Universidad Científica del Perú - UCP
Registrado en el Asiento Nº A00010 de la Partida Nº 11000318, Personas Jurídicas de Iquitos, Superintendencia de los Registros Públicos - SUNARP

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADEMICO DE INGENIERIA DE SISTEMAS DE INFORMACIÓN

INFORME FINAL DE TESIS

AUDITORÍA INFORMÁTICA CON LA METODOLOGIA COBIT 5 DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA – 2023

PARA OBTAR EL TITÚLO PROFESIONAL

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

- BACH. LUZ ANGELA GORDON DOZA
- BACH. ALEXANDER REYES MOZOMBITE

ASESOR:

- **LIC. CARLOS ENRIQUE MARTHANS RUIZ, Mtro.**

SAN JUAN BAUTISTA – MAYNAS – LORETO - PERÚ – 2024

DEDICATORIA

Dedico esta tesis a Dios, por brindarme vida y salud para poder concluir con este proyecto. A mis padres quienes me dieron vida, educación, apoyo y buenos consejos.

A mis maestros, por todo lo enseñado y aprendido, ahora aplicado para mi tesis.

A mi hijo quien fue pieza fundamental para no desmayar y seguir adelante.

BACH. LUZ ANGELA GORDON DOZA

DEDICATORIA

A Dios por su gran amor y brindarme salud, bienestar, sabiduría y apoyarme desde el principio para culminar el trabajo de suficiencia profesional.

A mis padres, Marilin Mozombite del Águila y Pedro Vilca Apaza, por acompañarme en cada paso que doy en la búsqueda de ser mejor persona y profesional.

A mi hijo, para que cada una de mis metas alcanzadas le quede de ejemplo.

BACH. ALEXANDER REYES MOZOMBITE

AGRADECIMIENTO

Agradezco en primer lugar a mis padres por todo el apoyo brindado en mis estudios universitarios, por su amor incondicional, comprensión y ánimo constante. Su fe en mis capacidades ha sido una fuente de motivación y fuerza durante todo mi recorrido académico.

También, agradezco a la Municipalidad Distrital de Punchana por proporcionar los recursos y el apoyo necesario para realizar esta investigación.

Finalmente, y no menos importante al PRONABEC (Programa Nacional de Becas y Crédito Educativo) Beca 18 por darme la oportunidad de poder cumplir uno de mis metas.

BACH. LUZ ANGELA GORDON DOZA

AGRADECIMIENTO

En primer lugar, agradezco a Dios y a mis padres que siempre me han brindado su apoyo incondicional para poder cumplir todos mis objetivos personales y académicos.

A la Municipalidad Distrital de Punchana, por brindarme la oportunidad de realizar el presente trabajo de auditoria tecnológica en su Institución.

A la universidad que me ha exigido tanto, pero al mismo tiempo me está permitiendo obtener mi tan ansiado título.

BACH. ALEXANDER REYES MOZOMBITE

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP

El presidente del Comité de Ética de la Universidad Científica del Perú - UCP

Hace constar que:

La Tesis titulada:

AUDITORÍA INFORMÁTICA CON LA METODOLOGIA COBIT 5 DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA – 2023

De los alumnos: **LUZ ANGELA GORDON DOZA Y ALEXANDER REYES MOZOMBITE,** de la Facultad de Ciencias e Ingeniería pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **15% de similitud**. Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 27 de febrero del 2024.

Mgr. Arq. Jorge L. Tapullima Flores
Presidente del Comité de Ética – UCP

JLTF/ri-a
72-2024

Resultado_UCP_SistemasDeInformación_2024_Tesis_LuzGo...

INFORME DE ORIGINALIDAD

15%	14%	2%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

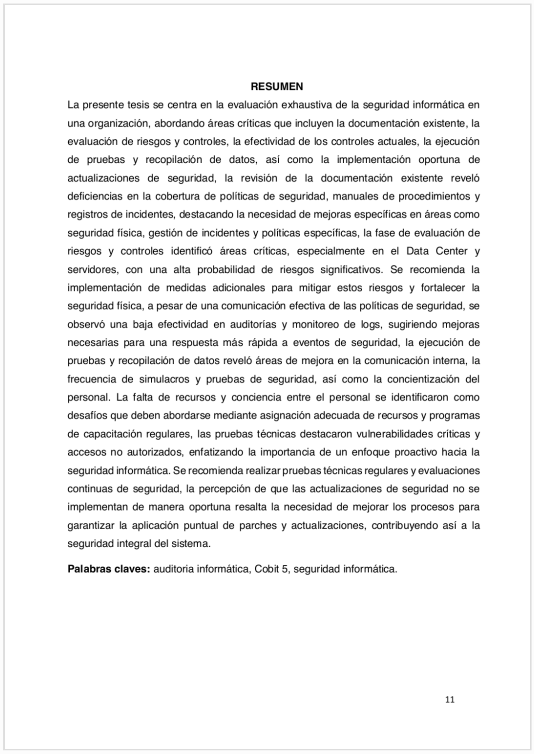
1	www.foroinnovatec.com Fuente de Internet	1%
2	repobiblio.cuc.uqroo.mx Fuente de Internet	1%
3	ri.ues.edu.sv Fuente de Internet	1%
4	repositorio.usmp.edu.pe Fuente de Internet	1%
5	repositorio.pucesa.edu.ec Fuente de Internet	1%
6	Submitted to Universidad Católica de Santa María Trabajo del estudiante	1%
7	www.przetargi.info Fuente de Internet	<1%
8	Submitted to Universidad Catolica Los Angeles de Chimbote Trabajo del estudiante	<1%

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Luz Angela Gordon Doza
Título del ejercicio:	Quick Submit
Título de la entrega:	Resultado_UCP_SistemasDeInformación_2024_Tesis_LuzGord...
Nombre del archivo:	MACION_LUZ_GORDON_Y_ALEXANDER_REYES_RESUMEN_RE...
Tamaño del archivo:	644.82K
Total páginas:	47
Total de palabras:	9,548
Total de caracteres:	53,967
Fecha de entrega:	27-feb.-2024 08:51a. m. (UTC-0500)
Identificador de la entre...	2305961228



RESUMEN

La presente tesis se centra en la evaluación exhaustiva de la seguridad informática en una organización, abordando áreas críticas que incluyen la documentación existente, la evaluación de riesgos y controles, la efectividad de los controles actuales, la ejecución de pruebas y recopilación de datos, así como la implementación oportuna de actualizaciones de seguridad, la revisión de la documentación existente reveló deficiencias en la cobertura de políticas de seguridad, manuales de procedimientos y registros de incidentes, destacando la necesidad de mejoras específicas en áreas como seguridad física, gestión de incidentes y políticas específicas, la fase de evaluación de riesgos y controles identificó áreas críticas, especialmente en el Data Center y servidores, con una alta probabilidad de riesgos significativos. Se recomienda la implementación de medidas adicionales para mitigar estos riesgos y fortalecer la seguridad física, a pesar de una comunicación efectiva de las políticas de seguridad, se observó una baja efectividad en auditorías y monitoreo de logs, sugiriendo mejoras necesarias para una respuesta más rápida a eventos de seguridad, la ejecución de pruebas y recopilación de datos reveló áreas de mejora en la comunicación interna, la frecuencia de simulacros y pruebas de seguridad, así como la concientización del personal. La falta de recursos y conciencia entre el personal se identificaron como desafíos que deben abordarse mediante asignación adecuada de recursos y programas de capacitación regulares, las pruebas técnicas destacaron vulnerabilidades críticas y accesos no autorizados, enfatizando la importancia de un enfoque proactivo hacia la seguridad informática. Se recomienda realizar pruebas técnicas regulares y evaluaciones continuas de seguridad, la percepción de que las actualizaciones de seguridad no se implementan de manera oportuna resalta la necesidad de mejorar los procesos para garantizar la aplicación puntual de parches y actualizaciones, contribuyendo así a la seguridad integral del sistema.

