem anterior y finalmente coloque su calificación según los criterios establecidos.

FASE	ACTIVIDAD	CRITERIOS EVALUADOR 1					OBSERVACIONES
		Claridad	Objetividad	Suficiencia	Coherencia	Pertinencia	
FASE PRELIMINAR	A1-Diagnóstico para conocer el estado actual de cumplimiento de la empresa.	4	4	4	4	4	.....
	A2- Selección de Normas, marcos y estándares según diagnóstico	4	4	4	4	4	.....
	A3- Diseño de modelo de auditoría de TI	4	4	4	4	4	.....
FASE 1 PLANIFICACIÓN	A4-Cronograma de actividades de alcance de auditoria	4	4	4	4	4	.....
	A5-Selección del equipo auditor	4	4	4	4	4	.....
	A6-Principio de confidencialidad de la auditoria	4	4	4	4	4	.....
	A7-Establecimiento del contacto inicial	4	4	4	4	4	.....
FASE 02 EJECUCION	A8-Verificar el cumplimiento de la gestión de los procesos	4	4	4	4	4	.....
	A9- Verificar el cumplimiento de la gestión de los proyectos	4	4	4	4	4	.....
	A10- Verificar el cumplimiento de la gestión de los recursos humanos	4	4	4	4	4	.....
	A11- Verificar el cumplimiento de la gestión del aseguramiento	4	4	4	4	4	.....
	A12- Verificar el cumplimiento de la gestión del sistema de control interno	4	4	4	4	4	.....
FASE 3 EVALUACIÓN	A13-Hallazgos y observaciones	4	4	4	4	4	.....
	A14- Informe Final	4	4	4	4	4	.....
FASE 4 REVISIÓN Y SEGUIMIENTO	A15- Actividades de seguimiento	4	4	4	4	4	.....
	A16- Verificación de acciones correctivas	4	4	4	4	4	.....
TOTAL, CRITERIO		4	4	4	4	4	
TOTAL, MODELO		4					

FIRMA DIGITAL

Firmado digitalmente por LOMPARTE ALVARADO ROMULO FERNANDO FIR 32180189 hard
Motivo: Doy V° B°
Fecha: 28/11/2022 01:22:46-0500

Anexo 3.5. Instrumento de recolección de datos con su respectiva evaluación por Experto 2

INFORME DE OPINION DE EXPERTO

Este informe tiene como objetivo someter a evaluación el modelo de auditoría de TI basado en un marco de ciberseguridad para el cumplimiento de política y normas, cuya finalidad es comprobar los criterios de claridad, objetividad, suficiencia, coherencia, pertinencia del modelo diseñado.

1. **Datos del Experto**

DATOS GENERALES DEL EXPERTO	
Nombres y apellidos:	Juliana del Pilar Mva Zapata
Grado académico y profesión:	Magister. Ing en Computación e Informática
Áreas de experiencia laboral:	Area de TI, Riesgos, Auditoría y Cumplimiento
Empresa donde labora:	Edpyme Alternativa
Tiempo de experiencia:	13 años

2. **Criterios de validación**

CRITERIOS DE VALIDACIÓN DEL MODELO DE AUDITORÍA DE TI		
Indicador	**Criterio**	**Valoración**
CLARIDAD	El contenido de las fases y de las actividades son legibles y comprensibles.	Rango del 0 al 4 Donde: 0=Nada adecuado 1=Poco Adecuado 2=Adecuado 3=Bastante adecuado 4=Muy Adecuado
OBJETIVIDAD	El contenido de las fases cumple con la finalidad de sus actividades involucradas.	
COHERENCIA	Las fases y actividades respetan las normas internacionales y el contexto de la empresa retail CONECTA S. A	
PERTINENCIA	Las fases y actividades consideran los elementos del contexto de la empresa CONECTA S.A y refleja la realidad.	
SUFICIENCIA	Las fases y actividades satisfacen el ámbito de Auditoría de TI dentro de la empresa retail CONECTA S. A	
RELEVANCIA	El proceso y sub procesos manifiestan importancia y prioridad según el contexto de la empresa.	

4

3. **Instrucciones**: Asigne una valoración del 0 al 4 que corresponda para cada criterio en cada actividad de acuerdo al cuadro de valoración presentado en el ítem anterior y finalmente coloque su calificación según los criterios establecidos.

FASE	ACTIVIDAD	CRITERIOS EVALUADOR 1					OBSERVACIONES
		Claridad	Objetividad	Suficiencia	Coherencia	Pertinencia	
FASE PRELIMINAR	A1-Diagnóstico para conocer el estado actual de cumplimiento de la empresa.	4	4	4	4	4	
	A2- Selección de Normas, marcos y estándares según diagnóstico	4	4	4	4	4	
	A3- Diseño de modelo de auditoria de TI	4	4	4	4	4	
FASE 1 PLANIFICACIÓN	A4-Cronograma de actividades de alcance de auditoria	4	4	4	4	4	
	A5-Selección del equipo auditor	4	4	4	4	4	
	A6-Principio de confidencialidad de la auditoria	4	4	4	4	4	
	A7-Establecimiento del contacto inicial	4	4	4	4	4	
FASE 02 EJECUCION	A8-Verificar el cumplimiento de la gestión de los procesos	4	4	4	4	4	
	A9- Verificar el cumplimiento de la gestión de los proyectos	4	4	4	4	4	
	A10- Verificar el cumplimiento de la gestión de los recursos humanos	4	4	4	4	4	
	A11- Verificar el cumplimiento de la gestión del aseguramiento	4	4	4	4	4	
	A12- Verificar el cumplimiento de la gestión del sistema de control interno	4	4	4	4	4	
FASE 3 EVALUACIÓN	A13-Hallazgos y observaciones	4	4	4	4	3	Aquí se deben determinar las observaciones y hallazgos
	A14- Informe Final	4	4	4	4	4	
FASE 4 REVISIÓN Y SEGUIMIENTO	A15- Actividades de seguimiento	4	4	4	4	4	
	A16- Verificación de acciones correctivas	4	4	4	4	4	
TOTAL, CRITERIO		4	4	4	4	3,93	
TOTAL, MODELO		3,98					

Conforme

JULIANA DEL PILAR ALVA ZAPATA
ING. EN COMPUTACION E INFORMATICA
REG. CIP. 200951

Anexo 3.5. Instrumento de recolección de datos con su respectiva evaluación por Experto 3

INFORME DE OPINION DE EXPERTO

Este informe tiene como objetivo someter a evaluación el modelo de auditoría de TI basado en un marco de ciberseguridad para el cumplimiento de política y normas, cuya finalidad es comprobar los criterios de claridad, objetividad, suficiencia, coherencia, pertinencia del modelo diseñado.

1. **Datos del Experto**

DATOS GENERALES DEL EXPERTO	
Nombres y apellidos:	Elio Eloy Campos Vásquez
Grado académico y profesión:	Ing. Informático y de Sistemas
Áreas de experiencia laboral:	Oficina de Tecnologías de Información y Comunicaciones
Empresa donde labora:	Municipalidad Provincial de Jaén
Tiempo de experiencia:	10 años

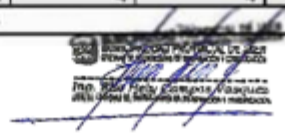
2. **Criterios de validación**

CRITERIOS DE VALIDACIÓN DEL MODELO DE AUDITORÍA DE TI		
Indicador	**Criterio**	**Valoración**
CLARIDAD	El contenido de las fases y de las actividades son legibles y comprensibles.	Rango del 0 al 4 Donde: 0=Nada adecuado 1=Poco Adecuado 2=Adecuado 3=Bastante adecuado 4=Muy Adecuado
OBJETIVIDAD	El contenido de las fases cumple con la finalidad de sus actividades involucradas.	
COHERENCIA	Las fases y actividades respetan las normas internacionales y el contexto de la empresa Retail CONECTA S. A	
PERTINENCIA	Las fases y actividades consideran los elementos del contexto de la empresa CONECTA S.A y refleja la realidad.	
SUFICIENCIA	Las fases y actividades satisfacen el ámbito de Auditoría de TI dentro de la empresa Retail CONECTA S. A	

MUNICIPALIDAD PROVINCIAL DE JAÉN
Ing. Elio Eloy Campos Vásquez
/ Cip: 130773

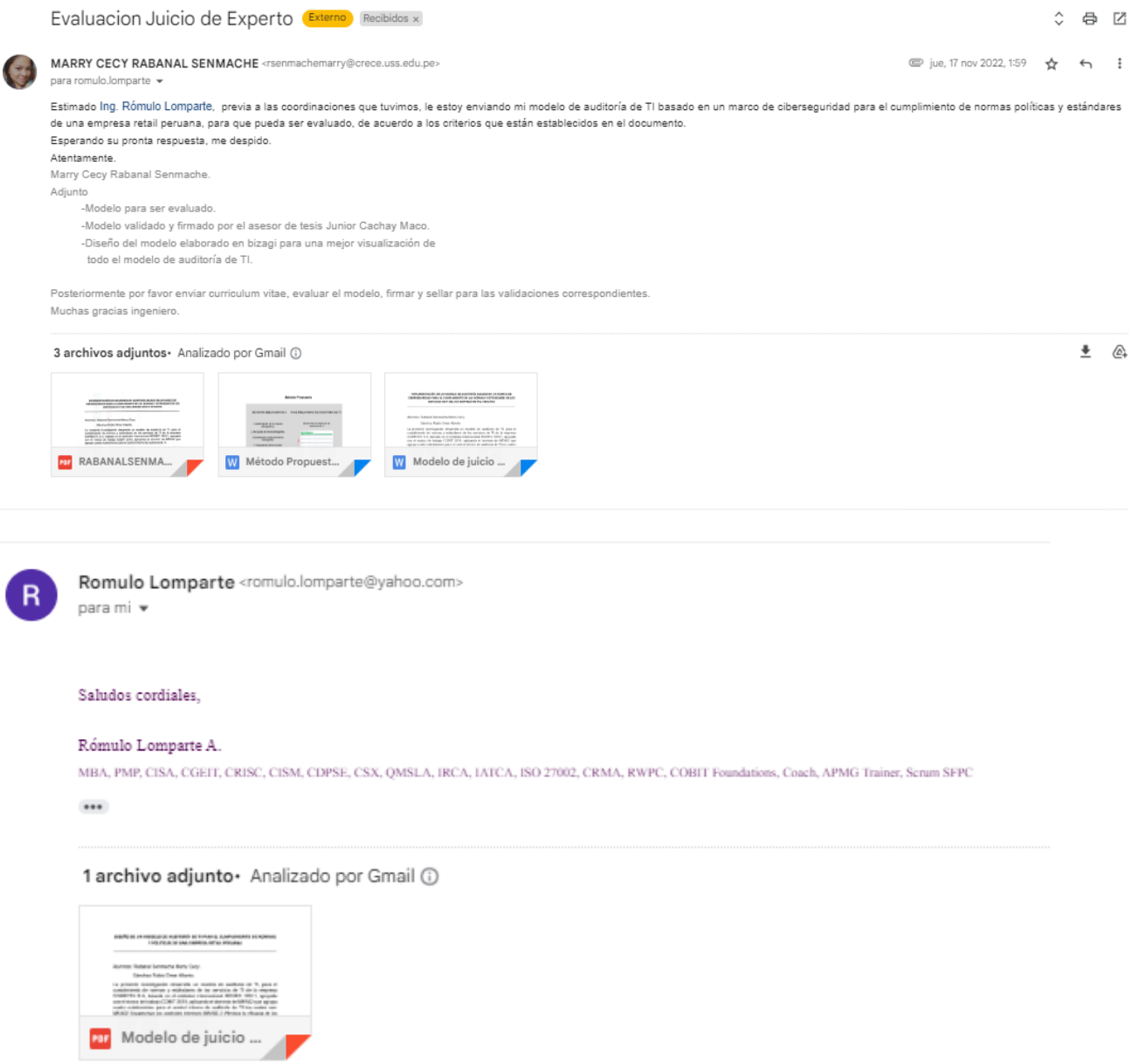
3. **Instrucciones:** Asigne una valoración del 0 al 4 que corresponda para cada criterio en cada actividad de acuerdo al cuadro de valoración presentado en el ítem anterior y finalmente coloque su calificación según los criterios establecidos.

FASE	ACTIVIDAD	CRITERIOS EVALUADOR 1					OBSERVACIONES
		Claridad	Objetividad	Suficiencia	Coherencia	Pertinencia	
FASE PRELIMINAR	A1-Diagnóstico para conocer el estado actual de cumplimiento de la empresa.	4	4	4	4	4	**********
	A2- Selección de Normas, marcos y estándares según diagnóstico	4	4	4	4	4	**********
	A3- Diseño de modelo de auditoría de TI	4	4	4	4	4	**********
FASE 1 PLANIFICACIÓN	A4-Cronograma de actividades de alcance de auditoria	4	4	4	4	4	**********
	A5-Selección del equipo auditor	4	4	4	4	4	**********
	A6-Principio de confidencialidad de la auditoria	4	4	4	4	4	**********
	A7-Establecimiento del contacto inicial	4	4	4	4	4	**********
FASE 02 EJECUCION	A8-Verificar el cumplimiento de la gestión de los procesos	4	4	4	4	4	**********
	A9- Verificar el cumplimiento de la gestión de los proyectos	4	4	4	4	4	**********
	A10- Verificar el cumplimiento de la gestión de los recursos humanos	4	4	4	4	4	**********
	A11- Verificar el cumplimiento de la gestión del aseguramiento	4	4	4	4	4	**********
	A12- Verificar el cumplimiento de la gestión del sistema de control interno	4	4	4	4	4	**********
FASE 3 EVALUACIÓN	A13-Hallazgos y observaciones	4	4	4	4	4	**********
	A14- Informe Final	4	4	4	4	4	**********
FASE 4 REVISIÓN Y SEGUIMIENTO	A15- Actividades de seguimiento	4	4	4	4	4	**********
	A16- Verificación de acciones correctivas	4	4	4	4	4	**********
TOTAL, CRITERIO		4	4	4	4	4	**********
TOTAL, MODELO		4					



Cip: 130773

Anexo 3.6. Evidencia de aceptación para evaluación de juicio de experto 1



Evaluacion Juicio de Experto Externo Recibidos ×

MARRY CECY RABANAL SENMACHE <rsenmachemarry@crece.uss.edu.pe> jue, 17 nov 2022, 1:59
para romulo.lomparte

Estimado Ing. Rómulo Lomparte, previa a las coordinaciones que tuvimos, le estoy enviando mi modelo de auditoría de TI basado en un marco de ciberseguridad para el cumplimiento de normas políticas y estándares de una empresa retail peruana, para que pueda ser evaluado, de acuerdo a los criterios que están establecidos en el documento.
Esperando su pronta respuesta, me despido.
Atentamente.
Marry Cecy Rabanal Senmache.
Adjunto
-Modelo para ser evaluado.
-Modelo validado y firmado por el asesor de tesis Junior Cachay Maco.
-Diseño del modelo elaborado en bizagi para una mejor visualización de todo el modelo de auditoría de TI.

Posteriormente por favor enviar curriculum vitae, evaluar el modelo, firmar y sellar para las validaciones correspondientes.
Muchas gracias ingeniero.

3 archivos adjuntos • Analizado por Gmail

RABANALSENMA... Método Propuest... Modelo de juicio ...

