UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS:

Auditoría interna basada en Cobit 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti, Lima 2023

Para optar el título profesional de:
INGENIERO DE SISTEMAS

PRESENTADO POR:
Bach. Yatsen QUISPE REYES

ASESOR:
Mg. Richard ZAPATA CASAVERDE

AYACUCHO - PERÚ

2024

DEDICATORIA

Dedico este mi trabajo de investigación a mis padres por encaminarme en mi proceso de formación y en mi desarrollo profesional, por estar siempre apoyándome y dándome muchas fuerzas. A Dios por siempre iluminarme y guiarme en toda mi vida.

AGRADECIMIENTO

Agradecer a todos los docentes de la UNSCH de la Escuela profesional de Ingeniera de sistemas por aportar en mi formación profesional y en los conocimientos adquiridos a lo largo de mi estudio universitario y agradecerle siempre a Dios por darme mucho conocimiento y darme el camino adecuado en todo mi proceso de formación.

RESUMEN

El presente proyecto de Auditoría Interna se realizó en la Infraestructura Informática GRUPO TECNOLÓGICO ALINTI, Calle José Neyra 365 urbanización la calera de la Merced Surquillo, tuvo como objetivo analizar la situación actual de las tecnologías de información, enfocándose en la auditoría interna y la infraestructura tecnológica de la Organización para detectar las principales debilidades y fortalezas.

Se desarrolló la auditoria y se considera como base los directrices general de COBIT 5.0, se efectuaron visitas a las instalaciones, Se llevaron a cabo encuestas y entrevistas de personal. Esta metodología también proporciona métodos y mediciones, Sin embargo, no establece procedimientos detallados no es radical, más bien tolerante y recomienda además otras normas o marcos, describir las conclusiones y recomendaciones de cada uno de los 17 componentes presentes en la colaboración fue una gran contribución para la organización, puesto que era posible señalar las desventajas existentes que beneficiaron a la compañía para aumentar la seguridad en la Infraestructura tecnológica.

Palabras claves: Auditoría interna basada en cobit 5, infraestructura informática seguridad

ABSTRACT

This Internal Audit project was conducted in the IT Infrastructure of GRUPO TECNOLÓGICO ALINTI, Calle José Neyra 365 urbanización la calera de la Merced Surquillo, with the objective of analyzing the current situation of information technology, focusing on internal audit and the technological infrastructure of the organization to detect the main weaknesses and strengths.

The audit was developed based on the general guidelines of COBIT 5.0, visits were made to the facilities, surveys and staff interviews were conducted. This methodology also provides methods and measurements, however, does not establish detailed procedures is not radical, rather tolerant and also recommends other standards or frameworks, describe the conclusions and recommendations of each of the 17 components present in the collaboration was a great contribution to the organization, since it was possible to point out the existing disadvantages that benefited the company to increase security in the technological infrastructure.

Keywords: Internal audit based on cobit 5, IT infrastructure security.

CONTENIDO

DEDICATORIA ii

AGRADECIMIENTO iii

RESUMEN iv

ABSTRACT v

CONTENIDO vi

ÍNDICE DE TABLA x

INTRODUCCIÓN xiv

CAPÍTULO I 17

PLANTEAMIENTO DE PROBLEMA 17

1.1. DIAGNOSTICO Y ENUNCIADO DEL PROBLEMA 17

1.2. FORMULACION DEL PROBLEMA DE INVESTIGACIÓN 17

1.2.1. PROBLEMA PRINCIPAL 17

1.2.2. PROBLEMA SECUNDARIO 17

CAPITULO II 19

OBJETIVO DE LA INVESTIGACIÓN 19

1.3. OBJETIVO GENERAL 19

1.4. OBJETIVO ESPECÍFICO 19

CAPITULO III 20

JUSTIFICACIÓN Y DELIMITACIÓN DE LA INVESTIGACIÓN 20

1.5. JUSTIFICACIÓN E IMPORTANCIA 20

1.5.1. JUSTIFICACIÓN 20
1.5.2. IMPORTANCIA DEL TEMA 21
1.6. DLIMITACIÓN 21
CAPITULO IV 22
VARIABLES E INDICADORES 22
1.7. DEFINICIÓN CONCEPTUAL DE LA VARIABLE 22
1.8. DEFINICIÓN OPERACIONAL 23
CAPITULO V 24
MARCO DE REFERENCIA DE LA INVESTIGACIÓN 24
1.9. ANTECEDENTES 24
Antecedentes Internacionales 24
Antecedentes Nacionales 25
1.10. MARCO TEÓRICO 28
1.10.1. AUDITORIA 28
1.10.2. AUDITORIA INTERNA 29
1.10.3. AUDITORIA INFORMÁTICA 30
1.10.4. SEGURIDAD FÍSICA 31
1.10.5. IMPORTANCIA DE SEGURIDAD FÍSICA 31
1.10.6. SEGURIDA LÓGICA 32
1.10.7. RIESGO 32
1.10.8. ANÁLISIS DE RIESGO 32
1.10.9. COBIT 33

1.10.10. COBIT 5 36
1.10.11. DOMINIO DE COBIT 5 37
1.10.12. PROCESOS DE COBIT 38
1.10.13. NORMA ISO 43
1.10.14. NORMA TÉCNICA PERUANAS EN AUDITORIA DE LA INFORMACIÓN 46
CAPITULO VI 47
METODOLOGÍA DE LA INVESTIGACIÓN 47
1.11. TIPO DE INVESTIGACIÓN 47
1.12. NIVEL DE INVESTIGACIÓN 47
1.13. DISEÑO DE INVESTIGACIÓN 47
1.14. POBLACIÓN Y MUESTRA 47
1.14.1. POBLACIÓN 47
1.14.2. MUESTRA 47
1.15. TÉCNICAS E INSTRUMENTOS PARA RECOLECIÓN DE DATOS 47
1.15.1. TÉCNICAS 47
1.15.2. INSTRUMENTOS 47
1.16. HIPÓTESIS DE LA INVESTIGACIÓN 48
1.17. PLAN DE AUDITORÍA 48
4.1. ALCANCE 49
4.2. GUIA DE AUDITORÍA 51
4.3. EVALUACIÓN DE CONTROLES 62

4.4. TÉCNICAS Y ANÁLISIS DE PROCESAMIENTOS DE DATOS 62

CAPITULO VII 63

RESULTADO Y DISCUSIÓN 63

4.5. RESULTADO 63

4.5.1. HALLAZGOS DE LA AUDITORÍA INTERNA 63

4.5.2. FASE DE EVALUACIÓN DE RIESGOS Y CONTROLES 77

4.6. DISCUSIÓN 97

CAPITULO VIII 99

CONCLUSIONES Y RECOMENDACIONES 99

4.7. CONCLUSIONES 99

4.8. RECOMENDACIONES 101

REFERENCIA BIBLIOGRÁFICA 102

ANEXOS 106

ANEXO A 106

ANEXO B 107

ANEXO C 108

ANEXO D 110

ANEXO E 111

ANEXO F 114

ÍNDICE DE TABLA

Tabla N°1.-Tipos de auditoria *28*

Tabla N°2.- Plan de auditoria *49*

Tabla N°3.-Guía de Auditoria (Componente 1) *51*

Tabla N°4.-Guía de Auditoria (Componente 2) *51*

Tabla N°5.-Guía de Auditoria (Componente 3) *52*

Tabla N°6.-Guía de Auditoria (Componente 4) *52*

Tabla N°7.-Guía de Auditoria (Componente 5) *53*

Tabla N°8.-Guía de Auditoria (Componente 6) *53*

Tabla N°9.- Guía de Auditoria (Componente 7) *54*

Tabla N°10.-Guía de Auditoria (Componente 8) *54*

Tabla N°11.-Guía de Auditoria (Componente 9) *55*

Tabla N°12.-Guía de Auditoria (Componente 10) *55*

Tabla N°13.- Guía de Auditoria (Componente 11) *56*

Tabla N°14.-Guía de Auditoria (Componente 12) *56*

Tabla N°15.-Guía de Auditoria (Componente 13) *57*

Tabla N°16.-Guía de Auditoria (Componente 14) *57*

Tabla N°17.-Guía de Auditoria (Componente 15) *58*

Tabla N°18.-Guía de Auditoria (Componente 16) *58*

Tabla N°19.-Guía de Auditoria (Componente 17) *59*

Tabla N°20.-Guía de Auditoria (Componente 18) *59*

Tabla N°21.-Guía de Auditoria (Componente 19) *60*

Tabla N°22.-Guía de Auditoria (Componente 20) *60*

Tabla N°23.-Guía de Auditoria (Componente 21) *61*

Tabla N°24.-Guía de Auditoria (Componente 22) *61*

Tabla N°25.-Guía de Auditoria (Componente 23) *62*

Tabla N°26.-Hallazgo de Auditoria (Componente 1) *63*

Tabla N°27.-Hallazgo de Auditoria (Componente 2) *64*

Tabla N°28.-Hallazgo de Auditoria (Componente 3) *64*

Tabla N°29.-Hallazgo de Auditoria (Componente 4) *65*

Tabla N°30.-Hallazgo de Auditoria (Componente 5) *65*

Tabla N°31.-Hallazgo de Auditoria (Componente 6) *66*

Tabla N°32.-Hallazgo de Auditoria (Componente 7) *66*

Tabla N°33.-Hallazgo de Auditoria (Componente 8) *67*

Tabla N°34.-Hallazgo de Auditoria (Componente 9) *67*

Tabla N°35.-Hallazgo de Auditoria (Componente 10) *68*

Tabla N°36.-Hallazgo de Auditoria (Componente 11) *68*

Tabla N°37.-Hallazgo de Auditoria (Componente 12) *69*

Tabla N°38.- Hallazgos de auditoría (componente 13) *69*

Tabla N°39.- Hallazgo de Auditoria (Componente 14) *70*

Tabla N°40.- Hallazgo de Auditoria (Componente 15) *70*

Tabla N°41.-Hallazgo de Auditoria (Componente 16) *71*

Tabla N°42.-Hallazgo de Auditoria (Componente 17) *71*

Tabla N°43.-Hallazgo de Auditoria (Componente 18) *72*

Tabla N°44.-Hallazgo de Auditoria (Componente 19) *73*

Tabla N°45.-Hallazgo de Auditoria (Componente 20) *73*

Tabla N°46.-Hallazgo de Auditoria (Componente 21) *74*

Tabla N°47.-Hallazgo de Auditoria (Componente 22) *74*

Tabla N°48.- Plan de Acción *75*

Tabla N°49.-Matriz de análisis de riesgos de la infraestructura de la oficina de informática *77*

Tabla N°50.-Matriz de análisis de riesgos de la infraestructura de la empresa del Grupo Tecnológico Alinti 77

Tabla N°51.-Matriz de análisis de riesgo de equipos de cómputo de la oficina de informática 78

TABLA N°52.- Análisis de riesgos de todos los componentes evaluados 79

..... 79

Tabla N°53.-Evaluación controles 80

Tabla N°54.- Lista de equipos 81

Tabla N°55.-Auditoria y planificación 82

Tabla N°56.-Planificaacion estratégica 83

Tabla N°57.-Politicas de información interna 84

Tabla N°58.-Tecnologías de información 85

Tabla N°59.-Medidas de seguridad 86

Tabla N°60.-Usuarios con contraseña 87

Tabla N°61.- Protección de herramientas 88

Tabla N°62.- Plan de contingencia 89

Tabla N°63.-Plan de restablecimiento 90

Tabla N°64.-Reubicacion de servidores 91

Tabla N°65.-Presupuesto para TI 92

Tabla N°66.-Almacen de equipos informáticos usados 93

Tabla N°67.-Control de TI 94

Tabla N°68.-Plan de acción en TI 95

Tabla N°69.-Sotfware libre 96

ÍNDICE DE FIGURAS

Figura 01: Evaluación del COBIT 5 ..... *36*

Figura 02: Business framework *37*

Figura 03: Dominios *38*

Figura 04: Procesos *43*

Figura 05: Áreas claves de Gobierno y la Gestión *45*

Figura 06: Principios de COBIT *46*

Figura 07: Análisis de riesgos de todos los componentes evaluados *79*

Figura 08: Auditoria y planificación *82*

Figura 09: Planificación estratégica *83*

Figura 10: Políticas de información interna *84*

Figura 11: Tecnología de información *85*

Figura 12: Medidas de seguridad *86*

Figura 13: Usuarios con contraseñas *87*

Figura 14: Herramientas de protección *88*

Figura 15: Plan de contingencia *89*

Figura 16: Plan de restablecimiento *90*

Figura 17: Reubicación de servidores *91*

Figura 18.- Presupuesto para TI *92*

Figura 19: Almacén de equipos informáticos usados *93*

Figura 20: Control de TI *94*

Figura 21: Plan de acción en TI *95*

Figura 22: Software libre *96*

INTRODUCCIÓN

En la era digital de hoy, las empresas confían mucho en sus sistemas y tecnologías de la información para funcionar con eficiencia y competitividad. La infraestructura informática es un componente crítico que soporta estos sistemas y, por lo tanto, requiere disposiciones de seguridad adecuadas a fin de salvaguardar la integridad, confidencialidad y disponibilidad de las informaciones y recursos tecnológicos.

Una de las áreas clave es la seguridad física de la seguridad informática que comprende los controles y mecanismos implementados para salvaguardar los activos físicos, como servidores, equipos de red, centros de datos e instalaciones, de amenazas potenciales como acceso no autorizado, desastres naturales, sabotaje o vandalismo. Una brecha en la seguridad física puede acarrear graves consecuencias, la pérdida de información valiosa, interrupciones en las operaciones o incluso daños irreparables a la infraestructura.

En este contexto, la auditoría interna desempeña un rol importante al haber evaluado la eficacia en los controles de seguridad física y proporcionado recomendaciones para fortalecer las áreas débiles. El marco de trabajo COBIT 5 (Objetivos de Control para la Información y Tecnologías Relacionadas) ofrece una guía integral para la Administración y gestión de las tecnologías de información, incluyendo prácticas y controles específicos para la seguridad física.

El Grupo Tecnológico Alinti, una compañía líder en el rubro de TI en Lima, reconoce la importancia crítica de proteger su infraestructura informática y garantizar la continuidad de sus operaciones. Por lo tanto, surgió haber evaluado los resultados de la auditoría interna basada en COBIT 5 para el control de la seguridad física de su infraestructura informática.

Los objetivos de la investigación descriptiva son, principal determinar cómo los resultados de la auditoría interna basada en COBIT 5 contribuyen al control efectivo de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti. Además, se analizaron dimensiones clave como la seguridad física, la infraestructura informática y los sistemas core de la organización, con el propósito de detectar dependencias de mejora y proponer recomendaciones para reforzar la seguridad y atenuar los riesgos. asociados.

Los resultados de este han beneficiado no solo para el Grupo Tecnológico Alinti, sino también para otras organizaciones que buscan implementar mejores prácticas de auditoría interna y controles de seguridad física para salvaguardar su infraestructura informática y proteger sus operaciones críticas.

CAPÍTULO I

PLANTEAMIENTO DE PROBLEMA

1.1. DIAGNÓSTICO Y ENUNCIADO DEL PROBLEMA

Actualmente la confidencialidad de los datos en las organizaciones va aumentando considerablemente y se hace más primordial puesto que se dedica a salvaguardar datos de los usuarios y organizaciones, la infraestructura y todo referido a la tecnología de la información. Por eso la auditoría Interna es una excelente herramienta que administra TI, aplicar normas, reglas, manuales, leyes, para disminuir inseguridades potenciales de seguridad en los recursos de TI.

La utilización de la tecnología en el Perú ha hecho posible la identificación de las necesidades de optimización y actualización. las diferentes medidas para un mayor control de los datos valiosos que deben mantenerlo seguro, distanciar o reducir al mínimo las inseguridades de los atacantes informáticos, es por eso que realizan una auditoría. Interna en la Infraestructura Informática del GRUPO TECNOLÓGICO ALINTI.

La Oficina de Informática del GRUPO TECNOLÓGICO ALINTI no ha realizado ninguna auditoría Interna que identifique los riesgos y peligros que afectan la seguridad de la información, la auditoría es importante dado que un descuido en la tecnología de la información y las comunicaciones implicaría la debilidad a los ataques informáticos y, sin duda, los datos serían muy fácil a cualquier ataque.

1.2. FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN

1.2.1. PROBLEMA PRINCIPAL

¿Cuáles son los resultados de la auditoría interna basada en Cobit 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti, Lima 2023?

1.2.2. PROBLEMA SECUNDARIO

a) ¿Cuáles son los resultados de la planeación y organización de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti?

b) ¿Cuáles son los resultados del proceso de ejecución de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti?

c) ¿Cuáles son los resultados de la evaluación de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti?

CAPITULO II

OBJETIVO DE LA INVESTIGACIÓN

1.3. OBJETIVO GENERAL

Determinar los resultados de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti, Lima 2023.

1.4. OBJETIVO ESPECÍFICO

a) Identificar los resultados de la planeación y organización de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti.

b) Describir los resultados del proceso de ejecución de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti.

c) Determinar los resultados de la evaluación de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti.

CAPITULO III

JUSTIFICACIÓN Y DELIMITACIÓN DE LA INVESTIGACIÓN

1.5. JUSTIFICACIÓN E IMPORTANCIA

1.5.1. JUSTIFICACIÓN

Perspectiva Teórica: debido a que toma como fundamento las teorías y sustento, en la actual investigación que lograron aportar al tema de estudio, con el fin de proporcionar conocimiento científico sobre la variable de estudio y un enfoque especializado para evaluar y fortalecer los sistemas de gestión interna en el medio tecnológico de una auditoría interna La Oficina podrá elaborar esa propuesta metodológica de Infraestructura informática disponer de un marco de referencia para llevar a cabo las auditorías de un modo más organizado. obteniendo informes previos pertinentes y coherentes, con la proyección de un informe final de auditoría con la fuente en la propuesta metodológica y los informes previos pertinentes y coherentes no incurra en errores, realice una buena gestión documentadas de los sistemas de información y tecnologías en todo ALINTI, y las recomendaciones la OTI haga un magnífico deber de servicios de los sistemas y tecnología de información. Así mismo, se espera, el resultado de esta investigación, que oriente a la Oficina de Tecnología de información del Grupo Tecnológico ALINTI y, sobre todo, a los especialistas en auditorías interna, que con esta herramienta les permita visualizar los procedimientos, técnicas y métricas de cada labor y, organizados en una estructura de cuatro fases relacionados, podrán elaborar satisfactoriamente el informe de auditoría.

Perspectiva Práctica: porque proporcionar un marco de trabajo efectivo para identificar vulnerabilidades, implementar medidas de seguridad y mitigar posibles riesgos en la infraestructura tecnológica. Esta perspectiva práctica destaca la relevancia de aplicar enfoques especializados de auditoría para garantizar la integridad y disponibilidad de los recursos tecnológicos del Grupo Tecnológico, asegurando su continuidad operativa y protección ante amenazas internas y externas.

Perspectiva Metodológica: esto justifica al ofrecer un enfoque estructurado y detallado para evaluar los controles de seguridad física, identificar posibles brechas y propone soluciones efectivas para fortalecer la protección de la infraestructura tecnológica. Esta perspectiva metodológica enfatiza la importancia

de utilizar herramientas y técnicas especializadas para llevar a cabo una auditoría completa y precisa que garantice la seguridad y confidencialidad de los datos en el entorno tecnológico del Grupo Tecnológico.

Perspectiva Social: el desarrollo del análisis beneficiara a muchas empresas, tanto públicas y privadas, porque va promover la confianza, la transparencia y la responsabilidad en la gestión de la seguridad de la información en el sector tecnológico y actualmente es una necesidad para realizar auditoría elaborados en las entidades públicas y privadas, de esta manera, los expertos tendrán en menor las dificultades al momento de hacer un examen de auditoría interna. Esta perspectiva social destaca el impacto positivo de una auditoría interna especializada en la protección de la infraestructura informática, no solo para el Grupo Tecnológico ALINTI Lima 2023, sino también para la sociedad en su conjunto al salvaguardar la integridad y recursos de los servicios tecnológicos ofrecidos.

1.5.2. IMPORTANCIA DEL TEMA

La auditoría interna de COBIT 5 en la empresa del grupo tecnológico ALINTI es de bastante importancia, con este proyecto de investigación se ha dado iniciativa en el desarrollo de una Auditoría Interna basada en COBIT 5 para el control de la seguridad física de la Infraestructura informática

1.6. DELIMITACIÓN

La investigación se realizó en la empresa tecnológico grupo ALINTI para el año 2024.

CAPITULO IV

VARIABLES E INDICADORES

1.7. DEFINICIÓN CONCEPTUAL DE LA VARIABLE

Variable de estudio: Auditoría Interna basada en COBIT 5

1.8. DEFINICIÓN OPERACIONAL

Variable	Definición Conceptual	Definición operacional	Dimensiones	indicadores	Escala de Medición
Auditoría Interna basada en COBIT 5	La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta que busca agregar valor y mejorar las actividades de una organización. Asiste a cumplir metas mediante un enfoque sistemático y disciplinado en la evaluación y mejora de la eficacia de los procesos de manejo de riesgo, control y gobierno. (Instituto de Auditores Internos, 2023)	Se evaluará la auditoría interna a través de un conjunto de procedimientos que incluyen la planeación y organización de la auditoría interna, proceso de ejecución de la auditoría interna y la evaluación de la auditoría interna según las mejores prácticas.	Planeación y organización de Auditoría Interna	Efectividad de os procesos de plan	Escala de cumplimiento: 1. Muy bajo 2. Bajo 3. Moderado 4. Alto 5. Muy alto
				Calidad de la información recopilada	
				La eficiencia en la detección de irregularidades	
			Proceso de ejecución de la Auditoría Interna	Cumplimiento de los procedimientos establecidos	
				La gestión de recursos	
				La eficacia en la identificación de hallazgos	
			Evaluación de la Auditoría Interna	Precisión de los informes de auditoria	
				La adherencia a estándares éticos y normativas	
				La efectividad de las recomendaciones	

Nota. Elaboración propia

CAPITULO V

MARCO DE REFERENCIA DE LA INVESTIGACIÓN

1.9. ANTECEDENTES

Antecedentes Internacionales

(Vargas et al.,2023) en su Investigación “Plan De Auditoría Para El Programa De Auditoría Interna Al Sistema De Gestión De Calidad De La Empresa Carnitas”. La investigación de este articulo tiene el propósito del estudio que fue determinar la aptitud de las auditorías internas para todas las entidades, evaluando el alcance, criterios, equipo auditor, labores o procedimientos, observaciones, fecha y hora de la auditoría, factores que deben permanecer constantes para evaluar la eficacia del SGA de la organización.

Se evalúa el sistema HACCP de la organización «Carnecitas» para desarrollar la actividad final sugerida en el diplomado. Posteriormente se realiza un programa de auditoría utilizando una herramienta basada en la norma ISO 19011:2018. Una vez decidido el programa de auditoría, se pasa al proyecto de un plan de auditoría, usando como técnica tablas, donde se determinan los hallazgos de la auditoría, señalando a su vez el hallazgo hallado.

Tras la auditoría de comprobación del sistema HACCP de la entidad “Carnecitas” se da las los resultados para que la entidad empiece a aplicar las acciones correctivas, para la mejorar el fortalecimiento de los procesos internos.

(Flores et al.,2023) en su Investigación “La auditoría interna en las entidades públicas y privados de Ecuador “. La investigación de este articulo tiene los principales objetivos de las auditorías internas en Ecuador se han reorientado como resultado de la investigación, lo que repercute en el fomento de un entorno de control positivo en el sector público. El objetivo del estudio fue conocer las variaciones en las prácticas de auditoría interna entre las organizaciones ecuatorianas del sector público y privado, con el fin de potenciar las funciones de los auditores internos. El enfoque empleado fue descriptivo, cualitativo y explicativo; se basó en el juicio profesional, la observación y artículos científicos, leyes, normas y reglamentos aplicables al tema de estudio. Los resultados de los informes de auditoría interna deben darse a conocer en términos de control interno sin funciones administrativas, y la auditoría externa debe proceder de conformidad con la Ley Orgánica de la Contraloría General del Estado, realice el seguimiento de la misma y del incumplimiento se deriven las sanciones que correspondan.

(Miranda y Jiménez, 2021). En su Investigación” Auditoría interna en el marco de la empresa privada costarricense “. El estudio de la gestión de riesgos, el gobierno corporativo, las auditorías internas y externas, y el control interno se ha desarrollado

en un esfuerzo por encontrar formas eficaces de apoyar el consigo de los objetivos de la entidad. El objetivo principal es conocer la opinión de la comunidad empresarial del país sobre la necesidad de los servicios de auditoría interna.

(Corzo , 2023). En su Investigación “Propuesta de mejora al proceso de auditoría interna para el SG-SST de la empresa DEFENDER LTDA bajo la ISO 45001:2018 “. La investigación de este articulo tiene el fin de evaluar el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) de la empresa DEFENDER LTDA en cumplimiento de los requisitos de la NTC ISO 45001:2018, fue necesario implementar un instrumento de auditoría interna. Con el objetivo de hacer un análisis inicial y aplicar un instrumento de control y seguimiento, la investigación para esta actividad se realizó bajo la metodología de investigación para el fortalecimiento corporativo. El resultado fue un índice de cumplimiento total del 62%, debido principalmente a que gran parte de la documentación existe, pero debe actualizarse o ser objeto de seguimiento de las labores. Para ello se ha formado un informe de la auditoría interna en el cual se explican recomendaciones, las cuales se espera sean oportunidades de mejorías propias para el sistema.