Palabras claves: auditoria informática, Cobit 5, seguridad informática.

UNIVERSIDAD CIENTÍFICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

ACTA DE SUSTENTACIÓN DE TESIS

Con Resolución Decanal N° 859-2023-UCP-FCEI del 18 de diciembre del 2023, la Facultad de Ciencias e Ingeniería de la Universidad Científica Del Perú - UCP designa como Jurado Evaluador de la **Tesis** a los señores:

- Ing. Jimmy Max Ramírez Villacorta, Mtro. — Presidente
- Ing. Tonny Eduardo Bardales Lozano, Mgr. — Miembro
- Ing. Christian Alfredo Arévalo Jesús, Mtro. — Miembro

Como Asesora: Lic. Carlos Enrique Marthans Ruíz, Mgr

En la ciudad de Iquitos, siendo las 10:00 am del día **5 de abril de 2024**, supervisado por la Secretaria Académica del Programa de Ingeniería de Sistemas de Información de la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú, se constituyó el Jurado para escuchar la sustentación y defensa del **Tesis:** ***AUDITORÍA INFORMÁTICA CON LA METODOLOGÍA COBIT 5 DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA-2023***

Presentado por los sustentantes: **GORDON DOZA LUZ ANGELA y REYES MOZOMBITE ALEXANDER**

Como requisito para optar el título profesional de:

INGENIERO DE SISTEMAS DE INFORMACIÓN

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: ABSUELTAS
El Jurado después de la deliberación en privado llegó a la siguiente conclusión:
Que la sustentación es APROBADO POR UNANIMIDAD

En fe de lo cual los miembros del Jurado firman el acta.

Ing. Jimmy Max Ramírez Villacorta, Mtro.
Presidente

Ing. Tonny Eduardo Bardales Lozano, Mgr
Miembro

Ing. Christian Alfredo Arévalo Jesús, Mtro.
Miembro

HOJA DE APROBACIÓN

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN
TESISTAS: **GORDON DOZA LUZ ANGELA y REYES MOZOMBITE ALEXANDER**

TESIS sustentada en acto publico el 5 de abril de 2024, a las 10:00 am

ING. JIMMY MAX RAMIREZ VILLACORTA, MTRO.
PRESIDENTE DE JURADO

ING. TONNY EDUARDO BARDALES LOZANO, MGR.
.MIEMBRO DE JURADO

ING. CHRISTIAN ALFREDO ARÉVALO JESÚS, MTRO.
MIEMBRO DE JURADO

LIC. CARLOS ENRIQUE MARTHANS RUÍZ, MGR
ASESOR

INDICE DE CONTENIDO

Página

INDICE DE FIGURAS

Página

INDICE DE TABLAS

RESUMEN

La presente tesis se centra en la evaluación exhaustiva de la seguridad informática en una organización, abordando áreas críticas que incluyen la documentación existente, la evaluación de riesgos y controles, la efectividad de los controles actuales, la ejecución de pruebas y recopilación de datos, así como la implementación oportuna de actualizaciones de seguridad, la revisión de la documentación existente reveló deficiencias en la cobertura de políticas de seguridad, manuales de procedimientos y registros de incidentes, destacando la necesidad de mejoras específicas en áreas como seguridad física, gestión de incidentes y políticas específicas, la fase de evaluación de riesgos y controles identificó áreas críticas, especialmente en el Data Center y servidores, con una alta probabilidad de riesgos significativos. Se recomienda la implementación de medidas adicionales para mitigar estos riesgos y fortalecer la seguridad física, a pesar de una comunicación efectiva de las políticas de seguridad, se observó una baja efectividad en auditorías y monitoreo de logs, sugiriendo mejoras necesarias para una respuesta más rápida a eventos de seguridad, la ejecución de pruebas y recopilación de datos reveló áreas de mejora en la comunicación interna, la frecuencia de simulacros y pruebas de seguridad, así como la concientización del personal. La falta de recursos y conciencia entre el personal se identificaron como desafíos que deben abordarse mediante asignación adecuada de recursos y programas de capacitación regulares, las pruebas técnicas destacaron vulnerabilidades críticas y accesos no autorizados, enfatizando la importancia de un enfoque proactivo hacia la seguridad informática. Se recomienda realizar pruebas técnicas regulares y evaluaciones continuas de seguridad, la percepción de que las actualizaciones de seguridad no se implementan de manera oportuna resalta la necesidad de mejorar los procesos para garantizar la aplicación puntual de parches y actualizaciones, contribuyendo así a la seguridad integral del sistema.

Palabras claves: auditoria informática, Cobit 5, seguridad informática.

ABSTRACT

This thesis focuses on the comprehensive assessment of cybersecurity within an organization, addressing critical areas such as existing documentation, risk and control evaluation, effectiveness of current controls, execution of tests and data collection, and timely implementation of security updates. The review of existing documentation revealed deficiencies in the coverage of security policies, procedure manuals, and incident records, emphasizing the need for specific improvements in areas such as physical security, incident management, and specific policies, the phase of risk and control evaluation identified critical areas, particularly in the Data Center and servers, with a high probability of significant risks. It is recommended to implement additional measures to mitigate these risks and strengthen physical security. Despite effective communication of security policies, a low effectiveness in audits and log monitoring was observed, suggesting necessary improvements for a quicker response to security events, the execution of tests and data collection revealed areas for improvement in internal communication, the frequency of drills and security tests, as well as staff awareness. The lack of resources and awareness among the staff were identified as challenges that need to be addressed through proper resource allocation and regular training programs, technical tests highlighted critical vulnerabilities and unauthorized access, emphasizing the importance of a proactive approach to cybersecurity. Regular technical tests and continuous security evaluations are recommended. The perception that security updates are not implemented in a timely manner underscores the need to improve processes to ensure the timely application of patches and updates, thereby contributing to the overall security of the system.