Romulo Lomparte <romulo.lomparte@yahoo.com>
para mi

Saludos cordiales,

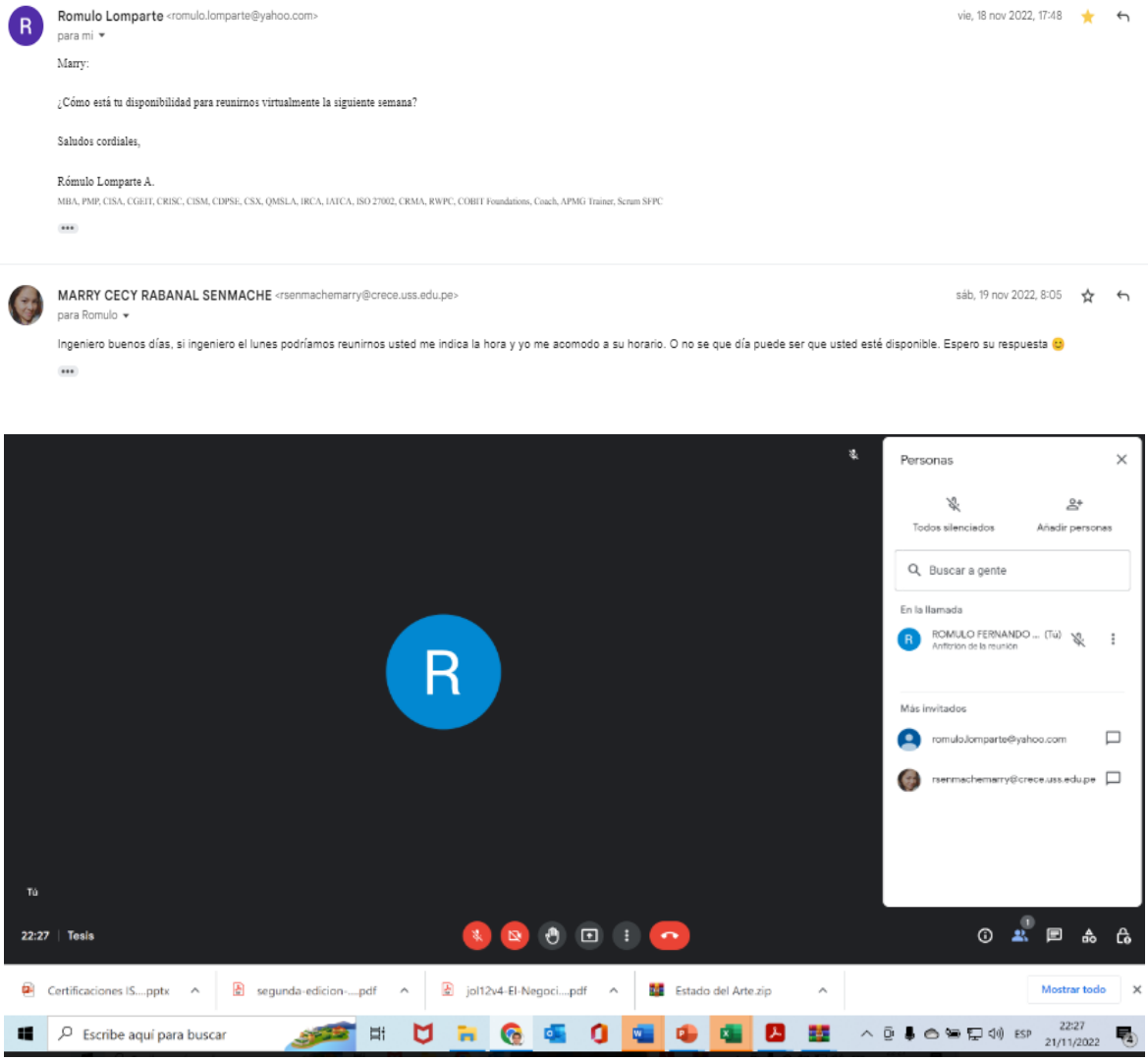
Rómulo Lomparte A.
MBA, PMP, CISA, CGEIT, CRISC, CISM, CDPSE, CSX, QMSLA, IRCA, IATCA, ISO 27002, CRMA, RWPC, COBIT Foundations, Coach, APMG Trainer, Scrum SFPC

1 archivo adjunto • Analizado por Gmail

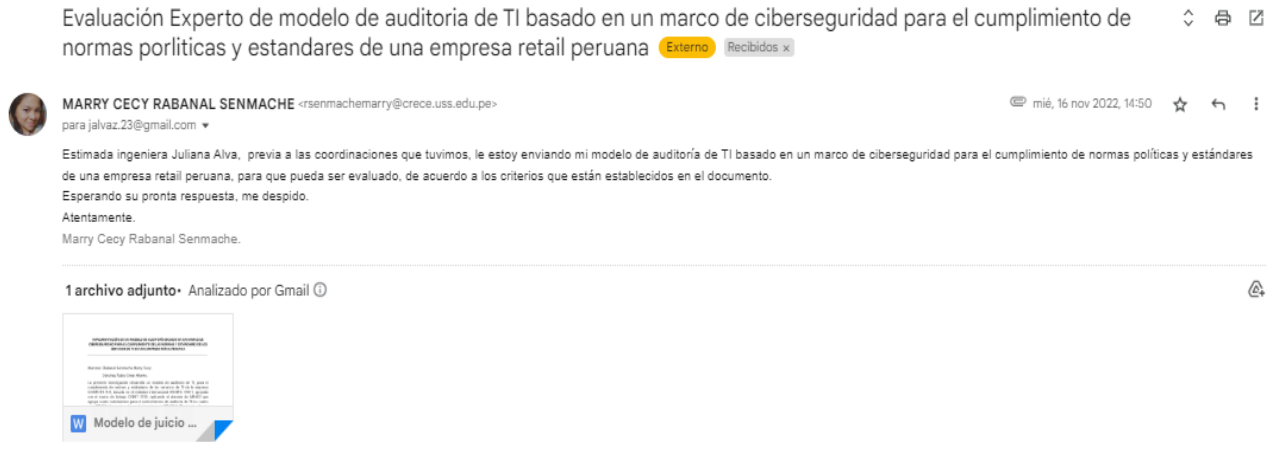
Modelo de juicio ...

MARRY CECY RABANAL SENMACHE <rsenmachemarry@crece.uss.edu.pe>
para Romulo

Muchas gracias ingeniero.
Saludos 🙂.



Anexo 3.7. Evidencia de aceptación para evaluación de juicio de experto 2



MARRY CECY RABANAL SENMACHE
Estimada ingeniera Juliana Alva, previa a las coordinaciones que tuvimos, le estoy enviando mi modelo de auditoría de TI basado en un marco de ciberseguridad pa

Juliana Alva <jalvaz.23@gmail.com>
para mi

Buenas noches Marry
Adjunto opinión

Atte

1 archivo adjunto · Analizado por Gmail

Opinion_experto....

MARRY CECY RABANAL SENMACHE
Muchas gracias ingeniera Juliana. Gracias por su apoyo.

Juliana Alva <jalvaz.23@gmail.com> jue, 17 nov 2022, 19:59
para mi

Buenas noches Marry
adjunto mi cv actualizado.

Saludos.

--
Atte.

Ing. Juliana Alva

1 archivo adjunto · Analizado por Gmail

cv_JulianaAlva_d...

MARRY CECY RABANAL SENMACHE <rsenmachemarry@crece.uss.edu.pe> jue, 17 nov 2022, 21:38
para Juliana

Muchas gracias ingeniería. Saludos cordiales.

Anexo 3.7. Evidencia de aceptación para evaluación de juicio de experto 3

Evaluación Experto del Diseño de un Modelo de Auditoría de TI para el Cumplimiento de Normas y Políticas de una Empresa Retail Peruana

Marry cecy Rabanal Senmache <rabanal.ingsistemas@gmail.com> 9:37 (hace 0 minutos)
para eliocv1486

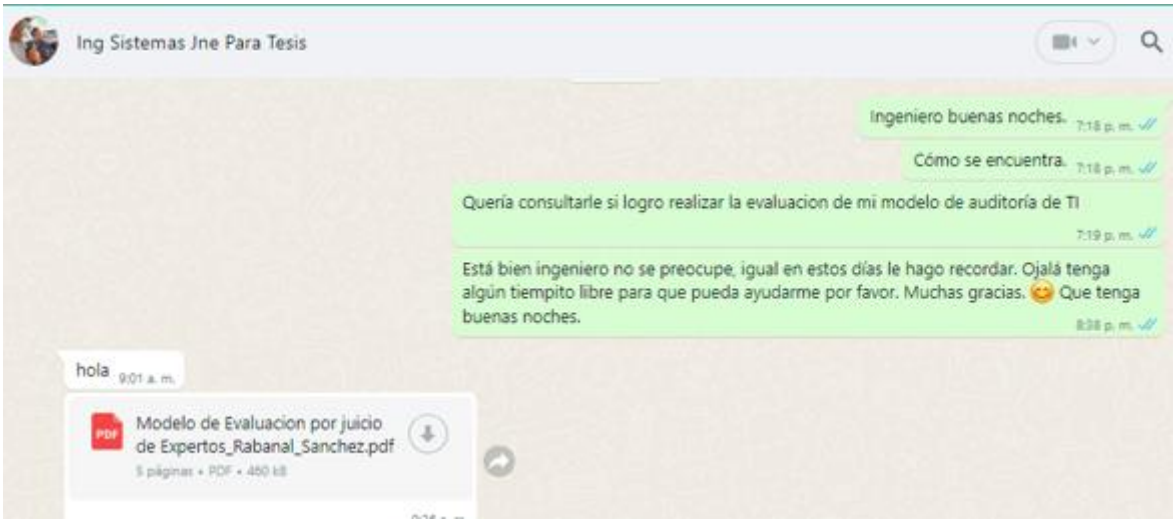
Estimado ingeniero **Elio Hely Campos Vasquez**, quien suscribe Marry Cecy Rabanal Senmache, previa a las coordinaciones, le estoy enviando mi modelo de auditoría de TI basado en un marco y en un estándar internacional para el cumplimiento de normas y políticas de una empresa retail peruana, para que pueda ser evaluado por juicio de experto, de acuerdo a los criterios que están establecidos en el documento.
Se solicita enviar su CV, para poder evidenciar su participación en la evaluación de juicio de experto.
Esperando su pronta respuesta, me despido.
Atentamente.
Marry Cecy Rabanal Senmache.
Sanchez Rubio Omar Alberto.

ADJUNTO.
-Modelo aprobado por asesor de tesis.
-Diseño para ser evaluado por juicio de experto.

2 archivos adjuntos · Analizado por Gmail

Modelo firmado p...

Modelo de Evalua...



Anexo 4. Consentimiento informado (Si la investigación se orienta a recopilar datos de personas).

Anexo 4.1 Curriculum de Experto 1

RÓMULO LOMPARTE
Tel. 472 6980 Cel. 999 638080
romulo.lomparte@yahoo.com

Licenciado en Computación y MBA. Líder en tecnologías de información con sólida y amplia experiencia para el sector comercial y financiero en dirección de proyectos de TI, auditoría, seguridad, ciberseguridad y consultoría en las mismas áreas. Habilidad para el desarrollo de talento, optimización de procesos, manejo de situaciones críticas con recursos limitados. Experiencia en uso de COSO, CobiT y procesos de Certificación Sarbanes-Oxley.

EXPERIENCIA LABORAL

ITG CONSULTING
Especializada en Auditoría, Seguridad, Ciberseguridad y Gobierno de TI

Gerente General *2013 – Actual*

SANNA
Red prestadora de servicio de salud

Sub Gerente de TI *2022– Actual*

RÓMULO LOMPARTE
Tel. 472 6980 Cel. 999 638080
romulo.lomparte@yahoo.com

Licenciado en Computación y MBA. Líder en tecnologías de información con sólida y amplia experiencia para el sector comercial y financiero en dirección de proyectos de TI, auditoría, seguridad, ciberseguridad y consultoría en las mismas áreas. Habilidad para el desarrollo de talento, optimización de procesos, manejo de situaciones críticas con recursos limitados. Experiencia en uso de COSO, CobiT y procesos de Certificación Sarbanes-Oxley.

EXPERIENCIA LABORAL

ITG CONSULTING

Especializada en Auditoría, Seguridad, Ciberseguridad y Gobierno de TI

Gerente General *2013 – Actual*

SANNA

Red prestadora de servicio de salud

Sub Gerente de TI *2022– Actual*

SUPRA NETWORKS

Consultora especializada en incrementar la productividad del negocio en organizaciones, aplicando eficazmente e integralmente las tecnologías de información.

Ingeniero Senior en Ciberseguridad *2019 – 2021*
Implementación y liderazgo de estrategias para la adecuada gestión de las políticas corporativas de ciberseguridad en organizaciones clientes.

JUEGOS PANAMERICANOS Y PARAPANAMERICANOS LIMA 2019

Segundo mayor evento multideportivo del mundo que congregará alrededor de 6700 deportistas, que participarán en 39 deportes y en 62 disciplinas panamericanas; y a más de 1890 para atletas, que participarán en 17 para deportes y 18 disciplinas parapanamericanas.

Responsable Ejecutivo de Comando, Coordinación y Comunicaciones (C3) *2018 – 2018*
Implementación de estrategias para el Sistema de Comando, Coordinación y Comunicación C3 en el Proyecto Especial y elaboración del plan operacional y de trabajo del área.

AVLA PERÚ

Compañía de seguros de cartas de fianza y pólizas de caución que inicia operaciones en el país con más de 1,300 millones de dólares en riesgo administrado y más de 10 mil clientes a nivel corporativo

Auditor General *2016 – 2018*
Planificaciòn estratégica de las evaluaciones de auditoría, cumplimiento regulatorio y colaboración en el refuerzo del gobierno corporativo.

GRUPO EPENSA

Compañía periodística multimedia con ventas anuales de 350 millones de soles y 900 colaboradores. 18 subsidiarias.

Gerente de TI *2011 - 2015*
Planificaciòn estratégica de TI para toda la corporación. Equipo de 35 personas. Reporte a Gerencia General.

- Implementación de la nueva solución core, optimizando e integrando los procesos periodísticos:
  - Optimización de cumplimiento de tiempo de cierres editoriales de 70% a 98%.
  - Reducción de pérdidas en Circulación por causa de retrasos, de 60,000 a 1,500 soles mensuales.
- Implementación de marco de Gobierno de TI, mejorando la atención de requerimientos de las unidades de negocio, optimizando el cumplimiento de sus necesidades de 45% a 100% anual.

- Mejora del nivel de servicio operativo bajo un esquema ITIL.
  - Incremento en el porcentaje de tickets atendidos de 63% a 96% mensual.
  - Mejora en la atención de porcentaje de incidentes de 65% a 100% mensual.
  - Aplicación de mejora continua en asesoría al usuario, generando reducción de número de tickets mensuales de 900 a 350 en el periodo de un año.

PACÍFICO SEGUROS

Compañía de seguros con ventas anuales de 550 millones de soles y 600 colaboradores.

Jefe de Auditoría de TI *2009 - 2011*

Evaluación de proyectos de sistemas, análisis de controles de TI y metodología ISO/IEC 27001. Reporte al Auditor General. 3 colaboradores.

- Optimización a través de implementación y administración de herramientas automatizadas con una mejora en el cumplimiento de los plazos del 60% al 90%. E incremento del número de evaluaciones en un 80%.
- Implementación de mecanismos de control de calidad, mejorando el cumplimiento de las actividades del nuevo modelo metodológico del 40% al 100%.
- Consultoría en el proyecto de Gobernabilidad de Tecnologías de Información a través de herramientas COBIT e ITIL., optimizando el alineamiento de proyectos a los objetivos estratégicos de 15% al 75% y mejora en la atención de% de tickets de solicitudes de 60% a 95% mensual.

ETEK INTERNATIONAL

Consultora en seguridad de TI con presencia en Latinoamérica, mejor integradora de la región. 4 colaboradores.

Consultor Senior de Seguridad TI *2008 - 2009*

Asesoramiento en gestión y evaluación de la seguridad de tecnologías de información basados en la Norma ISO 27001.

- Certificación de la Norma ISO 27001 en la mayor empresa de telecomunicaciones, primera empresa certificada con la norma en el país.

YANBAL INTERNATIONAL CORP.

Empresa trasnacional líder en venta directa de productos de belleza con ingresos anuales de USD 680 millones.

Auditor de Sistemas Corporativo *2007 - 2008*

Evaluación de los controles para de proyectos de sistemas y análisis de los controles de TI e ISO 17799.

- Optimización de las condiciones contractuales con los proveedores de TI, incrementando la rentabilidad en 2.5 millones de dólares.
- Aplicación preventiva de controles en las etapas de diseño de las soluciones de TI, reduciendo vulnerabilidades de seguridad de información de 26 a 3 mensuales y procesos de reprogramación de 8 a cero por mes.

BANCO DE CRÉDITO BCP

Banco líder del sistema con 9,000 colaboradores y presencia corporativa en Perú, USA, Panamá y Bolivia.

Supervisor del Servicio de Auditoría de Sistemas *1996 - 2007*

Evaluación de controles de proyectos de sistemas y procesos asociados a Sarbanes Oxley e ISO17799., de múltiples plataformas (Main Frame, Cliente/Servidor e Internet), supervisando 10 calificados profesionales.

- Detección y control anual de más de 350,000 ataques, debido a recomendaciones de seguridad y monitoreo de ataques a nivel corporativo, con sugerencias sobre configuraciones de firewalls e IDPs.
- Incremento del cumplimiento en 250% de servicios, después de la revisión contractual de outsoursing al Banco de Crédito de Bolivia.
- Diseño y elaboración del inventario y clasificación de riesgos para BCP Miami Agency, cumpliendo con estándares exigidos por la Reserva Federal de los Estados Unidos.

Auditor Senior 1997 - 2001
Auditor 1996 – 1997

ESTUDIOS

UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS, Magister en Dirección de Negocios, 2003
UNIVERSIDAD NACIONAL MAYOR DE SA MARCOS, Licenciado en Ciencias de la Computación, 1990

OTRAS ACTIVIDADES DE VOLUNTARIADO

- Consejo de Gobernabilidad de Tecnologías de Información (Illinois, USA) ISACA/ITGI, 2006- 2007.
- Presidente de la Asociación de Egresados de la Escuela de Postgrado de UPC, 2012 a la fecha.
- CGEIT Test Enhancement Subcommitee, 2014-2015.
- Expositor en Latin CACS, 2014.
- Expositor en CEIC – Las Vegas, 2015.
- Comité de Expertos sobre Cloud Computing – CSA, 2013 a la fecha.
- Government and Regulatory Advocacy Regional Subcommittee 2, 2010 a la fecha.
- Líder de la Comunidad de Entrega de Valor de TI – Val IT, 2012 a la fecha.
- Experto Revisor de la publicación Journal de Isaca, 2010 a la fecha.
- Decano del Colegio de Matemáticos, 2020 a la fecha
- Líder de Comunidad TI, PMI - Capítulo de Lima

MEMBRESIAS

Instituto de Auditores Internos – IIA, Instituto de Continuidad de Negocios – BCI, Instituto de Getsión de Proyectos - PMI

CURSOS Y TALLERES

Harvard University – Dirección de Negocios. Massachussetts Instiute of Technology (MIT) – OCW. IBM de México – Seguridad Perimetral. COSAPI DATA – Gerencia de Proyectos, 2014. Suite SAP.

CERTIFICACIONES

Project Management Professional PMP - Auditor Líder de Sistemas de Calidad Certificado – LAQMS – IATCA/IRCA. Information Security Foundation Based on ISO/IEC 27002 – EXIN. Risk Management Assurance – CRMA. Information Systems Auditor – CISA, Information Security Manager – CISM. Governance of Enterprise IT – CGEIT. Risk and Information Systems Control – CRISC. COBIT 5 Foundations, Certified Data Privacy Solutions Engineer – CDPSE, Remote Worker Professional Certificate – RWPC, Cybersecurity Professional – CSX, Coach Educativo en Neuropedagogia y Gestión del Talento, Scrum Foundation Professional Certificate - SFPC.