(Fahl y Amaral, 2023). En su Investigación “Servicio de diseño como enfoque de innovación en auditoría interna de entidades financieras “. La investigación de este artículo pretende examinar la idoneidad de las metodologías de Diseño de Servicios para su uso en unidades de Auditoría Interna (AI) de Instituciones Financieras (IF). Se parte del supuesto de que las unidades de AI son prestadoras de servicios, que ocupan una posición estratégica dentro de las organizaciones que es pertinente a su trabajo y que aportan conocimiento a los procesos de las áreas auditadas. La metodología de trabajo se basa en una investigación bibliográfica, con revisión bibliográfica sobre el tema, para la fundamentación técnica y automatización de los datos. Para recopilar la información, se realizó un estudio exploratorio utilizando la plataforma ScienceDirect, artículos de congresos y material complementario de portales de las entidades expertas en auditoría interna. Al analizar los datos se tuvo en cuenta el marco de las teorías de diseño de servicios y su adhesión a los procesos de AI. Como resultado, se confirmó la utilidad del Design Service -un enfoque iterativo- en relación con el establecimiento de nuevos procesos, herramientas y metodologías, acciones estratégicas de AI y nuevos diseños de servicios que sirvan de catalizadores para la creación de valor para los usuarios de servicios de AI.

Antecedentes Nacionales

(Gutiérrez, 2022). En su Investigación” La auditoría interna como control para la gestión de medianas y grandes empresas de construcción”. El objetivo principal del estudio fue inspeccionar el impacto de la aplicación de la auditoría interna como

control en la mejora de las prácticas de trabajo en las medianas y grandes entidades de construcción que operan en el distrito de Los Olivos. La metodología de investigación incluyó un enfoque cuantitativo, explicativo y descriptivo. La población fue de 330 personas y la muestra de 178. El cuestionario sirvió como instrumento y la encuesta sirvió como técnica. fue la encuesta, y el cuestionario validado sirvió de instrumento. Los datos se analizaron mediante métodos estadísticos. Fue factible extraer la conclusión de que las prácticas eficaces de auditoría interna como control, incide en la optimización de la gestión de medianas y grandes organizaciones del sector constructivo en el Distrito de Los Olivos. De esta manera, se puntualizó que se viene realizando el sistema de auditoría interno, y se confirmó que éste se desarrolla de manera inoportuna.

(Alzamora y Palomino , 2023). En su Investigación “Auditoría Interna y Gestión de Riesgos en las Cooperativas de Ahorro y Crédito de la Ciudad de Abancay, 2021”. La investigación en el año 2021, se llevó a cabo una investigación cuyo objetivo primordial fue establecer en qué medida la gestión de riesgos y la auditoría interna están relacionadas en las cooperativas de ahorro y crédito de Abancay. El tipo de investigación que se realizó fue de tipo fundamental y se categorizó como correlacional. Para realizar el estudio se empleó un diseño no experimental con un alcance transversal. Trescientos diecinueve trabajadores de siete cooperativas de ahorro constituyeron la población de estudio. Para recoger los datos necesarios se eligió una muestra probabilística de 175 trabajadores. El instrumento de recogida de datos fue un cuestionario sometido a pruebas estadísticas de fiabilidad y validación por expertos. Los resultados descriptivos mostraron que tanto la gestión de riesgos como la auditoría interna se consideraban excelentes. Además, se descubrió una asociación moderada. Además, se descubrió una asociación razonable entre la gestión de riesgos y auditoría interna, con un valor obtenido de 0,685. La conclusión más optima del estudio señalo que la auditoría interna se unió de manera representativa con la gestión de riesgos en las cooperativas de ahorro y crédito de la ciudad de Abancay.

(Tello, 2023) . En su Investigación” TRANSFORMACIÓN DIGITAL EN EL MANEJO DE LA INFORMACIÓN EN LAS AUDITORÍAS DE IMPLICANCIA CONTABLE EN ELPERÚ, 2022”. El objetivo del presente proyecto de estudio es concientizar sobre la importancia de la transformación digital en curso y cómo afecta al trabajo de auditoría contable en el sector privado. La dificultad se desarrolló en el ambiente de la pandemia de COVID-19, que alteró fundamentalmente nuestra forma de conectarnos y comprender el mundo y desencadenó la transformación digital global. El estudio emplea una metodología de participación-acción y un enfoque

cualitativo, lo que representa un método de investigación no experimental. Para ello, se examinó el corpus de investigación sobre el asunto y se ha hecho entrevista. A trabajadores con trayectoria en el rubro de la auditoría interna haciendo uso el muestreo no probabilístico u utilizando un criterio del investigador; el instrumento fue una ficha de entrevista realizado por el investigador y totalmente certificado, cuyos resultados fueron analizados y revisados adecuadamente para la realización de la tesis. Con los resultados se confirma que la transformación digital mejorará el desarrollo de los datos en las auditorías de inclinación en al ámbito de la contabilidad en el Perú.

(Avalos y Castillo, 2022). En su Investigación “Auditoría interna y gestión financiera en las empresas comerciales de Chimbote – 2021 “. La investigación en la presente investigación tuvo como objetivo general determinar la relación de la gestión financiera y la auditoría interna en los sectores comerciales de Chimbote - 2021. El estudio empleó una técnica transversal, correlacional, hipotético-deductiva, cuantitativa y un diseño no experimental. La técnica de encuesta se realizó a 130 empresas comerciales de Chimbote, de las cuales 97 proporcionaron información puntual sobre la situación de su empresa. El cuestionario demostró ser válido y confiable, como lo indica el índice alfa de Cronbach; los coeficientes para las variables auditoría interna y gestión financiera fueron de 0,977 y 0,904, respectivamente, lo que indica un alto nivel de correlación entre las variables. En consecuencia, la variable auditoría interna y la variable gestión financiera presentaron una correlación Rho de Spearman de 0,714. Además, el nivel de significación alcanzado en este caso fue de $p<0,001$, lo que significa que p es menor a 0,05, se concluye que existe correlación significativa entre la variable auditoría interna y la variable gestión financiera.

(Pinedo y Vilches, 2022). En su Investigación “Auditoría interna y gestión administrativa en la municipalidad provincial de Rioja, 2021 “La investigación se completó. El objetivo principal de la investigación fue conocer cómo se relacionan la auditoría interna y la gestión administrativa en la Municipalidad Provincial de Rioja, 2021.El enfoque utilizado para esta explicación fue transversal, descriptivo, correlacional y no experimental. En la muestra había cincuenta colaboradores municipales, de una población total de veintitrés.

A cada variable se le aplicó un cuestionario independiente, además de la prueba Rho de Spearman. Los resultados de la prueba de normalidad indicaron que existía normalidad. Sin embargo, la prueba estadística reveló que la significación bilateral estaba por debajo del margen de error. de error de 0,05 (0,000). Concluyendo que existe relación significativa entre la gestión administrativa y la auditoría interna en la Municipalidad Provincial de Rioja, 2021.

1.10. MARCO TEÓRICO

1.10.1. AUDITORIA

Es un examen cuyo objetivo, sistemático y profesional de los procedimientos realizadas para evaluarlas, comprobarlas y informar un informe con recomendaciones, recomendaciones y conclusiones (Aquino , Cuevas,Villarroel , 2023).

Es «una poderosa herramienta que permite la creación de valores y cultura organizacional, y por lo tanto permite supervisar y llevar el control interno de las demás dependencias» para ayudar a señalar las actividades de riesgo que ocurren al interior de la corporación. (Vilchez, 2023).

Describe detalladamente las funciones de una auditoría, enfocándote en la revisión de hechos, fenómenos y operaciones para asegurar su congruencia con lo planteado inicialmente, así como la observancia y respeto de políticas y instrucciones determinadas. Además, profundiza en la evaluación de la gestión y operación para ser optimo el uso de los recursos que estan disponibles (Mungabusi, 2021)

Estas dos definiciones nos brindan una comprensión fundamental sobre el concepto de auditoría, resaltando términos clave como supervisión, evaluación e identificación. Estos términos son cruciales para llevar a cabo adecuadamente las tareas inherentes a la actividad de auditoría de manera independiente.

Tabla N°1.-Tipos de auditoria

TIPO	DEFINICIÓN
Auditoria de Gestión y operación	Examina la efectividad, eficiencia, economía y naturaleza de una entidad en la formación de sus labores.
Auditorias Informáticas	Examina los medios de información y tecnologías.
Auditoria pública gubernamental	Se produce en organizaciones examinadoras en su grado alto, con el objeto de confirmar el desempeño de las labores administrativas y financieras.
Auditoria integral	Examina todos los datos financieros, estructuradas de la entidad, control interno, objetivos institucionales y base legal.
Auditorias forenses	Se implementa para aconsejar y averiguar estafas financieras y de moralidad.
Auditoria fiscal	Se examina la ejecución de los compromisos tributarios en las organizaciones

Auditoria financiera	Se examina el cumplimiento de los deberes tributarias en las organizaciones
Auditoría ambiental	Analiza las labores políticas y normativas ambientales con el objetivo de proteger la naturaleza
Auditoría interna	es un proceso mediante el cual una organización examina y evalúa de manera sistemática sus propios procedimientos y controles internos para asegurar que estén funcionando de manera eficaz. Su propósito es identificar áreas de mejora, confirmar el acatamiento de medidas, protocolos y instrucciones, y evaluar la eficiencia operativa, con el fin de fortalecer la gestión y reducir riesgos.
Auditoría externa	Es un examen autónomo ejecutado por alguien fuera a la entidad, con el propósito de revisar y evaluar la exactitud y la conformidad de los estados financieros y otros informes. Este proceso busca garantizar que la información financiera presentada sea veraz y cumpla con los estándares y regulaciones aplicables, proporcionando así una opinión imparcial sobre la integridad y la transparencia de la empresa.

Fuente: Elaboración propia con información (Urrutia, 2023)

1.10.2. AUDITORIA INTERNA

Según el investigador (Ramirez , 2023) la auditoría es una habilidad de evaluación. Cada auditoría tiene un centro de labor. Cada auditoría tiene una fin o plan. La evaluación se caracteriza por el hecho de que se basa en informes establecidos. La evaluación tiene como meta precisar la aprobación de lo evaluado frente a un criterio, mientras la auditoría se dirige sobre la aprobación de lo evaluado con respecto a un criterio, la evaluación ex post se restringe a dar a conocer su punto de vista sobre el acatamiento de los objetivos establecidas.

Según el investigador (Mungabusi, 2021) Mencionada, la auditoría interna se define como un proceso objetivo e independiente diseñado para aportar valor y optimizar las operaciones organizacionales mediante actividades de aseguramiento y consultoría.

Esta labor es llevada a cabo por especialistas que son trabajadores de la misma organización donde se realiza la auditoría. El resultado de su trabajo está orientado a satisfacer necesidades internas y brindar servicios a la entidad. La auditoría interna incluye diferentes tipos, tales como operativa, financiera y administrativa.

Dimensiones o indicadores:

Planeación y organización de Auditoría Interna: Para que un auditor interno pueda planificar su labor de manera apropiada, es fundamental que adquiera un conocimiento profundo sobre la organización, lo cual implica recopilar datos relevantes que le permitan comprender a cabalidad los sucesos, transacciones y prácticas que podrían tener una mayor relevancia en los estados financieros. Con el fin de llevar a cabo una planificación adecuada, el auditor interno debe recopilar información relacionada con diversos aspectos clave de la empresa. Esta recopilación de datos es un requisito indispensable para que el profesional pueda diseñar y realizarse un plan de auditoría efectivo a.

- La organización.
- Las necesidades de los ejecutivos.
- Las carencias de los auditores externos.
- Posibles eventualidades

  Según (Instituto de autores Internos, 2020).

Proceso de ejecución de la Auditoría Interna: El flujo de auditoría interna se basa en un conjunto organizado de etapas que incluyen la planificación, recolección y evaluación de evidencias, redacción de informes con hallazgos y observaciones y seguimiento de su implementación, con el fin de analizar la eficacia de los controles internos y fomentar. la mejora en el trámite según (Instituto de autores Internos, 2020).

Evaluación de la Auditoría Interna: Se refiere al análisis detallado de los procedimientos y controles dentro de una entidad, con el objetivo de optimizar su eficacia y eficiencia. Este proceso busca identificar oportunidades de mejora y asegurar que se alcancen los objetivos estratégicos, proporcionando recomendaciones fundamentadas según (Instituto de autores Internos, 2020).

1.10.3. AUDITORIA INFORMÁTICA

Dentro del marco de los componentes de control interno establecidos en una entidad, la auditoría desempeña un rol trascendental como componente clave. Su función primordial radica en proveer orientación y asesoramiento especializado a los máximos niveles de dirección. Esta asesoría abarca la identificación metódica de riesgos y áreas susceptibles de mejora, así como el diseño, puesta en marcha y mantenimiento continuo de sistemas de monitoreo y control en los ámbitos gerencial,

financiero, informático y operativo. El propósito ulterior es coadyuvar a que la organización alcance los resultados operacionales previstos, velando por el cumplimiento cabal de los objetivos estratégicos previamente delineados. En síntesis, las labores de auditoría representan un pilar medular para resguardar la integridad de los procesos organizacionales y garantizar su alineación con las metas establecidas (Ramirez , 2023).

La Auditoría informática hace conocimiento a la exploración práctica que se hace sobre los materiales de información que tiene una organización con el propósito de generar un informe sobre la situación en que se elaboran y se hacen uso de esos recursos (Carrera, 2019).'

Se trata de un procedimiento que llevan a cabo expertos del Área de Auditoría y Tecnologías de la Información y que está diseñado para confirmar y garantizar que las normas y directrices establecidas para la administración y el uso adecuado de la tecnología dentro de la empresa se siguen con prontitud y eficacia. (Núñez, 2022).

1.10.4. SEGURIDAD FÍSICA

Según (Chimbo y Narváez, 2022) menciona la seguridad como "El conjunto de estrategias de mitigación y prevenir las perdidas físicas a los sistemas de información y salvaguardar los datos acumulado en ellos

La debilidad externos a los que están expuestos los sistemas informáticos y las medidas preventivas que se pueden adoptar son los siguientes

- Anómalos naturales, como inundaciones, tormentas, terremotos, etc. Se pueden adoptar estrategias de mitigación como la instalación de los equipos en lugares adecuados dadas de las oportunas medidas de defensa.
- Peligros humanos, como actos inconscientes, actos atroces y desperfectos. Entre las estrategias de mitigación fueron: inspección de ingreso a datos personales, formación a usuarios en elemento de seguridad, etc.

Según (Encalada, 2023) .La auditoría en seguridad física es aquella labor que fiscaliza, identifica, evalúa, examina, investiga y recomienda, sobre el periodo de la actualidad en la seguridad en sus servicios básicos e infraestructura, sean estas institucionales, industriales, o de cualquier otra naturaleza.

1.10.5. IMPORTANCIA DE SEGURIDAD FÍSICA

Salvaguarda a los individuos y a la pertenencia de daños y robos. Estos son los medios por los cuales conserva la propiedad y la inspección sobre los bienes

tangibles e inmuebles. Sin seguridad física. Incluso la seguridad del individuo se pone en peligro. Esta es la acción de las necesidades humanas básicas

Son una mezcla de productos y métodos que comprimen la posibilidad de robo, daños y deterioros a la propiedad y los individuos. Si puedes tocarlo, puedes salvaguardar con seguridad física según (BLOG FETASA, 2024)

1.10.6. SEGURIDA LÓGICA

Según el autor (Encalada, 2023). Es el asunto mediante el cual se inspecciona y confirma aquellos accesos diseñados para proteger la integridad de la investigación acumulada en otros medios.

Al finiquitar cada auditoría presenta un informe con la estimación del contexto en cláusulas de seguridad, este se transforma en un instrumento, pues brinda a los dirigentes información precisa para la toma de decisiones.

1.10.7. RIESGO

Según (Instituto de autores Internos, 2020). Se describe a la posibilidad de que algunas actividades o condiciones puedan frenar que una empresa logre sus metas. Esto da a conocer un proceso de reconocimiento, observación y evaluación de riesgos que podrían chocar a las operaciones y procesos de la empresa La auditoría interna tiene como propósito inspeccionar estos riesgos para realizar controles que minimicen sus efectos, garantizando así la eficacia en el uso adecuado de recursos y el desempeño.

Según (Ramirez , 2023) Da conocer que un riesgo es un acontecimiento o conjunto de incidentes que pueden comprometer el proyecto de una empresa o impedir su triunfo. La explicación misma de riesgo siempre es discutida. Sin embargo, existe un convenio sobre las características comunes que deben tener todos los riesgos de tecnología de información:

- **Incertidumbre**: el incidente que caracteriza el peligro puede suceder o no, no existe seguridad sobre dicha actividad.
- **Perdida:** Si el riesgo se concretiza, habrá una serie de implicaciones negativas para la empresa. Si no hay resultados negativos, entonces no hay peligro.

1.10.8. ANÁLISIS DE RIESGO

Según el autor (Encalada, 2023) Este proceso metodológico goza de una amplia aceptación y es contemplado como un componente medular en el marco de ejecución de cualquier sistema de gestión orientado a resguardar la seguridad de la información dentro de una entidad. Su importancia radica en que permite cuantificar y establecer la relevancia que poseen los distintos activos de información para el

adecuado funcionamiento y protección de la organización. Los resultados obtenidos a partir de este riguroso análisis facultan a las áreas encargadas de la gestión de riesgos a recomendar e implementar las medidas de control y mitigación más idóneas para hacer frente a las amenazas identificadas, minimizando así el impacto potencial de cualquier incidente de seguridad.

Según el autor (Núñez, 2022) el estudio de peligros como el análisis que evalúa riesgos potenciales y hechos causales en un ambiente que existe o proyecto, con el centro de implantar controles de seguridad y de salvaguardar.

El recurso más conocido que se tenga son los datos y la IT, por lo tanto, deben existir métodos que asegure, lejos de la seguridad física que se ponga sobre los instrumentos en los cuales se reservar. Estos métodos brindan la seguridad lógica que consiste en la resistencia de barreras y procedimientos que protegen a los datos y únicamente permiten aceptar a ellos a los individuos autorizadas para hacerlo.

Existe un antiguo consejo en la seguridad informática que dicta: "lo que no está permitido debe estar prohibido" y ésta debe ser el objetivo logrado. Los fundamentos son:

- Prohibir el ingreso (de personal de la empresa y de las que pertenecen) a los programas y archivos.
- Garantiza que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no corresponden (sin una supervisión minuciosa).
- Garantice que se haga uso los datos, archivos y programas correctos en y por el procesamiento elegido.
- Garantiza que los datos transmitidos sean la misma que reciba el receptor al cual se ha enviado y que no le llegue a otro.
- garantizado que existen sistemas y pasos de emergencia alternativos de difusión entre distintos lugares.
- instaurar a cada 1 de los colaboradores por rango informático, con claves diferentes y permisos bien realizados, en todos y cada 1 de los sistemas o aplicaciones empleados.
- actualizar consta mente las contraseñas de acceso a los sistemas de cómputo.

1.10.9. COBIT

(Control Objectives for Information and Related Tecnology, Objetivos de Control para los Datos y Tecnologías Relacionadas) fue publicada en 1996 por el Instituto de Control de TI y la ISACA (Asociación de Auditoría y Control de Sistemas de Información) Según (Torres, 2022).

El Marco de trabajo COBIT es pequeño utilizado por un grupo estratégicos e individuos responsables de auditoría y desempeño para la ilustración de requerimientos, es decir es un marco de trabajo de gobernanza y tarea empresarial de tecnologías de información. Ayuda a los 27 gerentes a equilibrar riesgos. Los mecanismos de metodología COBIT son los siguientes Según (Torres, 2022).

- Marco: organizar y clasificar los objetivos del gobierno de tecnologías de información y las buenas prácticas de los dominios y procesos de tecnologías de información antes de asociarlos.
- Descripciones del proceso: hacer un proceso de referencia y de lenguaje común para todos en la entidad.
- Objetivos de control: hacer uso de los requisitos de alto nivel para un control efectivo de cada proceso de tecnologías de información.
- Directrices de gestión: determinar responsabilidades, acordar metas y medir el rendimiento e ilustrar la relación con otros procesos.
- Modelos de madurez: evaluar la madurez y la capacidad por proceso y ayudar a afrontar brechas.

El marco de trabajo COBIT va construir un marco para el gobierno y la gestión de las tecnologías de la información -básicamente, crear valor para las partes interesadas- y abarcar todos los métodos y funciones de la organización, el marco COBIT se basa en el gobierno de las tecnologías de la información y se fundamenta en cinco principios. Para aplicar sus procedimientos de forma que integre o implique a todas las dependencias y, en última instancia, divida los planes y eventos por rango, se ordena de acuerdo con otras normas como ISO. Para evaluar el grado de beneficios y obligaciones de los propietarios de los procesos de TI y de la organización, la orientación y metodología corporativas de COBIT implican vincular los objetivos corporativos a los de TI y ofrecer métricas de información y modelos de madurez. Los puntos primordiales que se toman en cuenta para entender el marco de trabajo COBIT son los siguientes según (Torres, 2022).

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) creó el marco COBIT (Control Objectives for Information and Related Technologies) para ayudar a las empresas a gestionar y supervisar su uso de las tecnologías de la información (TI).

COBIT 5.0 El principal objetivo es proporcionar a las empresas un conjunto de directrices y procedimientos que les permitan alcanzar sus objetivos informáticos y proteger sus activos.

Los usuarios de COBIT 5.0 se benefician de su investigación, desarrollo, publicación y promoción de objetivos de control de TI autorizados, actualizados

periódicamente, reconocidos en todo el mundo y generalmente aceptados. Esta ha sido la misión de la organización desde la creación de las normas. Los responsables Mediante la creación de un modelo de gobierno de TI, COBIT 5.0 facilita a las organizaciones la determinación de los controles necesarios para garantizar la seguridad de sus activos. También facilita que los usuarios entiendan y comprendan el nivel de seguridad de sus sistemas informáticos. Dado que contempla los sistemas en su contexto global y tiene en cuenta tanto los procesos informatizados como los manuales, el modelo COBIT 5.0 sirve de base en este caso. COBIT 5.0 es un marco para el gobierno y la gestión de TI. Es una evolución de COBIT 4.1 y pretende ayudar a las empresas a abordar cuestiones relacionadas con la gestión de riesgos, el cumplimiento y la coordinación de las TI con los objetivos empresariales.

COBIT 5.0, que permite un enfoque integral de la gestión empresarial y las TI, destaca el valor del gobierno de las TI y ofrece un marco para gestionar los recursos informáticos y tomar decisiones.

Cinco conceptos básicos constituyen la base del marco COBIT 5.0: Cumplir las exigencias de las partes interesadas:

COBIT 5.0 ayuda a las organizaciones a definir y gestionar las expectativas de las partes interesadas en los servicios de TI. Describe la gama de TI: Con su enfoque integral de la gestión de TI, COBIT 5.0 cubre todos los aspectos de TI. Adoptar una estrategia integral: COBIT 5.0 tiene en cuenta las relaciones entre los distintos componentes de TI y cómo afectan al negocio. Mantenga separadas la gestión y el gobierno:

La diferenciación entre la gestión de TI y las funciones de gobierno se establece claramente en COBIT 5.0. Fomento de un método centrado en los procesos: La piedra angular de COBIT 5.0 es un enfoque de la gestión de TI basado en procesos, que promueve una mayor efectividad y eficiencia en brindar servicios de TI.

COBIT 5.0 también define siete facilitadores de TI -principios, políticas y marcos de TI, procedimientos, estructuras organizativas, cultura, información, servicios y aplicaciones, e infraestructuras tecnológicas- que ayudan a las organizaciones a alcanzar sus objetivos empresariales. En pocas palabras,

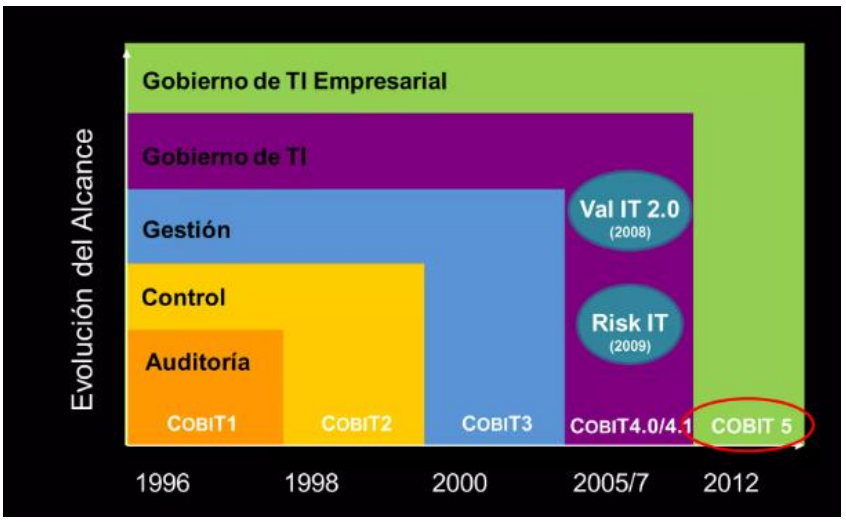
COBIT 5.0 es un marco de gobierno y gestión de TI que ayuda a las empresas a abordar las preocupaciones empresariales de gestión de riesgos, cumplimiento y alineación de TI con los objetivos empresariales. Se basa en cinco principios fundamentales y siete habilitadores de TI para cumplir sus objetivos.