Keywords: computer audit, Cobit 5, cybersecurity

CAPÍTULO I.- MARCO TEÓRICO:

1.1 Antecedentes de Estudio:

- ✓ **Antecedentes Internacionales:**

  Cuasapaz Narvaez, K. A., & Landázuri Narvaez, K. D. (2023), este estudio de investigación fue llevado a cabo con el propósito de ofrecer sugerencias para mitigar riesgos tecnológicos relacionados con la alineación de Tecnologías de la Información (TI) a los objetivos institucionales del Gobierno Autónomo Descentralizado (GAD) Municipal de Montúfar. El objetivo primordial es asegurar la salvaguarda de los activos fijos, la información gubernamental, y facilitar la gestión efectiva del GADMM. Se utilizó el marco de referencia COBIT 5 para identificar las fuentes de riesgos tecnológicos en los procesos de información y seguridad de la información, evaluando los niveles de capacidad de cada proceso seleccionado según COBIT 5, los resultados revelaron que los niveles identificados son inferiores a los niveles de capacidad esperados, lo cual impacta directamente en los criterios de información, poniendo en riesgo la integridad, seguridad y disponibilidad de los activos informáticos, se empleó una metodología cuali-cuantitativa para medir el nivel de capacidad de cada criterio de COBIT 5, inicialmente, se llevó a cabo una encuesta al personal del GAD Municipal de Montúfar para establecer el estado inicial de la institución, posteriormente, se implementó un plan de auditoría en el departamento de Tecnologías de la Información (TIC) para verificar los criterios definidos por COBIT 5, la evaluación de los procesos se realizó asignando niveles de capacidad del 0 al 5, donde 0 representa la valoración más baja y 5 la más óptima, tras analizar los procesos evaluados, se formuló un plan de acción que incluye recomendaciones para su potencial implementación dentro del departamento de TIC del GAD Municipal de Montúfar, se han propuesto planes de acción específicos para los procesos que no cumplen con los criterios de COBIT 5, buscando lograr una alineación efectiva de las TI con los objetivos institucionales y los servicios proporcionados por la entidad.

  Barreto Merino, L. J. (2022), El proyecto de investigación en curso detalla la realización de una Auditoría Informática utilizando la metodología COBIT 5 en la

Cooperativa de Transportes Patria durante el periodo 2020, ubicada en la ciudad de Riobamba, provincia de Chimborazo. Esta cooperativa se dedica a ofrecer servicios de transporte de pasajeros y encomiendas, utilizando recursos tecnológicos para optimizar sus procesos internos y alcanzar eficientemente sus objetivos de negocio, la auditoría se fundamenta en los principios de COBIT 5, un conjunto de mejores prácticas diseñado tanto para el Gobierno Corporativo como para la Administración en la gestión de tecnologías de la información. COBIT 5 se emplea para auditar la gestión y el control de los sistemas de información. En términos metodológicos, se utilizó un enfoque deductivo, combinando investigación de campo y documental con un enfoque mixto, tanto cualitativo como cuantitativo, en el nivel de investigación descriptivo, la población de estudio incluyó al personal administrativo y técnico de la sede de la Cooperativa de Transportes Patria, y se evaluó el Sistema Informático NOVO ERP. Las técnicas utilizadas para recopilar información crucial fueron encuestas, entrevistas y observación, con el objetivo de identificar deficiencias en el manejo de la seguridad de la información. Como conclusión, se destaca que la Auditoría Informática contribuye a garantizar la integridad física de los equipos, la información y la infraestructura tecnológica, lo que resulta en un aumento de la seguridad de la información en la Cooperativa.

Vargas García, H. H. (2019), en su investigación señala que, en Ecuador, las instituciones financieras muestran un enfoque prioritario en la mejora de sus canales de atención, destacando especialmente la atención digital. Este enfoque se debe a su capacidad para optimizar tanto los procesos internos como externos de los bancos. En consonancia con estas necesidades, la investigación actual tiene como objetivo primordial desarrollar una metodología de auditoría informática específicamente dirigida a evaluar el área de Control de Calidad de Software en bancos privados de tamaño mediano en Ecuador, para fundamentar esta propuesta, se ha tomado como referencia un banco mediano en Ecuador, donde se han identificado deficiencias en las etapas del ciclo de certificación de un sistema, resultando en un software de baja calidad. Como solución a esta problemática, se propone la creación de una herramienta diseñada para evaluar el área de Calidad de

Software. Esta herramienta se centrará en la identificación de procesos, métodos, actividades y controles dentro del área, y posteriormente, basándose en el Marco de referencia COBIT, establecerá relaciones con los dominios de COBIT, en última instancia, el diseño de la metodología propuesta se complementa con la descripción detallada de las fases que deben seguirse durante la ejecución de la auditoría. Cada fase se presenta de manera práctica y accesible, destinada a ser comprensible tanto para auditores expertos como para aquellos que se están iniciando en los procesos de ejecución de auditorías.

Machado Lloreda, B. J. (2018), en esta investigación se llevó a cabo una auditoría en seguridad informática sobre la Infraestructura Tecnológica y Sistema de Información de la Institución Educativa Escuela Normal Superior de Quibdó, utilizando el estándar COBIT. La evaluación abarcó diversos aspectos, incluyendo la gestión administrativa de la sala de cómputo, el cumplimiento de funciones y la prestación de servicios, la infraestructura física, la seguridad física, la ubicación, la infraestructura eléctrica, las redes, la gestión y actualización de la información, así como el acceso de usuarios al sistema de información y la utilización de la información, la recopilación de información se llevó a cabo mediante listas de chequeo específicas para cada objetivo de control COBIT, utilizando entrevistas y observación. Se procedió al análisis de riesgos mediante la metodología MAGERIT, identificando activos, amenazas y valorando los riesgos. Como resultado de este proceso, se formularon recomendaciones en respuesta a los hallazgos encontrados, además de proponer acciones preventivas y de mejora.

- ✓ **Antecedentes Nacionales:**

Encarnacion Nuñez, E. F. (2020), realizó una auditoría informática utilizando la metodología COBIT con el propósito de evaluar su impacto en la seguridad informática de la Sub Gerencia de Administración Tributaria de la Municipalidad Distrital de Hualmay, en el año 2018. En términos de diseño de investigación, este proyecto se enmarcó en un nivel correlacional, de tipo aplicado y transversal, con el objetivo de explorar la relación entre dos variables específicas en una situación

determinada, considerando el tiempo y el lugar, los participantes clave en este estudio fueron los 13 trabajadores de la Sub Gerencia de Administración Tributaria (SGAT), que representaron la población total y, debido a su tamaño reducido, se consideraron como la muestra completa (n=13). Las técnicas utilizadas para la recopilación de datos incluyeron encuestas electrónicas, entrevistas y observación. Para el análisis de datos, se emplearon herramientas como Microsoft Excel 365, Google Forms y SPSS Statistics 22, los resultados obtenidos a través de la prueba no paramétrica de chi-cuadrada, realizada con el software SPSS 22, revelaron que los valores para las hipótesis a), b), c), y la Hipótesis Principal fueron $\boldsymbol{x2}$ = 6.171, $\boldsymbol{x2}$ = 7.889, $\boldsymbol{x2}$ = 7.726 y $\boldsymbol{x2}$ = 6.454, respectivamente. Al contrastar estos valores con el valor teórico $\boldsymbol{x2}$ = 3.841, con un grado de libertad (gl = 1) y un nivel de significancia del 95% (α = 0.05), se concluyó que todas las hipótesis del investigador fueron aceptadas, los resultados indican de manera concluyente que la implementación de una auditoría informática basada en la metodología COBIT tiene un impacto positivo y significativo en la mejora de la seguridad informática en la Sub Gerencia de Administración Tributaria de la Municipalidad Distrital de Hualmay.