ACTIVIDAD DOCENTE

Profesor en tópicos de Gobierno de TI, Auditoria, Seguridad y Riesgos de TI, Ciberseguridad, Planeamiento Estratégico, BSC, Gestión de Proyectos, Mejora de Procesos, Gestión de Calidad, Protección de Datos, Antilavado de Activos, Prevención de Fraudes, Código de Ética, Dirección de Tesis, etc. en UNMSM, UPN, UPC, USAT, UTP, UPAO, BS Grupo, New Horizons, empresas públicas y privadas, etc. 2003 a las fecha.

IDIOMAS

Bilingüe Español-Inglés.

Anexo 4.2 Curriculum Vitae de Experto 2

ALVA ZAPATA, JULIANA DEL PILAR

Celular: 972678717 / Fijo: 074-215986
jalvaz@outlook.com / jalvaz.23@gmail.com

INFORMACION PERSONAL

- D.N.I.: 42900502
- Nacionalidad: Peruana
- Fecha de nacimiento: 23 de Febrero de 1985
- Estado Civil: Viuda
- RUC: 10429005022
- CCI-BCP: 002-30511755249107518
- CIP: 200951

PERFIL PROFESIONAL

Ingeniero en Computación e Informática, Maestro en gestión estratégica de Tecnologías de la Información. Con más de dos años de experiencia en docencia universitaria. Con más de nueve años de experiencia en el sector financiero en el área de sistemas, específicamente en; desarrollo de sistemas, gestión de proyectos, calidad de software, riesgos (crediticio y operacional, auditoria de Tecnologías de la Información y con certificaciones internacionales SFPC, CCI27001F y fundamentos en ciberseguridad.

GRADOS ACADEMICOS Y TITULOS PROFESIONALES

2003 - 2008 **UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO**
- **Titulado en Ingeniera en Computación e Informática.**

2015 - 2018 **UNIVERSIDAD SANTO TORIBIO DE MOGROVEJO**
- Maestría en Ingeniería de Sistemas y Computación con mención en Dirección Estratégica de TI.

EXPERIENCIA PROFESIONAL EN DOCENCIA

UTP – UNIVERSIDAD TECNOLÓGICA DEL PERU
Periodo: agosto 2021 – actualmente
Funciones: Docencia a tiempo parcial
Cursos:

- Algoritmos y estructuras
- Planeamiento estratégico de sistemas de información

ZEGEL IPAE
Periodo: mayo 2022 – Actualmente
Funciones: Docencia tiempo parcial
Cursos: Programación de base de datos

CIS USS – Centro de Informática y Sistemas (CIS) - USS
Periodo: noviembre 2021 – julio 2022
Funciones: Docencia tiempo parcial
Cursos: Computación 3 (tutor académico y virtual)

UNTRM – UNIVERSIDAD NACIONAL TORIBIO RODRIGUEZ DE MENDOZA
Periodo: 03/2020 – 03/2022
Resolución de consejo universitario N°130-2020 UNTRM/CU
Resolución de consejo universitario N°005-2021 UNTRM/CU
Cargo: docente a tiempo completo MINEDU
Funciones:

- Enseñanza de clases
- Asesoría de prácticas pre-profesionales y tesis de pregrado.
- Participación en eventos académicos
- Elaboración de artículos científicos
- Participación como jurado en prácticas pre-profesionales y tesis de pregrado.
- Participación en comisiones universitarias.

Cursos:

- Fundamentos de base de datos
- Ingeniería de software I y II
- Dinámica de sistemas
- Desarrollo de aplicaciones web II
- Aplicaciones en software libre II
- Pruebas de calidad de software

EXPERIENCIA PROFESIONAL

EDPYME ALTERNATIVA
Periodo: 07/2022 – Actualmente
Cargo: Oficial de cumplimiento
Área: Auditoria
Funciones:

- Evaluación de actividades de auditoría de TI
- Pruebas de controles
- Elaboración de informes de actividades
- Validación de data de provisiones y clasificación de créditos a través de software ACL
- Administración del sistema de información de auditoría.

EDPYME ALTERNATIVA
Periodo: 01/2022 – 06/2022
Cargo: Analista de Auditoria de TI
Área: Auditoria
Funciones:

- Evaluación de actividades de auditoría de TI
- Pruebas de controles
- Elaboración de informes de actividades
- Validación de data de provisiones y clasificación de créditos a través de software ACL
- Administración del sistema de información de auditoría.

CAJA SIPAN
Periodo: 05/2018 – 04/2019
Cargo: Analista de riesgos
Área: Riesgos
Funciones:

- Administración de base de datos de riesgos crediticio.
- Manejo de software de estadístico R Studio e IBM SPSS
- Elaboración de informes para comités de riesgos.
- Respuestas y levantamiento de observaciones de auditoria interna y externo sobre de riesgo operacional, seguridad de la información y continuidad del negocio.
- Apoyo en tareas de seguridad de información tales como: Las políticas y controles de seguridad en correspondencia con la evaluación de los procesos críticos para validar su cumplimiento o reporte de observaciones.

FINANCIERA EFECTIVA S.A.
Periodo: 04/2010 – 03/2018
Cargo: Analista de sistemas
Área: sistemas
Funciones:

- Analista de control de calidad de software; pruebas de estrés, control de versiones, seguimiento de indicadores.

- Apoyo a seguridad de la información; levantamiento de observaciones de la SBS, auditoria externa y auditoria interna. Revisión, cumplimiento de políticas y seguimiento a controles
- Analista de sistemas; desarrollo de software, manejo de base de datos, análisis funcional y gestión de proyectos

PRACTICAS PROFESIONAL

SUPERINTENDENCIA DE REGISTROS PÚBLICOS
Periodo: 02/2009 – 02/2010
Cargo: Prácticas Profesionales - Analista de la Información
Área: Archivo registral
Funciones:

- Proyecto de digitalización de Títulos y Planos Archivados.
- Asistencia y Manejo de sistemas registrales.
- Atención al usuario.

CERTIFICACIONES

Septiembre - 2022 **IGP – Innovación Gestión Buenas Prácticas**
- Curso de Certificación Oficial ISO/IEC 27001 Auditor Líder

Julio - 2022 **USACH – UNIVERSIDAD DE SANTIAGO DE CHILE**
- FUNDAMENTOS DE AUDITORIA A LA CIBERSEGURIDAD
  IDCQ: FLCLBWPJWS-SSGDQJRH-WHKNZZTDZQ

Marzo - 2021 **CERTIPROF**
- SCRUM FOUNDATION PROFESSIONAL CERTIFICAT (SFPC)
  IDCQ: 60446153

Junio - 2020 **CERTIPROF**
- ISO/IEC 27001/2013 FOUNDATION (I27001F)
  IDCQ: FLCLBWPJWS-SSGDQJRH-WHKNZZTDZQ

EXTENSION PROFESIONAL

03/2022 – 03/2022 **DEISTER SOFTWARE**
- **Base de datos IBM Informix.**

03/2019 – 05/2019 **UNIVERSIDAD SANTO TORIBIO DE MOGROVEJO**
- Diplomado en marketing digital

02/2012 – 12/2012 **CENTRO DE ENTRENAMIENTO EN TECNOLOGÍAS DE INFORMACIÓN**
- Especialista en el desarrollo de aplicaciones web con Java

11/2011 – 02/2012	**CENTRO DE ENTRENAMIENTO EN TECNOLOGÍAS DE INFORMACIÓN** ➢ Desarrollo de aplicaciones Visual Studio .NET y SQL Server 2008
05/2012 – 05/2012	**LAGERKVIST & PARTNERS** ➢ QlickView 10
01/2012 – 01/2012	**AB & AB** ➢ Genexus 10.1
11/2011 – 01/2012	**CENTRO DE ENTRENAMIENTO EN TECNOLOGÍAS DE INFORMACIÓN** ➢ Desarrollo de aplicaciones Visual Basic.NET y SQL Server 2008

IDIOMAS

01/2008 – 01/2009	**Centro de Idiomas de la Facultad De Ciencias Sociales y Educación "Pedro Ruiz Gallo"** ➢ Inglés - Nivel Intermedio (2009)

PARTICIPACION DE EVENTOS ACADEMICOS

PONENTE:

16 Junio 2022	**Centro de Informática y Sistemas (CIS) - USS** **"Seguridad en las aplicaciones de escritorio"**
14 Mayo 2022	**ISACA STUDENT GROUP – USS** **"gestión de riesgos de TI para financiera locales"**
28 Agosto 2021	**CENTRO DE PRODUCCION FISME - UNTRM** **"CURSO HERRAMIENTAS TIC PARA DOCENTES"**
28 Agosto 2021	**AUDIT AND CONTROL OF INFORMATION SISTEM SAC (AUDIT)** **"III CICLO DE CONFERENCIAS DE AUDITORIA Y CONTROL DE SISTEMAS DE INFORMACION"**
26 Marzo 2021	**UNIVERSIDAD TECNOLÓGICA DE MANZANILLO** **"SEMANA INTERNACIONAL DE LAS TECNOLOGÍAS DE LA INFORMACION (SITI) 2021"**
13 Julio 2020	**AUDIT AND CONTROL OF INFORMATION SISTEM SAC (AUDIT)** **"AUDITORIA DE SISTEMAS PARA FACTURACIÓN ELECTRÓNICA"**

Anexo 4.3 Curriculum de Jefe del Área de TI de la Empresa Conecta Retail S.A (Grupo EFE)

Hoja de Vida del Investigador Experto en Gestión de Proyectos de Software.

Jorge Andrés Cachay Arana

https://www.linkedin.com/in/jorge-andres-cachay-arana
979292836 / 962302075 - jcachay@hotmail.com; jcachay@yahoo.com

RESUMEN
Ingeniero de sistemas titulado de la Universidad Señor de Sipán de Chiclayo, egresado de MBA en la Universidad Pedro Ruiz Gallo de Chiclayo, con máss de 29 años en Jefatura de áreas de tecnología de la información en empresas líderes de los sectores reatil y Financiero. Gestión estratégica que contribuye directamente a los resultados del negocio, mejora de procesos y del servicio. Habilidad comprobada para interactuar con Proveedores, otras áreas del negocio. Formar, administrar y liderar equipos multidisciplinarios con foco en resolución de problemas del cliente.
Buena capacidad de análisis, comunicación efectiva, trabajo bajo presión, empatía con clientes, manejo de expectativas y situaciones complejas con orientación a resultados.

EXPERIENCIA LABORAL

ID	Cargo / Rol	Detalle
1	**Jefe de Sistemas Tiendas EFE**	Cargo ocupado durante los años 1993 al 2005. Interacción con las diferentes Gerencias Usuarias para la implementación de requerimientos de software: levantamiento de información, planificación y gestión de los mismos. Desarrollo de planes de prueba para control y calidad de los cambios implementados, liderando un equipo de 15 personas, logrando empatía con los clientes, constituyendo el nexo entre las diferentes áreas usuarias y el área de Sistemas.
2	**Jefe Corporativo de Desarrollo de Sistemas del Grupo EFE**	Cargo ocupado durante los años 2005 al 2021. Responsable de la gestión de requerimientos y sus implementaciones en las más de 200 tiendas de las 04 empresas del Grupo (Tiendas EFE, La Curacao, Motocorp y Financiera Efectiva), liderando equipo de hasta 20 personas, trabajando con equipos multidisciplinarios, tanto al interno del Grupo EFE como con proveedores. Participación activa en:

		Migración e implementación a nuevo sistema CORE de la Financiera. Migrar y centralizar el Sistema CORE del retail La Curacao (adquirida por el Grupo), al Sistema CORE de Tiendas EFE S.A. Integrar las 80 tiendas de La Curacao, al sistema CORE de la Financiera. Desarrollar y mantener operativos más de 15 sistemas del Grupo, tanto internos como Externos, así como integrarlos. Mejora continua en la metodología de Gestión de Proyectos de Sistemas, logrando optimizar la atención del servicio al cliente interno.
3	**Sub Gerente de Desarrollo de Sistemas**	Cargo ocupado durante los años 2022 hasta la actualidad. Participación activa en la migración al nuevo sistema Core del negocio Retail, así como en la migración e integración al nuevo sistema Core de la Financiera

ESTUDIOS Y CAPACITACIÓN

- INSTITUTO SUPERIOR TECNOLÓGICO "ELIAS AGUIRRE", CHICLAYO, Profesional *Técnico en Computación e Informática* (1987).
- UNIVERSIDAD PRIVADA SEÑOR DE SIPÁN – CHICLAYO, Ingeniero *de Sistemas (*2005, tercio superior).
- UNIVERSIDAD ESAN – SEDE CHICLAYO, Diplomado Internacional en Gerencia de Proyectos (2011, 5to superior).
- IPAE CHICLAYO, Diplomado en Finanzas (2013, tercio superior).
- UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO – LAMBAYEQUE, Maestría en Administración con mención en Gerencia Empresarial – (2015, Egresado, tercio superior)

Anexo 5.Evidencias de ejecución.

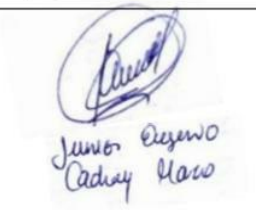
Anexo 5.1. Bitácora de documentos seleccionados y ficha de criterios de evaluación

Documentos Oficiales	Título del documento	Cant. Documentos
COBIT 2019	COBIT-2019-Framework-Introduction-and-Methodology_res_Spa_019	8
	COBIT-2019-Framework-Introduction-and-Management-Objectives _res_Spa_0519	
	COBIT 2019 Framework: Governance and Management Objectives	
	COBIT 2019 is a terrific resource for a wide range of business technology professional.	
	COBIT 5: Implementación	
	COBIT Focus Area: Information Security	
	ISACA developed this audit program as a companion to COBIT Focus: DevOps, Using COBIT 2019	
NIST	Implementing the NIST Cybersecurity Framework Using COBIT 2019	3
	Cybersecurity: Based on the NIST Cybersecurity Framework Audit Program	
	Connecting COBIT 2019 to the NIST Cybersecurity Framework	
ISO 19011	NORMA ISO 19011:2018 Directrices para la Auditoria de Sistemas de Gestión	2
	Norma Internacional ISO 19011	
ITIL	Gestión de servicios de TI basado en ITIL	3
	Using ITIL 4 and COBIT 2019 to create an Integrated I&T Framework Environment	
	COBIT 5 and ITIL Adaptation at a Saudi Municipality	
RISK	COBIT 5 Ford Risk	5
	Risk IT Framework	
	Risk IT Framework, 2nd Edition	
	Risk IT Practitioner Guide, 2nd Edition	
	Risk Scenarios Starter Pack | Digital	
TOTAL		21

Ficha de Criterios de Evaluación

CRITERIOS	Muy malo	Regular	Muy bueno
Dirigido	El marco, norma o estándar es dirigido para grandes empresas (1 punto)	El marco, norma o estándar es dirigido para pequeñas empresas (2.5 puntos)	El marco, norma o estándar es dirigido para pequeñas y medianas empresas (5 puntos)
Orientado	Orientado para control de gestión de riesgos y/o prácticas de seguridad de la información (1 punto)	Orientado a buscar prácticas en la gestión de conducta de mercado y/o buenas prácticas para la gestión de los sistemas de información (2.5 puntos)	Orientado para buenas prácticas en auditorías de a TI y/0 SGSI (5 puntos)
Constituido	Gobierno, riesgo y cumplimiento y/o framework, core y niveles de implementación (1 punto)	Etapas del ciclo de mejora continua y/o la ley N°26702 (2.5 puntos)	Objetivos de gobierno, gestión y/o directrices para las auditorías de los Sistemas de Información (5 puntos)
Finalidad	Cumplimiento regulatorio, controlar costes y revelar datos (1 punto)	Gestionar los riesgos de ciberseguridad y/o analizar y gestionar la seguridad de los SI (2.5 puntos)	Para relacionar las metas empresariales con las metas de TI y/o realizar auditoría eficaz en la gestión de los SI (5 puntos)

Fuente: Elaboración propia



Anexo 5.2. Ficha de resultados validada mediante declaración jurada

"AÑO DEL FORTALECIMIENTO DE LA SOBERANÍA NACIONAL"

DECLARACIÓN JURADA

Yo, Mg.Ing. JUNIOR EUGENIO CACHAY MACO identificado con DNI 44404838, domiciliado(a) en Calle Los Filántropos 188 - Urb. Latina - JLO

Departamento de Lambayeque, Provincia de Chiclayo y Distrito de Chiclayo.

DECLARO BAJO JURAMENTO lo siguiente:

Los tesistas, RABANAL SENMACHE MARRY CECY y SÁNCHEZ RUBIO OMAR ALBERTO, estudiantes de la carrera de Ingeniería de Sistemas en la Universidad Señor de Sipán, Lambayeque – Chiclayo, que están desarrollando su tesis que lleva por nombre "Diseño de un modelo de auditoría de TI para el cumplimiento de normas y estándares de una empresa retail peruana", han aplicado instrumentos que han sido validados por juicio de experto, para la ejecucion de la auditoría de TI, así mismo se ha validado el cuadro comparativo y criterios de selección de normas y estándares aplicados a auditorias de TI.

Manifiesto que lo mencionado corresponde a la verdad de hechos y tengo conocimiento que si lo declarado es falso me sujeto a los alcances de lo establecido en el Art. 438° del Código Penal, para aquellos que cometan falsedad, simulando o alterando la verdad intencionalmente.