Nuevas ideas como las áreas de enfoque y los factores de diseño se encuentran entre las mejoras de COBIT 5.0 que proporcionan más orientación para acomodar una estructura de gobierno a las demandas de la entidad.

Los componentes de diseño que ofrecen una conformidad actualizada con las normas, directrices y mejores prácticas mundiales, así como un mayor apoyo para adaptar un sistema de gobierno a las demandas de la empresa, aumentan la relevancia de COBIT.

COBIT 2019 es ahora más prescriptivo debido a la adición de nuevas herramientas y directrices para ayudar en la construcción de un marco de gobierno más adecuado. Estas modificaciones permiten elegir COBIT por otros motivos y tenerlo en cuenta en ámbitos que no están necesariamente centrados en las TI. Además, se ha adoptado un paradigma de «código abierto», que permite a la comunidad mundial de gobernanza ofrecer sugerencias de mejora del marco y sus productos derivados en tiempo real, así como compartir aplicaciones y contribuir a futuras actualizaciones. según (Quispe , 2024).

Figura 01: *Evaluación del COBIT 5*



Fuente (isaca,2018)

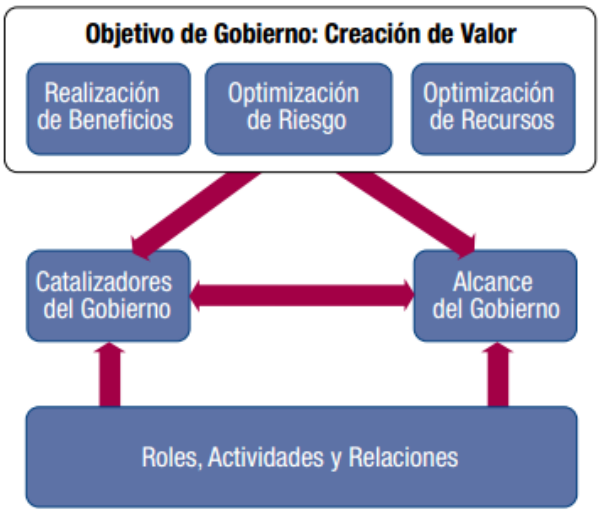
1.10.10. COBIT 5

Una colección de buenas prácticas para optimizar la gestión de los recursos tecnológicos es COBIT 5. El paradigma COBIT 5, dirigido a todas las áreas de una empresa, incluidos responsables de TI, beneficiarios y auditores, se utiliza para auditar la gestión y el control de los sistemas de TI. El objetivo de esta guía de referencia es proporcionar un enfoque de mejores prácticas para el Gobierno Empresarial de las Tecnologías de la Información (GEIT) basado en una fase de desarrollo continuo que debe adaptarse a las demandas de la empresa. de la organización (ISACA, 2012).

El COBIT 5 es genéricamente muy útil para las organizaciones de todas las dimensiones, tanto comerciales, como sin ánimo de utilidad o del sector público (ISACA, 2012).

Este enfoque ayuda a las entidades a preservar la paridad entre los beneficios generados por las tecnologías de la información, el grado de riesgo implicado y la utilización de los recursos. Cinco conceptos fundamentales para el gobierno y la gestión de riesgos constituyen la base de la gestión de peligros de las tecnologías de la información de COBIT 5 (Torres, 2022).

Figura 02: *Business framework*



Fuente (ISACA,2012)

1.10.11. DOMINIO DE COBIT 5

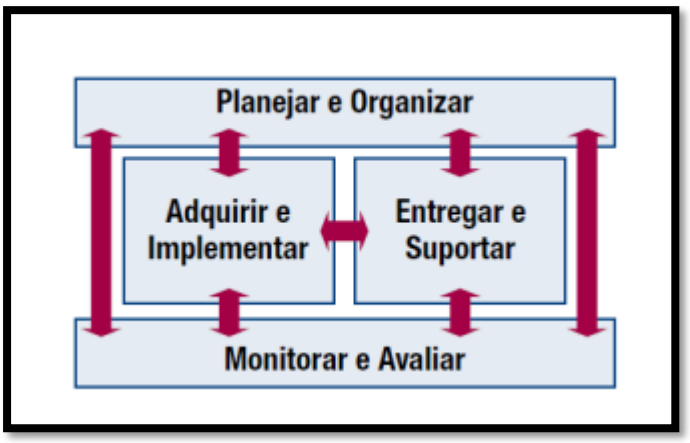
El modelo de similitud de procesos distribuidos tiene cinco dominios, uno para el gobierno y cuatro para la gestión, según COBIT 5 (Tello, 2023).

- Dominio 1 de gobernanza se llama como EDM: evalúa, orienta y supervisa, en el que se revisa la evaluación, orientación y supervisión; en etapa del dominio se realizan 5 procesos típicos de gobierno que garantiza los fines de la entidad, de modo que se alcancen los propósitos institucionales mediante la evaluación de las necesidades de las partes interesadas.
- Dominio 2 de gobernanza se llama como APO: alinea, planifica y organiza dentro de este dominio se constituyen 13 procesos de la gestión de TI que permiten ocultar las tácticas y técnicas que admiten reconocer como las TI contribuyan a avanzar los objetivos de la organización.
- Dominio 3 de gobernanza se llama como BAI: Adquirir e implementa, dentro de este dominio se constituyen 10 procesos de la gestión de TI

que el acceso a la directiva que las ideas novedoso a ejecutarse permitan satisfacer las necesidades de la organización.

- Dominio 4 de gobernanza se llama como DSS: Entregar, dar servicio y soporte, dentro de este dominio se constituyen 6 procesos de la gestión de TI que ayuda a la entrega de los servicios solicitados, con el propósito de lograr que los recursos tecnológicos se encuentren perfeccionados para cumplir con los metas institucionales.
- Dominio 5 de gobernanza se llama como MEA Supervisar, evaluar y valorar, contempla 3 procesos de la gestión de las TI con el objetivo de filtrar los errores de manera eficaz por medio de la evaluación del desempeño de los recursos tecnológicos para llevar que los controles internos implantados sean positivos y eficaces. El marco de trabajo COBIT 5, maneja 5 dominios visiblemente reconocidos, los cuales están subdivididos en 37 procesos

Figura 03: *Dominios*



Fuente (Isaca,2012)

1.10.12. PROCESOS DE COBIT

Alinear, Planificar y Organizar (APO): Este primer ámbito trata de las estrategias y tácticas e identifica las formas en que la tecnología de la información puede apoyar mejor los objetivos de la organización (ISACA, 2012).

PROCESOS:

➢ APO01. Supervisar el marco de gestión de las tecnologías de la información: Dejar claras la misión y la visión de la empresa en materia de tecnología de la información y defender su gobernanza. Establecer y mantener normas y procedimientos para la gestión de la información y el uso de la tecnología dentro de la

empresa para respaldar los objetivos de gobernanza relativos a las directrices y los valores de los altos cargos.

➢ APO02. Gestionar la estrategia: Brindar una visión general de la entidad y el entorno de TI que existen en la actualidad, así como el camino que debe tomarse en el futuro y las decisiones que deben tomarse para la transición al entorno ideal.

➢ APO03. Gestionar la arquitectura empresarial: Mediante la creación de modelos y prácticas esenciales que delinean las líneas de base y las arquitecturas objetivo, puede crear de manera eficiente y eficaz una arquitectura común que consta de procesos organizativos, información, datos, aplicaciones y capas de arquitectura tecnológica.

➢ APO04. Gestionar la innovación: Además de las tecnologías actuales, la innovación en los procesos empresariales y la innovación en TI, considere las oportunidades de innovación empresarial y las mejoras que pueden lograrse empleando nuevas tecnologías, servicios o innovaciones empresariales posibilitadas por TI.

➢ APO05. Gestión de la cartera: Adherirse a la visión de la arquitectura empresarial y aplicar todo el conjunto de normas de inversión estratégica. Los servicios y programas deben clasificarse, priorizarse y equilibrarse. La gestión de la demanda debe tener en cuenta los recursos disponibles, las limitaciones de financiación y su correspondencia con el valor y el riesgo de la empresa, así como con sus objetivos estratégicos.

➢ APO06 Gestionar el presupuesto y los costes: Con el fin de gestionar las operaciones financieras relacionadas con TI tanto en el negocio como en los departamentos de TI, gestionar metodologías presupuestarias formales y un mecanismo de reparto de costes justo y equitativo con el negocio. Esto incluye la presupuestación, la gestión de costes y beneficios y el establecimiento de prioridades de gasto.

➢ APO07. Gestionar los Recursos Humanos: Ofrecer un método organizado para garantizar la mejor disposición, posicionamiento, habilidades y experiencias del capital humano.

➢ AP008. Gestionar las relaciones: Dentro de las limitaciones presupuestarias y los parámetros de riesgo apropiados, gestionar la relación de la organización con TI de manera formal y transparente, centrándose en el propósito planificado compartido de producir resultados corporativos eficaces en apoyo de los objetivos estratégicos.

➢ AP009. Gestionar los acuerdos de servicio: Organizar servicios basados en TI y fases de servicio de acuerdo con los requisitos y normas de la entidad. Esto

incluye identificar, definir, diseñar, publicar, acordar y vigilar los servicios de TI, las fases de servicio y las métricas de productividad.

➢ APO10. Gestión de proveedores: Supervisar todas las formas de servicios de tecnología de la información de los proveedores para garantizar que cumplen las exigencias de la empresa. Esto incluye la selección de proveedores, la gestión de las relaciones con ellos, la gestión de los acuerdos y la revisión y supervisión de su rendimiento para garantizar la eficiencia y el cumplimiento adecuados.

➢ APO11. Gestionar la calidad: Establecer y comunicar normas de calidad para todas las etapas, procesos y resultados asociados de la entidad. Esto incluye controles, atención permanente a los detalles, el uso de métodos probados, normas para la mejora continua y esfuerzos efectivos para ser eficaces.

➢ APO12 Gestionar el riesgo: Dentro de las fases de tolerancia establecidas por la dirección ejecutiva de la organización, identificar, evaluar y reducir continuamente los riesgos relacionados con la tecnología de la información.

➢ APO13. Gestionar la seguridad: Establecer, implantar y supervisar un sistema de gestión de la seguridad de os datos.

Construir, Adquirir e Implementar (BAI): El objetivo de la gestión en este ámbito es certificar que los nuevos planes provoquen soluciones que compensen los requisitos de la empresa, que se completen en el plazo previsto y por debajo del presupuesto, que los sistemas recién instalados funcionen según lo previsto y que las modificaciones no interfieran con las operaciones en curso de la empresa. Las soluciones informáticas deben encontrarse, crearse o comprarse, desplegarse e integrarse en las operaciones corporativas para satisfacer una estrategia informática. (ISACA, 2012).

PROCESOS:

➢ BAI01. Gestión de Programas y Proyectos: Organizar y supervisar cada programa y proyecto de la cartera de inversiones de acuerdo con la estrategia de la empresa. Lanzar, organizar, gestionar, llevar a cabo y concluir iniciativas y proyectos con una revisión.

➢ BAI02. Gestionar la Definición de Requisitos: Encontrar solución y evaluar los requisitos antes de adquirirlos o crearlos para asegurarse de que satisfacen los procesos de negocio, las aplicaciones, la información/datos, la infraestructura y los servicios, y de que están en línea con las carencias estratégicos de la organización.

➢ BAI03. Gestionar la Identificación y Construcción de Soluciones: Recopilar y supervisar las soluciones descubiertas de conformidad con los requisitos

empresariales, lo que abarca las asociaciones con fabricantes y proveedores, el diseño, el desarrollo y la adquisición/contratación. Gestionar los requisitos, las pruebas, la configuración, los ensayos y el mantenimiento de la infraestructura, los servicios, los datos, las aplicaciones y los procesos empresariales.

➢ BAI04. Gestionar la Disponibilidad y la Capacidad: Se trata de localizar una igualdad entre la carencia de capacidad, rendimiento y disponibilidad, tanto ahora como en el futuro, y una prestación de servicios rentable. incluye la estimación de las necesidades futuras en función de los requisitos empresariales y la evaluación de las capacidades actuales.

➢ BAI05: Gestionar la facilitación del cambio organizativo: Aumentar la probabilidad de que todas las partes interesadas del negocio y la tecnología, así como todo el ciclo de vida del cambio, implementen con éxito el cambio organizativo en toda la entidad de manera oportuna y con bajo riesgo.

➢ BAI06. Gestionar el cambio: Tener autoridad sobre todas las alteraciones. Esto incluye el análisis de los efectos, la prioridad, la autorización, el seguimiento, la elaboración de informes, el cierre, la documentación, los cambios de emergencia y las normas y procedimientos para los cambios.

➢ BAI07. Gestionar la Aceptación del Cambio y la Transición: Aceptar e implantar formalmente soluciones novedosas. Aquí se incluyen la planificación de la implantación, la conversión de datos, las pruebas del sistema, la comunicación, la preparación del lanzamiento, la puesta en producción de servicios informáticos o procesos empresariales nuevos o modificados, el apoyo inicial a la producción y la revisión.

➢ BAI08. Gestionar el Conocimiento: Mantener conocimientos actualizados, verificados, fiables y pertinentes para apoyar todas las actividades del proceso y ayudar en la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, aplicación y retirada de los conocimientos.

➢ BAI09. Gestionar los Activos: Supervisar los activos informáticos durante su ciclo de vida para garantizar que se utilizarán para generar valor al mejor coste posible, que se mantendrán operativos, que son física y financieramente seguros y que los activos esenciales para mantener la capacidad de servicio son fiables y accesibles.

➢ BAI10. Gestión de la configuración: Establecer y preservar las relaciones y definiciones de las competencias y recursos fundamentales necesarios para llevar a cabo los servicios de TI. Como parte de esto, se incluye la recopilación de datos de configuración, el establecimiento de líneas de base, la verificación y auditoría de datos y el mantenimiento de repositorios de configuración.

Entregar, Dar Servicio y Soporte (DSS): Implica la prestación real de los servicios requeridos, incluida la prestación de servicios, la gestión de la seguridad y la continuidad, la asistencia a los usuarios de los servicios, la gestión de los datos y de las instalaciones operativas. (ISACA, 2012).

PROCESOS:

➢ DSS01. Gestionar las operaciones: Planificar, coordinar y ejecutar los procedimientos y tareas necesarios para ofrecer servicios de TI, tanto interna como externamente. Esto implica seguir procedimientos operativos estándar y realizar las tareas de supervisión necesarias.

➢ DSS02. Gestión de incidencias y solicitudes de servicio: Responder a las consultas de los usuarios de forma rápida y eficiente y gestionar todo tipo de incidencias. Restablecer el servicio normal; registrar y satisfacer las peticiones de los usuarios; y registrar, examinar, identificar, notificar y resolver problemas.

➢ DSS03. Resolución de problemas: Determinar, categorizar y resolver rápidamente los problemas y sus causas subyacentes para evitar incidentes recurrentes. Desarrollar sugerencias de mejora.

➢ DSS04. Gestionar la continuidad: Crear y mantener una estrategia que permita a TI y a la empresa abordar los problemas y las interrupciones con el fin de mantener las operaciones críticas para el negocio y los servicios esenciales de TI funcionando sin problemas, así como para mantener la información accesible a un nivel aceptable para la organización.

➢ DSS05. Gestionar los servicios de seguridad: Proteger los datos de la empresa de acuerdo con la política de seguridad para garantizar un nivel manejable de riesgo de seguridad de la información. Establezca y gestione las funciones de seguridad, los privilegios de acceso a la información y la supervisión de la seguridad.

➢ DSS06. Gestionar los controles de los procesos de negocio: Establecer y mantener controles adecuados de los procesos de negocio para garantizar que la información vinculada procesada interna o externamente respeta todas las normas de control de la información pertinentes.

Supervisar, Evaluar y Valorar (MEA): Para garantizar que se ajustan a las necesidades de control y son de alta calidad, todos los procesos informáticos deben someterse a evaluaciones periódicas. La gestión del rendimiento, el cumplimiento de la normativa, la aplicación del gobierno y la fiscalización del control interno se incluyen en este ámbito.

PROCESOS:

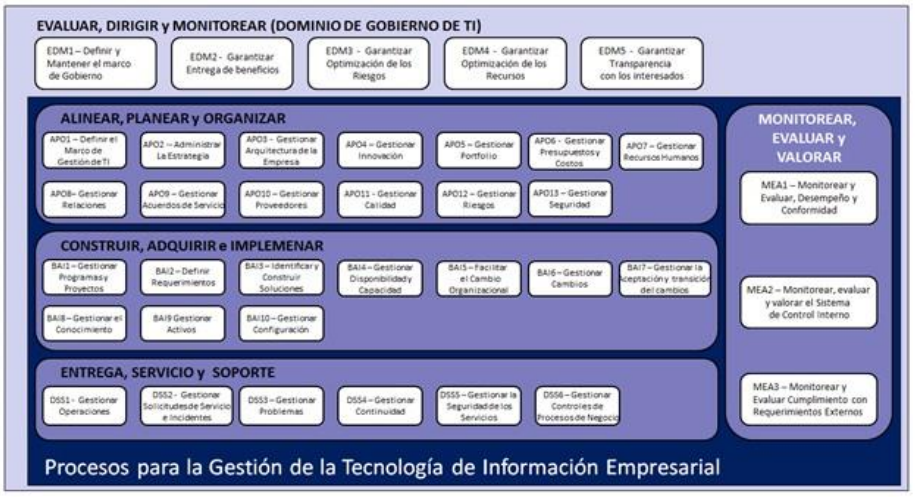
➢ MEA01. Seguimiento, examen y determinación del rendimiento y el cumplimiento: Recopilar, confirmar y evaluar objetivos y métricas de negocio, TI y procesos. Asegurarse de que los procedimientos se llevan a cabo de conformidad con los criterios de rendimiento, objetivos y métricas establecidos, y de que los informes se elaboran de forma sistemática y ordenada.

➢ MEA02. Supervisar, evaluar y valorar el sistema de control interno: Ayudar a la dirección a reconocer ineficiencias y lagunas de control y a adoptar medidas correctoras.

Acciones de mejora. Planificar, organizar y mantener normas para la evaluación de las actividades de control y garantía internos. Actividades de control y garantía internos.

➢ MEA03. Rastrear, examinar y determinar si se están cumpliendo los requerimientos externos: Evaluar si se están cumpliendo los contratos y las normativas en TI y en las operaciones empresariales que dependen de TI. Obtenga confirmación de que se han reconocido los requerimientos, se ha integrado el desempeño de la tecnología de información en el cumplimiento empresarial y se ha cumplido con el cumplimiento de TI.

Figura 04: *Procesos*



Fuente (ISACA,2012)

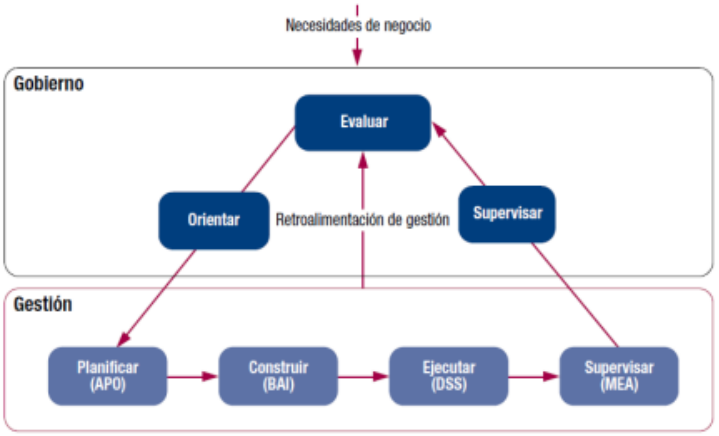
1.10.13. NORMA ISO

➢ ISO/IEC 38500.- La aceptación de los principios rectores y la metodología para poner en práctica la norma se apoyan en COBIT 5 de las formas que se indican a continuación. Seis ideas fundamentales constituyen la base de la norma ISO/IEC 38500:2008 - Gobierno corporativo de las tecnologías de la información. Esta sección explica las aplicaciones prácticas de cada principio,

así como la forma en que las directrices de COBIT 5 promueven las mejores prácticas. (ISACA, 2012).

- ✓ **Principio de Responsabilidad. -** El negocio (el cliente) y las TI (proveedor) deberían ayudar en una guía de cooperación utilizando conductos eficientes del comunicado basadas en relaciones auténticas y de confianza y demostrando transparencia con respecto al compromiso de llevar a cabo las labores y la comprobación de las misma
- ✓ **Principio de Estrategia. -** La planificación indispensable de la tecnología de información es un labor tediosa y crítica que requiere una precisa relación entre la unidad de negocio de la organización y los propósitos estáticamente valiosos de la tecnología de información.
- ✓ **Principio de Adquisición. -** Las soluciones de tecnología existen para aguantar los procesos de trabajo y deberíamos tener mucho cuidado de no recapacitar las alternativas de tecnología de información como algo apartado o solamente como un servicio o proyecto de tecnología. Por otra parte, una elección inoportuna de la arquitectura tecnológica, fallos a la hora de mantener una infraestructura técnica actual y apropiada o un abandono de talento humanos capacitado pueden dar como resultado un proyecto caído, una incapacidad para soportar las operaciones del trabajo o un reajuste en el valor del trabajo.
- ✓ **Principio de Rendimiento. -** La medida de la eficiencia del desempeño depende de que se tengan en cuenta dos aspectos clave: una definición clara de los objetivos de desempeño y el establecimiento métricamente eficiente para inspeccionar el logro de los objetivos
- ✓ **Principio de Conformidad. -** En el mercado general de la actualidad, apoyado por el acceso de Internet y las tecnologías de información avanzadas y sofisticadas, las organizaciones necesitan cumplir con un número cada vez más gigante de requisitos legales y regulados.
- ✓ **Principio de Comportamiento humano. -** La aplicación de cualquier cambio aportado por las tecnologías de información, incluyendo el gobierno de la tecnología de información en sí mismo, normalmente requiere cambios específicos culturales y de comportamiento tanto en el interior de las organizaciones como con los usuarios y socios del del trabajo.

Figura 05: *Áreas claves de Gobierno y la Gestión*



Fuente (ISACA,2018)

- ISO/IEC 27000

  Las próximas dependencias y dominios COBIT 5 están protegidas por las ISO/IEC 27000:

  - ✓ Los procesos de la seguridad y relativos al peligro en los dominios EDM, APO y DSS.
  - ✓ En la gran mayoría de labores conectadas con la seguridad en el interior de los procesos en otros dominios.
  - ✓ Actividades de supervisión y evaluación del dominio MEA.

- ISO/IEC 31000

  Las próximas dependencias y dominios COBIT 5 están protegidas por las ISO/IEC 31000:

  - ✓ Procesos reciproco a la gestión del peligro en los dominios EDM y APO.

ISO 19011

La ISO 19011: La norma internacional ISO 19011 proporciona orientación para las auditorías de sistemas de gestión. Es aplicable a todo tipo de organizaciones, independientemente de su tamaño, sector o ubicación, y fue creada por la Organización Internacional de Normalización (ISO). Las normas sobre la competencia e imparcialidad de los auditores se describen detalladamente en la norma ISO 19011, junto con una definición de los principios y procedimientos de auditoría. Su principal objetivo es orientar a los auditores sobre cómo planificar, llevar a cabo y supervisar auditorías eficaces y satisfactorias. Asimismo, el ámbito de aplicación de la norma ISO 19011 incluye todas las fases del proceso de auditoría, desde la planificación hasta el informe final y el seguimiento de las medidas correctoras. Para auditar

sistemas de gestión, como los de calidad, medio ambiente y salud y seguridad en el trabajo, entre otros, establece normas y estándares. Además, la norma ISO 19011 se implementa a todos los tipos de auditoría que existen, incluyendo auditorías internas, auditorías externas y auditorías mixtas. También se puede disponer para auditar de proveedores, subcontratistas y otras partes que interesados de la empresa.

Figura 06: *Principios de COBIT*

Fuente (ISACA,2012)

1.10.14. NORMA TÉCNICA PERUANAS EN AUDITORIA DE LA INFORMACIÓN

(Villadeza y Condori, 2022). El propósito de la Norma Técnica Peruana es ofrecer los datos necesarios para establecer, llevar a cabo, mantener y mejorar continuamente un sistema de gestión de seguridad de los datos. Para una entidad, proteger un sistema de gestión de seguridad de datos es una elección intencional. En el desarrollo y la ejecución de un sistema de gestión de la seguridad de la información empresarial influyen los objetivos y los puntos frágiles de la entidad, las especificidades de la seguridad, los procedimientos empresariales que se emplean y el tamaño y la configuración de la empresa. Se prevé todas estas variables conocidas se alteren a lo largo del tiempo.