Bautista Ushiñahua, M. A. (2020), en su proyecto de investigación titulado "Auditoría Informática con Metodología COBIT 4.5 para el Registro de Software y Hardware en el Área de Patrimonio de la Universidad Nacional de Ucayali: 2017" tiene como objetivo general llevar a cabo una Auditoría Informática utilizando la metodología COBIT 4.5 para el registro de software y hardware en el área de patrimonio de la Universidad Nacional de Ucayali en el año 2017, la población seleccionada para esta investigación está compuesta por los 8 trabajadores del área de patrimonio de la Universidad Nacional de Ucayali. La muestra utilizada es no probabilística, ya que coincide en tamaño con la población debido a la relativa pequeñez de esta, permitiendo su cobertura en términos de tiempo y recursos del investigador, en términos de nivel de investigación, se adscribe al enfoque descriptivo correlacional, de corte transversal, según la propuesta de Hernández, Fernández y Batista (2010). Este nivel de investigación se centra en la relación entre dos o más variables dentro de un mismo contexto y periodo de tiempo determinado. El instrumento principal utilizado para la recolección de datos es la encuesta, como resultado final de la

investigación, se presentan las conclusiones derivadas del análisis de la información recopilada a lo largo del proceso de auditoría informática en el área de patrimonio de la Universidad Nacional de Ucayali.

Chávez Ángeles, E. E. (2020, las organizaciones utilizan tecnologías de información y comunicación (TIC) con el propósito de facilitar la gestión y control de sus procesos internos, estableciendo la alineación con las estrategias empresariales como su principal directriz. Basándose en esta premisa, el objetivo general de este trabajo es presentar los resultados derivados de la implementación de la norma COBIT 5 en el proceso de transferencia de datos contables, financieros y administrativos del área de Gerencia General de la Empresa DATCO S&H; la organización considera crítico este proceso, sustentando tal consideración en el valor de la información transferida, especialmente en la elaboración de informes de gestión. Se trata de un proyecto viable que implica la aplicación de conocimientos, a través del uso de un modelo o marco de trabajo vinculado a la administración de recursos informáticos.

- ✓ **Antecedentes Locales:**

No se encontraron antecedentes locales

1.2 Bases Teóricas:

Auditoria informática:

La auditoría informática constituye un procedimiento sistemático y organizado cuyo propósito fundamental es evaluar y examinar la infraestructura tecnológica, sistemas de información, controles de seguridad, así como las políticas y procedimientos informáticos de una organización. Su enfoque central radica en proporcionar una evaluación imparcial y crítica del entorno informático de la entidad, con el objetivo de asegurar la integridad, confidencialidad, disponibilidad y el cumplimiento de los activos vinculados a la información.

Seguridad informática:

La Seguridad Informática se ocupa de salvaguardar la información almacenada en computadoras o redes, así como garantizar la protección del acceso a todos los recursos del sistema, como señala Baldeón (2012). Para lograr esto, es esencial evaluar y cuantificar los activos a proteger. Basándose en este análisis, se deben implementar medidas preventivas y correctivas que eliminen o reduzcan los riesgos asociados a niveles manejables, según lo destaca Morlanes (2012).

La adecuación y proporcionalidad de la seguridad deben considerarse en relación con el valor de los sistemas, el grado de dependencia de la organización de sus servicios y la probabilidad y magnitud de los posibles daños, según subraya Castro (2009). Los requisitos de seguridad son variables y dependerán de las características específicas de cada organización y sistema.

De acuerdo con Ramió J (2006), la seguridad informática se define como un conjunto de métodos y herramientas destinados a resguardar la información y, por ende, los sistemas informáticos, frente a cualquier amenaza, en un proceso en el que también participan las personas.

Los elementos fundamentales de la seguridad informática incluyen:

Confidencialidad: Garantiza que los componentes del sistema solo sean accesibles para usuarios autorizados.

Integridad: Asegura que los componentes del sistema solo puedan ser creados y modificados por usuarios autorizados.

Disponibilidad: Implica que los usuarios deben contar con acceso a todos los componentes del sistema cuando lo necesiten.

COBIT:

Control Objectives for Information and Related Technologies, se fundamenta en varios principios y conceptos clave, respaldados por la contribución de diversos autores y organizaciones.

Según la información proporcionada por ISACA en su obra "COBIT 5" del año 2012, COBIT 5 se presenta como un resultado de la mejora estratégica impulsada por ISACA. Este marco surge con la finalidad de liderar la próxima generación de guías relacionadas con el Gobierno y la Administración de la información y los Activos Tecnológicos en las Organizaciones. Construido sobre más de 15 años de experiencia práctica, COBIT 5 se ha desarrollado para abordar las necesidades de los interesados y alinearse con las actuales tendencias en las técnicas de gobierno y administración relacionadas con la Tecnología de la Información (TI)

Principios Fundamentales de COBIT

IT Governance Institute (ITGI): La ITGI, una entidad fundadora de COBIT, ha sido central en el desarrollo del marco. Su trabajo, como se presenta en publicaciones

clave como "Cobit 4.1" y "Cobit 5," establece los fundamentos y principios rectores de COBIT.

ISACA (Information Systems Audit and Control Association): ISACA, junto con la ITGI, ha sido una fuerza impulsora en el desarrollo y mantenimiento de COBIT. Sus publicaciones y guías, incluyendo el "COBIT Framework," son fuentes clave para entender los principios y la aplicación práctica de COBIT.

Figura 01: Principios de COBIT

Fuente: ISACA 2012

Ciclo de Vida de COBIT:

Val IT y Risk IT: Desarrollados por ISACA, Val IT (para la entrega de valor de TI) y Risk IT (para la gestión de riesgos en TI) han influido en el enfoque del ciclo de vida de COBIT. Estos conceptos están integrados en COBIT 5 para abordar la creación, entrega y sostenimiento del valor a lo largo del tiempo.

Gobernanza de TI:

Peter Weill y Jeanne W. Ross: En su libro "IT Governance: How Top Performers Manage IT Decision Rights for Superior Results," los autores ofrecen perspectivas importantes sobre la gobernanza de TI, concepto fundamental en COBIT.

Marco de Madurez:

Philippe Kruchten: Su trabajo sobre modelos de madurez de procesos, como se presenta en "The Rational Unified Process: An Introduction," ha influido en el enfoque de COBIT hacia la mejora continua y la evaluación del nivel de madurez.

Modelo de referencia COBIT:

De acuerdo con la Guía de Implementación COBIT 5, publicada por ISACA en 2012, se abordan los siguientes temas esenciales:
Ubicar el Gobierno de Tecnologías de la Información (IT) dentro de la estructura organizacional.

Iniciar los primeros pasos hacia un modelo de Gobierno de IT más avanzado.
Abordar los desafíos y considerar los factores cruciales para el éxito de la implementación.

Facilitar la gestión del cambio en el contexto del Gobierno de IT.
Implementar procesos de mejora continua para fortalecer el Gobierno de IT de manera constante.

Explorar la aplicación y utilización efectiva de COBIT 5 y sus componentes en el ámbito de la organización.

Los Modelos de Madurez destinados a controlar los procesos de Tecnologías de la Información (TI) se centran en la creación de un método de puntuación que permita

a una organización autoevaluarse en una escala que va desde inexistente hasta optimizada, representada por valores que oscilan de 0 a 5. Este enfoque se deriva del modelo de madurez originalmente definido por el Software Engineering Institute para evaluar la capacidad de desarrollo de software.