FIRMA _____

NOMBRES Y APELLIDOS: Junior Eugenio Cachay Maco

FECHA: 14-12-22

DNI: 44404838

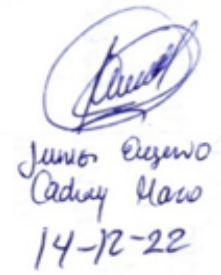
HUELLA DACTILAR

Cuadro comparativo de marcos y estándares

Item	ITIL	COBIT 2019	ISO 19011	NIST	ISO 27001	RISK IT
Dirigido a	Empresas pequeñas, medianas y grandes	Empresas Grandes, medianas y pequeñas	Empresas pequeñas, medianas y grandes	Empresas medianas y grandes	Empresas pequeñas, medianas y grandes	Empresas medianas y grandes
Orientado a	Buenas prácticas en el beneficio a los servicios de TI	Aplicar buenas prácticas en los recursos de TI	Auditoria a los sistemas de gestión organizacional	Orientado al análisis de los riesgos empresariales	Requisitos que establecen la documentación y evaluación de SGS en las organizaciones	Buenas practicas aplicadas a la gestión de riesgos
Constituido por	Compuesto por Ciclo de vida del servicio	Objetivos de gobierno, gestión y cumplimiento. Compuesto por proceso de control organizacional.	Compuesto en principios, gestión en competencia y evaluación de auditores	Compuestos por elementos, eventos y procesos	Compuesto por cláusulas y controles de los SI	Está constituido por áreas para el control interno
Finalidad	Evaluación de calidad de prestación regular	Cumplimiento de metas organizacionales	Finalidad de una planeación y realización de las auditorías.	Proporcionar principios básicos y requisitos para la protección de la información.	Tiene la final de definir los controles ineludibles para garantizar la integridad y disponibilidad de la información	Mide el grado de riesgos de las empresas

	ITIL	**COBIT 2019**	NIST	**ISO 19011**	ISO 27001	RISK IT
DIRIGIDO	5	5	5	5	5	1
ORIENTADO	1	5	2,5	5	5	2,5
CONSTITUIDO	2,5	5	2,5	5	5	5
FINALIDAD	2,5	5	2,5	5	2,5	2,5
PROMEDIO	2,8	5	3,1	5	4,4	2,8

Fuente: Elaboración propia.



Anexo 5.2.1. Criterios de evaluación de normas y marcos

CRITERIOS	Muy malo	Regular	Muy bueno
Dirigido	El marco, norma o estándar es dirigido para grandes empresas (1 punto)	El marco, norma o estándar es dirigido para pequeñas empresas (2.5 puntos)	El marco, norma o estándar es dirigido para pequeñas y medianas empresas (5 puntos)
Orientado	Orientado para control de gestión de riesgos y/o prácticas de seguridad de la información (1 punto)	Orientado a buscar prácticas en la gestión de conducta de mercado y/o buenas prácticas para la gestión de los sistemas de información (2.5 puntos)	Orientado para buenas prácticas en auditorías de a TI y/0 SGSI (5 puntos)
Constituido	Gobierno, riesgo y cumplimiento y/o framework, core y niveles de implementación (1 punto)	Etapas del ciclo de mejora continua y/o la ley N°26702 (2.5 puntos)	Objetivos de gobierno, gestión y/o directrices para las auditorías de los Sistemas de Información (5 puntos)
Finalidad	Cumplimiento regulatorio, controlar costes y revelar datos (1 punto)	Gestionar los riesgos de ciberseguridad y/o analizar y gestionar la seguridad de los SI (2.5 puntos)	Para relacionar las metas empresariales con las metas de TI y/o realizar auditoría eficaz en la gestión de los SI (5 puntos)

Fuente: Elaboración propia

Anexo 5.3. Bitácora de tiempo de ejecución del modelo de Auditoria.

	Tesistas	fecha	hora de inicio	Hora de fin	Actividad	Horas día	Total
FASE DE PLANIFICACION FASE 1	Marry - Omar	3 y 4 - Oct	8:00	13:00	Desarrollo de los objetivos y el alcance de auditoría de TI	5:00	10
		5-Oct	8:00	9:00	Reunión de presentación de objetivos	1:00	1
		5-Oct	9:30	10:30	Reunión de presentación del alcance de auditoria de TI	1:00	1
		6-Oct	10:30	12:30	Selección y presentación del equipo auditor	2:00	2
		7-Oct	8:00	13:00	Reunión con equipo auditor y representantes de la empresa para firmar acta de principio de confidencialidad para el acceso a la información.	5:00	5
		9-Otc	8:00	13:00	Reunión con equipo auditor y representantes de la empresa para establecer las pautas de la auditoria.	5:00	5
					TOTAL DE HORAS FASE DE PLANIFICACION		**24**
FASE DE EJECUCION FASE 2	Marry - Omar	10-Oct	8:00	5:00	Evaluación de la gestión de los procesos del área de TI de la empresa. (Verificar si existen controles de acceso al sistema, datos y programas)	8:00	8
		11-Oct	8:00	5:00	Evaluación de la gestión de los proyectos de software del área de TI de la empresa (Verificar si se gestionan los riesgos en los proyectos)	8:00	8
		12-Oct	8:00	5:00	Evaluación de la gestión de los recursos de del área de TI de la empresa (Verificar si se tiene el personal idóneo para el cumplimiento de funciones de manera eficiente)	8:00	8
		13-Oct	8:00	5:00	Evaluación de la gestión del aseguramiento del área de TI de la empresa (Verificar si la empresa cuenta con actividades de planificación, iniciativas de aseguramiento, para alcanzar objetivos)	8:00	8
		14-Oct	8:00	5:00	Evaluación de la gestión del sistema de control del área de TI de la empresa (Verificar si existen roles establecidos para el monitoreo y seguimiento de los controles internos)	8:00	8
					TOTAL DE HORAS FASE DE EJECUCION		**40**
FASE DE VERIFICACION FASE 3	Marry - Omar	16 y 17-Oct	08:00	5:00	Elaboración de matriz de hallazgos y observaciones de la auditoria de TI.	8:00	16
		18-Oct	8:00	5:00	Elaboración del Informe de Auditoria	8:00	8
		19-Oct	8:00	13:00	Presentación de Hallazgos y observaciones	5:00	5
		20-Oct	8:00	13:00	Remisión de Informe de Auditoria	5:00	5
		21-Oct	8:00	13:00	Verificación de la revisión del informe de auditoría por parte del auditado.	5:00	5
		23-Oct	8:00	13:00	Elaboración de la matriz de satisfacción	5:00	5
		24-Oct	8:00	13:00	Presentación y llenado de la matriz de satisfacción, para medir el nivel de aceptación de la auditoria por la empresa auditada.	5:00	5
					TOTAL DE HORAS FASE DE VERIFICACION		**49**
FASE DE SEGUIMIENTO Y MEJORA FASE 4	Marry - Omar	25-Oct	08:00	5:00	Elaboración de actividades de seguimiento	8:00	8
		8-Nov	08:00	5:00	Verificación de acciones correctivas	8:00	8
					TOTAL HORAS FASE DE SEGUIMIENTO Y MEJORA		**16**
TOTAL HORAS DE TIEMPO DE EJECUCION DEL MODELO EN LA EMPRESA CONECTA RETAIL S.A							**129**

Fuente: Elaboración propia

Anexo 5.4. Ficha para selección de objetivos de gestión y gobierno de COBIT 2019, aplicando Ingeniería Inversa

Elaboración de la matriz "Metas de negocio KONECTA RETAIL S.A vs Metas Empresariales COBIT 2019

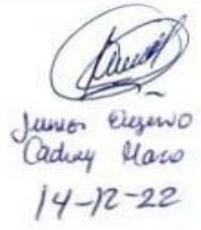
METAS DE CONECTA RETAIL S.A	METAS EMPRESARIALES COBIT 2019
M1. Concientizar a todo el personal, para que cada trabajador sea consciente de la importancia de sus actividades y rol en la protección de la información de la Institución.	APO07
M2.Poder revisar periódicamente los controles y procedimientos de cada uno de los procesos de la empresa de manera proactiva.	DSS06
M3. Mantener registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.	MEA04
M4. Contar con controles y procedimientos que permiten reducir, eliminar o evitar (mitigar) los riesgos identificados.	MEA02
M5. Contar con un conjunto de políticas para una adecuada administración de los riesgos basados en los proyectos de software en el área de TI.	BAI11

Matriz de "Resultado de análisis del cuadro de relacionamiento de metas empresariales y metas de alineamiento"

METAS DE CONECTA RETAIL S.A	METAS ALINEAMIENTO COBIT 2019	METAS EMPRESARIALES COBIT 2019
M1. Concientizar a todo el personal, para que cada trabajador sea consciente de la importancia de sus actividades y rol en la protección de la información de la Institución.	AG12	APO07
M2. Poder revisar periódicamente los controles y procedimientos de cada uno de los procesos de la empresa de manera proactiva.	AG09	DSS06
M3. Mantener registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.	AG11	MEA04
M4. Contar con controles y procedimientos que permiten reducir, eliminar o evitar (mitigar) los riesgos identificados.	AG07	MEA02
M5. Contar con un conjunto de políticas para una adecuada administración de los riesgos basados en los proyectos de software en el área de TI.	AG11	BAI11

Matriz de "Resultado de análisis del cuadro de relacionamiento de objetivos de gobierno y gestión con metas de alineamiento"

OBJETIVOS DE GOBIERNO Y GESTION	METAS DE ALINEAMIENTO COBIT 2019	METAS DE CONECTA RETAIL S.A
APO07	AG12	M1. Concientizar a todo el personal, para que cada trabajador sea consciente de la importancia de sus actividades y rol en la protección de la información de la Institución.
DSS06	AG09	M2. Poder revisar periódicamente los controles y procedimientos de cada uno de los procesos de la empresa de manera proactiva.
MEA04	AG11	M3. Mantener registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.
MEA02	AG07	M4. Contar con controles y procedimientos que permiten reducir, eliminar o evitar (mitigar) los riesgos identificados.
BAI11	AG11	M5. Contar con un conjunto de políticas para una adecuada administración de los riesgos basados en los proyectos de software en el área de TI.



Anexo. 5.4.1. Criterios de selección de los objetivos de gestión COBIT 2019

CRITERIOS	Muy malo	Regular	Excelente
Dominios dirigidos al control interno	Dominios dirigidos para dar servicio y soporte (1 punto)	Dominios dirigidos para el alineamiento y organización de servicios (2 puntos)	Dominios dirigidos para la gestión del control interno (4 puntos)
Dominios para realizar autoevaluaciones de control interno	Dominio para la gestión de información y tecnología (1 punto)	Dominio para gestionar e identificar construcción de soluciones de TI y gestionar controles de proceso de negocio (2 puntos)	Proceso para autoevaluaciones de control y proceso para la implementación de prácticas en auditorías de TI y/0 SGSI (4 puntos)
Dominios para el seguimiento y monitoreo del control interno	Domino para gestionar la aceptación y cambios de TI (1 punto)	Dominio para gestionar problemas de TI (2 puntos)	Dominio para la supervisión de control interno y proceso (4 puntos)

Fuente: Elaboración propia

Anexo. 5.4.2. Criterio de evaluación del objetivo de gestión MEA de COBIT 2019

CRITERIOS	Muy malo	Regular	Muy bueno
Metas empresariales	Brindar calidad de información financiera (1 punto)	Cumplimiento de IT y soporte al cumplimiento de negocio (2 puntos)	Cumplimiento de leyes y regulaciones externas (4 puntos)
Orientado	Recopilar y evaluar las metas y métricas de alineamiento de la empresa y/o Planificar y ejecutar iniciativas de aseguramiento para cumplir con requisitos internos (1 punto)	Asegurar que los requisitos sean identificados y cumplidos (2 puntos)	Supervisar y evaluar continuamente el entorno de control incluyendo evaluaciones y auto concienciación (4 puntos)
Finalidad	Proporcionar transparencia en el rendimiento y la conformidad y/o facilitar a la organización el diseño y desarrollo de iniciativas (1 punto)	Asegurarse de que la empresa cumpla con todos los requisitos externos (2 puntos)	Dar información transparente a las partes interesadas (4 puntos)

Fuente: Elaboración propia

Anexo. 5.4.3. Objetivos de gobierno de COBIT 2019 seleccionados

11 OBJETIVOS DE GESTIÓN	6 OBJETIVOS DE GESTIÓN	14 OBJETIVOS DE GESTION	4 OBJETIVOS DE GESTIÓN
DOMINIO CONSTRUIR ADQUIRIR E IMPLEMENTAR	**DOMINIO ENTREGAR DAR SERVICIO Y SOPORTE**	**DOMINIO ALINEAR, PLANEAR Y ORGANIZAR**	**DOMINIO MONITOREAR EVALUAR Y VALORAR**
BAI01: Gestionar los programas.	**DSS01:** Gestionar las operaciones.	**APO01:** Marco de gestión de TI Gestionado.	**MEA01:** Gestionar el monitoreo del rendimiento y la conformidad.
BAI02: Gestionar la definición de requerimientos.	**DSS02:** Gestionar las peticiones y los incidentes del servicio.	**APO02:** Estrategia gestionada.	**MEA02:** Gestionar el sistema de control interno.
BAI03: Gestionar la identificación y construcción de soluciones.	**DSS03:** Gestionar los problemas.	**APO03:** Arquitectura empresarial gestionada.	**MEA03:** Gestionar el cumplimiento de los requerimientos externos.
BAI04: Gestionar la disponibilidad y la capacidad.	**DSS04:** Gestionar la continuidad.	**APO04:** Innovación gestionada.	**MEA04:** Gestionar el aseguramiento.
BAI05: Gestionar los cambios organizativos.	**DSS05:** Gestionar los servicios de seguridad.	**APO05:** Portafolio administrado.	
BAI06: Gestionar los cambios de TI.	**DSS06:** Gestionar los controles de los procesos de negocio.	**APO06:** Manejo de presupuesto y costos.	
BAI07: Gestionar la aceptación y la transición de los cambios de TI.		**APO07:** Recursos Humanos administrados.	
BAI08: Gestionar el conocimiento.		**APO08:** Relaciones administradas.	
BAI09: Gestionar los activos.		**APO09:** Contratos de servicios gestionados.	
BAI10: Gestionar la configuración.		**APO10:** Proveedores Gestionados.	
BAI11: Gestionar los proyectos.		**ºAPO11:** Calidad gestionada.	
		APO12: Riesgo gestionado.	
		APO13: Seguridad administrada.	
		APO14: Datos administrados.	

Anexo 5.5. Ficha resumen de evaluación del modelo por expertos en auditoría de TI

Fases	Actividad	Criterios Evaluador 1					Criterios Evaluador 2					Criterios Evaluador 3				
		Claridad	Objetividad	Suficiencia	Coherencia	Pertinencia	Claridad	Objetividad	Suficiencia	Coherencia	Pertinencia	Claridad	Objetividad	Suficiencia	Coherencia	Pertinencia
FASE 1 DIAGNÓSTICO Y PLANIFICACIÓN.	A1-Diagnóstico para conocer el estado actual de cumplimiento de la empresa.	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	A2-Identificacion de incumplimiento de políticas y normas en los servicios de TI	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	A3-Cronograma de tiempo de ejecución de la auditoría de TI	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	A4- Selección de Normas, marcos y estándares según diagnóstico	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
FASE 02 IMPLEMENTACIÓN	A5- Diseño de modelo de auditoría de TI	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	A6- Ejecución de las actividades de auditoría de TI.	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
FASE 3 EVALUACIÓN DE AUDITORÍA DE TI	A7- Evaluación de resultados	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4
	A8 - Informe de Auditoría	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
FASE 4 REVISIÓN Y SEGUIMIENTO	A9- Revisión y seguimiento de cumplimiento objetivos	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	A10- Seguimiento de verificación de acciones correctivas.	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
TOTAL CRITERIO		3.93					4					4				
TOTAL MODELO		3.98														

Anexo 5.6 Bitácora de recolección de información enfocada en las políticas del área de TI de la empresa CONECTA RETAIL S.A.

CONECTA RETAIL S.A. efe la curacao	FORMATO DE BITACORA DE RECOPILACIÓN Y VERIFICACIÓN DE INFORMACIÓN ISO 19011 (Claúsula 6.4.7)	Responsable de creación: Rabanal Senmache Marry Cecy Responsable de actualización: Sánchez Rubio Omar Alberto	**Versión: N°01**
		FECHA DE CREACIÓN : 01-10-2023 FECHA DE ACTUALIZACIÓN: 01-03-2024	

BITÁCORA DE RECOPILACIÓN DE INFORMACIÓN

Código del documento	Nombre Documento	Descripción	Versión	Fecha de creación archivo	Elaborado	Fecha de actualización	Modificaciones	Observaciones
MPRO.2011.SIST.001.01	MPRO de conexión de terceros a la red de efectiva	Documento, registros de evidencias sobre políticas y responsabilidades, que dictan las pautas sobre las cuales se deben regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A.C, vinculadas con el manual de procedimientos de conexión de terceros.	1	08/06/2011	**Jefe de comunicaciones y soporte**	x	**Versión inicial**	x
MPRO.2011.SIST.001.02	MPRO de conexión de terceros a la red de efectiva	Documento, registros de evidencias sobre políticas y responsabilidades, que dictan las pautas sobre las cuales se deben regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A.C, vinculadas con el manual de procedimientos de conexión de terceros.	2	08/06/2011	Área de ingeniería de procesos	25/10/2013	Actualización de políticas relacionadas y formato de documento	La frecuencia de uso del documento es por demanda (cada vez que sea solicitado)
MPP.2012.RIES.005.01	MPP de continuidad del negocio	Documento, registros de evidencias sobre metodología, políticas y procedimientos que permitan implementar una adecuada Gestión de la continuidad del negocio según la realidad de la empresa CONECTA RETAIL S.A.C	1	27/10/2012	Área de ingeniería de procesos	x	Versión inicial	x
MPP.2012.RIES.005.02	MPP de continuidad del negocio	Documento, registros de evidencias sobre metodología, políticas y procedimientos que permitan implementar una adecuada Gestión de la continuidad del negocio según la realidad de la empresa CONECTA RETAIL S.A.C	2	27/10/2012	Área de ingeniería de procesos	19/03/2013	Adecuaciones *Capitulo 4, por circular G 164 - 2012. *Capitulo 2 y 5 Metodología de la continuidad del negocio, inclusión de la evaluación de riesgos de continuidad.	El documento es de aplicación de instancias organizas previstas en el manual de organización y funciones de la empresa.