CAPITULO VI

METODOLOGÍA DE LA INVESTIGACIÓN

1.11. TIPO DE INVESTIGACIÓN

La investigación que se realizo es de tipo: observacional, descriptivo.

1.12. NIVEL DE INVESTIGACIÓN

La investigación descriptiva es aquella que trata de especificar los medios, características y perfiles de un individuo, grupo, sociedad, proceso, entidad y otros elementos objeto de estudio (Hernandez et al., 2014).

El presente estudio de investigación es de nivel descriptivo, porque se buscó identificar todos los resultados de una guía de auditoría interna que ayude a reconocer peligros de seguridad en la infraestructura tecnológica.

1.13. DISEÑO DE INVESTIGACIÓN

Según el investigador (Hernandez et al,. 2014) Define la investigación no experimental como un conjunto de investigaciones que se llevan a cabo sin modificar ninguna variable, sino que se limitan a visualizar los acontecimientos que tienen lugar en su hábitat natural en tiempo real, con la intención de examinarlos posteriormente.

El diseño de este estudio de investigación es no experimental porque no se alterarán las variables de los factores de riesgo, que son meramente percibidas.

1.14. POBLACIÓN Y MUESTRA

1.14.1. POBLACIÓN

Infraestructura informática (hardware y software) de Grupo Tecnológico Alinti, Lima 2023.

Aproximadamente fueron 45 unidades de infraestructura, incluyendo equipos físicos y sistemas de software.

1.14.2. MUESTRA

Componentes de la infraestructura informática (hardware y software) con riesgo identificado del Grupo Tecnológico Alinti, Lima 2023.

Aproximadamente fueron 18 unidades de infraestructura, incluyendo equipos físicos y sistemas de software.

1.15. TÉCNICAS E INSTRUMENTOS PARA RECOLECIÓN DE DATOS

1.15.1. TÉCNICAS

- Observación
- Análisis documental

1.15.2. INSTRUMENTOS

- Ficha y observación
- Ficha de análisis documental

1.16. HIPÓTESIS DE LA INVESTIGACIÓN

No todos los estudios cuantitativos se basan en hipótesis. El objetivo original del estudio no es una condición importante para el planteamiento de hipótesis. Las investigaciones cuantitativas que pretenden intuir una figura o acontecimiento o cuyo enfoque indica que su magnitud será explicativa o correlacional son ejemplos de exploraciones cuantitativas que generan hipótesis. (Hernandez et al, 2014).

"La creación de hipótesis no es necesaria para la investigación descriptiva; en su lugar, basta con formular algunas preguntas de investigación que, como se ha señalado anteriormente, se derivan de los objetivos, la explicación del conflicto y, lo que es más obvio, el marco teórico que sustenta el estudio." (Bernal, 2010)

Se seleccionó este estudio porque es de carácter descriptivo y no plantea ninguna hipótesis.

1.17. PLAN DE AUDITORÍA

El presente proyecto de investigación de auditoría tuvo como objetivo realizar una propuesta de un marco de trabajo COBIT 5 como metodología para llevar a cabo estimación absoluta y un análisis profundo de los diferentes procesos, controles y componentes que se va aplicar actualmente en el área de la oficina de tecnología de la información dentro de la empresa.

El COBIT 5 es una herramienta completa ordenada con los objetivos principales de la organización, el enfoque de esta auditoría interna se concentrará específicamente en inspeccionar los componentes de las tecnologías de la información.

fundamentándome en las actividades de recolección de información ejecutadas en mi función de bachiller, donde se llevaron a cabo entrevistas y observaciones, se ha procedido a esquematizar un protocolo de trabajo detallado para la elaboración de una auditoría interna. Este plan prioriza la revisión de aquellos recursos tecnológicos de información que representan mayor peligro posible para la empresa, en función de las carencias y áreas críticas previamente conocidas. En consecuencia, se ha auditado los siguientes activos de tecnología de información vinculadas a la Oficina de Informática de la organización del grupo tecnológico ALINTI:

Tabla N°2.- *Plan de auditoria*

Seguridad física	Evaluar la protección de datos. programas, instalaciones, equipos, red y personal de la empresa	1. Control de accesos de los usuarios a los equipos	Alto
		2. Informe de accesos y visitas a las instalaciones.	Alto
		3. Inventario de equipos y software.	Medio
		4.Revisión de la red (Factor: ambiental, físico, humano)	Alto
		5.Controles para instalación de dispositivos externos.	Alto
Respaldo y plan de contingencia	Verificar la existencia de respaldos de la información vital para el funcionamiento de la empresa, tanto físico y digital y cumplan los requisitos adecuados	1.Respaldo de la información importante de la empresa	Alto
		2. Plan de continuidad	Alto
		3. Plan de contingencia	Alto
		4. Plan de mantenimiento de hardware y software	Medio
Documentación de SW y HW	Corroborar la existencia de documentación de todo lo adquirido por la empresa en materia de informática, manuales, facturas, contrato, además de documentación detallada de los sistemas que la empresa adquirió	1. Existe licenciamiento de los aplicativos instalados en el equipo informático.	Medio
		2. Existencia de documentos de adquisición de equipos y software, contrato legal del proveedor de internet.	Alto
		3. Documentación de los sistemas utilizados para los servicios de la empresa.	Medio

Área	Objetivo	Componentes	Riesgo
Evaluación de la auditoría interna	Ejecutar de manera eficiente y efectiva las actividades planeadas de auditoría	1. Revisión de los procesos de auditoría	Alto
		2. Análisis de hallazgos y recomendaciones	Medio

Área	Objetivo	Componentes	Riesgo
Planificación y organización de la auditoría interna	Evaluar de manera integral y sistemática los procesos, sistemas y controles internos de una empresa.	1. Evaluación de riesgos	Alto
		2. Establecimiento de objetivos y alcance	Alto
		3. Asignación de recursos	Alto
		4. Programación de actividades	Alto
		5. Controles para la instalación de dispositivos externos	Alto

Área a auditar	Objetivo	Componentes	Riesgo
Proceso de Ejecución de la auditoría interna	Ejecutar de manera eficiente y efectiva las actividades planeadas de auditoría	1. Recolección de evidencias	Bajo
		2. Evaluación de controles	Medio
		3. Comunicación de hallazgos	Bajo

Fuente. Elaboración propia

4.1. ALCANCE

Esta iniciativa técnica se enfocó en realizar una propuesta de una auditoría interna orientada a evaluar los mecanismos de seguridad física sobre la infraestructura informática de la empresa del GRUPO TECNOLÓGICO ALINTI Para llevar a cabo este examen, se emplearon los lineamientos y buenas prácticas establecidas en el marco de trabajo COBIT 5.0, el cual sirvió como guía metodológica para el análisis exhaustivo del entorno tecnológico objeto de revisión. El proceso de auditoría se programó y realizado durante el período comprendido entre los meses de de marzo y agosto del año 2024.

4.2. GUIA DE AUDITORÍA

Se creó un cuadro de fuente de conocimiento por cada objetivo de control seleccionado para la auditoría informa.

Componente 01: Control de acceso de los usuarios a los servicios de internet

Tabla N°3.-*Guía de Auditoria (Componente 1)*

	Guía de Auditoria
Dominio	Entregar, dar servicio y soporte (DSS)
Proceso	DSS05: Gestionar los servicios de seguridad
Practica	DSS05.2: Gestionar la seguridad de la red y las conexiones.
Objetivo	Para proteger los datos en todas las modalidades de conexión, se ha utilizado mecanismos de seguridad y procedimientos de gestión
N.º	**Procedimiento**
1	Se ha comprobado por intermedio de una entrevista al personal del rubro para saber si existe reglas y protocolos de control de acceso para el uso del servicio de internet Wifi
2	Se ha comprobado las normas que son adecuados para el uso del servicio de internet.

Nota. Fuente de elaboración propia

Componente 02: Control de accesos de los usuarios a los equipos

Tabla N°4.-*Guía de Auditoria (Componente 2)*

	Guía de Auditoria
Dominio	Entregar, dar servicio y soporte (DSS)
Proceso	DSS05: Gestionar los servicios de seguridad
Practica	DSS05.3: Gestionar la seguridad de los puestos de usuario final
Objetivo	Se ha salvaguardado las estaciones de trabajo de los usuarios finales (ordenadores de sobremesa, portátiles, servidores y otros dispositivos) y confirmar las directrices de uso y acceso a los equipos
N.º	**Procedimiento**
1	Se ha pedido al responsable del área una lista de los ordenadores que están en uso, el número de usuarios que lo utilizan y el número de horas que se utilizan al día.
2	Se ha confirmado la presencia de políticas de seguridad de los equipos de los usuarios finales mediante una entrevista.

Nota: Fuente de elaboración propia

Componente 03: Informes de accesos y visitas a las instalaciones

Tabla N°5.-*Guía de Auditoria (Componente 3)*

	Guía de Auditoria
Dominio	Entregar, dar servicio y soporte (DSS).
Proceso	DSS05: Gestionar los servicios de seguridad.
Practica	DSS05.5: Gestionar el acceso físico a los activos de TI.
Objetivo	Se ha establecido protocolos formales que permita conceder, limitar y revocar acceso a las distintas instalaciones, inmuebles y áreas físicas de acuerdo con las necesidades de la organización, incluyendo emergencias.
N.º	**Procedimiento**
1	Se ha procedido realizar una inspección directo con el objetivo de constatar si cada uno de los usuarios si todos los usuarios que accedan a los sistemas y a las instalaciones y que cuenten con un método de identificación de manera única y tienen derechos de acceso de acuerdo con sus roles de la organización.
2	Las medidas de seguridad para la entrada a la zona de servidores y a la zona de operaciones dentro de la oficina de informática se ha confirmado mediante un examen directo.

Nota: Fuente de elaboración propia

Componente 04: Inventario de equipos y software

Tabla N°6.-*Guía de Auditoria (Componente 4)*

	Guía de Auditoria
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI09: Gestionar los activos
Practica	BAI09.1: Identificar y registrar activos actuales
Objetivo	Se ha supervisado, medido, analizado, informado y revisado la disponibilidad, el interés y la capacidad de tecnología de información.
N.º	**Procedimiento**
1	Se ha realizado una entrevista directa al encargado del rubro para ver la veracidad del inventario de todo los hardware y software de reserva en caso de que algo vaya mal
2	Si existió un control de inventario, si he visitado el almacén para confirmar su presencia.

Nota: Fuente de elaboración propia

Componente 05: Revisión de la Red (Factor ambiental, físico y humano)

Tabla N°7.-*Guía de Auditoria (Componente 5)*

	Guía de Auditoria
Dominio	Entregar, dar Servicio y Soporte (DSS).
Proceso	DSS05: Gestionar los servicios de Seguridad.
Practica	DSS05.2: Gestionar la seguridad de la red y las conexiones.
Objetivo	Se ha utilizado medios de control de seguridad y protocolos de gestión conectados para protegerse los datos en todos los modos de conexión en el área de TI dentro de la empresa.

N.º	**Procedimiento**
1	A continuación, hemos procedido a verificar que los equipos informáticos y las instalaciones de la red interna se han realizado correctamente mediante una inspección directa.
2	Se ha realizado una entrevista al encargado de área sobre los protocolos de seguridad que cuenta las instalaciones de comunicaciones y su flexibilidad en el acceso.

Nota: Fuente de elaboración propia

Componente 6: Controles para la instalación y uso de dispositivos externos

Tabla N°8.-*Guía de Auditoria (Componente 6)*

	Guía de Auditoria
Dominio	Entregar, dar Servicio y Soporte (DSS).
Proceso	DSS05: Gestionar los servicios de Seguridad.
Practica	DSS05.3: Gestionar la seguridad de los puestos de usuario final.
Objetivo	Se ha inspeccionado si hay algún tipo de control para el uso de periféricos, restricción y alcance.

N.º	**Procedimiento**
1	Se ha entrevistado a los miembros responsables del personal para averiguar si disponen de estrategias para limitar la instalación y el uso de equipos externos (USB, HDD).

Nota: Fuente de elaboración propia

Componente 7: Respaldo de información crítica

Tabla N°9.- *Guía de Auditoria (Componente 7)*

	Guía de Auditoria
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS04: Gestionar la Continuidad
Practica	DSS04.7: Gestionar acuerdos de respaldo
Objetivo	Se ha mantenido la disponibilidad de los datos críticos de la organización
N.º	**Procedimiento**
1	Se ha realizado una entrevista al personal de dicha área para conocer la realidad de respaldos de la información primordial de la entidad.
2	Se ha inspeccionado si los respaldos son digitales (HDD, Flash, dispositivos
3	Mediante una entrevista inspeccionar si existe un protocolo de respaldo de dato

Nota: Fuente de elaboración propia

Componente 8: Plan de continuidad

Tabla N°10.-*Guía de Auditoria (Componente 8)*

	Guía de Auditoria
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS04: Gestionar la Continuidad
Practica	DSS04.1: Definir la política de continuidad del negocio, objetivos y alcance
Objetivo	Se ha defendido los objetivos y parámetros de los planes de continuidad de la empresa en caso de catástrofes naturales o sucesos provocados intencionadamente que pudieran interrumpir todas o alguna de sus actividades informáticas.
N.º	**Procedimiento**
1	Se ha entrevistado al personal de esta empresa para averiguar si existe una estrategia sobre qué hacer en caso de catástrofe natural o impulsado por el ser humano.
2	Se ha solicitado información sobre la estrategia de continuidad de la organización y las acciones se ha realizado en caso de incidente o catástrofe natural.

Nota: Fuente de elaboración propia

Componente 9: Plan de contingencia

Tabla N°11.-*Guía de Auditoria (Componente 9)*

	Guía de Auditoria
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS02: Gestionar las peticiones y los Incidentes de Servicio
Practica	DSS02.5: Resolver y recuperarse de incidentes
Objetivo	Para restablecer el servicio informático, se ha registrado, se ha solicitado y se ha aceptado las soluciones a corto plazo que se hayan encontrado. A continuación, se ha llevado a cabo las operaciones de recuperación.

N.º	**Procedimiento**
1	Se ha entrevistado al personal de este departamento para confirmar que se ha puesto un plan de reserva en situación de contingencia.
2	Se ha solicitado información sobre el protocolo de contingencia para saber qué debe hacerse si surge algún problema que impida la celebración de los actos organizativos.

Nota: Fuente de elaboración propia

Componente 10: Plan de mantenimiento de Hardware y Software

Tabla N°12.-*Guía de Auditoria (Componente 10)*

	Guía de Auditoria
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS01: Gestionar las Operaciones
Practica	DSS01.3: Supervisar la infraestructura de TI
Objetivo	Se ha examinado la infraestructura informática y las acciones asociadas. Se ha mantenido registros de todas las actividades de mantenimiento de hardware y software por orden cronológico.

N.º	**Procedimiento**
1	Se ha realizado una entrevista para ver la existencia de un protocolo de mantenimiento de TI
2	Se ha confirmado que los registros de las acciones de mantenimiento de hardware y software son supervisados por el protocolo de mantenimiento de las TIC.

Nota: Fuente de elaboración propio

Componente 11: Existen licenciamiento de aplicativos instalados de equipos informáticos

Tabla N°13.- *Guía de Auditoria (Componente 11)*

	Guía de Auditoria
Dominio	Construir, adquirir e Implementar (BAI)
Proceso	BAI09: Gestionar los Activos
Practica	BAI09.5: Administrar licencias
Objetivo	Se ha garantizado que se ha mantenido la cantidad adecuada de licencias de software para satisfacer las carencias de la entidad mediante la gestión de licencias.

N.º	**Procedimiento**
1	Se ha solicitado al responsable del área información sobre las licencias de los programas que están instalados en los ordenadores de la entidad.
2	Se ha examinado las situaciones de la licencia del software antes de utilizarlo. En la empresa

Nota: Fuente de elaboración propia

Componente 12: Existencia de documentos de adquisición de equipos y software, contrato legal de proveedor de internet (ISP)

Tabla N°14.-*Guía de Auditoria (Componente 12)*

	Guía de Auditoria
Dominio	Alinear, Planificar y Organizar (APO)
Proceso	APO10: Gestionar los Proveedores
Practica	APO10.3: Gestionar contratos y relaciones con proveedores
Objetivo	Se ha elegido a los proveedores de acuerdo con procedimientos rigurosos y equitativos que garanticen la selección del candidato más cualificado.

N.º	**Procedimiento**
1	Se ha solicitado al supervisor de zona que firme y proporcione las facturas de las compras de hardware, software y servicios de Internet.
2	Analizar la eficacia de la colaboración con los proveedores y señalar las áreas que requieren mejoras.

Nota: Fuente de elaboración propia

Componente 13: Documentación de los sistemas utilizados para los servicios de la empresa

Tabla N°15.-*Guía de Auditoria (Componente 13)*

	Guía de Auditoria
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI04: Gestionar la Disponibilidad y Capacidad
Practica	BAI04.4: Supervisar y revisar la Disponibilidad y la Capacidad
Objetivo	Se ha averiguado si la empresa dispone de documentación sobre los sistemas que ha adquirido y si contiene toda la información necesaria para mantener el sistema cuando sea necesario.

N.º	**Procedimiento**
1	Se ha preguntado al personal responsable por la documentación (código, arquitectura y diagramas) de los sistemas que ha adquirido la empresa.

Nota: Fuente de elaboración propia

Componente 14: Evaluación de riesgos

Tabla N°16.-*Guía de Auditoria (Componente 14)*

	Guía de Auditoria
Dominio	Supervisar y Administrar (APO)
Proceso	APO09: Evaluar y gestionar riesgos.
Practica	APO12.04: Evaluación de Riesgos.
Objetivo	Se ha evaluado de manera íntegra y detallada los peligros afiliados a los procesos, sistemas y controles internos, asegurando un nivel adecuado de control y mitigación de riesgos

N.º	**Procedimiento**
1	Se ha identificado y examinado a fondo los riesgos críticos vinculados a las operaciones de la entidad, sistemas y controles internos
2	Se ha valorado las probabilidades y el impacto de los peligros identificados que se ha determinado su importancia y gestionarlos de manera prioritaria.

Nota: Fuente de elaboración propia

Componente 15: Establecimiento de objetivos y alcance

Tabla N°17.-*Guía de Auditoria (Componente 15)*

	Guía de Auditoria
Dominio	Gobernanza y Administración (APO).
Proceso	APO02: Definir la estrategia.
Practica	APO02.03: Establecer los objetivos y el alcance
Objetivo	Se ha establecido claramente los objetivos y alcance de la auditoría interna que ha abarcar cado áreas críticas de los procesos y controles internos de la entidad

N.º	**Procedimiento**
1	Se ha definido de forma precisa y detallada los objetivos y el alcance de la auditoría interna que se ha incluido aspectos críticos de los procesos y controles internos.

Nota: Fuente de elaboración propia

Componente 16: Asignación de recursos

Tabla N°18.-*Guía de Auditoria (Componente 16)*

	Guía de Auditoria
Dominio	Dirigir, Gestionar y Operar (BAI).
Proceso	BAI06: Gestionar recursos humanos.
Practica	BAI06.04: Asignar personal adecuado.
Objetivo	Se ha asignado recursos de manera eficaz, incluyendo personal competente y herramientas tecnológicas, que se ha ejecutado las actividades de auditoría interna de manera eficiente y efectiva

N.º	**Procedimiento**
1	Se ha designado recursos apropiados, como personal capacitado y tecnología necesaria, que se ha llevado a cabo las auditorías internas de forma eficiente.

Nota: Fuente de elaboración propia

Componente 17: Programación de actividades

Tabla N°19.-*Guía de Auditoria (Componente 17)*

	Guía de Auditoria
Dominio	Alinear, Planificar y Organizar (APO).
Proceso	APO04: Gestionar la calidad de los procesos.
Practica	APO04.05: Programar actividades.
Objetivo	Se ha planificado con precisión y flexibilidad las actividades de auditoría interna que se ha abordado los aspectos críticos identificados en la fase de planificación.
N.º	**Procedimiento**
1	Se ha elaborado un plan detallado que permita programar las actividades de auditoría interna con enfoque en los puntos críticos identificados durante la planificación.

Nota: Fuente de elaboración propia

Componente 18: Controles para la instalación de dispositivos externos

Tabla N°20.-*Guía de Auditoria (Componente 18)*

	Guía de Auditoria
Dominio	Alinear, Planificar y Organizar (APO).
Proceso	APO10: Gestionar proyectos.
Practica	APO10.02: Gestionar la implementación y operación.
Objetivo	Se ha establecido controles específicos para la instalación y uso de equipos externos con el fin de proteger la integridad y confidencialidad de la información de la organización.
N.º	**Procedimiento**
1	Se ha desarrollado medidas de control específicas que ha garantizado la adecuada instalación y utilización de dispositivos externos para proteger los datos de la organización.

Nota: Fuente de elaboración propia.

Componente 19: Revisión de los procesos de auditoría

Tabla N°21.-*Guía de Auditoria (Componente 19)*

	Guía de Auditoria
Dominio	Dirigir, Gestionar y Operar (BAI)
Proceso	BAI07: Realizar auditorías
Practica	BAI07.01: Recopilar evidencias
Objetivo	Obtener evidencias de manera sistemática para proteger los hallazgos y conclusiones de la auditoría

N.º	**Procedimiento**
1	Se ha realizado una recopilación detallada y precisa de evidencias que protegió resultados y conclusiones de la auditoría.

Nota: Fuente de elaboración propia

Componente 20: Análisis de hallazgos y recomendaciones

Tabla N°22.-*Guía de Auditoria (Componente 20)*

	Guía de Auditoria
Dominio	Dirigir, Gestionar y Operar (BAI)
Proceso	BAI07: Realizar auditorías
Practica	BAI07.02: Evaluar controles
Objetivo	Se ha valorado los controles existentes para reconocer áreas de mejoría y garantizo la eficacia de los procedimientos de auditoría

N.º	**Procedimiento**
1	Se ha realizado una evaluación exhaustiva de los controles que reconoció posibles debilidades o mejoras necesarias.

Nota: Fuente de elaboración propia

Componente 21: Recolección de evidencias

Tabla N°23.-*Guía de Auditoria (Componente 21)*

	Guía de Auditoria
Dominio	Dirigir, Gestionar y Operar (BAI)
Proceso	BAI07: Realizar auditorías
Practica	BAI07.03: Comunicar hallazgos
Objetivo	Se ha comunicado de forma clara y efectiva los resultados encontrados durante la auditoría ha proporcionado la toma de decisiones y la ejecución de hechos correctivas.

N.º	**Procedimiento**
1	Se ha comunicado de manera precisa y oportuna los hallazgos identificados durante la auditoría para fomentar la gestión proactiva

Nota: Fuente de elaboración propia

Componente 22: Evaluación de controles

Tabla N°24.-*Guía de Auditoria (Componente 22)*

	Guía de Auditoria
Dominio	Dirigir, Gestionar y Operar (BAI)
Proceso	BAI06: Gestionar recursos humanos
Practica	BAI06.01: Revisar procesos de auditoría
Objetivo	Se ha evaluado de manera detallada los procesos de auditoría que garantizo su eficiencia y eficacia.

N.º	**Procedimiento**
1	Se ha ejecutado una revisión general de los procesos de auditoría que reconoció áreas de mejoramiento y optimización

Nota: Fuente de elaboración propia

Componente 23: Comunicación de hallazgos

Tabla N°25.-*Guía de Auditoria (Componente 23)*

	Guía de Auditoria
Dominio	Dirigir, Gestionar y Operar (BAI)
Proceso	BAI07: Realizar auditorías
Practica	BAI07.04: Analizar hallazgos y recomendar acciones
Objetivo	Se ha analizado de forma minuciosa los hallazgos de la auditoría interna y se proporcionó recomendaciones efectivas para mejorar los procesos y controles.
N.º	**Procedimiento**
1	Se ha realizado un análisis profundo de los hallazgos identificados durante la auditoría y se ha identificado recomendaciones precisas para mejorar las operaciones de la organización

Nota: Fuente de elaboración propia

4.3. EVALUACIÓN DE CONTROLES

a) Evaluación de la Madurez: COBIT 5 define los niveles de madurez, que deben utilizarse para evaluar la madurez de los procesos de TI.
b) Prueba de Controles: Realizar pruebas para confirmar la eficacia de los controles. Esto podría implicar la realización de entrevistas, la revisión de la documentación, la comprobación de las transacciones y observaciones.
c) Análisis de Riesgos: Determinar y evaluar los riesgos relacionados con el gobierno y la gestión de TI en la empresa del Grupo Tecnológico Alinti.

4.4. TÉCNICAS Y ANÁLISIS DE PROCESAMIENTOS DE DATOS

Las informaciones obtenidas mediante la aplicación de los instrumentos fueron analizados y tratados con programas computarizados tales como el aplicativo Microsoft Excel.

Se utilizaron las herramientas y recursos relacionados con Auditoría Interna y el Análisis de Riesgo recomendados por la COBIT 5 e ISO/IEC 27001 y se seleccionó aquella que más se adecue a la realidad de la empresa del Grupo Tecnológico ALINTI.