Frente a estos niveles, que han sido adaptados para cada uno de los treinta y cuatro procesos de TI establecidos por COBIT, la administración tiene la capacidad de realizar un mapeo o comparación, teniendo en cuenta:

El estado actual de la organización: identificando dónde se encuentra la organización en términos de madurez.

El estado actual de la industria: comparando la organización con las mejores prácticas de la industria.

El estado actual de los estándares internacionales: realizando una comparación adicional con respecto a estándares reconocidos a nivel mundial.

La estrategia de mejora de la organización: estableciendo dónde la organización aspira a encontrarse en términos de madurez.

Figura 02: Sistema de Gobierno COBIT

Fuente: COBIT 2019

1.3 Definición de Términos Básicos:

- Seguridad informática: Conjunto de prácticas, políticas y tecnologías destinadas a proteger la información y los sistemas informáticos de amenazas, daños o accesos no autorizados.

- COBIT: crónimo de "Control Objectives for Information and Related Technologies", es un marco de gobierno y gestión de tecnologías de la información (TI) desarrollado por ISACA.

- Dominios COBIT: Agrupaciones temáticas que representan áreas clave de enfoque para la gestión de TI, como planificación y organización, adquisición e implementación, entrega y soporte, supervisión y evaluación.

- Madurez de procesos: Evaluación de la capacidad de los procesos de una organización para lograr sus objetivos y cumplir con sus metas

CAPÍTULO II.- PLANTEAMIENTO DEL PROBLEMA:

2.1 Descripción del Problema:

La Municipalidad Distrital de Punchana, al igual que muchas entidades gubernamentales a nivel internacional y nacional, se enfrenta a desafíos significativos en la gestión de su infraestructura tecnológica. La creciente complejidad de las amenazas cibernéticas, las demandas de transparencia y eficiencia en la administración pública, así como las cambiantes regulaciones a nivel global y local, han generado la necesidad imperante de realizar una auditoría informática integral, la creciente sofisticación de las amenazas cibernéticas a nivel internacional plantea riesgos para la seguridad de los sistemas informáticos. La Municipalidad distrital de Punchana se encuentra expuesta a posibles ataques que podrían comprometer la confidencialidad e integridad de la información sensible, a nivel nacional, la legislación sobre seguridad informática y protección de datos se ha vuelto más rigurosa. La entidad debe cumplir con normativas específicas que exigen estándares de seguridad más elevados y una gestión más eficiente de los recursos informáticos, La Municipalidad Distrital de Punchana ha experimentado un crecimiento en su infraestructura tecnológica sin una adecuada planificación. Esto ha resultado en una red compleja y heterogénea, lo que dificulta la gestión efectiva de la seguridad y la implementación de buenas prácticas para ello se debe evaluar la seguridad y cumplimiento de las normas existentes, ello con la finalidad de Identificar y mitigar riesgos relacionados con Cyber amenazas, para alinear la infraestructura con normativas nacionales e internacionales, también para asegurar que la entidad cumpla con las regulaciones nacionales de seguridad informática y protección de datos ,optimizar la Infraestructura a nivel local, establecer estándares y procedimientos para la gestión eficiente de la infraestructura tecnológica local, mejorando la seguridad y la eficiencia operativa, las metas de implementar Controles de Seguridad Internacionalmente Reconocidos, establecer medidas de seguridad que cumplan con estándares internacionales reconocidos para mitigar amenazas cibernéticas, certificación de Cumplimiento Nacional, Obtener certificaciones que validen el cumplimiento de normativas nacionales en materia de seguridad informática y protección de datos, estandarización y Optimización Local,

Implementar la metodología COBIT para estandarizar y optimizar procesos informáticos a nivel local, mejorando la eficiencia y seguridad.

2.2 Formulación del Problema:

2.2.1 Problema General:

- ✓ ¿Cómo se realiza una Auditoria Informática con la metodología COBIT en la municipalidad distrital de Punchana en el año 2023?

2.2.2 Problemas Específicos:

1) ¿De qué manera se puede auditar la seguridad informática utilizando el marco de trabajo COBIT 5 en la unidad de tecnologías de la información de la municipalidad distrital de Punchana?

2) ¿De qué manera se puede elaborar un plan para mejorar la seguridad informática para la unidad de tecnologías de la información de la municipalidad distrital de Punchana?

2.3 Objetivos:

2.3.1 Objetivo General:

- ✓ Evaluar la seguridad informática en la unidad de tecnologías de la información de la municipalidad distrital de Punchana con la metodología COBIT.

2.3.2 Objetivos Específicos:

1) Evaluar la seguridad informática mediante una auditoria informática utilizando el marco de trabajo COBIT 5 en la unidad de tecnologías de la información de la municipalidad distrital de Punchana.

2) Elaborar planes para mejorar la seguridad informática para la unidad de tecnologías de la información de la municipalidad distrital de Punchana.

2.4 Hipótesis:

- No Aplica.

2.5 Variables:

2.5.1 Identificación de Variables:

- **Variable 1:** Auditoría informática con la Metodología COBIT

2.5.2 Definición Conceptual de las Variables:

- **Definición Conceptual de las Variables:**

2.5.3 Operacionalización de las Variables:

Tabla N° 01.- Operacionalización de variables:

Variables	Dimensiones	Indicadores	Instrumento de Recolección de Datos
Auditoria informática con la Metodología COBIT	Implementación	Objetivo de controles	• Entrevista • Ficha de observación • Análisis documental

Fuente: Elaboración Propia

CAPÍTULO III.- METODOLOGÍA:

3.1 Tipo y Diseño de Investigación:

- **Tipo o enfoque de la Investigación:**

El tipo de investigación es aplicada, porque buscaremos resolver problemas prácticos y contribuir directamente al mejoramiento o innovación en procesos existentes, en este caso, la auditoría informática busca mejorar la seguridad y eficiencia de los sistemas de información en la Municipalidad Distrital de Punchana y la aplicación de la Metodología COBIT implica

directamente mejoras en los procesos informáticos y de seguridad, lo que tiene una aplicación práctica inmediata en el entorno municipal.

- **Diseño de la Investigación:**

El diseño de investigación es no experimental descriptiva simple, porque vamos a describir y evaluar el estado actual de la seguridad informática en la unidad de tecnologías de la información de la Municipalidad Distrital de Punchana.

3.2 Población y Muestra:

- **Población:**

Los 07 trabajadores de la unidad de tecnologías de la información de la Municipalidad Distrital de Punchana.

- **Muestra:**

La muestra está compuesta por toda la población que comprende los 7 trabajadores de la unidad de tecnologías de la información de la municipalidad distrital de Punchana establecida en la siguiente tabla:

Tabla N° 02.- Trabajadores de la Unidad de TI

Puesto	Cantidad
Jefe de la unidad	1
Soporte técnico	4
Programador	1
Soporte redes	1
Total	7

Fuente: Recursos humanos

3.3 Técnicas, instrumentos y procedimientos de recolección de datos:

- **Técnica de Recolección de Datos:**

✓ Entrevista: se elaboró un cuestionario de preguntas para evaluar el nivel de seguridad informática en el que se encuentra la unidad de tecnologías de la información de la municipalidad distrital de Punchana.

✓ Análisis documental: se revisó los documentos concernientes a la seguridad informática con que cuenta la unidad de tecnologías de la información de la municipalidad distrital de Punchana.