MPP.2012.RIES.005.03	MPP de continuidad del negocio	Documento, registros de evidencias sobre metodología, políticas y procedimientos que permitan implementar una adecuada Gestión de la continuidad del negocio según la realidad de la empresa CONECTA RETAIL S.A.C	3	27/10/2012	Área de ingeniería de procesos	28/08/2013	Actualización *Capitulo II, Responsabilidades. Incorporación de funciones de los coordinadores en la continuidad del negocio. *Capitulo II Políticas: Actualización del análisis de impacto del negocio.	x
MPP.2012.RIES.005.04	MPP de continuidad del negocio	Documento, registros de evidencias sobre metodología, políticas y procedimientos que permitan implementar una adecuada Gestión de la continuidad del negocio según la realidad de la empresa CONECTA RETAIL S.A	4	27/10/2012	Area de ingeniería de procesos / Riesgo Operacional	01/10/2014	Actualización *Capitulo 1: Objetivo y alcance. *Capitulo 2: Metodología de la gestión de continuidad del negocio y metodologías del análisis de impacto del negocio. *Capitulo 4: Diseño de flujo del proceso. *Capitulo 5: Incorporación de los anexos. **Plan de gestión de crisis. **Plan de recuperación de los servicios de tecnología. **Plan de continuidad operativa **Plan de emergencia.	Los temas no comprendidos o cualquier punto no considerado en el manual, debe ser motivo de análisis, por parte del área de ingeniería de procesos.
MPP.2013.SIST.003.01	MPP de Desarrollo de Software	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A., vinculando con el desarrollo de software.	1	30/01/2013	Area de ingeniería de procesos	x	x	x
MPP.2012.RIES.003.01	MPP de seguridad de la información	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A.C, vinculando con la gestión de Seguridad de la Información.	1	22/10/2012	Area de ingeniería de procesos / Riesgo Operacional	22/10/2012	Versión inicial	x
MPP.2012.RIES.003.02	MPP de seguridad de la información	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A.C, vinculando con la gestión de Seguridad de la Información.	2	22/10/2012	Area de ingeniería de procesos / Riesgo Operacional	31/07/2013	Actualización *Capitulo II, Responsabilidades. Incorporación de funciones de los coordinadores en la seguridad de la información.	El presente manual se enmarca dentro de las políticas y procedimientos generales establecidos en circular N°140-2009 Gestión de seguridad de la información.
MPP.2012.RIES.003.02	MPP de seguridad de la información	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A.C, vinculando con la gestión de Seguridad de la Información.	3	22/10/2012	Area de ingeniería de procesos / Riesgo Operacional	01/09/2014	Actualización *Capitulo II - Políticas (PO-012): Incorporación de propietarios y custodios de los activos de la información y de los criterios para la clasificación de la confidencialidad. *Clasificación II - Políticas (PO-024) Reclasificación de políticas del numeral 2.10 a PO-025 y PO-026. *Capitulo IV - Actualización del proceso.	El presente manual se enmarca dentro de las políticas y procedimientos generales establecidos en el reglamento de gestión de riesgos resolución SBS 37-2008.
MPP.2012.RIES.003.04	MPP de seguridad de la información	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A.C, vinculando con la gestión de Seguridad de la Información.	4	22/10/2012	Area de ingeniería de procesos / Riesgo Operacional	01/11/2014	Actualización *2.3.1. Política de seguridad de cuentas de usuario (PO-001), numeral 2.3.1.3 y 2.3.1.6 *2.4.1 Política de uso de computadores personales (PO-004), numeral 2.4.1.6. *2.4.2 Política de uso de computadores personales (PO-005), numeral 2.4.2.2. *2.9.1. Políticas de respaldos (PO-022), numeral 2.9.1.1.	El presente manual se enmarca dentro de las políticas y procedimientos generales establecidos LA Ley N°29733 - Ley de protección de datos personales.
MP.GP	MP de Gestión de proyectos de software	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades para la gestión de la empresa, que dictan las pautas sobre las cuales regir las actividades vinculadas con el proceso de gestión de proyectos de la empresa CONECTA RETAIL S.A.C	1	2011	Area de gestión de proyectos de software	x	Versión inicial	El proceso de gestión de proyectos de software debe ajustarse a lo establecido en el documento, debiendo tener en cuenta las consideraciones establecidas en el MPP de gestión normativa.

CONECTA RETAIL S.A. efe la curacao	FORMATO DE LA EMPRESA CONECTA RETAIL S.A.C VERIFICACIÓN DE SEGURIDAD DE ACTIVOS DE TI COBIT 2019 - DSS06 Métrica - (Número de activos críticos)	Revisado por: JORGE CACHAY ARANA Aprobado por: JORGE CACHAY ARANA	**Versión: N°01**
		FECHA CREACIÓN : 15/11/2022	FECHA DE ACTUALIZACIÓN: 11/10/2023

MATRIZ DE VERIFICACIÓN DE SEGURIDAD DE ACTIVOS DE TI

Nombre del activo	Descripción del activo	Tipo de activo	Nivel de confidencialidad	Tipo de ubicación del activo	Propiedad del activo	VALORIZACIÓN DE CRITICIDA DE ACTIVOS					
						Confidencialidad	Integridad	Disponibilidad	Valor	Nivel de Tasación	Total de activos críticos
MPRO de conexión de terceros a la red de efectiva	Documento, registros de evidencias sobre políticas y responsabilidades, que dictan las pautas sobre las cuales se deben regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A, vinculadas con el manual de procedimientos de conexión de terceros.	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A	LOGICO, FISICO	**Área de comunicaciones y soporte**	1	3	2	2	Bajo	
MPRO de conexión de terceros a la red de efectiva	Documento, registros de evidencias sobre políticas y responsabilidades, que dictan las pautas sobre las cuales se deben regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A.C, vinculadas con el manual de procedimientos de conexión de terceros.	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A.C	LOGICO, FISICO	Área de ingeniería de procesos	1	3	2	2	Bajo	
MPP de continuidad del negocio	Documento, registros de evidencias sobre metodología, políticas y procedimientos que permitan implementar una adecuada Gestión de la continuidad del negocio según la realidad de la empresa CONECTA RETAIL S.A.C	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A	LOGICO, FISICO	Área de ingeniería de procesos	1	3	2	2	Bajo	
MPP de continuidad del negocio	Documento, registros de evidencias sobre metodología, políticas y procedimientos que permitan implementar una adecuada Gestión de la continuidad del negocio según la realidad de la empresa CONECTA RETAIL S.A.C	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A	LOGICO, FISICO	Área de ingeniería de procesos	1	3	2	2	Bajo	

MPP de continuidad del negocio	Documento, registros de evidencias sobre metodología, políticas y procedimientos que permitan implementar una adecuada Gestión de la continuidad del negocio según la realidad de la empresa CONECTA RETAIL S.A.C	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A	LOGICO, FISICO	Área de ingeniería de procesos	1	3	2	2	Bajo	
MPP de continuidad del negocio	Documento, registros de evidencias sobre metodología, políticas y procedimientos que permitan implementar una adecuada Gestión de la continuidad del negocio según la realidad de la empresa CONECTA RETAIL S.A.C	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A	LOGICO, FISICO	Área de ingeniería de procesos / Riesgo Operacional	1	3	2	2	Bajo	
MPP de Desarrollo de Software	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A.C, vinculando con el desarrollo de software.	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A	LOGICO, FISICO	Área de ingeniería de procesos	1	3	2	2	Bajo	
MPP de seguridad de la información	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A.C, vinculando con la gestión de Seguridad de la Información.	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A.C	LOGICO, FISICO	Área de ingeniería de procesos / Riesgo Operacional	1	3	2	2	Bajo	
MPP de seguridad de la información	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A, vinculando con la gestión de Seguridad de la Información.	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A.C	LOGICO, FISICO	Area de ingeniería de procesos / Riesgo Operacional	1	3	2	2	Bajo	
MPP de seguridad de la información	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A, vinculando con la gestión de Seguridad de la Información.	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A.C	LOGICO, FISICO	Area de ingeniería de procesos / Riesgo Operacional	1	3	2	2	Bajo	

MPP de seguridad de la información	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A, vinculando con la gestión de Seguridad de la Información.	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A	LOGICO, FISICO	Area de ingeniería de procesos / Riesgo Operacional	1	3	2	2	Bajo	
MPP de seguridad de la información	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades, que dicten las pautas sobre las cuales, se debe regir las actividades realizadas por todas las instancias de la empresa CONECTA RETAIL S.A, vinculando con la gestión de Seguridad de la Información.	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A	LOGICO, FISICO	Area de ingeniería de procesos / Riesgo Operacional	1	3	2	2	Bajo	
MP de Gestión de proyectos de software	Documento, registros de evidencias sobre políticas, procedimientos y responsabilidades para la gestión de la empresa, que dictan las pautas sobre las cuales regir las actividades vinculadas con el proceso de gestión de proyectos de la empresa CONECTA RETAIL S.A	Físico/Electrónico	Confidencial de la empresa CONECTA RETAIL S.A	LOGICO, FISICO	Area de gestión de proyectos de software	1	3	2	2	Bajo	

PUNTUACION DE CRITERIOS			
VALOR DEL ACTIVO	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**
MUY ALTO (5)	La información asociada al activo es solo accedida por el personal de alto rango	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 0% pues su perdida afectaría de forma irreversiblemente a la empresa CONECTA RETAIL S.A	Se requiere que el activo nunca se encuentre disponible, pues su carencia afectaría irreversiblemente a la empresa CONECTA RETAIL S.A
ALTO (4)	La información asociada al activo es restringida y solo personal de un proyecto específico puede acceder a ella	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 15% pues su perdida afectaría gravemente a la empresa CONECTA RETAIL S.A	Se considera que el activo puede estar disponible por al menos una hora, porque su carencia afectaría gravemente a la empresa CONECTA RETAIL S.A
MEDIO (3)	La información es confidencial y solo puede acceder personal de áreas internas	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 50% pues su perdida afectaría de manera considerable a la empresa CONECTA RETAIL S.A	Se considera que el activo puede estar disponible un día, porque su carencia afectaría considerablemente a la empresa CONECTA RETAIL S.A
BAJO (2)	La información es de uso interno y solo personal de la empresa CONECTA RETAIL puede acceder a ella.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 85% pues su perdida afectaría parcialmente a la empresa CONECTA RETAIL S.A	Se considera que el activo puede estar disponible por al menos una hora, porque su carencia afectaría gravemente a la empresa CONECTA RETAIL S.A
MUY BAJO (1)	La información asociada al activo es pública	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 100% pues su no impacta en la empresa CONECTA RETAIL S.A	Se considera que el activo puede estar disponible, porque su carencia no impacta a la empresa CONECTA RETAIL S.A

Anexo 5.7. Ficha evaluativa de actividades de COBIT 2019 enfocadas en las políticas del área de TI de la empresa

Anexo 5.7.1. *MEA02 – COBIT 2019*

Dominio: Monitorizar, evaluar y valorar Objetivo de gestión: MEA02 — Gestionar el sistema de control interno				
N°	MEA02.01 Supervisar los controles internos.	Cumple		Justificación
		SI	NO	
1	Identificar los límites del sistema de control interno. Por ejemplo, considerar cómo los controles internos de la organización, tienen en cuenta las actividades de desarrollo o producción externalizadas y/o ubicadas en otro país (offshore, término en inglés).	X		Supervisar, hacer benchmarking y mejorar continuamente el entorno de control y el marco de control de IT, para alcanzar los objetivos de la organización
2	Evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de servicio cumplen con los requisitos legales y regulatorios y con sus obligaciones contractuales.	X		
3	Realizar actividades de supervisión y evaluación del control interno basadas en estándares de gobierno de la organización y marcos y prácticas aceptados por la industria. Incluye también la supervisión y evaluación de la eficacia y eficiencia de las actividades de supervisión gerencial.	X		
4	Asegurar que las excepciones de control se comuniquen, se sigan y analicen prontamente, y que se prioricen e implementen acciones correctivas apropiadas, conforme al perfil de gestión de riesgos (p. ej., clasificar algunas excepciones como riesgo clave y otras como riesgo no clave).		X	
5	Considerar evaluaciones independientes del sistema de control interno (p. ej., por auditoría interna o compañeros).	X		
6	Mantener el sistema de control interno, considerando los cambios continuos en el riesgo del negocio y de I&T, el entorno de control de la organización y los procesos del negocio y de I&T relevantes. Si hay una brecha, evaluar y recomendar cambios.	X		
7	Evaluar regularmente el desempeño del marco de control, a través de una comparación con estándares y buenas prácticas aceptadas por la industria. Considerar la adopción formal de una estrategia de mejora continua de la supervisión del control interno.	X		

N°	MEA02.02 Revisar la eficacia de los controles del proceso de negocio.	Cumple		Justificación
		SI	NO	
1	Entender y priorizar el riesgo de los objetivos de la organización.	X		MEA02.02 Revisar la eficacia de los controles del proceso de negocio. Revisar la operación de los controles, incluidas la supervisión y la evidencia de las pruebas, para asegurar que los controles de los procesos de negocio operan eficazmente. Incluir actividades para mantener evidencia de la operación efectiva de los controles mediante mecanismos, como pruebas periódicas, supervisión continua, evaluaciones independientes, centros de mando y control y centros de operaciones de red.
2	Identificar controles clave y desarrollar una estrategia adecuada para validar los controles.	X		
3	Identificar información que indicará si un entorno de control interno está funcionando de forma eficaz.	X		
4	Conservar evidencias de la eficacia del control.	X		
5	Desarrollar e implementar procedimientos rentables para obtener esta información de acuerdo a los criterios de calidad de la información correspondientes.	X		

N°	MEA02.03 Realizar autoevaluaciones de control.	Cumple		Justificación
		SI	NO	
1	Definir una estrategia acordada y consistente para realizar autoevaluaciones de control y coordinarse con auditores internos y externos.	X		Alentar a la gerencia y a los dueños de los procesos para que mejoren los controles de forma proactiva mediante un programa continuo de autoevaluación que evalué la integridad y la efectividad del control de la gestión de los procesos, políticas y contratos.
2	Mantener planes de evaluación e identificación de criterios y alcance para llevar a cabo las autoevaluaciones. Planificar la comunicación de los resultados del proceso de autoevaluación al negocio, a TI y a la dirección general y al consejo de administración. Considerar estándares de auditoría interna en el diseño de las autoevaluaciones.		X	
3	Determinar la frecuencia de las autoevaluaciones periódicas, considerando globalmente la eficacia y eficiencia de la supervisión continua.		X	
4	Asignar las responsabilidades de la autoevaluación a los individuos adecuados para garantizar la objetividad y la competencia.	X		
5	Proporcionar revisiones independientes para garantizar la objetividad de la autoevaluación y permitir que se compartan buenas prácticas de control interno de otras empresas.		X	
6	Comparar los resultados de las autoevaluaciones con los estándares y buenas prácticas de la industria.	X		
7	Resumir e informar de los resultados de las autoevaluaciones y benchmarking para tomar acciones correctivas.		X	

N°	MEA02.04 Identificar e informar las deficiencias de control.	Cumple		Justificación
		SI	NO	
1	Comunicar procedimientos para el escalamiento de las excepciones de control, análisis de la causa raíz y notificación a los dueños del proceso y a las partes interesadas de I&T.	X		Identificar las deficiencias de control y analizar e identificar sus causas raíz subyacente. Escalar las deficiencias de control e informar a las partes interesadas.
2	Considerar el riesgo empresarial relacionado para establecer umbrales para el escalamiento de las excepciones de control y fallos.	X		
3	Identificar, reportar y registrar las excepciones de control. Asignar responsabilidades para su resolución e informar de su estado.	X		
4	Decidir qué excepciones de control deberían comunicarse a la persona responsable de la función y qué excepciones deberían escalarse. Informar a los dueños del proceso y a las partes interesadas.	X		
5	Hacer un seguimiento de todas las excepciones para garantizar que se han abordado las acciones acordadas.	X		
6	Identificar, iniciar, seguir e implementar acciones correctivas que surjan de las evaluaciones de control y los reportes.	X		

Anexo *5.7.1.1.Verificación de cumplimiento MEA02*

MEA02 — Gestionar el sistema de control interno		
DOMINIOS	CUMPLIMIENTO	%
MEA02.01 Supervisar los controles internos.	Supervisar, hacer benchmark y mejorar continuamente el entorno de control y el marco de control de I&T, para alcanzar los objetivos de la organización	100%
MEA02.02 Revisar la eficacia de los controles del proceso de negocio.	MEA02.02 Revisar la eficacia de los controles del proceso de negocio. Revisar la operación de los controles, incluidas la supervisión y la evidencia de las pruebas, para asegurar que los controles de los procesos de negocio operan eficazmente. Incluir actividades para mantener evidencia de la operación efectiva de los controles mediante mecanismos, como pruebas periódicas,	75%
MEA02.03 Realizar autoevaluaciones de control.	Alentar a la gerencia y a los dueños de los procesos para que mejoren los controles de forma proactiva mediante un programa continuo de autoevaluación que evalue la integridad y la efectividad del control de la gestión de los procesos, políticas y contratos.	75%
MEA02.04 Identificar e informar las deficiencias de control.	Identificar las deficiencias de control y analizar e identificar sus causas raíz subyacentes. Escalar las deficiencias de control e informar a las partes interesadas.	50%