CAPITULO VII

RESULTADO Y DISCUSIÓN

4.5. RESULTADO

4.5.1. HALLAZGOS DE LA AUDITORÍA INTERNA

Se ha aplicado cada uno de las técnicas y instrumentos durante la auditoría interna se evidenció en las siguientes tablas

ÁREA DE SEGURIDAD FÍSICA

Se ha evaluado los 22 componentes, se obtuvieron las siguientes tablas:

Resultado de Objetivo Principal

Componente 01: Control de accesos de los usuarios a los equipos

Tabla N°26.-*Hallazgo de Auditoria (Componente 1)*

ALINTI ENERGÍA VERDE	**GRUPO TECNOLÓGICO ALINTI**
Hallazgos de la Auditoría	
Componente	Control de accesos de los usuarios a los equipos
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.3: Gestionar la seguridad de los puestos de usuario final
Objetivo	Se ha verificado las políticas de uso y acceso a los dispositivos y proteja las estaciones de trabajo de los usuarios finales (portátiles, ordenadores de sobremesa, servidores y otros dispositivos).
Resultados	
En respuesta a una solicitud de información sobre la gestión del acceso de los usuarios a los dispositivos informáticos, se descubrió que no existían registros sobre el control de los dispositivos, su ubicación dentro de cada unidad con sus equipos correspondientes, sus horas de funcionamiento, los dispositivos averiados o el control de acceso al servidor. Cabe mencionar que los 20 trabajadores afirman que los procedimientos son fundamentales e imprescindibles porque ayudan a tener un mejor sistema de seguridad, aunque después de la entrevista se descubrió que no existían protocolos de seguridad para los equipos de los usuarios finales. estructura en el interior del área informática.	

Nota. Fuente de elaboración propia

Componente 02: Informes de accesos y visitas a las instalaciones

Tabla N°27.-*Hallazgo de Auditoria (Componente 2)*

GRUPO TECNOLÓGICO ALINTI	
Hallazgos de la Auditoría	
Compon	Informes de accesos y visitas a las instalaciones
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.5: Gestionar el acceso físico a los activos de TI
Objetivo	se ha determinado y se ha aplicado procedimiento para permiso, limitar y revocar acceso a los ambientes, edificios y dependencias de acuerdo con las carencias de la organización, incluyendo emergencias
Resultados	
A la entrada de la organización ALINTI, se exigió a todos los 20 trabajadores que utilicen sus credenciales. También se exigió los informes de acceso y visita, y se avisa verbalmente de la entrada por la radio de comunicación interna de la organización. A continuación, se solicitó autorización a la unidad administrativa. Dependiendo de las circunstancias. También se le ha pedido que se identifiquen, que indiquen a qué unidad se dirigen y si van a asistir a una reunión. La zona de operaciones dispone de un sistema de vigilancia que permite el seguimiento por cámara.	

Nota: Fuente de elaboración propia

Componente 03: Inventario de equipos y software

Tabla N°28.-*Hallazgo de Auditoria (Componente 3)*

GRUPO TECNOLÓGICO	
Hallazgo de la Auditoria	
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI09: Gestionar los activos
Práctica	BAI09.1: Identificar y registrar activos actuales
Componente	Inventario de equipos y software
Objetivo	Se ha supervisado, se ha medido, se ha analizado, se ha informado y revisado la disponibilidad, el rendimiento y la capacidad de TI
Resultados	
En la actualidad, la empresa no dispone de un almacén donde se guarden los ordenadores y otros equipos electrónicos, sino que todos los equipos se almacenan sin ningún tipo de registro, como se descubrió durante la entrevista. Tampoco existe un inventario de hardware o software.	

Nota. Fuente de elaboración propia

Componente 04: Revisión de la Red (Factor ambiental físico y humano)

Tabla N°29.-*Hallazgo de Auditoria (Componente 4)*

	GRUPO TECNOLÓGICO ALINTI
	Hallazgos de la Auditoría
Componente	Revisión de la Red (Factor ambiental, físico y humano)
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.2: Gestionar la seguridad de la red y las conexiones
Objetivo	Se ha empleado medidas de seguridad y dimensiones de gestión que se ha relacionado para poder salvaguardar los datos en todos los modos de conexión en la dependencia de tecnología de información de la organización
	Resultados
Al observar las instalaciones de red y cuarto de comunicaciones, se verifico que cada uno de las instalaciones y equipos estuvieran conectadas correctamente y de manera ordenada, con respecto a estándares como el cableado estructurado, la empresa aun no lo ha implementado por completo en todas las áreas.	

Nota: Fuente de elaboración propia

Componente 5: Controles para la instalación y uso de dispositivos externos

Tabla N°30.-*Hallazgo de Auditoria (Componente 5)*

	GRUPO TECNOLÓGICO ALINTI
	Hallazgos de la Auditoría
Componente	Controles para la instalación y uso de dispositivos externos
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Gestionar los servicios de Seguridad
Práctica	DSS05.3: Gestionar la seguridad de los puestos de usuario final
Objetivo	Se ha comprobado si hay algún tipo de vigilancia para el uso de periféricos,
	Resultado
La organización no tiene protocolos de limitaciones de acceso en cuanto al uso de equipos externos según nos mencionan los 20 trabajadores del área.	

Nota: Fuente de elaboración propia

ÁREA DE RESPALDO Y PLAN DE CONTINGENCIA

Se ha evaluado los 4 componentes, se obtuvieron los siguientes detalles:

Componente 6: Respaldo de información crítica

Tabla N°31.-*Hallazgo de Auditoria (Componente 6)*

GRUPO TECNOLÓGICO ALINTI

Hallazgos de la Auditoría	
Componente	Respaldo de información crítica
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS04: Gestionar la Continuidad
Práctica	DSS04.7: Gestionar acuerdos de respaldo
Objetivo	Se ha mantenido la disponibilidad de la información crítica de la empresa

Resultados

Inmediatamente de la entrevista realizada a los 20 trabajadores de la organización, se pudo comprobar que, si hay respaldos de datos trascendental de la organización, estos soportes se los hace en el servidor en la nube. También se pudo comprobar que no tienen una organización de respaldo de dato, solamente se realiza un respaldo periódico sin ningún control o vigilancia de parte del administrador de la organización.

Nota: Fuente de elaboración propia

Componente 7: Plan de continuidad

Tabla N°32.-*Hallazgo de Auditoria (Componente 7)*

GRUPO TECNOLÓGICO ALINTI

Hallazgos de la Auditoría	
Componente	Plan de continuidad
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS04: Gestionar la Continuidad
Práctica	DSS04.1: Definir la política de continuidad del negocio,
Objetivo	Se ha puntualizado y demostrado los planes y el alcance de las políticas de continuidad de la organización en casos de desastres naturales o incidentes causados que puedan dañar las operaciones totales o paralelos de tecnología de información

Resultados

Los 20 trabajadores en las distintas áreas mencionaron que no hay un plan de continuidad ante un desastre natural o realizado y que en un corto o largo plazo lo estarán implementado.

Nota: Fuente de elaboración propia

Componente 8: Plan de contingencia

Tabla N°33.-*Hallazgo de Auditoria (Componente 8)*

GRUPO TECNOLÓGICO ALINTI	
Hallazgos de la Auditoría	
Componente	Plan de contingencia
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS02: Gestionar las peticiones y los Incidentes de Servicio
Práctica	DSS02.5: Resolver y recuperarse de incidentes
Objetivo	Se ha documentado, gestionado y ratificado soluciones reconocidas o transitorios y se ha hecho acciones de mejoría para arreglar el servicio de tecnología de información.
Resultados	
Se verifico que, en caso de errores de los SI, la organización no cuenta con un plan de contingencia, ya que si pasará algún inconveniente se llamaría a los trabajadores responsables que puedan solucionar rápida a los conflictos.	

Nota: Fuente de elaboración propia

Componente 9: Plan de mantenimiento de Hardware y Software

Tabla N°34.-*Hallazgo de Auditoria (Componente 9)*

GRUPO TECNOLÓGICO ALINTI	
Hallazgos de la Auditoría	
Componente	Plan de mantenimiento de Hardware y Software
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS01: Gestionar las Operaciones
Práctica	DSS01.3: Supervisar la infraestructura de TI
Objetivo	Se ha inspeccionado la infraestructura de tecnología de información y los sucesos relacionados y acumulados los registros ordenadamente de las instrucciones de mantenimiento de Hardware y Software.
Resultados	
El área tiene un plan de mantenimiento de prevención y disciplinario de los dispositivos, pero no cuenta con un registro de eventos, la cual sería muy importante para poder medir el desempeño de los 20 trabajadores.	

Nota: Fuente de elaboración propia

ÁREA DE DOCUMENTACIÓN DE SW Y HW

Se ha evaluado los 3 componentes, se obtuvieron los siguientes detalles

Componente 10: Existe licenciamiento de los aplicativos instalados en el equipo informático

Tabla N°35.-*Hallazgo de Auditoria (Componente 10)*

GRUPO TECNOLÓGICO ALINTI	
	Hallazgos de la Auditoría
Componente	Existe licenciamiento de los aplicativos instalados en el equipo
Dominio	Construir, adquirir e Implementar (BAI)
Proceso	BAI09: Gestionar los Activos
Práctica	BAI09.5: Administrar licencias
Objetivo	Se ha gestionado las licencias de software de forma que se mantenga el número perfecto de licencias para soportar los requisitos de la empresa.
	Resultados
En la mayoría de equipos de la empresa cuenta con licencia originales y las condiciones son óptimas, pero cuenta también con trabajadores remoto lo cual, se desconoce si esos equipos tienen licencia.	

Nota: Fuente de elaboración propia

Componente 11: Existencia de documentos de adquisición de equipos y software, contrato legal de proveedor de internet (ISP).

Tabla N°36.-*Hallazgo de Auditoria (Componente 11)*

GRUPO TECNOLÓGICO ALINTI	
	Hallazgos de la Auditoría
Componente	Existencia de documentos de adquisición de equipos y software, contrato legal de proveedor de internet (ISP)
Dominio	Alinear, Planificar y Organizar (APO)
Proceso	APO10: Gestionar los Proveedores
Práctica	APO10.3: Gestionar contratos y relaciones con proveedores
Objetivo	Se ha elegido proveedores que están decidido a las prácticas justas y formales que afirmen la clasificación del que mejor se adecue a las exigencias.
	Resultados
Se ha constatado la presencia de documentos de obtención de dispositivos y software y contratos legales de proveedores de internet, se notó que la organización tiene un contrato legal, preservando por el área sistemas, no se puede acceder físicamente pero el trabajador aseguró la existencia del mismo	

Nota: Fuente de elaboración propia

Componente 12: Documentación de los sistemas utilizados para los servicios de la empresa

Tabla N°37.-*Hallazgo de Auditoria (Componente 12)*

GRUPO TECNOLÓGICO ALINTI	
	Hallazgos de la Auditoría
Componente:	Documentación de los sistemas utilizados para los servicios de la empresa
Dominio	Construir, Adquirir e Implementar (BAI)
Proceso	BAI04: Gestionar la Disponibilidad y Capacidad
Práctica	BAI04.4: Supervisar y revisar la Disponibilidad y la Capacidad
Objetivo	Se ha establecido la existencia de la documentación de los sistemas obtenidos por la organización y si esta documentación tiene toda la información primordial para dar mantenimiento al sistema en caso preciso.
Resultados	
No cuenta con documentación especifica o bien elaborada ya que, SGA es un sistema recién creado con el propósito de gestionar las acciones de la entidad.	

Nota: Fuente de elaboración propia

PLANIFICACIÓN Y ORGANIZACIÓN DE LA AUDITORIA INTERNA

Se ha evaluado los 5 componentes, se obtuvieron los siguientes detalles

Resultado obtenido de objetivo específico 1:

Componente 13: Evaluación de riesgo

Tabla N°38.- *Hallazgos de auditoría (componente 13)*

GRUPO TECNOLÓGICO ALINTI	
	Hallazgos de la Auditoría
Componente	Evaluación de riesgo
Dominio	Alinear, Planificar y Organizar (APO).
Proceso	APO09: Evaluar y gestionar riesgos
Práctica	APO12.04: Evaluación de Riesgo
Objetivo	En la meta se identificó los riesgos críticos relacionados con los procesos, sistemas y controles internos que garantizo un nivel adecuado de control y mitigación.
Resultados	
La identificación exhaustiva y análisis detallado de los riesgos críticos que afectan a los procesos, sistemas y controles internos en el entorno de la organización. Este enfoque asegura la evaluación completa de los riesgos para una gestión efectiva y una correcta mitigación de los mismos, conforme a los estándares de COBIT 5, con miras a mejorar la eficiencia y efectividad de la auditoría interna.	

Nota: Fuente de elaboración propia

Componente 14: Establecimiento de objetivos y alcance

Tabla N°39.- *Hallazgo de Auditoria (Componente 14)*

GRUPO TECNOLÓGICO ALINTI	
Hallazgos de la Auditoría	
Componente	Establecimiento de objetivos y alcance
Dominio	Alinear, Planificar y Organizar (APO)
Proceso	APO02: Definir la estrategia.
Práctica	APO02.03: Establecer objetivos y alcance
Objetivo	Se ha definido de manera precisa y clara los objetivos y alcance de la auditoría interna, abarcando aspectos fundamentales de los procesos y controles internos.
Resultados	
Se ha establecido de forma detallada los objetivos y alcance de la auditoría interna para cubrir áreas críticas de los procesos y controles internos, asegurando una correcta gestión de riesgos y cumplimiento de los objetivos organizativos. Esta metodología garantizo una coherencia y alineación efectiva entre los objetivos de la auditoría y los objetivos estratégicos de la organización, conforme a las directrices de COBIT 5.	

Nota: Fuente de elaboración propia

Componente 15: Asignación de recursos

Tabla N°40.- *Hallazgo de Auditoria (Componente 15)*

GRUPO TECNOLÓGICO ALINTI	
Hallazgos de la Auditoría	
Componente:	Asignación de recursos
Dominio	Alinear, Planificar y Organizar (APO)
Proceso	APO07: Gestión de recursos humanos
Práctica	APO07.03: definición de Roles y responsabilidades
Objetivo	Se ha garantizado la definición optima clara y comprensión de roles y responsabilidades.
Resultados	
Se ha mejorado en la transparencia y la rendición de cuentas en la organización y mejorar en la confidencialidad de la información.	

Nota: Fuente de elaboración propia

Componente 16: Programación de actividades

Tabla N°41.-*Hallazgo de Auditoria (Componente 16)*

GRUPO TECNOLÓGICO ALINTI	
	Hallazgos de la Auditoría
Componente	Programación de actividades
Dominio	Alinear, Planificar y Organizar (APO).
Proceso	APO01: Gestionar el marco de TI
Práctica	APO01.02: Establecer la estrategia de Ti.
Objetivo	Se ha definido las técnicas de TI alineada con los objetivos comerciales.
Resultados	
Se ha mejorado en la alineación entre TI y los objetivos comerciales	

Nota: Fuente de elaboración propia

Componente 17: Controles para la instalación de dispositivos externos

Tabla N°42.-*Hallazgo de Auditoria (Componente 17)*

GRUPO TECNOLÓGICO ALINTI	
	Hallazgos de la Auditoría
Componente	Controles para la instalación de dispositivos externos
Dominio	Entregar, dar Servicio y Soporte (DSS)
Proceso	DSS05: Garantizar la seguridad de los sistemas.
Práctica	DSS05.04: Gestionar los servicios de seguridad.
Objetivo	Se ha establecido controles para la instalación de dispositivos
Resultados	
Se ha incluido la implementación de controles robustos que regulen y aseguren la correcta instalación de equipos externos, salvaguardando los datos crítica de la organización de posibles vulnerabilidades y riesgos de seguridad. Esta estrategia se enfocó en fortalecer la seguridad de TI mediante controles específicos para la instalación de dispositivos externos, contribuyendo a una gestión eficaz de la seguridad de los datos y minimizando las posibles amenazas.	

Nota: Fuente de elaboración propia

PROCESO DE EJECUCIÓN DE LA AUDITORÍA INTERNA

Se ha evaluado los 3 componentes, se obtuvieron los siguientes detalles

Resultado obtenido del objetivo específico 2:

Componente 18: Recolección de evidencias

Tabla N°43.-*Hallazgo de Auditoria (Componente 18)*

GRUPO TECNOLÓGICO ALINTI

Hallazgos de la Auditoría	
Componente:	Recolección de evidencias
Dominio	Monitorear, Evaluar y Evaluar el desempeño (MEA).
Proceso	MEA03: Asegurar el cumplimiento con políticas Normas y
Práctica	MEA.03.02: Recopilación de Evidencia.
Objetivo	Se ha garantizado la recopilación adecuada, análisis presentación de evidencias durante la auditoría interna que se ha respaldado las conclusiones y hallazgos asegurando la integridad y validez de la información obtenida.

Resultados

La recolección efectiva de evidencia durante la auditoría interna garantizo la veracidad y facilidad de los hallazgos permitiendo una evaluación precisa del cumplimiento con políticas, normas y procedimientos establecidos. Esto facilito la identificación de área de mejorar y el fortalecimiento de los controles internos para disminuir peligros y mejorar la eficiencia operativa.

Nota: Fuente de elaboración propia

Componente 19: Evaluación de controles

Tabla N°44.-*Hallazgo de Auditoria (Componente 19)*

GRUPO TECNOLÓGICO ALINTI	
Hallazgos de la Auditoría	
Componente:	Evaluación de controles
Dominio	Entregar, Servicio y Soporte (DSS).
Proceso	DSS04: Garantizar un servicio continuo
Práctica	DSS04.03: Realizar Evaluaciones de Control
Objetivo	Se ha evaluado la efectividad de los controles ejecutados que garantizo la continuidad de los servicios de TI y la protección de la información.
Resultados	
La evaluación periódica de los controles permitió reconocer posibles debilidades, vulnerabilidades y desviaciones en el cumplimiento de las políticas de seguridad, lo que contribuyó a la mejora continua de la postura de seguridad de la entidad y a la mitigación de peligros.	

Nota: Fuente de elaboración propia

Componente 20: comunicación de hallazgos

Tabla N°45.-*Hallazgo de Auditoria (Componente 20)*

GRUPO TECNOLÓGICO ALINTI	
Hallazgos de la Auditoría	
Componente	comunicación de hallazgos
Dominio	Entrega, Soporte y Monitoreo (EDM).
Proceso	EDM03: Asegurar la Entrega de Valor de TI
Práctica	EDM03.04: comunicar hallazgos y recomendaciones.
Objetivo	Se ha comunicado de manera efectiva los hallazgos de auditoría y las recomendaciones resultantes que garantizo una comprensión clara y una acción oportuna por parte de los interesados.
Resultados	
El comunicado adecuado de los hallazgos y recomendaciones permitió a la dirección y a las partes interesadas tomar decisiones informadas, que han mejorado gestión de riesgos y la eficacia de los controles internos, y hallan promovido la transparencia y la rendición de cuentas en la entidad.	

Nota: Fuente de elaboración propia

EVALUACIÓN DE LA AUDITORIA INTERNA

Se ha evaluado los 2 componentes, se obtuvieron los siguientes detalles

Resultado obtenido de objetivo específico 3:

Componente 21: Revisión de los procesos de auditoría

Tabla N°46.-*Hallazgo de Auditoria (Componente 21)*

GRUPO TECNOLÓGICO ALINTI	
Hallazgos de la Auditoría	
Componente	Revisión de los procesos de auditoría
Dominio	Entrega, Soporte y Monitoreo (EDM)
Proceso	EDM04: Asegurar la Conformidad con Requisitos Externos
Práctica	EDM04.02: Revisar Procesos de Auditoría
Objetivo	Se ha revisado regularmente los procesos de auditoría que garantizo su eficacia y alineación con los requisitos externos, normativas y estándares aplicables.
Resultados	
La revisión periódica de los procesos de auditoría permitió identificar oportunidades de mejora, asegurar la conformidad con los requisitos legales y normativos, y fortalecer la calidad y credibilidad de las actividades de auditoría interna.	

Nota: Fuente de elaboración propia

Componente 22: Análisis de hallazgos y recomendaciones

Tabla N°47.-*Hallazgo de Auditoria (Componente 22)*

GRUPO TECNOLÓGICO ALINTI	
Hallazgos de la Auditoría	
Componente	Análisis de hallazgos y recomendaciones
Dominio	Alinear, Planificar y Organizar (APO)
Proceso	APO09: Evaluar y Gestionar Riesgos
Práctica	APO09.04: Analizar Hallazgos y Formular Recomendaciones
Objetivo	Se ha analizado de manera exhaustiva los hallazgos de auditoría, se ha evaluado los riesgos asociados y se formuló recomendaciones efectivas para abordar las deficiencias
Resultados	
El análisis detallado de los hallazgos y la formulación de recomendaciones pertinentes permitió mitigar riesgos y las mejoras que se han hecho y los controles internos y se ha promovido la eficacia operativa en la organización, fomentando una cultura de mejora continua y cumplimiento.	

Nota: Fuente de elaboración propia

Tabla N°48.- *Plan de Acción*

ÁREA DE CONTROL	CONTROLES IMPLEMENTADOS	PROPUESTAS DE MEJORA	ACCIONES REALIZADAS	RECURSOS UTILIZADOS
Firewall y técnicas de detección de delitos	Se instalaron Firewall y se configuro un, sistemas básicos de detección de instrucciones (IDS)	Se recomendó implementar firewalls de próxima generación de detección y prevención de instrucciones (IDS).	1.-se evaluaron proveedores de firewall de próxima generación y sistemas de IDPS 2.-Se adquirieron e instalaron los nuevos sistemas 3.-se configuraron las políticas de seguridad y se realizaron pruebas continuas	Talento humano:1 ingeniero de redes, 1 analista de seguridad. Financiero:4000 soles /firewalls y IDPS). Tecnológicos: equipos y software de seguridad avanzada
Actualizaciones habituales de software	Se configuraron actualizaciones automáticas para software crítico y se realizaron procesos manuales para otras aplicaciones	Se recomendó implementar una solución de gestión de parches centralizadas para todas las aplicaciones y sistemas y sistemas operativos	1.-Se seleccionó e implementó un sistema de gestión de parches. 2.-Se configuraron actualizaciones y programas. 3.-Se realizaron auditorias periódicas para asegurar la efectividad del sistema	Talento humano: 1 administrador de sistemas,1 técnico de soporte. Financiero:4000 soles (software de gestión de parches). Tecnológicos: herramientas de gestión de parches

Gestión de identificaciones y acceso	Se implemento control de acceso basado en roles y autentificación por contraseña	Se recomendó implementar autentificación multifactor y mejorar la gestión de identidades con un sistema de administración de identidades y acceso	1.-Se seleccionó e implemento un sistema y una solución 2.-Se configuró el sistema para todos los accesos críticos 3.-Se capacitó al personal en el uso del nuevo sistema	Talento humano. 1 especialista en seguridad Financiero: 3000 soles (sistema MFA Y IAM) Tecnológico: software y hardware MFA Y IAM solución
Auditoría y monitoreo de página web	Se realizo un monitoreo básico de tráfico web y auditorias periódicas manuales	Se recomendó implementar herramientas de escaneo de vulnerabilidades web y un sistema de monitoreo en tiempo real para actividades sospechosas	1.- Se evaluaron y adquirieron herramientas de escaneos de vulnerabilidad web 2.-Se configuraron sistemas de monitoreo en tiempo real 3.- Se realizaron auditorias y ajustes periódicos	Talento humano: 1 analista de seguridad Financiero: 2000 soles (herramientas de escaneo y monitoreo) Tecnológico: software de escaneo y vulnerabilidades de monitoreo

Nota. Elaboración propia

4.5.2. FASE DE EVALUACIÓN DE RIESGOS Y CONTROLES

Tabla N°49.-*Matriz de análisis de riesgos de la infraestructura de la oficina de informática*

Oficina de informática										
Amenazas probabilidad		Degradación			Impacto			Estimación de Riesgo		
		DC	DI	DD	IC	II	ID	RC	RI	RD
Falla de solución en el respaldo de datos	3	3	2	3	Alto	Moderado	Alto	Alto	Medio	Bajo
Accesos indebidos a sistemas internos	2	2	3	2	Media	Alta	Moderado	Medio	Medio	Bajo
Infección por ransomware	2	2	3	3	Medio	Alta	Alto	Alto	Medio	Bajo
Perdida de información critica	2	2	2	3	Media	Moderada	Alto	Medio	Bajo	Bajo

Nota. Elaboración propia

Tabla N°50.-Matriz de análisis de riesgos de la infraestructura de la empresa del Grupo Tecnológico Alinti

Infraestructura de la empresa del Grupo Tecnológico Alinti										
Amenazas probabilidad		Degradación			Impacto			Estimación de Riesgo		
		DC	DI	DD	IC	II	ID	RC	RI	RD
Interrupción de suministro eléctrico	2	2	2	3	Media	Moderada	Alto	Alto	medio	Bajo
Errores en la configuración de software	3	3	2	2	Alta	Moderada	Moderado	Medio	Medio	Bajo
Exposición a malware desde dispositivos externos	2	2	3	3	Media	Alta	Alto	Alto	Medio	Bajo

Problemas de acceso a la red debido a los fallos en el hardware	2	2	2	2	Media	Moderada	Moderado	Medio	Bajo	Bajo