✓ Observación: se hizo una visita a las instalaciones de la municipalidad para visualizar el estado situacional de los activos informáticos de la municipalidad distrital de Punchana.

- **Instrumento de Recolección de Datos:**

✓ Cuestionario de preguntas estructurada
✓ Ficha de observación
✓ Dispositivos de almacenamiento

- **Procedimiento de Recolección de Datos:**

✓ Recolectar políticas, procedimientos, manuales, registros y otros documentos relacionados con los procesos de TI de la Municipalidad Distrital de Punchana.
✓ Utilizar las entrevistas con el personal clave para obtener información cualitativa sobre la implementación de los controles y prácticas de TI.
✓ Recolectar resultados de pruebas técnicas, como escaneos de vulnerabilidades y pruebas de penetración, para evaluar la seguridad de los sistemas.

3.4 Procesamiento y análisis de datos:

- ✓ Codificar los datos para facilitar su análisis. Asignar códigos o etiquetas a las categorías relevantes, como controles específicos de COBIT 5.
- ✓ Analizar documentos y entrevistas utilizando técnicas de análisis de contenido para identificar patrones, temas y tendencias relacionadas con la implementación de COBIT 5.
- ✓ Utilizar los indicadores clave de rendimiento (KPIs) definidos para evaluar cuantitativamente el desempeño de los procesos de TI.

CAPÍTULO IV.- RESULTADOS:

Objetivo 1. Evaluar la seguridad informática mediante una auditoria informática utilizando el marco de trabajo COBIT 5 en la unidad de tecnologías de la información de la municipalidad distrital de Punchana.

Para realizar esta evaluación nos guiaremos de los siguientes pasos:

1. Fase de Inicio: Planificación y Preparación:

- Objetivo: Evaluar la eficiencia y eficacia de los controles de seguridad informática implementados en la unidad de tecnologías de la información de la municipalidad distrital de Punchana.

- Alcance: Sistemas críticos de la Unidad de Tecnologías de la Información de la municipalidad distrital de Punchana, incluyendo la gestión de acceso y la protección de datos.

- Formación del Equipo de Auditoría:

  El equipo estará conformado por: Bach. Luz Ángela Gordon Doza y el Bach. Alexander Reyes Mozombite

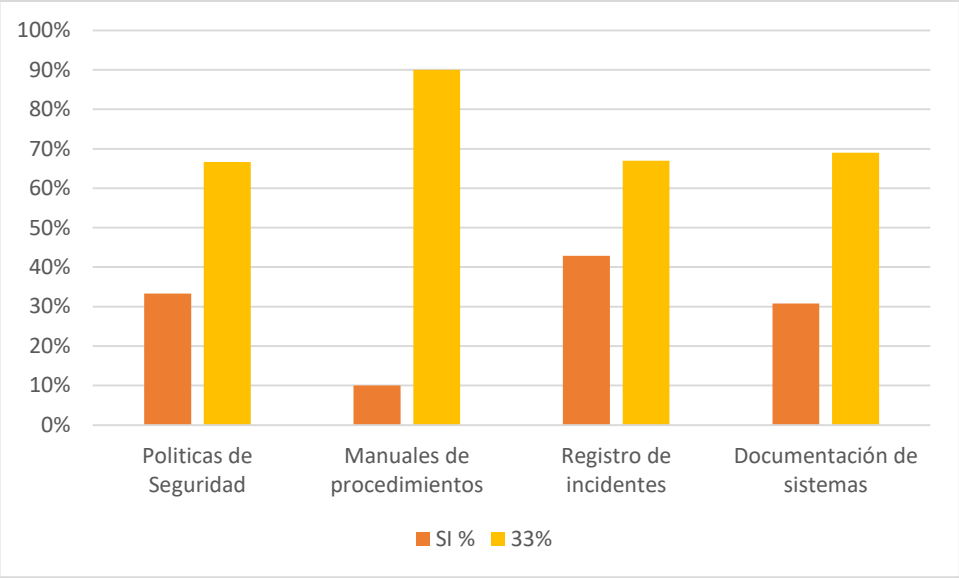
- Revisión de Documentación Existente:

Tabla N° 03: Revisión de documentación existente

Categoría	Tipo	Evaluación (Si o No)
Políticas de seguridad	Política de Acceso y Control de Usuarios	Si
	Política de Contraseñas	Si
	Política de Seguridad Física	No
	Política de Respaldo y Recuperación	Si
	Política de Seguridad de Red	No
	Política de Actualización de Software	Si
	Política de Gestión de Incidentes	No
	Política de Seguridad de la Información Confidencial	No
	Política de Monitoreo y Auditoría	No
	Política de Educación y Concientización en Seguridad	No
	Política de Seguridad en el Desarrollo de Aplicaciones	No
	Política de Gestión de Vulnerabilidades	No
Manuales de procedimientos	Manual de Procedimientos de Gestión de Incidentes de Seguridad Informática	No
	Manual de Procedimientos de Gestión de Accesos	No
	Manual de Procedimientos de Respaldo y Recuperación de Datos	No
	Manual de Procedimientos de Mantenimiento de Hardware y Software	Si
	Manual de Procedimientos de Administración de Redes	No
	Manual de Procedimientos de Seguridad de la Información	No
	Manual de Procedimientos de Auditoría Informática	No
	Manual de Procedimientos de Desarrollo de Software	No
	Manual de Procedimientos de Soporte Técnico	No
	Manual de Procedimientos de Gestión de Activos de TI	No
Registros de incidentes	Registro de Incidentes de Seguridad Informática	No
	Registro de Ataques a la Red	No
	Registro de Problemas de Hardware	Si
	Registro de Problemas de Software	Si
	Registro de Incidentes de Soporte Técnico	Si
	Registro de Fallos en el Sistema	No
	Registro de Amenazas y Vulnerabilidades Detectadas	No
Documentación de sistemas	Diagrama de Arquitectura del Sistema	No
	Manual del Usuario	Si
	Diccionario de Datos	Si
	Diagramas de Flujo de Procesos	No
	Modelo de Datos	No
	Procedimientos de Respaldo y Recuperación	No
	Planes de Continuidad del Negocio y Recuperación ante Desastres	No
	Manuales de Instalación y Configuración	Si
	Contratos y Licencias de Software	Si
	Informe de Pruebas y Validación	No
	Diagramas de Red	No
	Historial de Cambios y Versiones	No
	Manuales de Actualización	No

Fuente: Elaboración propia

Figura 03: Revisión de documentación existente



De la tabla 03 se puede evidenciar que de los 12 documentos que se revisaron respecto a la categoría políticas de seguridad solo cumple con 4 representando el 33%, de la categoría manuales de procedimientos de los 10 documentos solo cuenta con 1 representando el 10%, de la categoría registro de incidentes de los 7 documentos solo cuenta con 3 representando el 43%, y de la categoría documentación de sistemas de los 13 documentos solo cuenta con 4 representando el 31%.