Anexo 5.7.2. *MEA04 – COBIT 2019*

Dominio: Monitorizar, evaluar y valorar Objetivo de gestión: MEA04 — Gestionar el aseguramiento				
N°	**MEA04.01 Asegurar que los proveedores de aseguramiento sean independientes y estén cualificados.**	**Cumple**		**Justificación**
		SI	**NO**	
1	Establecer la adherencia a los códigos éticos y de estándares vigentes (p. ej. código de ética profesional de ISACA) y otros estándares de aseguramiento de la industria y específicos de la localización geográfica (p. ej. los IT Audit and Assurance Standards of ISACA y el International Framework for Assurance Engagements (IAASB Assurance Framework) del International Auditing and Assurance Standards Board (IAASB's)).	X		Asegurar que las entidades que realizan la evaluación sean independientes de la función, grupos u organizaciones incluidos en el alcance. Las entidades que realizan la evaluación deben demostrar una actitud y apariencia apropiadas.
2	Establecer la independencia de los proveedores del aseguramiento.	X		
3	Establecer la competencia y la cualificación de los proveedores del aseguramiento.	X		
N°	**MEA04.02 Desarrollar una planificación de iniciativas de aseguramiento basada en riesgos.**	**Cumple**		**Justificación**
		SI	**NO**	
1	Entender la estrategia y prioridades de la empresa.	X		Determinar objetivos de aseguramiento basados en evaluaciones del entorno y contextos interno y externo, el riesgo de no lograr las metas empresariales, y las oportunidades asociadas al logro de esas mismas metas.
2	Entender el contexto interno de la empresa. Esta comprensión ayudará al profesional de aseguramiento a evaluar mejor las metas empresariales y la importancia relativa de las metas de alineamiento y metas empresariales, así como las amenazas más importantes para estas metas. A su vez, esto contribuirá a definir un mejor y más relevante alcance para el compromiso con el aseguramiento.	X		
3	Entender el contexto externo de la empresa. Esta comprensión ayudará al profesional del aseguramiento a comprender mejor las metas empresariales y la importancia relativa de las metas de alineamiento y metas empresariales, así como las amenazas más importantes para estas metas. A su vez, esto contribuirá a definir un mejor y más relevante alcance para el compromiso con el aseguramiento.	X		
4	Desarrollar un plan anual global para las iniciativas de aseguramiento que incluya los objetivos consolidados de aseguramiento.		X	

N°	**MEA04.03 Determinar los objetivos de la iniciativa de aseguramiento.**	**Cumple**		**Justificación**
		SI	**NO**	
1	Definir el objetivo de aseguramiento de la iniciativa de aseguramiento mediante la identificación de las partes interesadas en esta iniciativa de aseguramiento y sus intereses.	X		Definir y acordar con todas las partes interesadas los objetivos de la iniciativa de aseguramiento.
2	Acordar los objetivos de alto nivel y los límites organizativos del compromiso de aseguramiento.	X		
3	Considerar el uso de la cascada de metas de COBIT y sus distintos niveles para expresar el objetivo del aseguramiento.	X		
4	Asegurar que los objetivos del compromiso del aseguramiento consideren los tres componentes de valor del objetivo: obtener beneficios que respalden los objetivos estratégicos, optimizar el riesgo de que no se alcancen los objetivos estratégicos y optimizar los niveles de recursos requeridos para lograr los objetivos estratégicos.		X	
N°	**MEA04.04 Definir el alcance de la iniciativa de aseguramiento.**	**Cumple**		**Justificación**
		SI	**NO**	
1	Definir todos los componentes de gobierno en el alcance de la revisión, es decir, los principios, políticas y marcos de referencia; procesos; estructuras organizativas; cultura, ética y comportamiento; información; servicios, infraestructura y aplicaciones; personas, habilidades y competencias.	X		Definir y acordar con todas las partes interesadas el alcance de la iniciativa de aseguramiento, con base en los objetivos de aseguramiento.
2	Basándose en el alcance establecido, definir un plan de compromiso, que incluya la información que debe recopilarse y las partes interesadas que deben entrevistarse.	X		
3	Confirmar y perfeccionar el alcance con base en el conocimiento de la arquitectura empresarial.		X	
4	Perfeccionar el alcance del compromiso de aseguramiento, conforme a los recursos disponibles.		X	

Anexo 5.7.2.1.*Verificación de cumplimiento MEA04*

MEA04 — Gestionar el aseguramiento		
DOMINIOS	**CUMPLIMIENTO**	**%**
MEA04.01 Asegurar que los proveedores de aseguramiento sean independientes y estén cualificados.	Asegurar que las entidades que realizan la evaluación sean independientes de la función, grupos u organizaciones incluidos en el alcance. Las entidades que realizan la evaluación deben demostrar una actitud y apariencia apropiadas.	100%
MEA04.02 Desarrollar una planificación de iniciativas de aseguramiento basada en riesgos.	Determinar objetivos de aseguramiento basados en evaluaciones del entorno y contextos interno y externo, el riesgo de no lograr las metas empresariales, y las oportunidades asociadas al logro de esas mismas metas.	75%
MEA04.03 Determinar los objetivos de la iniciativa de aseguramiento.	Definir y acordar con todas las partes interesadas los objetivos de la iniciativa de aseguramiento.	75%
MEA04.04 Definir el alcance de la iniciativa de aseguramiento.	Definir y acordar con todas las partes interesadas el alcance de la iniciativa de aseguramiento, con base en los objetivos de aseguramiento.	50%

Anexo *5.7.3.DSS06 – COBIT 2019*

DSS06 - Gestionar los controles de procesos de negocio				
N°	DSS06.01 - Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.	Cumple		Justificación
		SI	NO	
1	Identificar y documentar las actividades de control necesarias para procesos clave del negocio para satisfacer los requisitos de control para los objetivos estratégicos, operativos, de reporte y de cumplimiento.	X		La jefatura de riesgo operacional se encarga del cumplimiento de la politica de seguridad de la información en los contratos, estableciendo formulas que esten alineadas a las metas empresariales y lo establecido en las normas de CONECTA RETAIL S.A.
2	Priorizar las actividades de control de acuerdo al riesgo inherente al negocio. Identificar controles clave.	X		
3	Garantizar la propiedad de las actividades de control clave.	X		
4	Implementar controles automáticos.	X		
5	Monitorizar continuamente las actividades de control de principio a fin para identificar oportunidades de mejora.	X		
6	Mejorar de forma continua el diseño y operación de los controles de proceso del negocio.	X		

N°	DSS06.02 - Controlar el procesamiento de la información	Cumple		Justificación
		SI	NO	
1	Autenticar al originador de las transacciones y comprobar que el individuo tiene la autoridad para originar la transacción.	X		Se desarrollan politicas para asegurar que la información considerada como critica y que tenga los controles ante un acceso no autorizado.
2	Garantizar una adecuada segregación de tareas con relación al origen y aprobación de las transacciones.	X		
3	Comprobar que las transacciones son precisas, completas y válidas. Los controles podrían incluir secuencia, límite, rango, validez, razonabilidad, comprobación de tablas, existencia, verificación de clave, dígito de verificación, completitud, comprobaciones de duplicados y relaciones lógicas y ediciones temporales. Los criterios y parámetros de validación deberían estar sujetos a revisiones y confirmaciones periódicas. Validar los datos de entrada y editarlos o, cuando sea aplicable, devolverlos para su corrección lo más cerca posible del punto de origen.	X		
4	Sin comprometer los niveles de autorización de la transacción original, corregir y reenviar los datos que se introdujeron de forma errónea. Cuando sea adecuado para la reconstrucción, conservar documentos fuente originales durante el periodo de tiempo adecuado.		x	
5	Mantener la integridad y la validez de los datos durante el ciclo de procesamiento. Asegurar que la detección de transacciones erróneas no interrumpe el procesamiento de transacciones válidas.	X		
6	Manipular el resultado de forma autorizada, entregarlo al destinatario adecuado y proteger la información durante la transmisión. Verificar la exactitud e integridad del resultado.	X		
7	Mantener la integridad de los datos durante interrupciones inesperadas en el procesamiento del negocio. Confirmar la integridad de los datos después de fallos en el procesamiento.	X		
8	Antes de pasar datos de transacciones entre aplicaciones internas y funciones operativas/de negocio (dentro o fuera de la empresa), comprobar el trato adecuado, la autenticidad del origen y la integridad del contenido. Mantener la autenticidad y la integridad durante la transmisión o el transporte.	X		

N°	DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.	Cumple		Justificación
		SI	NO	
1	Asignar roles y responsabilidades conforme a las descripciones del cargo y las actividades aprobadas del proceso de negocio.	X		CONECTA RETAIL S.A desarrolla políticas de adquisición, desarrollo y mantenimiento de sistemas informáticos. Tiene por objetivo controlar el proceso de desarrollo, proteger la información crítica, apoyar en el control del proceso de puesta a producción y contar con un adecuado control de cambios.
2	Asignar niveles de autoridad para la aprobación de transacciones, límites de transacción y cualquier otra decisión relacionada con el proceso de negocio, conforme a roles de trabajo aprobados.	X		
3	Asignar roles para actividades sensibles para que haya una clara segregación de funciones.	X		
4	Asignar derechos de acceso y privilegios basado en lo mínimo requerido para realizar las actividades laborales, conforme a roles de trabajo predefinidos. Eliminar o revisar derechos de acceso de forma inmediata si el rol de trabajo cambia o si un miembro del personal deja el área de proceso de negocio. Revisar periódicamente para asegurar que el acceso sea adecuado para las amenazas, riesgo, tecnología y necesidades empresariales actuales.	X		
5	Concienciar y formar regularmente sobre los roles y responsabilidades, para que todos entiendan sus responsabilidades; la importancia de los controles; y la seguridad, integridad, confidencialidad y privacidad de la información de la compañía en todas sus formas.	X		
6	Garantizar que los privilegios administrativos están asegurados, rastreados y controlados de forma suficiente y eficaz para prevenir el mal uso.	X		
7	Revisar periódicamente las definiciones de control de acceso, los logs y los informes de excepción. Asegurar que todos los privilegios de acceso son válidos y están alineados con los miembros actuales del personal y sus roles asignados.	X		

N°	DSS06.04 Gestionar errores y excepciones.	Cumple		Justificación
		SI	NO	
1	Revisar errores, excepciones y desviaciones.	X		Las incidencias registradas y su tratamiento se reportan de manera peiodica. La empresa CONECTA RETAIL S.A, cuenta con una escala de clasificacion de la información de los procesos según su nivel de criticidad. Se gestionan los controles necesarios parab la gestión de excepciones
2	Hacer un seguimiento, corregir, aprobar y reenviar los documentos fuente y las transacciones.	X		
3	Mantener evidencia de acciones correctivas.		x	
4	Definir y mantener procedimientos para asignar la propiedad de errores y excepciones, corregir errores, anular errores y manejar condiciones fuera del balance.	X		
5	Informar de manera oportuna sobre errores relevantes de procesamiento de la información del negocio para realizar un análisis de causa raíz y de tendencia.	X		
N°	DSS06.05 Asegurar la trazabilidad y la rendición de cuentas de los eventos de información	Cumple		Justificación
		SI	NO	
1	Obtener la información fuente, evidencias de soporte y el registro de transacciones.	X		El area de sistemas es la encargada de aplica controles respectivos en los sistemas de la empresa que aseguran la confidencialidad de la información del cliente.
2	necesidades operativas, de reportes financieros y de cumplimiento.	X		
3	Disponer de la información fuente, las evidencias de soporte y el registro de las transacciones conforme a la política de retención.	X		
N°	DSS06.06 Asegurar los activos de información.	Cumple		Justificación
		SI	NO	
1	Restringir el uso, distribución y el acceso físico a la información de acuerdo con su clasificación.	X		Las areas que tengan acceso los activos de TI, deberan tener los cuidados respectivos para que esta información tenga carácter restringido solo para nivel de acceso respectivo.
2	Proporcionar una concienciación y formación adecuada sobre el uso.	X		
3	Aplicar las políticas y procedimientos de seguridad para la clasificación y uso aceptable de datos y para proteger los activos de información que están bajo control del negocio.	X		
4	Identificar e implantar procesos, herramientas y técnicas para verificar el cumplimiento de forma razonable.	X		
5	Informar al negocio y a otras partes interesadas sobre violaciones y desviaciones.	X		

Anexo 5.7.3.1.*Verificación de cumplimiento DSS06*

DSS06 - Gestionar los controles de procesos de negocio		
DOMINIOS	CUMPLIMIENTO	%
DSS06.01 - Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.	La jefatura de riesgo operacional se encarga del cumplimiento de la politica de seguridad de la información en los contratos, estableciendo formulas que esten alineadas a las metas empresariales y lo establecido en las normas de CONECTA RETAIL S.A.	100%
DSS06.02 - Controlar el procesamiento de la información	Se desarrollan politicas para asegurar que la información considerada como critica y que tenga los controles ante un acceso no autorizado.	87%
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.	CONECTA RETAIL S.A desarrolla políticas de adquisición, desarrollo y mantenimiento de sistemas informáticos. Tiene por objetivo controlar el proceso de desarrollo, proteger la información crítica, apoyar en el control del proceso de puesta a producción y contar con un adecuado control de cambios.	100%
DSS06.04 Gestionar errores y excepciones.	Las incidencias registradas y su tratamiento se reportan de manera peiodica. La empresa CONECTA RETAIL S.A, cuenta con una escala de clasificacion de la información de los procesos según su nivel de criticidad. Se gestionan los controles necesarios parab la gestión de excepciones	80%
DSS06.05 Asegurar la trazabilidad y la rendición de cuentas de los eventos de información	El area de sistemas es la encargada de aplica controles respectivos en los sistemas de la empresa que aseguran la confidencialidad de la información del cliente.	100%
DSS06.06 Asegurar los activos de información.	Las areas que tengan acceso los activos de TI, deberan tener los cuidados respectivos para que esta información tenga carácter restringido solo para nivel de acceso respectivo.	100%

Anexo *5.7.4. BAI11 – COBIT 2019*

Objetivo de gestión: BAI11 – Gestionar los proyectos				
N°	BAI11.01 Mantener un enfoque estándar en la gestión de programas.	Cumple		Justificación
		SI	NO	
1	Mantener y hacer cumplir una estrategia estándar de gestión de proyectos, alineada con el entorno específico de la empresa y con las buenas prácticas, conforme a procesos definidos y al uso de la tecnología correcta. Asegurar que la estrategia cubra todo el ciclo de vida y las disciplinas a seguir, incluida la gestión del alcance, recursos, riesgo, coste, calidad, tiempo, comunicación, involucramiento de las partes interesadas, adquisiciones, control de cambio, integración y obtención de beneficios.	x		Se realiza una gestión estandar de forma parcial en cuanto a la gestión de proyectos. Se evidencia que se proporciona capacitaciones a los gestores de los proyectos, para posteriormente certificarlos en base a los aprendizajes obtenidos en cuanto a gestion de proyectos.
2	Proporcionar una capacitación en gestión de proyectos adecuada y considerar la certificación para los gestores de proyecto.	x		
3	Establecer una oficina de gestión de proyectos (PMO) que mantenga una estrategia estándar para la gestión de programas y proyectos en toda la organización. La PMO respalda todos los proyectos mediante la creación y mantenimiento de plantillas de documentación de proyectos requeridos, proveyendo formación y buenas prácticas para los gestores de proyecto, seguimiento de las métricas sobre el uso de buenas prácticas para la gestión de proyectos, etc. En algunos casos, la PMO podría también informar sobre el progreso del proyecto a la alta dirección y/o las partes interesadas, ayudar a priorizar proyectos y asegurar el respaldo de todos los proyectos con los objetivos globales de negocio de	x		
4	Evaluar las lecciones aprendidas sobre el uso de la estrategia de gestión de proyectos. Actualizar las buenas prácticas, herramientas y plantillas, conforme sea necesario.		x	

N°	BAI11.02 Establecer e iniciar un proyecto	Cumple		Justificación
		SI	NO	
1	Crear un entendimiento común sobre el alcance del proyecto entre las partes interesadas, proporcionarles una clara declaración por escrito que defina la naturaleza, el alcance y los	x		La empresa cuenta con un SGSI la cual busca que los activos esten siempre protegidos de los riesgos que los afecten y establecen metodologias para identificar y evaluar los riesgos con tecnicas de control idoneas para minimizarlos.
2	Garantizar que cada proyecto tenga uno o más patrocinadores con la autoridad suficiente para gestionar la ejecución del proyecto dentro del programa global.	x		
3	Asegurar que las partes interesadas y los patrocinadores de la empresa (empresa y TI) acuerden y acepten los requisitos del proyecto, incluidas las definiciones de los criterios de éxito del proyecto (aceptación) y los indicadores clave de rendimiento (KPI).	x		
4	Nombrar a un gestor dedicado para el proyecto. Asegurar que el individuo tenga los conocimientos tecnológicos y de negocio requeridos y, las competencias y habilidades proporcionales para gestionar el proyecto de forma eficaz y eficiente	x		
5	Asegurar que la definición del proyecto describe los requisitos de un plan de comunicación del proyecto que identifique las comunicaciones internas y externas del proyecto.	x		
6	Con la aprobación de las partes interesadas, mantener la definición del proyecto a lo largo del mismo y reflejar el cambio de requisitos.	x		
7	Hacer un seguimiento de la ejecución del proyecto, establecer mecanismos como la elaboración regular de informes en cada fase, revisiones por fases o liberaciones, de forma oportuna y con la aprobación correspondiente.		x	