Fuente. Elaboración propia

Tabla N°51.-Matriz de análisis de riesgo de equipos de cómputo de la oficina de informática

Equipos de cómputo de la Oficina de informática										
Amenazas probabilidad		Degradación			Impacto			Estimación de Riesgo		
		DC	DI	DD	IC	II	ID	RC	RI	RD
Fallas en el sistema de enfriamiento	3	3	2	2	Alta	Moderada	Moderado	Alta	Medio	Bajo
Desgaste de uso prolongado	2	2	1	2	Media	Baja	Moderado	Medio	Bajo	Bajo
Interrupción de red debido a fallos de hardware.	3	3	2	3	Alta	Moderada	Alto	Alto	Medio	Bajo
Errores en actualizaciones de software	2	2	2	2	Media	Moderada	Moderado	Medio	Bajo	Bajo
Fuga de datos por vulnerabilidades	2	3	3	3	Alta	Alta	Alto	Alto	Medio	Bajo
Configuración incorrecta del sistema	2	2	2	2	Media	Moderada	Moderado	Medio	Bajo	Bajo
Accesos no autorizados a equipos	3	3	3	3	Alta	Alta	Alto	Alto	Medio	Bajo
Uso indebido de privilegios de administrador	2	2	3	3	Media	Alta	Alto	Medio	Bajo	Bajo
Revelación accidental de información	2	2	2	2	Media	Moderada	Moderado	Medio	Bajo	Bajo
Manipulación física de equipos	2	2	3	2	Media	Alta	Moderado	Medio	Bajo	Bajo

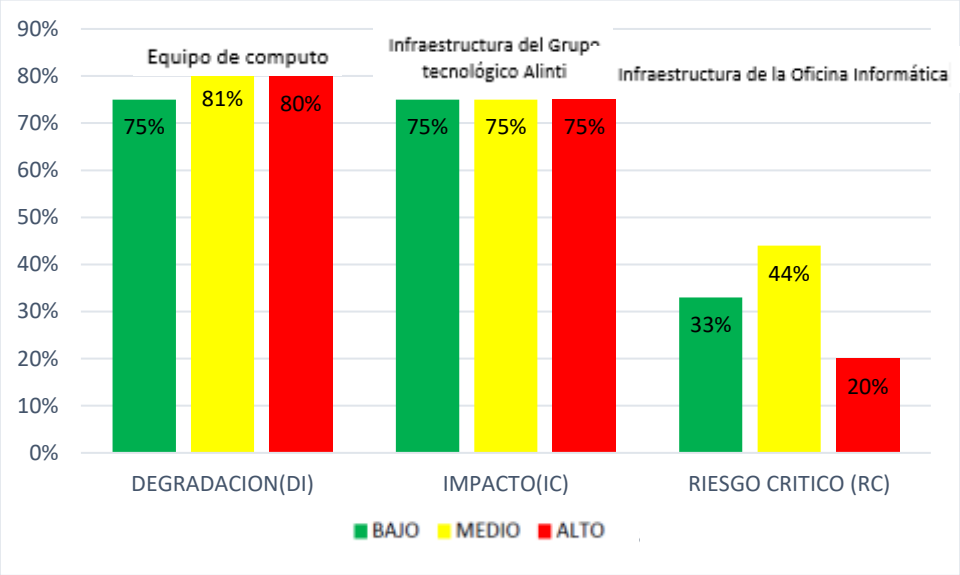
Fuente. Elaboración propia

TABLA N°52.- Análisis de riesgos de todos los componentes evaluados

CATEGORÍA	EQUIPO DE COMPUTO	INFRAESTRUCTURA DEL GRUPO TECNOLÓGICO ALINTI	INFRAESTRUCTURA DE LA OFICINA DE INFORMÁTICA
PROBABILIDAD (DC)	78%	75%	75%
DEGRADACION(DI)	75%	75%	33%
IMPACTO(IC)	81%	75%	44%
RIESGO CRÍTICO (RC)	80%	75%	20%

Nota. Elaboración propia

Figura 07: Análisis de riesgos de todos los componentes evaluados



Nota : De las tablas 48,49 y 50 y la figura 7 se puede visualizar que el que tiene mayor probalidad de riesgo es el componente de equipo de computo con 80% de riesgo alto y tambien la infrestructura de la oficina de informática con un 20%(Elaboracion propia).

Tabla N°53.-*Evaluación controles*

Tipo de control	Tipo de control (Alto/Medio /Baja) Observaciones	Observaciones
Medidas de seguridad de la tecnología de información	Alto	Medidas bien argumentadas y informadas
Firewalls y técnicas de detección de delitos	Alto	Configuración actualizada, pero se solicita monitoreo permanente.
Actualizaciones habituales de software de uso	Medio	Desarrollos eficaces de aplicaciones de actualizaciones.
Gestión de identificación y ingreso	Medio	instrucciones implementadas, pero hay dependencias para optimizar en la gestión de accesos.
Auditorías y monitoreo de páginas web	Baja	La ejecución de auditoría y monitoreos de las páginas web es limitada; se indica optimizar.
Respaldo de seguridad y métodos de recuperación	Media	Se ejecutan respaldo de seguridad de manera frecuente, y los métodos de recuperación están bien determinados
Instrucción en concientizar en la seguridad para los trabajadores	Alta	Reuniones de formaciones habituales, pero se puede optimizar la participación activa de los trabajadores.

Seguridad física de los dispositivos y centros de información	Alta	Restricción de acceso y control de seguridad eficaces.

Fuente (elaboración propia)

Tabla N°54.- *Lista de equipos*

N°	EQUIPOS
1	IMPRESORA LASER 408dn
2	PC 11TH GEN INTEL(R) CORE(TM) I5
3	LAPTOP HP 7TH GEN CORE(TM) I5
4	LAPTOP LENOVO 8TH GEN CORE I5
5	SERVIDOR DE RESPALDO

*Fuente :*Elaboracion propia

ANÁLISIS DE LA ENTREVISTA REALIZADA AL TRABAJADOR DE LA EMPRESA DEL GRUPO TECNOLÓGICO ALINTI

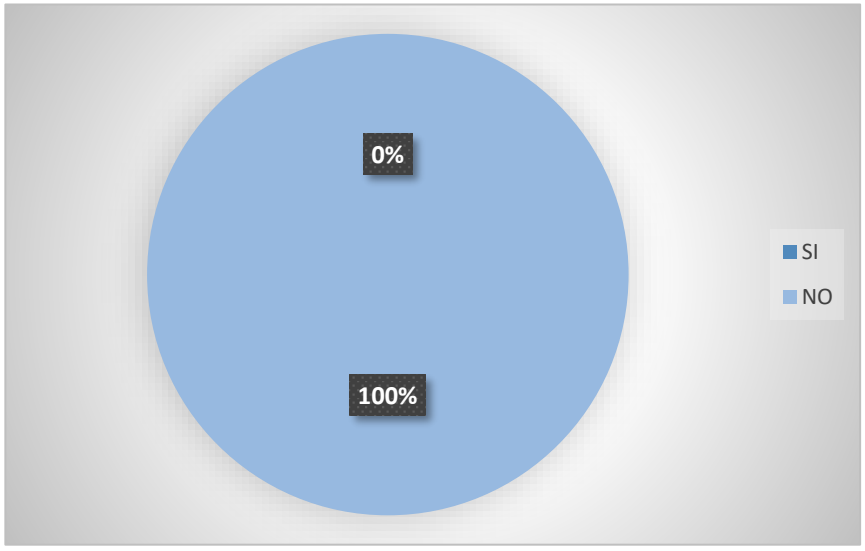
¿Se ha realizado alguna vez algún tipo de auditoría en la oficina de informática?

Tabla N°55.-*Auditoria y planificación*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	20	100%
TOTAL	20	100%

Fuente: Elaboración propia

Figura 08: *Auditoria y planificación*



Nota:En el gráfico nos representa que de un total de 20 trabajadores entrevistados el 100% menciona que no se hiso ninguna auditoría interna y el 0% son las que nos dicen nada(Elaboracion propia).

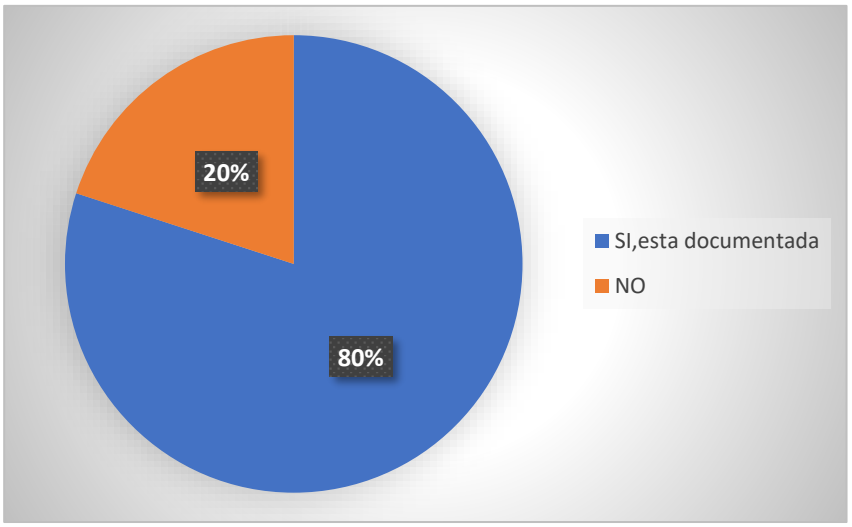
¿La oficina de Informática cuenta con una planificación estratégica?

Tabla N°56.-*Planificacion estratégica*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI,está documentada	16	80%
NO	4	20%
TOTAL	20	100%

Fuente.Elaboración

Figura 09: *Planificación estratégica*



Nota: En el gráfico vemos que el 20% representan los 4 trabajadores que se ha entrevistado ,mencionan que no hay planificación estratégica en el la organización y el 80% representa a los 16 trabajadores que mencionan que si hay planificación estratégica y esta documentado (Elaboración propia).

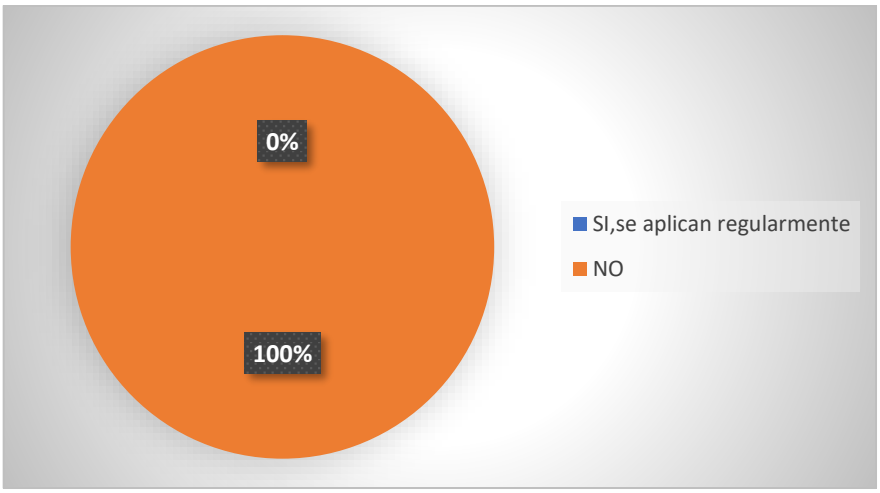
¿Existen protocolos informáticos internas que se estén aplicando?

Tabla N°57.-*Politicas de información interna*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI,se aplican regularmente	0	0%
NO	20	100%
TOTAL	20	100%

Fuente :Elaboracion propia

Figura 10: *Políticas de información interna*



*Nota:*en el gráfico vemos que el 100% representa a los 20 trabajadores que se han entrevistado , que no conocen ningún protocolo informática interna dentro de la organización y el 0% no menciona nada(Elaboración propia)

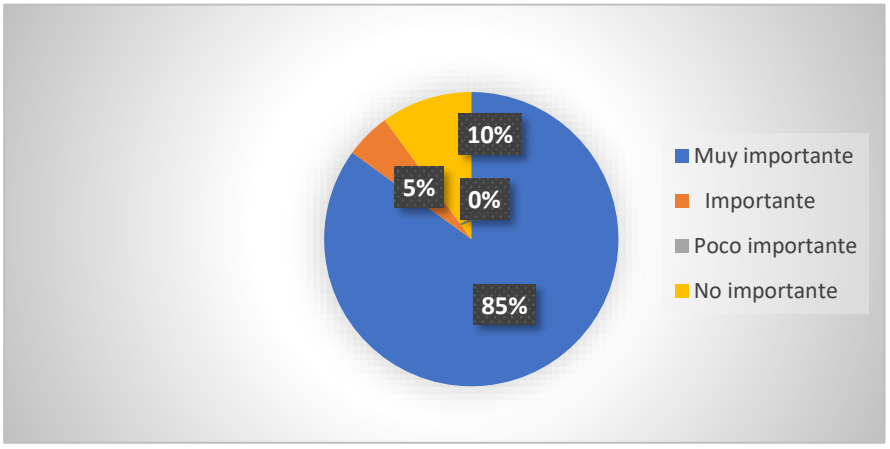
¿Qué tan importante son las tecnologías de información para la organización?

Tabla N°58.-*Tecnologías de información*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
Muy importante	17	85%
Importante	1	5%
Poco importante	0	0%
No importante	2	10%
TOTAL	20	100%

Fuente :.elaboracion propia

Figura 11: *Tecnología de información*



Nota: En el gráfico no muestra el 85% representa los 17 trabajadores que fueron entrevistados, ellos mencionan que son muy importante las TI, el 5% representa a 1 trabajador que menciona que es importante la TI, el 0% menciona que es poco importante la TI y el 10% representa a los 2 trabajadores, menciona que no es importante (Elaboración propia).

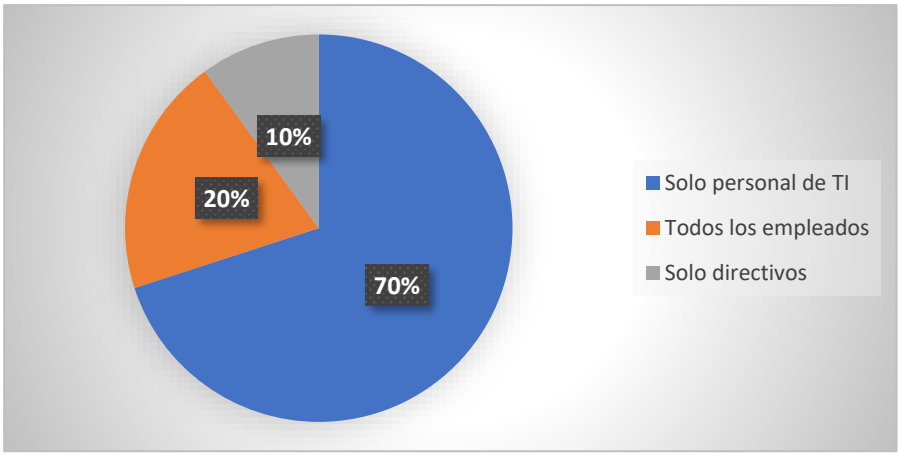
¿Quiénes están capacitados para ingresar a los registros y programas de la organización?

Tabla N°59.-*Medidas de seguridad*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
Solo personal de TI	14	70%
Todos los empleados	4	20%
Solo directivos	2	10%
TOTAL	20	100%

Fuente: elaboración propia

Figura 12: *Medidas de seguridad*



Nota: En la gráfica vemos que el 70% representa los 14 trabajadores que, ellos mencionan que solo los personales de TI pueden ingresar a los registros y programas. El 20% representa los 4 trabajadores, ellos mencionan que todos los empleados pueden ingresar y el 10% representa los trabajadores, ellos mencionan que solo los directivos pueden acceder (Elaboración propia).

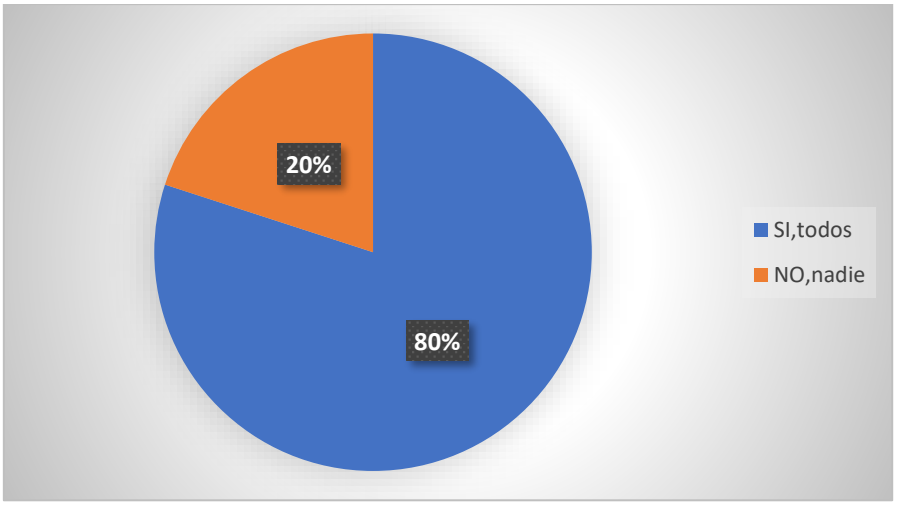
¿Todos los colaboradores de la organización tienen usuario y contraseña para ingresar a sus dispositivos de trabajo?

Tabla N°60.-*Usuarios con contraseña*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI.todos	16	80%
NO,nadie	4	20%
TOTAL	20	100%

Fuente: elaboración propia

Figura 13: *Usuarios con contraseñas*



Nota: En el gráfico vemos que el 80% representa a los 16 trabajadores que se han entrevistado , menciona que si,todos tiene usuario y contraseña en su dispositivo de trabajo dentro de la organización y el 20% menciona que no tienen(Elaboración propia).

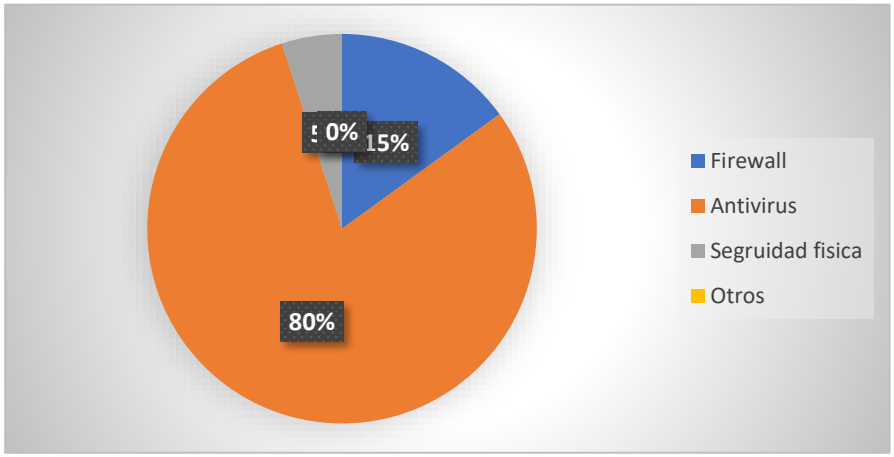
¿Qué medidas de seguridad existen en El Grupo Tecnológico Alinti?

Tabla N°61.- *Protección de herramientas*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
Firewall	3	15%
Antivirus	16	80%
Segruidad fisica	1	5%
Otros	0	0%
Total	20	100%

Fuente .Elaboracion propia

Figura 14: *Herramientas de protección*



Nota: En la gráfica vemos que el 80% representa los 16 trabajadores, ellos mencionan que la medida de seguridad debe ser con el antivirus, el 15% representa a los 3 trabajadores, ellos mencionan que deben ser los firewalls, el 5% representa 1 trabajador, menciona que la seguridad física y el 0% no menciona nada (Elaboración propia).

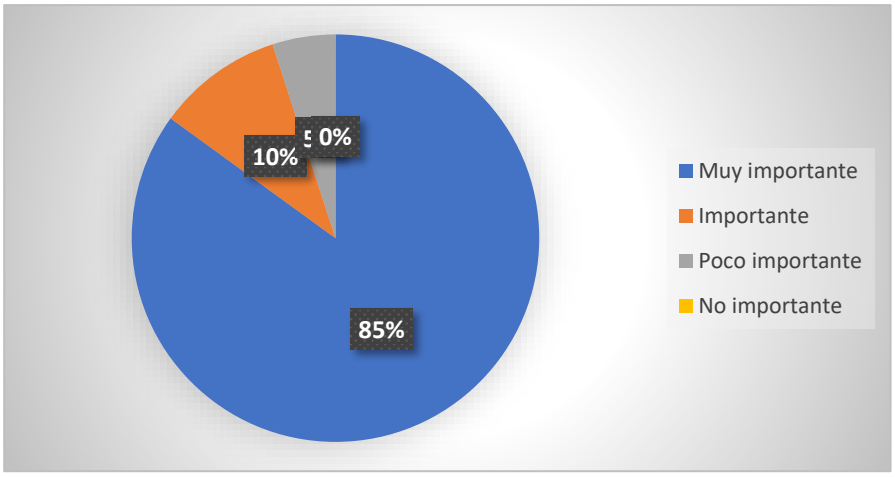
¿Es primordial aplicar un plan de contingencia?

Tabla N°62.- *Plan de contingencia*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
Muy primordial	17	85%
Primordial	2	10%
Poco primordial	1	5%
No primordial	0	0%
Total	20	100%

Fuente.Elaboracion propia

Figura 15: *Plan de contingencia*



Nota: En la gráfica vemos que el 85% representa los 17 trabajadores, ellos mencionan que es muy primordial aplicar un plan de contingencia, el 10% representa a los 2 trabajadores, ellos mencionan que son primordiales, el 5% representa 1 trabajador, menciona que es poco primordial y el 0% no menciona nada (Elaboración propia).

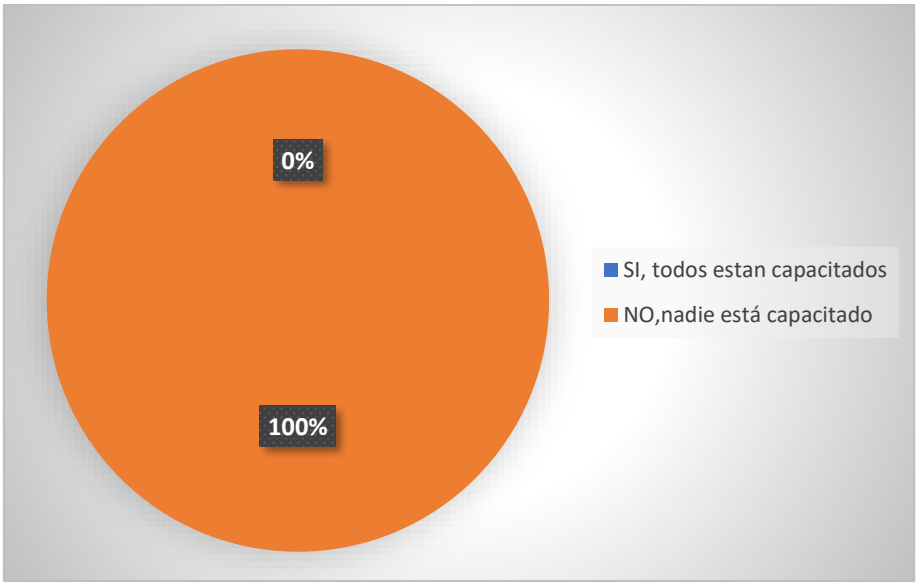
¿El colaborador está capacitado para un ataque informático?

Tabla N°63.-*Plan de restablecimiento*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI,todos estan capacitados	0	0%
NO.nadie esta capacitado	20	100%
TOTAL	20	100%

Fuente.Elaboración propia

Figura 16: *Plan de restablecimiento*



Nota: en el gráfica vemos que el 100% representa a los 20 trabajadores que se han entrevistado , mencionan que nadie está capacitado ante un ataque informático dentro de la organización y el 0% no menciona nada(Elaboración propia)

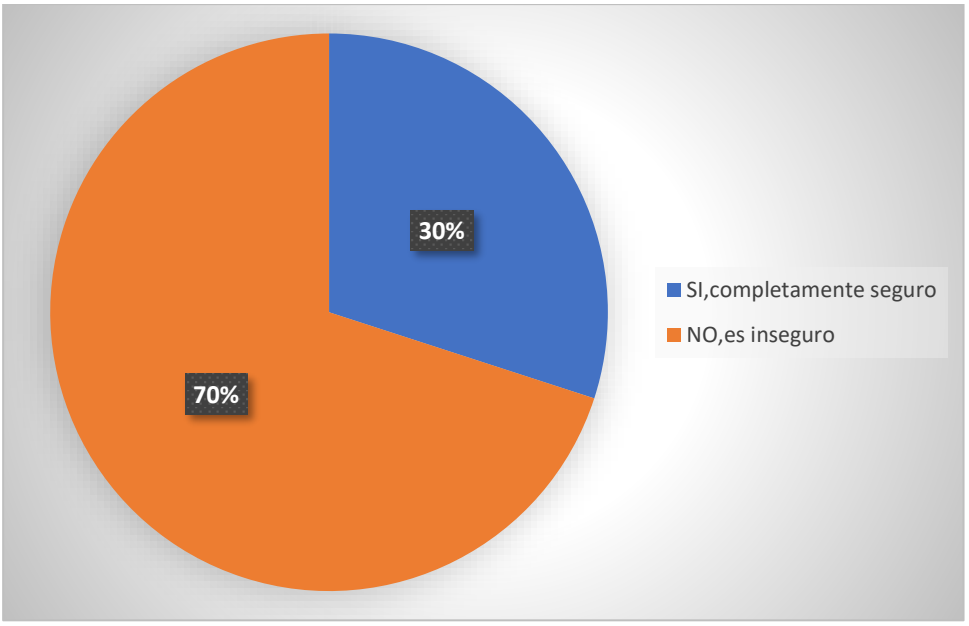
¿El lugar de los servidores cuenta con todas las seguridades físicas adecuadas?