2. Fase de Evaluación de Riesgos y Controles:

- Análisis de riesgos:

Tabla N° 04: Matriz de análisis de riesgos Data Center

Data Center o Centro de Datos										
Amenazas	Probabilidad	Degradación			Impacto			Estimación del riesgo		
		DC	D I	DD	IC	II	ID	RC	RI	RD
Daño por agua	3	1	1	4	Despreciable	Despreciable	Crítico	Bajo	Bajo	Alto
Avería de origen físico o lógico	2	1	1	4	Despreciable	Despreciable	Crítico	Bajo	Bajo	Medio
Corte del suministro eléctrico	4	1	1	4	Despreciable	Despreciable	Crítico	Bajo	Bajo	Alto
Errores del administrador	2	2	2	4	Moderado	Moderado	Crítico	Medio	Medio	Medio
Errores de mantenimiento / actualización de equipos (hardware)	2	1	1	3	Despreciable	Despreciable	Crítico	Bajo	Bajo	Medio
Caída del sistema por agotamiento de recursos	2	1	1	4	Despreciable	Despreciable	Crítico	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	3	3	1	Critico	Critico	Despreciable	Alto	Alto	Bajo
Abuso de privilegios de acceso	2	3	3	2	Critico	Critico	Moderado	Medio	Medio	Medio

Fuente: Elaboración propia

Tabla N° 05: Matriz de análisis de riesgos red LAN

Red LAN										
Amenazas	Probabilidad	Degradación			Impacto			Estimación del riesgo		
		DC	D I	DD	IC	II	ID	RC	RI	RD
Fallo de servicios de comunicaciones	2	1	1	4	Despreciable	Despreciable	Crítico	Bajo	Bajo	Medio
Errores del administrador	2	1	2	4	Despreciable	Menor	Crítico	Bajo	Bajo	Medio
Fugas de información	2	3	1	1	Moderado	Despreciable	Despreciable	Medio	Bajo	Bajo
Caída del sistema por agotamiento de recursos	2	1	1	3	Despreciable	Despreciable	Moderado	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	3	3	1	Moderado	Moderado	Despreciable	Medio	Medio	Bajo
Abuso de privilegios de acceso	2	3	3	3	Moderado	Moderado	Moderado	Medio	Medio	Medio
Divulgación de información	2	2	1	1	Menor	Despreciable	Despreciable	Bajo	Bajo	Bajo

Fuente: Elaboración propia

Tabla N° 06: Matriz de análisis de riesgos de la infraestructura de la unidad de Tecnologías de la Información

Oficina de Informática y Telecomunicaciones										
Amenazas Probabilidad		Degradación			Impacto			Estimación de riesgo		
		DC	D I	DD	IC	II	ID	RC	RI	RD
Daños por agua	3	1	1	2	Despreciable	Despreciable	Menor	Bajo	Bajo	Bajo
Alteración accidental de la información	2	1	2	1	Despreciable	Menor	Despreciable	Bajo	Bajo	Bajo
Fugas de información	2	3	1	1	Moderado	Despreciable	Despreciable	Medio	Bajo	Bajo
Divulgación de información	2	3	1	1	Moderado	Despreciable	Despreciable	Medio	Bajo	Bajo

Fuente: Elaboración propia

Tabla N° 07: Matriz de análisis de riesgos de equipos de cómputo servidores

Equipos de Cómputo Servidores										
Amenazas	Probabilidad	Degradación			Impacto			Estimación del riesgo		
		DC	IC	II	IC	II	ID	RC	RI	RD
Daño por agua	3	1	1	4	Despreciable	Despreciable	Crítico	Bajo	Bajo	Alto
Avería de origen físico o lógico	2	1	1	3	Despreciable	Despreciable	Crítico	Bajo	Bajo	Medio
Corte de suministro eléctrico	4	1	1	4	Despreciable	Despreciable	Crítico	Bajo	Bajo	Alto
Errores de los usuarios	2	3	3	3	Crítico	Crítico	Crítico	Medio	Medio	Medio
Errores del administrador	2	3	3	4	Crítico	Crítico	Crítico	Medio	Medio	Medio
Errores de configuración	2	1	4	1	Despreciable	Crítico	Despreciable	Bajo	Medio	Bajo
Escapes de información	2	3	1	1	Crítico	Despreciable	Despreciable	Medio	Bajo	Bajo
Alteración accidental de la información	2	1	3	1	Despreciable	Crítico	Despreciable	Bajo	Bajo	Bajo
Fugas de información	2	2	1	1	Moderado	Despreciable	Despreciable	Medio	Bajo	Bajo
Errores de mantenimiento/actualización de equipo (hardware)	2	1	1	4	Despreciable	Despreciable	Crítico	Bajo	Bajo	Medio
Errores de mantenimiento/actualización de equipo (software)	2	1	3	3	Despreciable	Crítico	Crítico	Bajo	Medio	Medio
Caída del sistema por agotamiento de recursos	2	1	1	4	Despreciable	Despreciable	Crítico	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	3	3	3	1	Crítico	Crítico	Despreciable	Alto	Alto	Bajo
Abuso de privilegios de acceso	2	3	3	3	Crítico	Crítico	Crítico	Medio	Medio	Medio
Divulgación de la información	2	2	1	1	Moderado	Despreciable	Despreciable	Medio	Bajo	Bajo
Manipulación de equipos	2	4	1	4	Crítico	Despreciable	Crítico	Medio	Bajo	Medio

Fuente: Elaboración propia

Tabla N° 08: Matriz de análisis de riesgos de la infraestructura de la Municipalidad

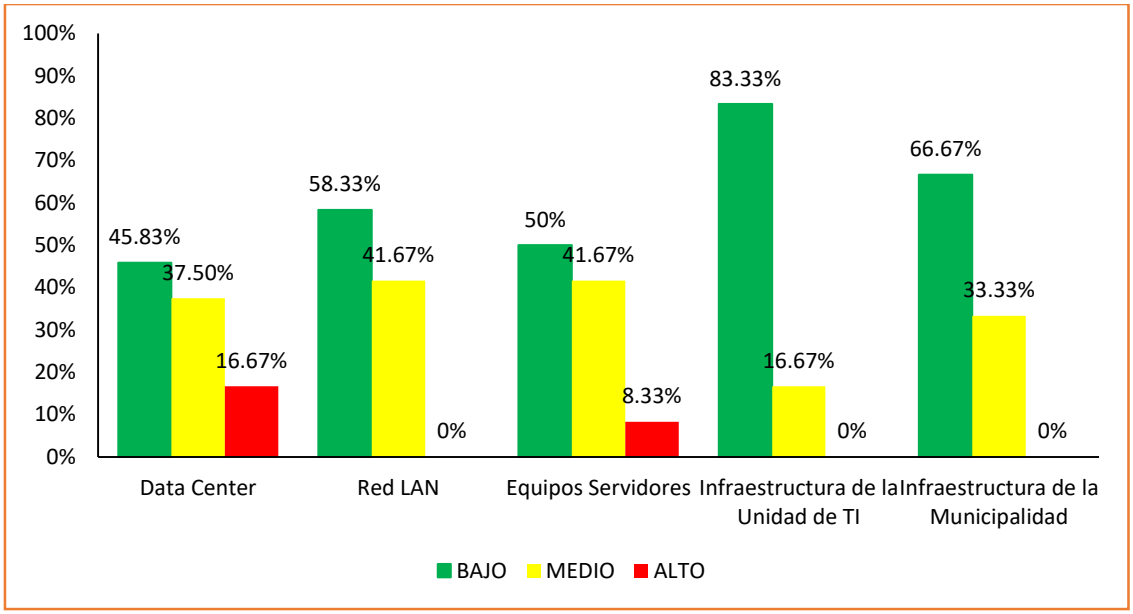
Infraestructura de la Municipalidad										
Amenazas	Probabilidad	Degradación			Impacto			Estimación de riesgo		
		DC	D I	DD	IC	II	ID	RC	RI	RD
Daños por agua	3	1	1	2	Despreciable	Despreciable	Moderado	Bajo	Bajo	Medio
Alteración accidental de la información	2	1	2	1	Despreciable	Moderado	Despreciable	Bajo	Medio	Bajo
Fugas de información	2	2	1	1	Moderado	Despreciable	Despreciable	Medio	Bajo	Bajo
Divulgación de información	2	2	1	1	Moderado	Despreciable	Despreciable	Medio	Bajo	Bajo