N°	BAI11.03 Gestionar la participación de las partes interesadas	Cumple		Justificación
		SI	NO	
1	Planificar cómo las partes interesadas dentro y fuera de la organización se identificarán, analizarán, involucrarán y gestionarán durante el ciclo de vida del proyecto	x		Cada parte interesada contempla un rol dentro y fuera de la organización, los cuales tienen asignada un área y una función.
2	Identificar, involucrar y gestionar a las partes interesadas estableciendo y manteniendo los niveles de coordinación, comunicación y relación adecuadas para garantizar que estén involucrados en el proyecto.	x		
3	Analizar los intereses, requisitos y compromiso de las partes interesadas. Implementar medidas correctivas si fuera necesario.	x		
N°	BAI11.04 Desarrollar y mantener el plan del proyecto	Cumple		Justificación
		SI	NO	
1	Desarrollar un plan de proyecto que proporcione información para permitir a la dirección controlar su progreso de forma progresiva. El plan debería incluir detalles de los entregables y los criterios de aceptación del proyecto, recursos y responsabilidades internos y externos requeridos, estructuras de división del trabajo y paquetes de trabajo claros, estimaciones sobre los recursos requeridos, plan / fases de hitos/liberaciones, dependencias clave, presupuesto y costes e identificación de una ruta crítica.	x		La empresa conecta define política y define las reglas, centradas en el tema de seguridad, que deben ser consideradas en la ejecución, Continuidad y Término de los proyectos CONECTA RETAIL S.A.
2	Mantener el plan del proyecto y los planes dependientes (p. ej., plan de riesgos, plan de calidad, plan de obtención de beneficios). Asegurar que los planes estén actualizados y reflejen el progreso actual y los cambios materiales aprobados	x		
3	Asegurar que haya una comunicación efectiva de los planes del proyecto e informes de progresos. Asegurar que todos los cambios realizados a los planes individuales se reflejen en otros planes.	x		
4	Determinar las actividades, interdependencias y colaboración y comunicación requeridas en el proyecto y entre los múltiples proyectos de un programa.	x		
5	Asegurar que cada hito esté acompañado de un entregable significativo que requiere su revisión y confirmación	x		
6	Establecer una línea de referencia del proyecto (p. ej. coste, calendario, alcance, calidad) que se revise, apruebe e incorpore adecuadamente al plan integrado del proyecto.	x		

N°	BAI11.05 Gestionar la calidad del proyecto	Cumple		Justificación
		SI	NO	
1	Para proporcionar el aseguramiento de la calidad de los entregables del proyecto, identificar la propiedad y las responsabilidades, procesos de revisión de la calidad, criterios de éxito y métricas de rendimiento.	x		La jefatura de riesgo operacional se encarga del cumplimiento de la politica de seguridad de la información en los contratos, documentos de proyectos. Asi mismo los proyectos debden contar con procedimeintos operativos y de controll necesarios para los requerimientos legales que sean cumplidos según lo establecido.
2	Identificar las tareas y prácticas de aseguramiento requeridas para respaldar la acreditación de sistemas nuevos o modificados durante la planificación del proyecto. Incluirlos en los planes integrados. Asegurar que las tareas garantizan que los controles internos y, las soluciones de seguridad y privacidad satisfacen los requisitos definidos	x		
3	Definir los requisitos para la validación y verificación independiente de la calidad de los entregables en el plan	x		
4	Realizar actividades de aseguramiento y control de calidad conforme al plan de gestión de calidad y el SGC.	x		

N°	BAI11.06 Gestionar el riesgo del proyecto.	Cumple		Justificación
		SI	NO	
1	Establecer una estrategia formal de gestión de riesgos de proyectos alineada con el marco de gestión de riesgos empresariales (ERM). Asegurar que la estrategia incluya la identificación, análisis, respuesta, mitigación, monitorización y control del riesgo.	x		La empresa CONECTA RETAIL S.A cuenta con un plan para identificación de riesgos e incidencias, el personal a cargo gestiona cada uno de los procesos de acuerdo al área asignada.
2	Asignar a personal adecuadamente calificado la responsabilidad de ejecutar el proceso de gestión de riesgos de proyectos de la empresa dentro de un proyecto y asegurar que esto se incorpore en las prácticas de desarrollo de soluciones. Considerar asignar este rol a un equipo independiente, sobre todo si se requiere un punto de vista objetivo o si un proyecto se considera crítico	x		
3	Identificar los dueños de las acciones para evitar, aceptar o mitigar el riesgo.	x		
4	Realizar la evaluación de riesgos del proyecto, identificando y cuantificando el riesgo continuamente durante todo el proyecto. Gestionar y comunicar el riesgo de forma adecuada dentro de la estructura de gobierno del	x		
5	Reevaluar el riesgo del proyecto periódicamente, incluyendo un inicio a cada fase del proyecto principal como parte de evaluaciones de solicitudes de cambio mayores	x		
6	Mantener y revisar el registro de riesgos del proyecto, de todos los riesgos potenciales del proyecto y un registro de mitigación de riesgo de todos los problemas presentados y su resolución. Analizar periódicamente el log para ver las tendencias y problemas recurrentes con la finalidad de garantizar que se corrigen las causas raíz.	x		

N°	BAI11.07 Supervisar y controlar los proyectos.	Cumple		Justificación
		SI	NO	
1	Establecer y usar una serie de criterios de proyecto incluidos, pero no limitados a, el alcance, beneficio esperado para el negocio, calendario, calidad, coste y nivel de riesgo.	x		Los sistemas core de la empresa CONECTA RETAIL S.A, cuentan con mecanismos de detección de anomalias que avisen al administrador responsable cuando ocurra cualquier evento.
2	Informar a las partes interesadas identificadas clave acerca del progreso del proyecto, desviaciones con respecto a los criterios clave de rendimiento del proyecto establecidos (como, pero no limitado a, los beneficios empresariales esperados), y posibles efectos positivos y negativos en el proyecto	x		
3	Documentar y enviar los cambios necesarios a las partes interesadas clave del proyecto para su aprobación antes de su adopción. Comunicar los criterios revisados a los gestores de proyecto para su uso en futuros informes de rendimiento.	x		
4	Para los entregables producidos en cada iteración, entrega o fase del proyecto, obtener aprobación y conformidad de los gestores y usuarios designados en las funciones de negocio y de TI afectadas.	x		
5	Basar el proceso de aprobación en criterios de aceptación definidos, acordados con las partes interesadas clave antes del comienzo de la fase del proyecto o iteración entregable.	x		
6	Evaluar el proyecto en las fases, liberaciones o iteraciones mayores acordadas. Establecer decisiones formales de seguir o no seguir adelante conforme a los criterios críticos de éxito predeterminados.	x		
7	Establecer y activar un sistema de control de cambio para el proyecto con la finalidad de que todos los cambios de la línea de referencia del proyecto (p. ej. alcance, beneficios de negocio esperados, calendario, calidad, coste, nivel de riesgo) se revisen, aprueben e incorporen en el plan integrado del proyectos en línea con el marco de gobierno de proyectos y programas.		x	
8	Medir el rendimiento de los proyectos con respecto a los criterios clave de rendimiento del proyecto. Analizar las desviaciones causadas con respecto a los criterios clave de rendimiento del proyecto y evaluar los efectos positivos y negativos en el proyecto.		x	
9	Supervisar los cambios en el proyecto y revisar los criterios clave de rendimiento del proyecto para determinar si siguen representando medidas de progreso válidas	x		
10	Recomendar y supervisar medidas correctivas, cuando sea necesario, conforme al marco de gobierno del proyecto.	x		

N°	BAI11.08 Gestionar los recursos del proyecto y los paquetes de trabajo.	Cumple		Justificación
		SI	NO	
1	Identificar las necesidades de recursos del negocio y de TI para el proyecto y asignar roles y responsabilidades adecuados, con escalamiento, y autoridad para la toma de decisiones acordadas y comprendidas.	x		Cada empleado se le asigna un rol y una área en el cual implementan varias actividades a su cargo. De acuerdo a su rol cumple funciones y elabora su plan de actividades.
2	Identificar las habilidades y tiempo requeridos por todos los individuos involucrados en las fases del proyecto con relación a los roles definidos. Asignar personal a los roles conforme a la información de habilidades disponibles (p. ej., matriz de habilidades de TI).	x		
3	Utilizar una gestión de proyectos experta y los recursos de líderes de equipo con las habilidades apropiadas al tamaño, complejidad y riesgo del proyecto.	x		
4	Considerar y definir claramente los roles y responsabilidades de otras partes involucradas, incluyendo finanzas, legal, adquisiciones, recursos humanos, auditoría interna y cumplimiento.	x		
5	Definir y acordar claramente la responsabilidad de la adquisición y gestión de productos y servicios de terceros y, gestionar la relación.	x		
6	Identificar y autorizar la ejecución del trabajo conforme al plan del proyecto.	x		
7	Identificar las brechas del plan del proyecto y proporcionar retroalimentación al gestor de proyectos para que las corrija	x		

N°	BAI11.09 Cerrar un proyecto o iteración.	Cumple		Justificación
		SI	NO	
1	Obtener la aceptación de las partes interesadas para los entregables del proyecto y transferir la propiedad.	x		Al finalizar el proyecto, se realiza la recopilacion de lecciones aprendidas de los participantes del proyecto. Se analizan los datos y se realizan las recomendaciones pertinenetes para mejorar el proyecto actual y futuros.
2	Definir y aplicar los pasos claves para el cierre del proyecto, incluidas las revisiones post-implementación que evalúan si un proyecto ha alcanzado los resultados deseados.	x		
3	Planificar y ejecutar revisiones post-implementación para determinar si los proyectos ofrecen los resultados esperados. Mejorar la gestión del proyecto y la metodología de procesos de desarrollo de sistemas.	x		
4	Identificar, asignar, comunicar y hacer un seguimiento a cualquier actividad incompleta requerida para garantizar que el proyecto ofrezca los resultados requeridos en términos de capacidades y, que los resultados contribuyen como se esperaba a los beneficios del programa		x	
5	De forma regular, y al finalizar el proyecto, recopilar las lecciones aprendidas de los participantes del proyecto. Revisarlas junto con las actividades clave que llevaron a obtener beneficios y valor. Analizar los datos y realizar recomendaciones para mejorar el proyecto actual y el método de gestión de proyectos para proyectos futuros.	x		

Anexo *5.7.4.1. Verificación de cumplimiento BAI11*

Objetivo de gestión: BAI11 – Gestionar los proyectos		
DOMINIOS	**CUMPLIMIENTO**	**%**
BAI01.01 Mantener un enfoque estándar en la gestión de proyectos.	Se realiza una gestión estandar de forma parcial en cuanto a la gestión de proyectos. Se evidencia que se proporciona capacitaciones a los gestores de los proyectos, para posteriormente certificarlos en base a los aprendizajes obtenidos en cuanto a gestion de proyectos.	75%
BAI11.02 Establecer e iniciar un proyecto	La empresa cuenta con un SGSI la cual busca que los activos esten siempre protegidos de los riesgos que los afecten y establecen metodologias para identificar y evaluar los riesgos con tecnicas de control idoneas para minimizarlos.	86%
BAI11.03 Gestionar la participación de las partes interesadas	Cada parte interesada contempla un rol dentro y fuera de la organización, los cuales tienen asignada un área y una función.	100%
BAI11.04 Desarrollar y mantener el plan del proyecto	La empresa conecta define política y define las reglas, centradas en el tema de seguridad, que deben ser consideradas en la ejecución, Continuidad y Término de los proyectos CONECTA RETAIL S.A.	90%
BAI11.05 Gestionar la calidad del proyecto	La jefatura de riesgo operacional se encarga del cumplimiento de la politica de seguridad de la información en los contratos, documentos de proyectos. Asi mismo los proyectos debden contar con procedimeintos operativos y de controll necesarios para los requerimientos legales que sean cumplidos según lo establecido.	100%
BAI11.06 Gestionar el riesgo del proyecto.	La empresa CONECTA RETAIL S.A cuenta con un plan para identificación de riesgos e incidencias, el personal a cargo gestiona cada uno de los procesos de acuerdo al área asignada.	100%
BAI11.07 Supervisar y controlar los proyectos.	Los sistemas core de la empresa CONECTA RETAIL S.A, cuentan con mecanismos de detección de anomalias que avisen al administrador responsable cuando ocurra cualquier evento.	80%
BAI11.08 Gestionar los recursos del proyecto y los paquetes de trabajo.	Cada empleado se le asigna un rol y una área en el cual implementan varias actividades a su cargo. De acuerdo a su rol cumple funciones y elabora su plan de actividades.	90%
BAI11.09 Cerrar un proyecto o iteración.	Al finalizar el proyecto, se realiza la recopilacion de lecciones aprendidas de los participantes del proyecto. Se analizan los datos y se realizan las recomendaciones pertinenetes para mejorar el proyecto actual y futuros.	80%

Anexo *5.7.5. APO07 – COBIT 2019*

Objetivo de gestión: APO07—Gestionar los recursos humanos				
N°	**APO07.01 Adquirir y mantener una dotación de personal suficiente y adecuada**	**Cumple**		**Justificación**
		SI	**NO**	
1	la empresa como la función de TI tengan los suficientes recursos para apoyar las metas y los objetivos empresariales, procesos y controles empresariales y las iniciativas habilitadas por I&T de forma adecuada y apropiada.	X		Todos los nuevos empleados pasan por un periódo de evaluación, y luego son entrenados según sus competencias mas relevantes.
2	Mantener los procesos de contratación y retención de personal empresarial y de TI en línea con todas las políticas y procedimientos de personal de la empresa.	X		
3	Establecer una estructura de recursos flexible, como el uso de transferencias, contratistas externos y acuerdos de servicio con terceros, para apoyar el cambio en las necesidades empresariales.	X		
4	Incluir verificaciones de antecedentes en el proceso de contratación de TI para empleados, contratistas y terceros. El alcance y frecuencia de estas verificaciones debe depender de la sensibilidad y/o criticidad de la función.	X		
N°	**APO07.02 Identificar al personal clave de TI.**	**Cumple**		**Justificación**
		SI	**NO**	
1	Como precaución de seguridad, proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que tomarán las personas clave.	X		Periodicamente realizan un análisis y determinan cual es el personal indispensable y luego definen un plan de capacitación para convertirlo en no indispensablse, compartiendo la filosofia compartir conocimientos.
2	Tomar las acciones pertinentes relativas a cambios laborales, en especial terminación de contratos.	X		
3	Usar la captura de conocimientos (documentación), intercambio de conocimientos, planificación de sucesión y personal de respaldo para minimizar la dependencia en un único individuo que realice un trabajo crítico.	x		
4	Comprobar regularmente los planes de respaldo de personal.	x		Formalidad de constancias de respaldo

N°	**PO07.03 Mantener las habilidades y competencias del personal**	**Cumple**		**Justificación**
		SI	**NO**	
1	Identificar las habilidades y competencias disponibles actuales, tanto de recursos internos como externos.	x		Realizan la identificación del personal clave, en base a ello se crean grupos de intercambio de conocimientos, para mantener habilidades y amplir el campo de conocimiento en todos los empleados que son claves.
2	Identificar las brechas entre las habilidades requeridas y las disponibles Desarrollar planes de acción, como capacitación (habilidades técnicas y de conducta), contratación, reasignación y cambio de las estrategias de abastecimiento, para resolver las brechas desde el punto de vista individual y colectivo.	x		
3	Revisar los materiales y programas de capacitación de forma regular. Garantizar su idoneidad con respecto a los requisitos en constante evolución de la empresa y su impacto sobre el conocimiento, capacidades y habilidades necesarias.	x		
4	Proporcionar acceso a los repositorios de conocimiento para respaldar el desarrollo de habilidades y competencias.	x		
5	Desarrollar y ofrecer programas de capacitación conforme a los requisitos del proceso y organizativos, incluidos los requisitos para el conocimiento empresarial, control interno, conducta ética, seguridad y privacidad.	x		
6	Realizar evaluaciones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Evaluar la planificación de los reemplazos.	x		

N°	**APO07.04 Evaluar y reconocer/recompensar el rendimiento laboral de los empleados.**	**Cumple**		**Justificación**
		SI	**NO**	
1	Considerar las metas empresariales/funcionales como el contexto para establecer metas individuales.	X		Se establecen metas, que incentivan al personal a ser mas productivo y a cambio se le otorgan incentivos monetarios y certificaciones que acreditan sus habilidades.
2	Establecer metas individuales alineadas con las metas empresariales y de I&T relevantes. Basar las metas en objetivos específicos, medibles, alcanzables, relevantes y en tiempo (SMART) que reflejen las competencias principales, los valores empresariales y las habilidades requeridas para los roles.	X		
3	Proporcionar retroalimentación oportuna acerca del rendimiento comparado con las metas individuales.	X		
4	Proporcionar instrucciones específicas para el uso y el almacenamiento de la información personal en el proceso de evaluación, en cumplimiento de la legislación vigente sobre datos personales y laboral vigente.	X		
5	Recopilar resultados de evaluación de rendimiento de 360 grados.		x	
6	Proporcionar planes formales de planificación y de desarrollo profesional conforme a los resultados del proceso de evaluación para fomentar el desarrollo de competencias y las oportunidades para el avance personal y para reducir la dependencia de individuos clave. Proporcionar coaching a los empleados sobre el rendimiento y la conducta cuando sea apropiado.	x		Presupuesto
7	Implementar un proceso de remuneración/reconocimiento que premie el compromiso adecuado, desarrollo de competencias y logro de las metas de desempeño. Asegurar que el proceso se aplique de forma consistente y en línea con las políticas organizativas.	x		