Tabla N°64.-*Reubicacion de servidores*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI,completamente seguro	6	30%
NO,es inseguro	14	70%
TOTAL	20	100%

Fuente. Elaboración propia

Figura 17: *Reubicación de servidores*



Nota: En el gráfico vemos que el 70% representa a los 14 trabajadores que se han entrevistado , ellos mencionan que no cuentan y es inseguro las seguridades físicas dentro de la organización y el 30% menciona que si es completamente seguro seguridad física(Elaboración propia).

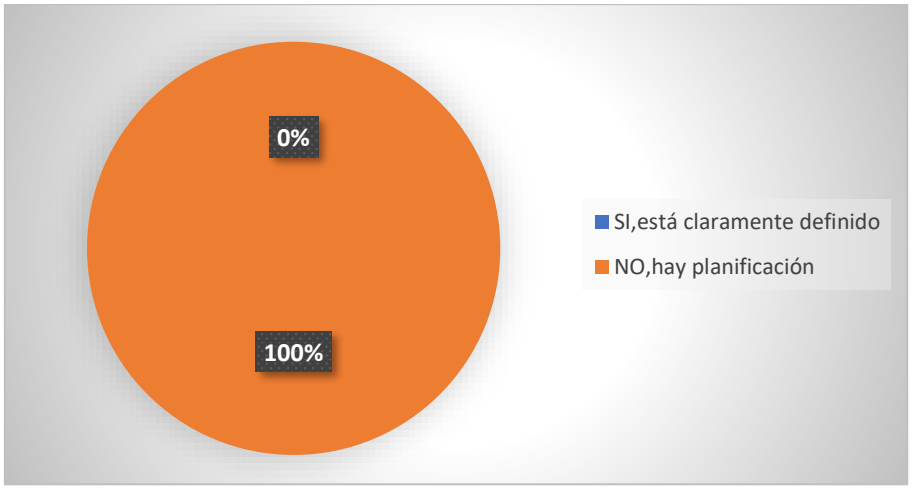
¿Hay alguna planificación en cuanto a la inversión anual para el área de TI dentro del Grupo Tecnológico Alinti?

Tabla N°65.-*Presupuesto para TI*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI,está claramente definido	0	0%
NO,hay planificación	20	100%
TOTAL	20	100%

Fuente. Elaboración propia

Figura 18.- *Presupuesto para TI*



Nota: En el gráfico vemos que el 100% representa a los 20 trabajadores que se han entrevistado , ellos menciona que no hay planificacion de inversión anual para el área de oficina de informática dentro de la organización y el 0% no menciona nada(Elaboración propia).

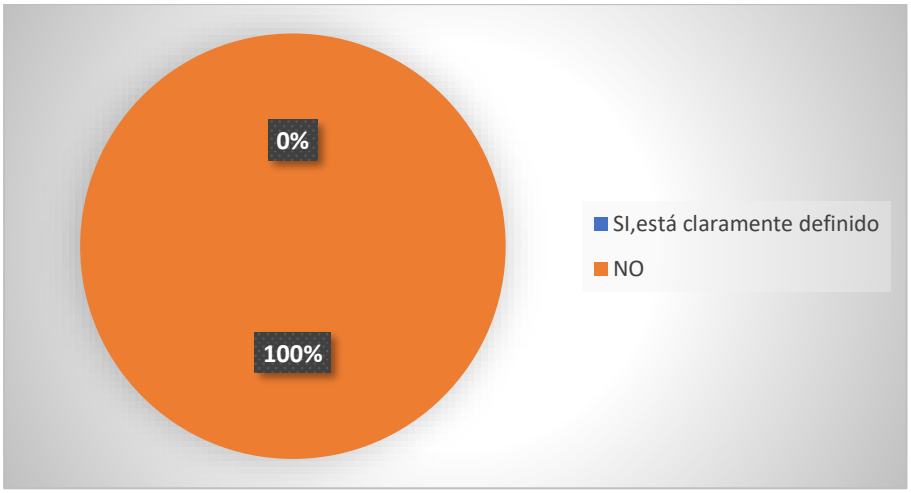
¿Tiene un lugar específico para los dispositivos informáticos nuevos o dañados, partes y piezas?

Tabla N°66.-*Almacen de equipos informáticos usados*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI,está claramente definido	0	0%
NO	20	100%
TOTAL	20	100%

Fuente. Elaboración propia

Figura 19: *Almacén de equipos informáticos usados*



Nota: En el gráfico vemos que el 100% representa a los 20 trabajadores que se han entrevistado , ellos menciona que no hay un lugar especifico para los dispositivos informáticos nuevos o dañados,partes y piezas dentro de la organización y el 0% no menciona nada(Elaboración propia).

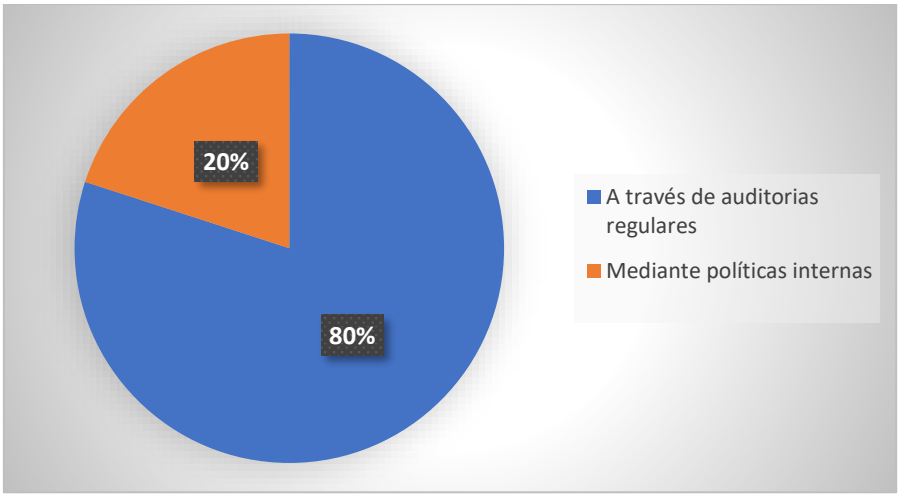
¿En este momento cómo se controlan las tecnologías de información en la organización?

Tabla N°67.-*Control de TI*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
A través de auditorias regulares	16	80%
Mediante políticas internas	4	20%
TOTAL	20	100%

Fuente. Elaboración propia

Figura 20: *Control de TI*



Nota: En el gráfico vemos que el 80% representa a los 16 trabajadores que se han entrevistado , menciona que se controla a través de auditorias regulares la tecnología de información dentro de la empresa y el 20% menciona que mediante políticas internas (Elaboración propia).

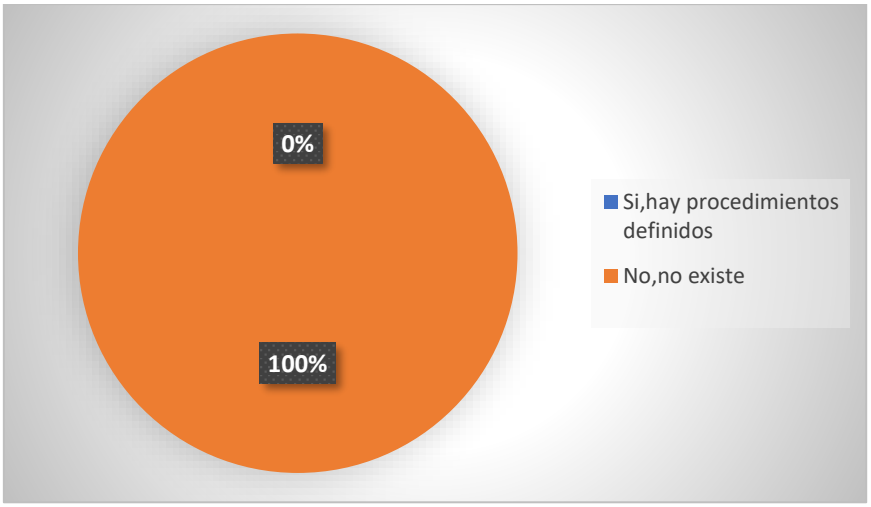
¿Existe una normativa para restablecer operaciones en caso de un fallo en la tecnología de información?

Tabla N°68.-Plan de acción en TI

ALTERNATIVA	FRECUENCIA	PORCENTAJE
Si,hay procedimientos definidos	0	0%
No,no existe	20	100%
TOTAL	20	100%

Fuente. Elaboración propia

Figura 21: *Plan de acción en TI*



Nota: En el gráfico vemos que el 100% representa a los 20 trabajadores que se han entrevistado , ellos menciona que no hay procedimientos definidos para restablecer operaciones ante un suceso en fallo de la TI y el 0% menciona que no existe(Elaboración propia).

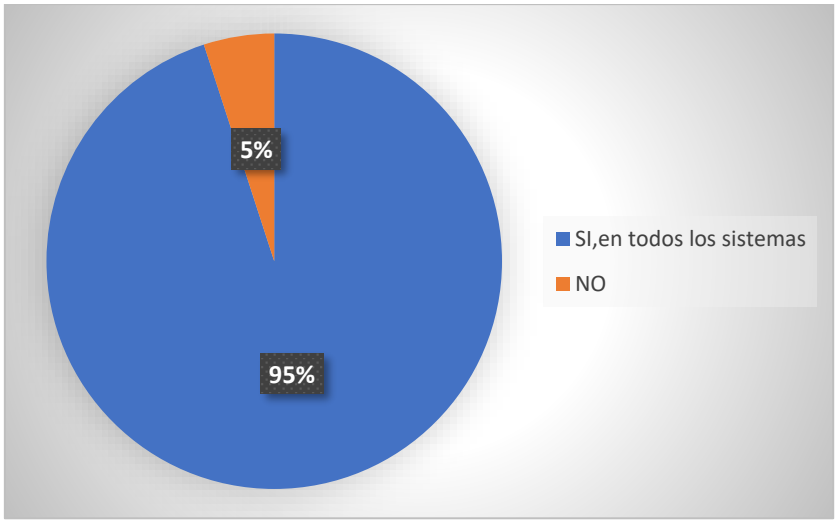
¿La organización del Grupo Tecnológico Alinti usa software libre?

Tabla N°69.-*Sotfware libre*

ALTERNATIVA	FRECUENCIA	PORCENTAJE
Si,en todo los sistemas	19	95%
No	1	5%
TOTAL	20	100%

Fuente. Elaboración propia

Figura 22: *Software libre*



Nota: En el gráfico vemos que el 95% representa a los 19 trabajadores que se han entrevistado , ellos menciona que utilizan en todo los sistemas sotfware libre y el 5% menciona que no utilizan (Elaboración propia).

4.6. DISCUSIÓN

Con los resultados logrados en la investigación podemos concluir que:

- En la investigación ejecutada y con la posición de defender, ya que una auditoría interna si permite evaluar los procesos de manera eficiente la seguridad física de la Infraestructura informática del Grupo tecnológico ALINTI, esta investigación tuvo como finalidad establecer el nivel de capacidad de los procesos de tecnología de información dentro de la empresa a través de la metodología COBIT 5 que proporciono examinar los procesos no aplicados o mal ejecutados.
- Los resultados obtenidos se asemejan a la investigación de (Vargas et al.,2023)**:** "Plan De Auditoría Para El Programa De Auditoría Interna Al Sistema De Gestión De Calidad De La Empresa Carnitas". En la cual determinar la aptitud de las auditorías internas para todas las entidades

  En la investigación ejecutada en la organización del Grupo tecnológico ALINTI en la cual logro resultado de un informe en base a los hallazgos hallados, determinando los procesos del área de calidad alcanzando definir los dominios y procesos de COBIT 5 e identificar las debilidades demostrativas en pocos procesos del área. el cual es una versión más actualizada de los procesos que se van a auditar, tiene aproximaciones a la hora de implementar una auditoría interna, pero COBIT 5 divide los procesos de gobierno y de administración de la tecnología de información empresarial en dos.
- Así mismo (Pinedo y Vilches, 2022). En su Investigación "Auditoría interna y gestión administrativa en la municipalidad provincial de Rioja, 2021 concluye que es necesario de realizar una propuesta de una auditoría interna .La investigación ejecutada en la infraestructura informática del Grupo Tecnológico ALINTI, la cual logro como resultado un informe de mitigación de riesgos que permitió a la oficina de informática, conocer los riesgos de tecnologías de información se estaban presentando, se alcanzó establecer normas dentro del oficina informática para que los procesos de la información se empleen de una forma selecta. La presente investigación nos concede como resultado un plan de acción personalizado para la oficina de informática ya que este arrojó resultados en los cuales se concretó los procesos que no se aplican correctamente, mediante las normas de COBIT

5 se procedió a evaluar los procesos de tecnologías de información dentro de la empresa y posteriormente crear el plan de acción con sus respectivas recomendaciones.

- De esta manera se ha plasmado de una manera más eficiente y eficaz una auditoría interna dentro de la empresa del Grupo Tecnológico ALINTI dentro de la oficina de informática.

CAPITULO VIII

CONCLUSIONES Y RECOMENDACIONES

4.7. CONCLUSIONES

- De acuerdo al objetivo general, se focalizaron en los resultados fundamentales de la auditoría interna basada en COBIT 5 para supervisar la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti en Lima durante el año 2023.

  Este análisis ha permitido entender cómo este modelo de auditoría contribuye a una vigilancia efectiva de los activos tecnológicos críticos.

  La empresa presenta deficiencias significativas en el control de acceso y en la gestión de dispositivos, así como la falta de protocolos de seguridad y documentación adecuada. Aunque existen respaldos de información y un plan de mantenimiento de hardware y software, carecen de un plan de continuidad ante desastres y no se han establecidos protocolos para el uso de dispositivos externos.
- De acuerdo al objetivo específico 1, se han identificado los aspectos esenciales de la planificación y organización de la auditoría interna utilizando COBIT 5 para administrar la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti, proporcionando un esquema organizado y estructurado para enfrentar los desafíos de seguridad.

  Se realizo una evaluación detallada de riesgos que ayudan a mitigarlos efectivamente. Además, se ha logrado una alineación clara entre los objetivos y el alcance de la auditoria. La asignación de recursos ha mejorado bastante la transparencia en la gestión de información, mientras la programación de actividades ha fortalecido la conexión entre la TI y los objetivos comerciales, finalmente se han implementado controles para asegurar una mayor seguridad en la instalación de dispositivos externos.
- De acuerdo al objetivo específico 2, se han revelado los detalles significativos del proceso de ejecución de la auditoría interna basada en COBIT 5 para mantener la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti, asegurando que se mantenga la integridad y la seguridad de la infraestructura a lo largo del tiempo.

La recolección de evidencias ha permitido identificar áreas de mejora y fortalecer los controles internos, lo que contribuye a reducir riesgos y aumentar la eficiencia operativa. Además, la evaluación continua de estos controles ha potenciado su efectividad en la gestión de riesgos.

Finalmente, la comunicación de los hallazgos ha optimizado la gestión la gestión de riesgos y mejorado la eficacia de los controles internos en la empresa del Grupo Tecnológico alinti.

- De acuerdo al objetivo específico 3, se han analizado las particularidades de la evaluación de la auditoría interna basada en COBIT 5 para asegurar la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti e mantengan efectivas y adecuadas, proporcionando una visión clara de cómo se puede medir y mejorar continuamente la protección de los recursos informáticos.

  Ha permitido identificar oportunidades de mejora en los procesos de auditoría interna, A través de los análisis de hallazgos y recomendaciones se ha podido mitigar riesgos y fortalecer los controles internos. estas acciones han promovido una mayor eficiencia operativa dentro de la empresa del Grupo Tecnológico Alinti.

4.8. RECOMENDACIONES

Como resultado de la auditoría interna con la información recopilados y analizados, se brindará las recomendaciones respectivas, con el propósito de contribuir con información importante sobre los componentes auditados.

- Se recomienda fortalecer los protocolos de seguridad mediante la implementación de medidas robustas para el control de acceso y la gestión de dispositivos ,lo que asegura la protección de los activos tecnológicos además se recomienda desarrollar un plan de continuidad ante desastre que contemple estrategias claras para la recuperación de datos y operaciones críticas .Finalmente es recomendable mejora la documentación de políticas y prácticas de seguridad para facilitar la supervisión y garantizar el cumplimiento normativo.
- Se recomienda realizar una revisión periódica de riesgos para adaptarse a las amenazas emergentes y ajustar los controles de seguridad en consecuencia .la capacitación continua de los trabajadores en relación de políticas de seguridad y la correcta utilización de recursos para la auditoría interna, asegurando que estén alineados con los objetivos de seguridad para maximizar su efectividad.
- Se recomienda implementar herramienta de monitoreo que evalué continuamente los controles de seguridad y facilité la recolección de evidencias. Establecer canales de comunicaciones efectiva para difusión de hallazgos y recomendaciones es esencial para asegurar que toda la organización este informada. Además, se debe fortalecer la evaluación de controles internos mediante revisiones periódicas que garanticen su alineación con los objetivos de auditoría.
- Se recomienda desarrollar un plan de mejora continua de los procesos de auditoría ,incorporando feedbck y lecciones aprendidas de auditorías anteriores .Es importante establecer indicadores de desempeño que permiten medir la efectividad de los controles internos y la seguridad de la infraestructura informática .finalmente ,fomentar una cultura organizacional que valore la seguridad informática y que incentivara a los trabajadores a participar activamente en la protección de los recursos tecnológicos.

REFERENCIA BIBLIOGRÁFICA

Tello, B. (2023). *Transformación Digital en el manejo de la Información en las Auditorias de Implicania Contable en el Perú,2022.* Cusco, Perú. https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/5798/Bryan_Tesis_maestro_2023.pdf?sequence=1&isAllowed=y

Alzamora y Palomino , A. (2023). *Auditoría Interna y Gestión de Riesgos en las Cooperativas de Ahorro y Crédito de la Ciudad de Abancay, 2021.* Abancay, Apurimac, Perú. https://repositorio.utea.edu.pe/handle/utea/656

Aquino , Cuevas,Villarroel , R. (2023). *El modelo COBIT 5 para Auditoría Informática de los Sistemas de Información Académica de la Universidad Nacional Jorge Basadre Grohmann.* Tacna, Perú. https://doi.org/10.48168/innosoft.s11.a56

Avalos y Castillo, A. (2022). *Auditoría interna y gestión financiera en las empresas comerciales de Chimbote – 2021.* Chimbote, Perú. https://doi.org/https://hdl.handle.net/20.500.12692/92540

Bernal, C. (2010). *Metodología de la investigación. Bogotá, Colombia: Pearson Education.*

BLOG FETASA. (2024). *Seguridad Física.* https://www.blogfetasa.es/que-es-la-seguridad-fisica-definicion-y-conceptos/

Carrera, B. (2019). *AUDITORIA INFORMÁTICA MEDIANTE LA APLICACIÓN DE LA METODOLOGÍA COBIT, PARA EL CONTROL OPERATIVO DE LOS PROCESOS INFORMÁTICOS EN LA EMPRESA NEXUS TECHNOLOGIES.* Ambato, Ecuador. https://dspace.uniandes.edu.ec/handle/123456789/9890

Chimbo, J., & Narváez, B. (2022). *Auditoría Informática a los Sistemas de Información Aplicados por el gobierno Autónomo descentralizado de Cantó´n Guaranda,provincia Bolívar,2021*. Guaranda, Ecuador. https://dspace.ueb.edu.ec/bitstream/123456789/4899/1/PROYECTO%20DE%20INVESTIGACI%c3%93N%20CH%26N-signed-signed-signed.pdf

Corzo , E. (2023). *Propuesta de mejora al proceso de auditoría interna para el SG-SST de la empresa DEFENDER LTDA bajo la ISO 45001:2018.* Bucaramanga, Colombia. http://repositorio.uts.edu.co:8080/xmlui/handle/123456789/13687

Encalada, G. (2023). *Auditoría Informática Física y Lógica mediante el uso de Metología Magerit en la unidad educativa " Alessandro Volta" Periodo 2022.* El Carmen. https://repositorio.uleam.edu.ec/bitstream/123456789/4600/1/ULEAM-INFOR-0121.pdf

Fahl y Amaral, R. (2023). *Servicio de diseño como enfoque de innovación en auditoría interna de entidades financieras.* Araraqua, Brasil. https://doi.org/https://doi.org/10.35992/pdm.5vi1.1134

Flores,Cruz ,Sánchez, A. (2023). *La auditoría interna en las entidades públicas y privados de Ecuador.* Machala, Ecuador. https://doi.org/https://doi.org/10.33996/revistaenfoques.v7i26.162

Gutiérrez, R. (2022). *La auditoría interna como control para la gestión de medianas y grandes empresas de construcción.* Lima, Perú. https://doi.org/https://doi.org/10.35381/cm.v8i2.704

Hernandez,Fernandez,Baptista, R. (2014). *Metología de la Investigación.* 6ta.

Instituto de autores Internos. (2020). *Normas internacionales para la practica Profesional de la Auditoria Interna.* https://doi.org/hthttps://na.theiia.org/standards/Pages/Standards.aspx

ISACA. (2012). *Un Marco de Negoocio para el Gobierno y la Gestión de las TI de la Empresa.*

Isaca. (2019). *2019 Guía de implementación: Implementación y optimización de una solución de Gobierno de Información y Tecnología.* https://doi.org/https://www.isaca.org/resources/cobit.

Metología de la investigación. (s.f.).

Miranda y Jiménez, G. (2021). *Auditoría interna en el marco de la empresa.* San Jose, Costa Rica. https://doi.org/10.22458/rna.v12i1.3513

Mungabusi, N. (2021). *LA AUDITORÍA INTERNA Y SU INCIDENCIA EN LAS OPERACIONES FINANCIERAS Y ADMINISTRATIVAS DE LA COAC "KULLKI WASI", PERÍODO 2018-2019.* Riobamba, Ecuador. http://dspace.unach.edu.ec/handle/51000/8089

Núñez, A. (2022). *AUDITORÍA INFORMÁTICA A LA "COOPERATIVA DE AHORRO Y CRÉDITO RIOBAMBA LTDA AGENCIA MATRIZ,CANTÓN RIOBAMBA,PROVINCIA DE CHIMBORAZO,PERIODO 2020.* Riobamba, Ecuador. http://dspace.espoch.edu.ec/bitstream/123456789/16760/1/82T01298.pdf

Pinedo y Vilches, B. (2022). *Auditoría interna y gestión administrativa en la municipalidad provincial de Rioja, 2021.* Rioja, Perú. https://doi.org/https://hdl.handle.net/20.500.12692/112137

Quispe , J. (2024). *Análisis de la Auditoría en los sistemas de información.* LIma, Perú. https://repositorio.upci.edu.pe/handle/upci/1067

Ramirez , N. (2023). *AUDITORÍA INFORMÁTICA EN LA SEGURIDAD DE LA INFORMACIÓN SEGÚN LA ISO 27001 EN EMPRESAS COMERCIALES DE EL CARMEN.* El carmen. https://repositorio.uleam.edu.ec/bitstream/123456789/4594/1/ULEAM-INFOR-0118.PDF

Torres, O. (2022). *Análisis sobre la aplicación de framework:COBITt,PMI,CMMI comparado con ITIL v4 en las empresas del sector privado en la Gestión de servicio TI.* Valle del Chalco Solidario, México. http://ri.uaemex.mx/bitstream/handle/20.500.11799/113271/ANALISIS%20SOBRE%20LA%20APLICACION%20DE%20FRAMEWORKS.pdf?sequence=1&isAllowed=y

Urrutia, J. (2023). *Auditoría de gestión en la empresa Avícola Pamelita.* Ambato, Ecuador. https://repositorio.uta.edu.ec:8443/handle/123456789/39857

Vargas,Rojas,Pineda, Vergara,Heredia, A. (2023). *Plan De Auditoría Para El Programa De Auditoría Interna Al Sistema De Gestión De Calidad De La Empresa Carnitas.* Bogota, Colombia. https://doi.org/https://repository.unad.edu.co/handle/10596/59094

Vilchez, J. (2023). *La auditoría de desempeño y su impacto en la calidad de los servicios municipales del distrito de Ventanilla –2022.* Lima, Ventanilla, Perú. https://doi.org/https://hdl.handle.net/20.500.12672/21385

Villadeza y Condori, k. (2022). *Diseño de un Sistema de Gestión de la Seguridad de la Información basado en la Norma técnica Peruana-ISO/IEC 27001:2024 para la Municipalidad Distrital de huáscar 2022.* Huáscar. https://repositorio.unheval.edu.pe/handle/20.500.13080/8238

ANEXOS

ANEXO A

Autorización para recolección de información para trabajo de investigación

ALINTI

Año de la unidad, la paz y el desarrollo

Lima,30 de diciembre 2023

CARTA MÚLTIPLE N°01

Señor:

Hernán Asto Cabezas

Presente. –

ASUNTO : **AUTORIZACIÓN PARA LA RECOLECCIÓN DE INFORMACIÓN PARA REALIZAR TRABAJO DE INVESTIGACIÓN**

REFERENCIA : **SOLICITUD N°01**

Por medio del presente y comunicarle en respuesta a su solicitud de realizar estudios de investigación sobre **"AUDITORÍA INTERNA BASADA EN COBIT 5 PARA EL CONTROL DE LA SEGURIDAD FÍSICA DE LA INFRAESTUCTURA INFORMÁTICA DEL GRUPO TECNOLÓGICO ALINTI, LIMA 2023".** Se concede la autorización y facilidades correspondientes para dicha investigación.

Sin otro particular me suscribo de ustedes.

Atentamente

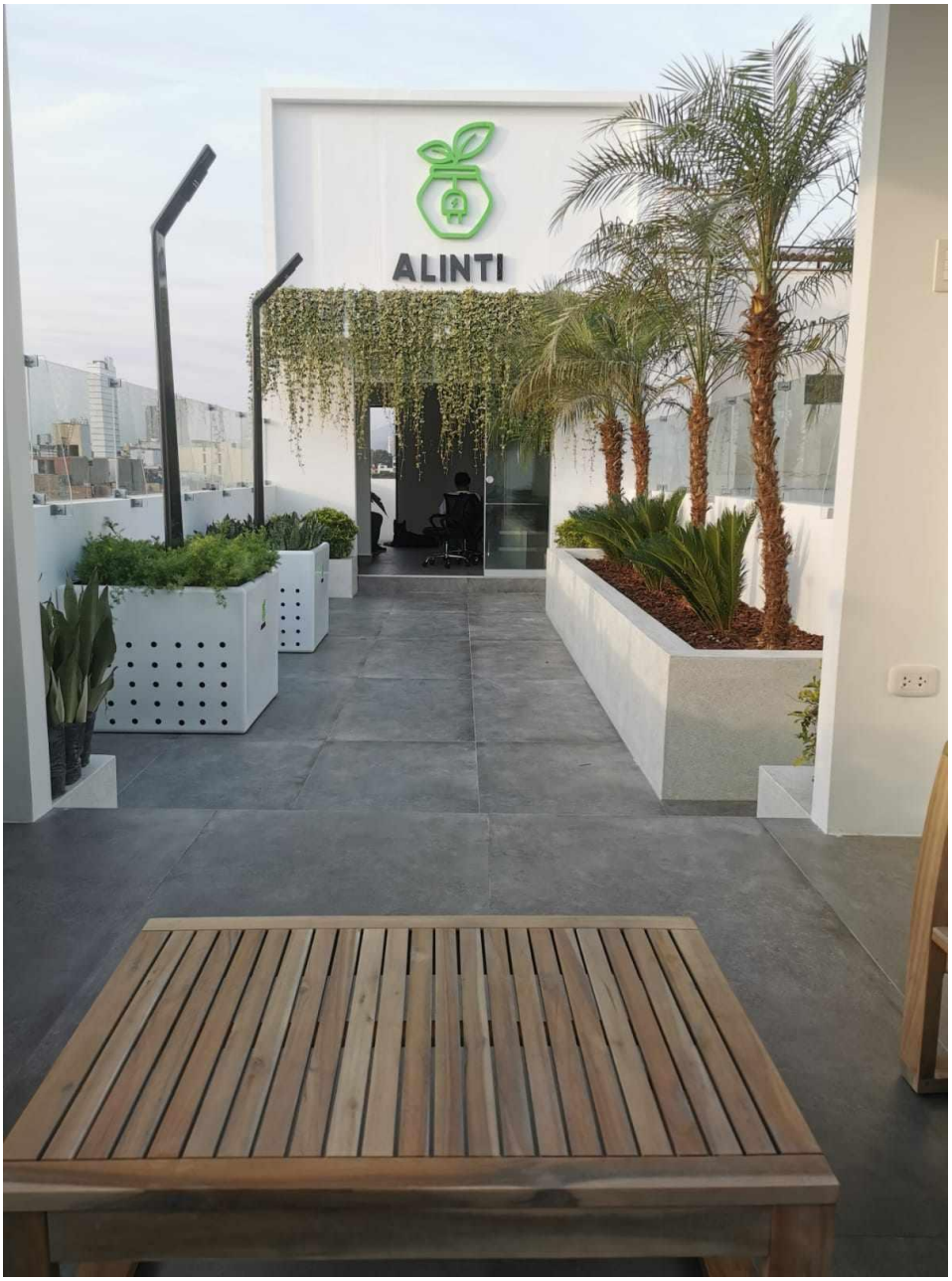
CEO: HERNÁN ASTO CABEZAS

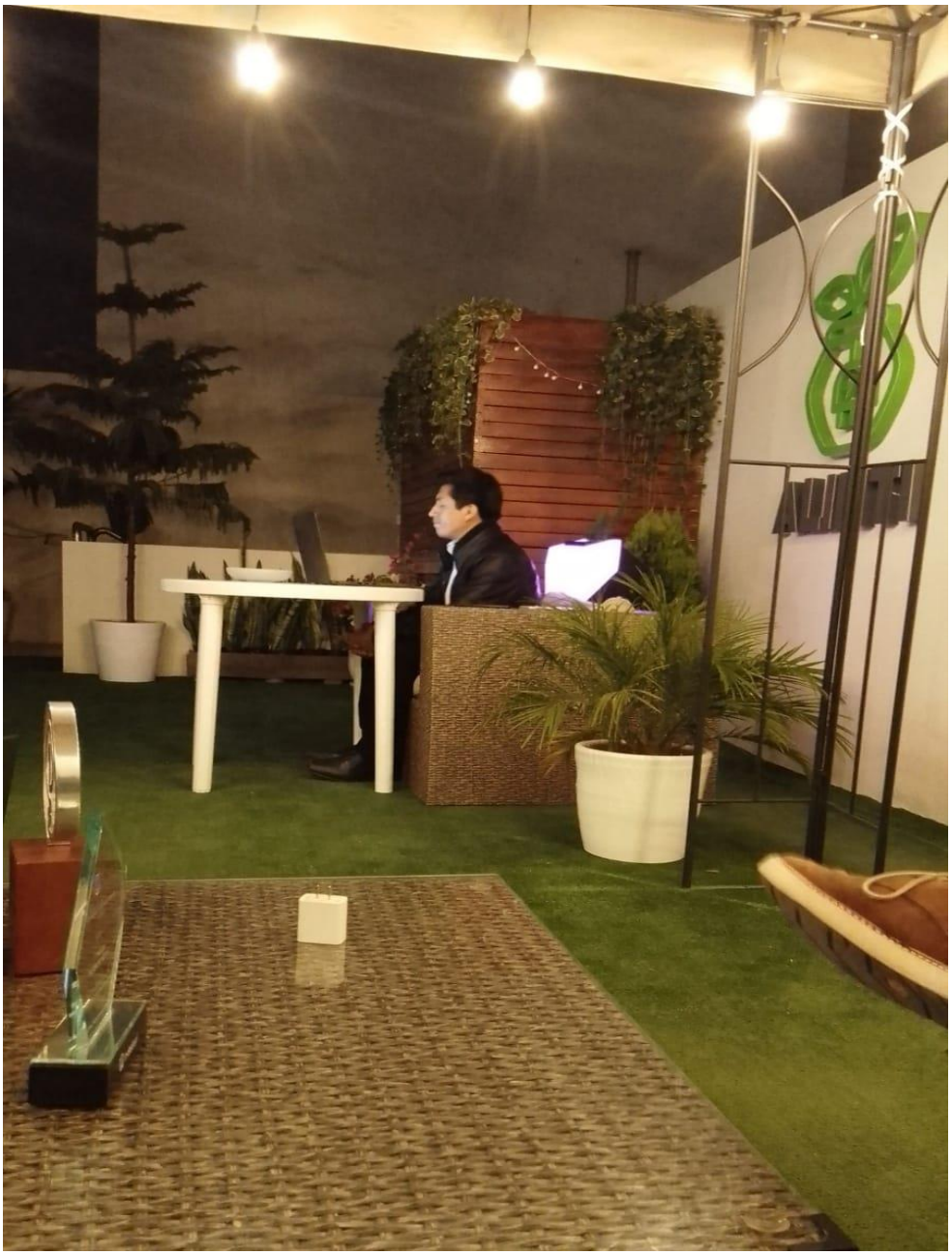
ANEXO B

Directiva del Grupo Tecnológico Alinti

ANEXO C

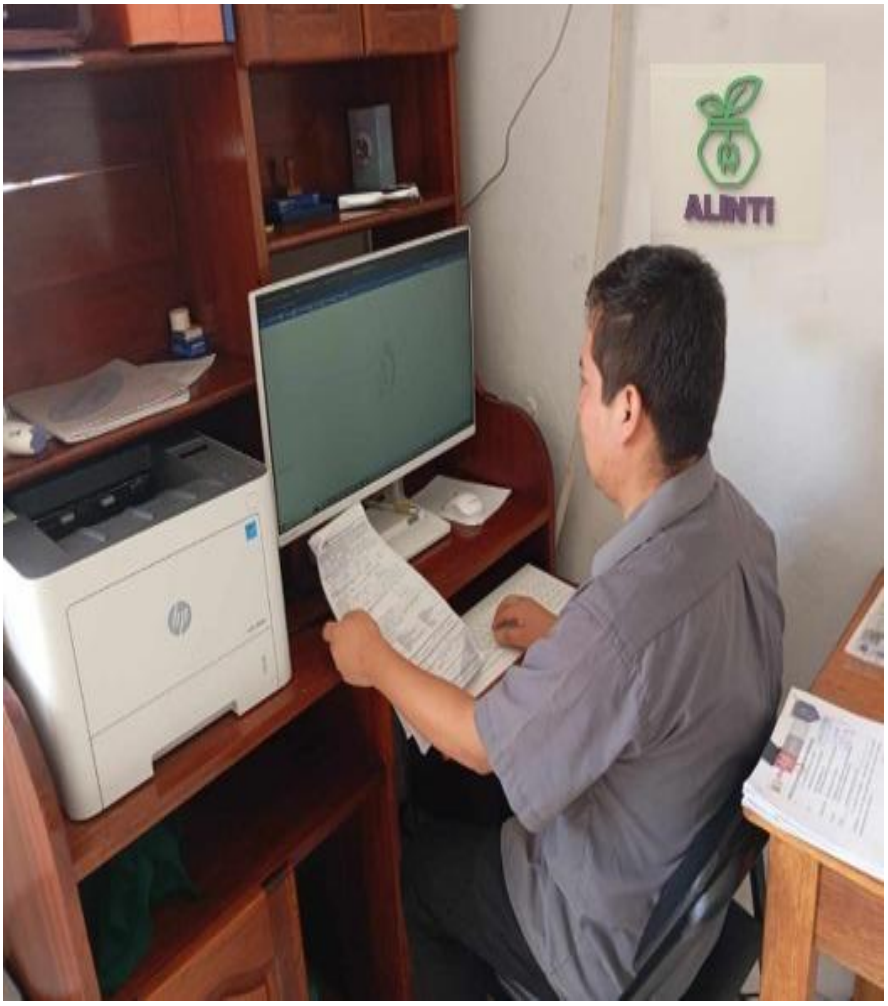
Infraestructura informática





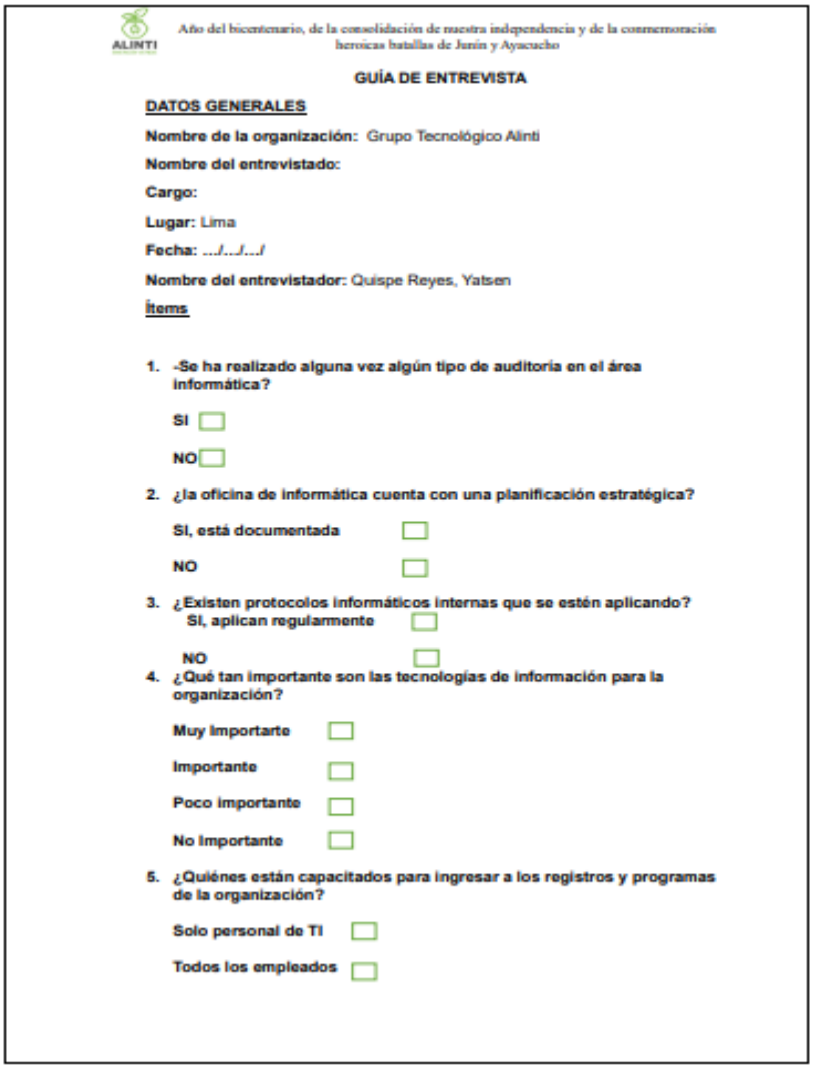
ANEXO D

Oficina de informática



ANEXO E

Guía de entrevista



ALINTI

Año del bicentenario, de la consolidación de nuestra independencia y de la conmemoración heroicas batallas de Junín y Ayacucho

GUÍA DE ENTREVISTA

DATOS GENERALES

Nombre de la organización: Grupo Tecnológico Alinti

Nombre del entrevistado:

Cargo:

Lugar: Lima

Fecha: .../.../.../

Nombre del entrevistador: Quispe Reyes, Yatsen

Ítems

1. **-Se ha realizado alguna vez algún tipo de auditoria en el área informática?**

   SI ☐

   NO ☐

2. **¿la oficina de informática cuenta con una planificación estratégica?**

   SI, está documentada ☐

   NO ☐

3. **¿Existen protocolos informáticos internas que se estén aplicando?**

   SI, aplican regularmente ☐

   NO ☐

4. **¿Qué tan importante son las tecnologías de información para la organización?**

   Muy Importarte ☐

   Importante ☐

   Poco importante ☐

   No Importante ☐

5. **¿Quiénes están capacitados para ingresar a los registros y programas de la organización?**

   Solo personal de TI ☐

   Todos los empleados ☐

Solo directivos ☐

Otros ☐

6. ¿Todos los colaboradores de la organización tienen usuario y contraseña para ingresar a sus dispositivos de trabajo?

   SI, todos ☐

   NO, nadie ☐

7. ¿Qué medidas de seguridad existen en El Grupo Tecnológico Alinti?

   Firewall ☐
   Antivirus ☐
   Seguridad Física ☐
   Otros ☐

8. ¿Es primordial aplicar un plan de contingencia?

   Muy importarte ☐
   Importante ☐
   Poco importante ☐
   No importante ☐

9. ¿El colaborador está capacitado para enfrentar un ataque informático?

   SI, todos están capacitados ☐

   NO, nadie está capacitado ☐

10. ¿El lugar de los servidores cuenta con todas las seguridades físicas adecuadas?

    SI, completamente seguro ☐

    NO, es inseguro ☐

11. ¿Hay alguna planificación en cuanto a la inversión anual para el área de TI dentro del Grupo Tecnológico Alinti?

Si, está claramente definida ☐

NO, no hay planificación ☐

12. ¿Tienen un lugar específico para los dispositivos informáticos nuevos o dañados, partes y piezas?

Si, está claramente definido ☐

NO ☐

13. ¿En este momento cómo se controlan las tecnologías de información en la organización?

A través de auditorías regulares ☐

Mediante políticas internas ☐

14. ¿Existe una normativa para restablecer operaciones en caso de un fallo en la tecnología de información?

Si. hay procedimiento definido ☐

NO, no existe ☐

15. ¿La organización del Grupo Tecnológico ALINTI usa software libre?

Si, en todos sistemas ☐

Si, en algunos sistemas ☐

NO ☐

No estoy seguro/a ☐

ANEXO F

Formato de hallazgo de la auditoría

ALINTI ENERGÍA VERDE	**GRUPO TECNOLÓGICO ALINTI**
Hallazgos de la Auditoría	
Componente:	
Dominio	
Proceso	
Practica	
Objetivo	
Resultados	

AUDITORÍA INTERNA BASADA EN COBIT 5 PARA EL CONTROL DE LA SEGURIDAD FÍSICA DE LA INFRAESTUCTURA INFORMÁTICA DEL GRUPO TECNOLÓGICO ALINTI, LIMA 2023.

PROBLEMÁTICA	OBJETIVOS	HIPÓTESIS	VARIABLES	MÉTODOS DE INVESTIGACIÓN
GENERAL	**GENERAL**			
¿Cuáles son los resultados de la auditoría interna basada en Cobit 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti, Lima 2023?	Determinar los resultados de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti, Lima 2023.	Las investigaciones de tipo descriptivo no requieren formular hipótesis.	X=Auditoría Interna basada en COBIT 5 DIMENSIONES: X1: Planeación y organización de Auditoría Interna X2: Proceso de ejecución de la Auditoría Interna X3: Evaluación de la Auditoría Interna	**TIPO DE INVESTIGACIÓN** Observacional, descriptivo. **NIVEL DE INVESTIGACIÓN** Descriptivo **DISEÑO** No experimental **POBLACIÓN** Infraestructura informática de Grupo Tecnológico Alinti, Lima 2023. Aproximadamente fueron 45 equipos. **MUESTRA** Equipos tecnológicos de infraestructura informática con riesgo del Grupo Tecnología Alinti, Lima 2023. Aproximadamente fueron 18 Equipos. **TÉCNICA** ➢ Observación
ESPECÍFICOS	**ESPECÍFICOS**			
¿Cuáles son los resultados de la planeación y organización de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti? ¿Cuáles son los resultados del proceso de ejecución de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la	Identificar los resultados de la planeación y organización de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti. Describir los resultados del proceso de ejecución de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la			

infraestructura informática del Grupo Tecnológico Alinti? ¿Cuáles son los resultados de la evaluación de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti?	infraestructura informática del Grupo Tecnológico Alinti. Determinar los resultados de la evaluación de la auditoría interna basada en COBIT 5 para el control de la seguridad física de la infraestructura informática del Grupo Tecnológico Alinti.			➢ Análisis documental **INSTRUMENTO** ➢ Ficha y observación ➢ Ficha de Análisis documental

UNSCH | FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ACTA DE SUSTENTACION DE TESIS N° 099-2024-FIMGC

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

En la Universidad Nacional de San Cristóbal de Huamanga de la ciudad de Ayacucho, en cumplimiento a la **Resolución Decanal N° 768-2024-FIMGC-D,** a los trece días del mes de diciembre de 2024, siendo las 04:00 p.m., reunidos en el Auditorio de la Escuela Profesional de Ingeniería de Minas, bajo la presidencia de la MSc. Ing. José Ernesto ESTRADA CÁRDENAS y los miembros; Mg. Ingª. Edith Felicitas GUEVARA MOROTE, Dr. Manuel Avelino LAGOS BARZOLA y Mg. Richard ZAPATA CASAVERDE, actuando como secretario docente el MSc. Ing. Kelvis BERROCAL ARGUMEDO, para proceder a la sustentación de tesis para optar el Título Profesional de Ingeniero de Sistemas, del bachiller:

Yatsen QUISPE REYES

Quien presentó la tesis denominada:

Auditoría interna basada en Cobit 5 para el control de la seguridad física de la infraestuctura informática del grupo tecnológico Alinti, Lima 2023

Los señores miembros del jurado luego de expuesto la tesis y absueltas las preguntas, delibera y lo declaran:

APROBADO CON NOTA QUINCE (15)

Siendo las 5:50 p.m. del día 13 de diciembre de 2024, culmina el acto de sustentación de tesis, y en conformidad a lo actuado los miembros del jurado firmamos al pie del presente.

MSc. Ing. ESTRADA CÁRDENAS, José Ernesto
Presidente

Mg. Ingª Edith Felicitas GUEVARA MOROTE
Miembro

Dr. Manuel Avelino LAGOS BARZOLA
Miembro

Mg. Richard ZAPATA CASAVERDE
Miembro -Asesor

MSc. Ing. Kelvis BERROCAL ARGUMEDO
Secretario docente de la FIMGC

cc:
Archivo

FACULTAD DE INGENIERÍA
DE MINAS, GEOLOGÍA Y CIVIL
Av. Independencia S/N
Ciudad Universitaria
Central Tel 066 312510
Anexo 151

CONSTANCIA DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

CONSTANCIA Nº 016-2025-KPS-FIMGC/UNSCH

El que suscribe; responsable verificador de originalidad de trabajos de tesis de pregrado con el software Turnitin, en segunda instancia para las **Escuelas Profesionales** de la **Facultad de Ingeniería de Minas, Geología y Civil**; en cumplimiento a la **Resolución de Consejo Universitario Nº 039-2021-UNSCH-CU**, Reglamento de Originalidad de Trabajos de Investigación de la Universidad Nacional San Cristóbal de Huamanga y **Resolución Decanal Nº 697-2024-FIMGC-D**, deja constancia de originalidad de trabajo de investigación, que el/la Sr./Srta.

Nombres y Apellidos	:	Yatsen Quispe Reyes
Escuela Profesional	:	INGENIERÍA DE SISTEMAS
Título de la Tesis	:	AUDITORÍA INTERNA BASADA EN COBIT 5 PARA EL CONTROL DE LA SEGURIDAD FÍSICA DE LA INFRAESTRUCTURA INFORMÁTICA DEL GRUPO TECNOLÓGICO ALINTI, LIMA 2023
Evaluación de la Originalidad	:	**4%** Índice de Similitud
Identificador de la entrega	:	2621047095

Por tanto, según los Artículos 12, 13 y 17 del Reglamento de Originalidad de Trabajos de Investigación, es **PROCEDENTE** otorgar la **Constancia de Originalidad** para los fines que crea conveniente.

En señal de conformidad y verificación se firma la presente constancia

Ayacucho, 22 de marzo de 2025

FIRMA DIGITAL

Firmado digitalmente por: PERALTA SOTOMAYOR Karel FAU 20143660754 soft
Motivo: Soy el autor del documento
Fecha: 31/03/2025 16:30:46-0500

Con depósito para Sustentación y Tramites
C.c. Archivo

FACULTAD DE INGENIERIA DE MINAS, GEOLOGIA Y CIVIL
Av. Independencia S/N Ciudad Universitaria
Central Tel. 066 312510
Anexo 151

AUDITORÍA INTERNA BASADA EN COBIT 5 PARA EL CONTROL DE LA SEGURIDAD FÍSICA DE LA INFRAESTRUCTURA INFORMÁTICA DEL GRUPO TECNOLÓGICO ALINTI, LIMA 2023

por Yatsen Quispe Reyes

Fecha de entrega: 21-mar-2025 09:05a.m. (UTC-0500)
Identificador de la entrega: 2621047095
Nombre del archivo: M.N_073-2025-FIMGC-UNSCH._2_.pdf (3.45M)
Total de palabras: 23906
Total de caracteres: 145425

AUDITORÍA INTERNA BASADA EN COBIT 5 PARA EL CONTROL DE LA SEGURIDAD FÍSICA DE LA INFRAESTRUCTURA INFORMÁTICA DEL GRUPO TECNOLÓGICO ALINTI, LIMA 2023

INFORME DE ORIGINALIDAD

4%	4%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.utc.edu.ec Fuente de Internet	1%
2	repositorio.unsch.edu.pe Fuente de Internet	1%
3	hdl.handle.net Fuente de Internet	1%
4	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	1%
5	repository.unad.edu.co Fuente de Internet	<1%
6	repositorio.ucp.edu.pe Fuente de Internet	<1%
7	dspace.unach.edu.ec Fuente de Internet	<1%

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		