N°	APO07.05 Planificar y hacer seguimiento del uso de los recursos humanos del negocio y de TI.	Cumple		Justificación
		SI	NO	
1	Crear y mantener un inventario de recursos humanos empresariales y de TI.	x		Todos los empleados se comprometen a conocer y cumplir las politicas de seguridad generica de la empresa CONECTA RETAIL S.A, asi mismo asisten a charlas y capacitaciones de entramiento en materias de seguridad.
2	Entender la demanda actual y futura de recursos humanos para contribuir a lograr los objetivos de I&T y ofrecer servicios y soluciones conforme al portafolio de iniciativas relacionadas con I&T, al portafolio de inversión futura y necesidades operativas diarias.	x		
3	Identificar las carencias y proporcionar recomendaciones sobre los planes de abastecimiento, así como de los procesos de contratación de personal empresarial y de TI. Crear y revisar la planificación de personal, mediante un seguimiento de su uso real.		x	
4	Mantener una información adecuada sobre el tiempo dedicado a las distintas tareas, trabajos, servicios o proyectos.	x		

N°	APO07.06 Gestionar al personal contratado	Cumple		Justificación
		SI	NO	
1	Implementar las políticas y procedimientos del personal contratado	x		El jefe directo tiene la obligacion de informar y capacitar a todos los empleados sobre los riesgos que se presentan según su cargo que desempeña y esta expuesto, asi mismo debe entrenarlo, para hacer frente a estos riesgos y lograr minimizarlo de la manera mas oportuna.
2	Al inicio del contrato, obtener el acuerdo formal de los contratistas de que deben cumplir con el marco de control de I&T empresarial, así como con las políticas y verificaciones de seguridad, control del acceso físico y lógicos, uso de las instalaciones, requisitos de confidencialidad de la información y acuerdos de no revelación.	x		
3	Avisar a los contratistas de que los directivos se reservan el derecho a supervisar e inspeccionar todo el uso de los recursos de TI, incluido el correo electrónico, comunicaciones de voz y todos los programas y archivos de datos.	x		
4	Como parte de sus contratos, proporcionar a los contratistas una definición clara de sus roles y responsabilidades, incluidos los requisitos explícitos para documentar su trabajo conforme a los estándares y formatos acordados.	x		
5	Revisar el trabajo de contratistas y basar la aprobación de los pagos en los resultados.	x		Se cumple para renovaciones de contratos
6	En contratos formales y no ambiguos, definir todo el trabajo realizado por personal externo.	x		
7	Realizar revisiones periódicas para garantizar que el personal contratado haya firmado y aceptado todos los acuerdos necesarios.	x		
8	Realizar revisiones periódicas para garantizar que los roles de los contratistas y los derechos de acceso sean adecuados y conforme a los contratos.	x		

5.7.5.1. Verificación de cumplimiento APO07

Objetivo de gestión: APO07—Gestionar los recursos humanos		
DOMINIOS	**CUMPLIMIENTO**	**%**
APO07.01 Adquirir y mantener una dotación de personal suficiente y adecuada	Todos los nuevos empleados pasan por un periódo de evaluación, y luego son entrenados según sus competencias mas relevantes.	100%
APO07.02 Identificar al personal clave de TI.	Periodicamente realizan un análisis y determinan cual es el personal indispensable y luego definen un plan de capacitación para convertirlo en no indispensablse, compartiendo la filosofia compartir conocimientos.	100%
PO07.03 Mantener las habilidades y competencias del personal	Realizan la identificación del personal clave, en base a ello se crean grupos de intercambio de conocimientos, para mantener habilidades y amplir el campo de conocimiento en todos los empleados que son claves.	100%
APO07.04 Evaluar y reconocer/recompensar el rendimiento laboral de los empleados.	Se establecen metas, que incentivan al personal a ser mas productivo y a cambio se le otorgan incentivos monetarios y certificaciones que acreditan sus habilidades.	86%
APO07.05 Planificar y hacer seguimiento del uso de los recursos humanos del negocio y de TI.	Todos los empleados se comprometen a conocer y cumplir las politicas de seguridad generica de la empresa CONECTA RETAIL S.A, asi mismo asisten a charlas y capacitaciones de entramiento en materias de seguridad.	75%
APO07.06 Gestionar al personal contratado	El jefe directo tiene la obligacion de informar y capacitar a todos los empleados sobre los riesgos que se presentan según su cargo que desempeña y esta expuesto, asi mismo debe entrenarlo, para hacer frente a estos riesgos y lograr minimizarlo de la manera mas oportuna.	100%

5. Otros que considere pertinente.

Anexo 6.1. Ficha validada de evaluación de cumplimiento de políticas internas del área de TI de la empresa CONECTA RETAIL S.A, por el jefe de Are de TI de desarrollo de software.

POLÍTICAS DE LA EMPRESA CONECTA S.A.C			
N°	Politicas	Observaciones	% Cumplimiento
1	**Politicas de seguridad Lógica**	Esta politica abarca todos los recursos informaticos de la empresa CONECTA RETAIL S.A.C. Y aquellos usuarios que son definidos implicitamente en los sistemas y que sirve para realizar	90%
2	**Politicas de Seguridad Personal**	El area de sistemas realiza periodicamente una revision de los equipos portatiles asignados a trabajadores , registrando los estados de estos y el motivo del cambio. El area de de riegos definira la	90%
3	**Poliitica de seguridad fisica y ambiental**	Esta politica se aplica a todas las areas de la empresa CONECTA RETAIL S.A.C que usa los servicios tecnologicos de la empresa. Esta politica abarca todos los centros de computo que cuentan con	100%
4	**Politicas para el inventario de activos y classificación de la**	Esta politica cuenta con escalas de clasificación de la información, según su nivel de criticidad. La gerencia de sistemas es la responsable de realizar el inventario de los activos de tecnologia de la	80%
5	**Politicas para la administracion de operaciones y comunicaciones**	Esta politica se enfoca en definir las reglas de seguirdad para el area de TI de la empresa CONECTA RETAIL S.A.C. El sistema core del negocio cuenta con mecanismos que les permite detectar	100%
6	**Politica de adquisición, desarrollo y mantenimiento de sistemas informáticos**	Esta politica controla el proceso de desarrollo, protege la informacion critica y apoya en el control de la ejecucion y mejora del proceso . El area de sistemas lleva el control responsable de los sistemas, software, licencias, etc.	100%
7	**Politicas de respaldo**	Esta politica define las reglas que norman el manejo de los repaldos de los sistemas de produccion de la empresa CONECTA RETAL S.A.C.	100%
8	**Politicas de seguridad de la información**	Se involucran politicas que logren asegurar la información que se considera como critica y que se apliquen los controles necesarios ante su acceso no autorizado.	90%
9	**Politicas de cumplimiento normativo**	Involucra politicas que aseguran que los requerimientos legales o de regulaciones sean cumplidos cuando corresponda, ,incorporado a una logica interna de aplicaciones informáticas.	100%
10	**Politicas de gestión de incidentes de seguridad de la información**	Involucra que a traves de notofocaciones de eventos y puntos debiles de seguridad, se mejore los procedimientos y responsabilidades que se deben seguir para mejorar la seguridad de la información	100%
11	**Politicas de subcontratación definitiva**	Esta politica involucra que en caso haya suspensión del servicio, se realice subcontrataciones para no afectar los ingresos, solvencia o continuidad operativa del negocio.	100%
PROMEDIO GLOBAL DE CUMPLIMIENTO			

Anexo 6.2. Evidencia de reuniones efectuadas con el jefe de área de TI de la oficina de desarrollo de software de la empresa CONECTA RETAIL S.A.

Anexo 6.3. Carta del jefe de Área de TI de la oficina de desarrollo de software, que evidencia que se nos han remitido documentos confidenciales de la empresa CONECTA RETAIL S.A para poder realizar la investigación y al mismo tiempo evidenciar que se realizaron las entrevistas pertinentes para obtener datos necesarios para el desarrollo y aplicación del modelo de auditoria de TI basado en el cumplimiento de normas y políticas de la empresa en estudio.

"Año del Fortalecimiento de la Soberanía Nacional"

Lambayeque - Chiclayo

11 de Diciembre, 2022

En el presente documento suscriben los tesistas, RABANAL SENMACHE MARRY CECY; SÁNCHEZ RUBIO OMAR ALBERTO, estudiantes de la carrera de Ingeniería de Sistemas en la Universidad Señor de Sipan, Lambayeque – Chiclayo, con el tema "Diseño de un modelo de auditoria de TI para el cumplimiento de normas y estándares de una empresa retail peruana".

Tienen la finalidad de poner en evidencia la veracidad y la legitimidad de los documentos brindados, como también de certificar las entrevistas realizadas al jefe encargado del área de desarrollo de TI, el ingeniero Jorge Andrés Cachay Arana, de la empresa en estudio CONECTA RETAIL S.A para el desarrollo del trabajo de investigación de los tesistas y su debida sustentación de la legitimidad de los datos suministrados por los entrevistados y dar rigor científico necesario a los resultados.

Jorge Cachay Arana

Anexo 6.4. Captura de documentos donde se encuentras las políticas internas de la empresa CONECTA RETAIL S.A.


Financiera
Efectiva
Ingeniería de Procesos

MANUAL DE POLIT

Seguridad de la Info

Establecer las políticas, procedimientos y responsabilidades, que dicten las regir las actividades realizadas por todas las instancias de Efectiva, vinculadas la Información.

Sr. Juan A. Buendía Sardón
Gerente de Riesgos

Sr. Javier Sánch
Gerent

USO INTERNO

Cualquier uso, copia o distribución total o parcial de este documento no autorizado está est
El contenido íntegro de este documento es de propiedad de FINANCIERA EFECTIVA. Autorizo
colaboradores de la empresa, en caso haya llegado a usted por error agradeceremos
La versión vigente se encuentra publicada en la página de

CONECTA RETAIL S.A.	FORMATO DE LA EMPRESA CONECTA RETAIL S.A MATRIZ DE HISTORIAL DE POLITICAS	Responsable: Jorge Arana Cachay Cargo: Jefe del Área de TI	**Versión: N°01**
		FECHA DE CREACIÓN : 15/11/2022	

HISTORIAL DE POLÍTICAS DE LA EMPRESA

N°	Código	Nombre Documento	Nombre del sector	Nombre de la política	Descripción	Versión	Fecha de Actualización	Elaborado	Políticas Relacionadas	Áreas Afectadas	Responsables de cumplimiento	Existe Evidencia		Observación
												SI	NO	
1	MPP.2012.RIES.003.04	MPP - SI	Seguridad lógica	Política de seguridad de cuentas de usuario (PO-001)	Esta política define las reglas que controlan la creación y mantenimiento de cuentas de acceso a los sistemas críticos de la empresa CONECTA RETAIL S.A.	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Políticas de asignación y custodia de claves de usuario (PO-002) *Política de asignación y custodia de claves administradoras (PO-003)	*Todos los empleados de la empresa CONECTA RETAIL S.A.C, con cuentas de usuario en los sistemas críticos. *Usuarios externos que deban acceder temporalmente según sistemas transaccionales de la empresa CONECTA S.A.	Sistemas y Riesgos.	x		Esta política abarca los sistemas críticos de CONECTA S.A.C. que requieran la creación de cuentas de acceso
2	MPP.2012.RIES.003.04	MPP - SI	Seguridad lógica	Política de asignación y custodia de claves a Usuari	Esta política define las reglas de custodia de claves de acceso otorgadas a usuarios de los sistemas críticos de	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Políticas de seguridad de cuentas de usuario (PO-001) *Política de asignación y custodia de claves	*Sistemas, Riesgos y todos los empleados de efectiva que custodian uno o más claves de acceso a los sistemas con los que se trabaja en la empresa	Sistemas y Riesgos.	x		Esta política define la custodia de claves de usuarios, incluye los usuarios de la empresa CONECTA S.A. tengan

				os (PO -002)	CONECTA RETAIL S.A.				administradoras (PO-003)				claves de usuario.
3	MPP.2012.RIES.003.04	MPP - SI	Seguridad lógica	Políticas de asignación y custodia de claves administradoras (PO-003)	Esta política define las reglas que controlan la asignación y custodia de claves cuyo usuario tiene acceso limitado a un sistema operativo, una base de datos o una aplicación y que son indispensables para instalar o modificar características fundamentales al sistema que controlan	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Políticas de seguridad de cuentas de usuario (PO-001) *Política de asignación y custodia de claves administradoras (PO-003)	*Sistemas, riesgos, gerencia general	Sistemas y Riesgos.	**x**		Esta política abarca todos los recursos informáticos de la empresa CONECTA RETAIL S.A. Y aquellos usuarios que son definidos implícitamente en los sistemas y que sirve para realizar instalaciones de software, administrar sistemas, asignar roles, etc.

4	MPP.2012.RIES.003.04	MPP - SI	Seguridad de Personal	Política de uso de computadoras personales (PO-004)	Esta política define las reglas del uso de computadoras personales por parte de los empleados de la empresa CONECTA RETAIL S.A.	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Política del uso de computadoras portátiles (PO-005) *Políticas del uso de internet (PO-006) *Políticas de seguridad de recursos humanos (PO-007) *Políticas de capacitación en temas de seguridad (PO-008)	*Todos los empleados con accesos a computadoras personales.	Sistemas y Riesgos.	**x**		Está terminantemente prohibido enviar al exterior de la empresa (dispositivos) información relativa a las operaciones relacionadas a los clientes de la empresa CONECTA RETAIL S.A y documento.
5	MPP.2012.RIES.003.04	MPP - SI	Seguridad de Personal	Políticas de uso de computadoras portátiles (PO-005)	El uso de computadoras portátiles aplica a todo el personal previamente aprobado por su gerencia de área y validado por la gerencia de sistemas.	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Política del uso de computadoras personales (PO-004) *Políticas del uso de internet (PO-006) *Políticas de seguridad de recursos humanos (PO-007) *Política de compra de laptops.	*Todos los empleados (gerentes y jefes de área) con acceso a computadoras portátiles y personal que por motivos de viajes se le asigne una laptop del área de sistemas.	Sistemas y Riesgos.	**x**		El área de sistemas realiza periódicamente una revisión de los equipos portátiles asignados a trabajadores, registrando los estados de estos y el motivo del cambio.

6	MPP.2012.RIES.003.04	MPP - SI	Seguridad de Personal	Políticas de uso de internet (PO-006)	Esta política aplica a toda la red de la empresa CONECTA RETAIL S.A.	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Política del uso de computadoras personales (PO-004) *Política del uso de computadoras portátiles (PO-005) *Políticas de seguridad de recursos humanos (PO-007) *Políticas de capacitación en temas de seguridad (PO-008)	*Todas las áreas de la empresa	Sistemas y Riesgos.	**x**		Todos los usuarios de la empresa CONECTA RETAIL S.A.C., deben adaptarse a las reglas cuando necesiten conectarse a internet.
7	MPP.2012.RIES.003.04	MPP - SI	Seguridad de Personal	Política de seguridad de recursos humanos (PO-007)	Esta política define que todos los nuevos empleados, deben pasar un periodo de evaluación.	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Política del uso de computadoras personales (PO-004) *Política del uso de computadoras portátiles (PO-005) *Políticas del uso de internet (PO-006) *Políticas de capacitación en temas de	*Recursos humanos	Sistemas y Riesgos.	**x**		Se debe informar a cada empleado de los riesgos a los cuales el cargo a ser desempeñado está expuesto, y debe tomar las medidas para evitarlos.

								seguridad (PO-008)						
8	MPP.2012.RIES.003.04	MPP - SI	Seguridad de Personal	Política de capacitación en temas de seguridad (PO-008)	Esta política define las reglas, centradas en el tema de seguridad que deben ser consideradas en la capacitación y entrenamiento del personal	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Política del uso de computadoras personales (PO-004) *Política del uso de computadoras portátiles (PO-005) *Políticas del uso de internet (PO-006) *Políticas de seguridad de recursos humanos (PO-007)	*Recursos humanos y riesgo	Sistemas y Riesgos.	**x**		El área de riegos definirá la capacitación del personal involucrado en SI
9	MPP.2012.RIES.003.04	MPP - SI	Seguridad física y ambiental	Política de seguridad física en los centros de cómputo (PO-009)	Esta política está constituida por el conjunto de medios destinados a proteger a las personas, instalaciones, datos, equipos, suministros y	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Política de seguridad de redes (PO-010) *Políticas de conexión de terceros (PO-011)	*Riesgos y sistemas	Sistemas y Riesgos.	**x**		Esta política abarca todos los centros de cómputo de la empresa CONECTA RETAIL S.A.que cuentan con servidores y

					muebles que constituyen los recursos fundamentales para el proceso de la información computarizada.								controladores de comunicaciones para el desarrollo de la información.
10	MPP.2012.RIES.003.04	MPP - SI	Seguridad física y ambiental	Política de seguridad de redes (PO-010)	Esta política define las reglas y criterios de seguridad que deben estar presentes en la red, protege la integridad y asegura la estabilidad de la red operada por la empresa RETAIL S.A.	1	22/10/2012	Gerente de Riesgos /Gestión de ingeniería de Procesos	*Política de seguridad física en los centros de cómputo (PO-009) *Políticas de conexión de terceros (PO-011)	*Riesgos y sistemas	Sistemas y Riesgos.	**x**		Adaptable a todas las áreas de la empresa CONECTA RETAIL S.A. que usa los servicios tecnológicos de la empresa.

Matriz de Políticas de la Empresa CONECTA RETAIL S.A. Elaboración propia

Reporte de similitud

NOMBRE DEL TRABAJO

Diseño de un Modelo de Auditoría de TI p ara el Cumplimiento de Normas y Políticas de una Empresa Ret

AUTOR

Marry Cecy / Omar Alberto Rabanal Sen mache / Sánchez Rubio

RECUENTO DE PALABRAS

22833 Words

RECUENTO DE CARACTERES

122425 Characters

RECUENTO DE PÁGINAS

119 Pages

TAMAÑO DEL ARCHIVO

3.7MB

FECHA DE ENTREGA

May 9, 2024 9:50 PM GMT-5

FECHA DEL INFORME

May 9, 2024 9:51 PM GMT-5

6% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 4% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 4% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)