Fuente: Elaboración propia

Tabla N° 09: Leyenda de Abreviaturas de la matriz de riesgos

DC	Degradación en la Confidencialidad
DI	Degradación en la Integridad
DD	Degradación en la Disponibilidad
IC	Impacto en la Confidencialidad
II	Impacto en la Integridad
ID	Impacto en la Disponibilidad
RC	Riesgo en la Confidencialidad
RI	Riesgo en la Integridad
RD	Riesgo en la Disponibilidad

Figura 04: Análisis de riesgo de todos los componentes evaluados



De las tablas 04, 05, 06, 07 y la figura 04 se puede evidenciar que el que tiene mayor probabilidad de riesgo es el componente data center con un 16.67% de riesgo alto y también los equipos servidores con un 8.33%.

Evaluación de controles Actuales:

Tabla N° 10: Evaluación de Controles actuales

Tipo de control	Efectividad (Alta/Media /Baja)	Observaciones
Políticas de seguridad de la información	Alta	Políticas bien documentadas y comunicadas
Firewalls y sistemas de detección de intrusiones	Alta	Configuración actualizada, pero se requiere monitoreo constante.
Actualizaciones regulares de software y parches	Media	Proceso eficiente de aplicación de parches y actualizaciones.
Gestión de identidad y acceso	Media	Procedimientos implementados, pero hay áreas para mejorar en la gestión de accesos.
Auditorías y monitoreo de logs	Baja	La implementación de auditorías y monitoreo de logs es limitada; se recomienda mejorar.

Copias de seguridad y planes de recuperación	Media	Se realizan copias de seguridad de manera regular, y los planes de recuperación están bien definidos.
Formación en conciencia de seguridad para el personal	Alta	Sesiones de formación periódicas, pero se puede mejorar la participación activa del personal.
Protección física de los equipos y centros de datos	Alta	Acceso físico restringido y medidas de seguridad efectivas.

Fuente: Elaboración propia

3. Fase de Ejecución: Recopilación de Datos y Pruebas:

- Entrevistas:

Tabla N° 11: Pregunta 1 ¿Considera que las políticas de seguridad informática en la Unidad de Tecnologías de la Información son claras y comprensibles?

políticas de seguridad informática

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente de acuerdo	2	28,6	28,6	28,6
De acuerdo	2	28,6	28,6	57,1
Neutral	3	42,9	42,9	100,0
Total	7	100,0	100,0	

Fuente: Elaboración propia

De la tabla 11 se puede evidenciar que el 28.6% de los encuestados está totalmente de acuerdo que las políticas de seguridad informática en la Unidad de Tecnologías de la Información son claras y comprensibles, el 28,6% está de acuerdo y el 42,9% es neutral.

Tabla N° 12: Pregunta 2 ¿Con qué frecuencia se llevan a cabo simulacros o pruebas de seguridad informática en la unidad?

Pruebas de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	4	57,1	57,1	57,1
	Casi Nunca	3	42,9	42,9	100,0
	Total	7	100,0	100,0	

Fuente: Elaboración propia

De la tabla 12 se puede evidenciar que el 57,1% de los encuestados señala que nunca se llevan a cabo simulacros o pruebas de seguridad informática en la unidad y el 42,9% señala que casi nunca.

Tabla N° 13: Pregunta 3 ¿Cómo evaluaría la eficacia de los controles de acceso físico a los recursos informáticos en su área de trabajo?

eficacia de los controles de acceso físico

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Neutral	4	57,1	57,1	57,1
Poco efectivos	3	42,9	42,9	100,0
Total	7	100,0	100,0	

Fuente: Elaboración propia

De la tabla 13 se puede evidenciar que el 57,1% de los encuestados es neutral al evaluar la frecuencia que se lleva a cabo los simulacros o pruebas de seguridad informática en la unidad, y el 42,9% señala que son poco efectivos.

Tabla N° 14: Pregunta 4 ¿Ha recibido capacitación sobre buenas prácticas de seguridad informática en el último año?

capacitación sobre buenas prácticas de seguridad informática

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si ocasionalmente	3	42,9	42,9	42,9
No pero me gustaría recibir capacitación	4	57,1	57,1	100,0
Total	7	100,0	100,0	

Fuente: Elaboración propia

De la tabla 14 se puede evidenciar que el 42,9% de los encuestados señala que se da capacitación sobre buenas prácticas de seguridad informática si se da ocasionalmente, el 57,1% señala que no se da capacitación, pero si le gustaría recibirla.

Tabla N° 15: Pregunta 5 En su opinión, ¿cuál es el mayor desafío actual en términos de seguridad informática en la Unidad de Tecnologías de la Información?

Seguridad informática

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Falta de recursos	4	57,1	57,1	57,1
Falta de conciencia entre el personal	3	42,9	42,9	100,0
Total	7	100,0	100,0	

Fuente: Elaboración propia

De la tabla 15 se puede evidenciar que el 57,1% de los encuestados señala que por la falta de recursos no se da capacitación sobre buenas prácticas de seguridad informática en el último año y el 42,9% señala que es por falta de conciencia entre el personal.

Tabla N° 16: Pregunta 6 ¿Cómo calificaría la respuesta de la unidad ante incidentes de seguridad informática?

incidentes de seguridad informática

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Neutral	4	57,1	57,1	57,1
	Lenta	3	42,9	42,9	100,0
	Total	7	100,0	100,0	

Fuente: Elaboración propia

De la tabla 16 se puede evidenciar que el 57,1% de los encuestados señala como neutral la calificación a la respuesta de la unidad ante incidentes de seguridad informática, el 42,9% califica como lenta a la respuesta a los incidentes.

Tabla N° 17: Pregunta 7 ¿Se realiza una evaluación periódica de vulnerabilidades en los sistemas de la Unidad de Tecnologías de la Información?

Respuesta de la unidad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
ocasionalmente	3	42,9	42,9	42,9
No pero se necesita	4	57,1	57,1	100,0
Total	7	100,0	100,0	

Fuente: Elaboración propia

De la tabla 17 se puede evidenciar que el 42,9% de los encuestados señala que ocasionalmente se realiza una evaluación periódica de vulnerabilidades en los sistemas de la Unidad de Tecnologías de la Información, el 57,1% señala que no, pero se necesita.

Tabla N° 18: Pregunta 8 ¿Cómo considera la comunicación interna sobre temas de seguridad informática dentro de la Unidad de Tecnologías de la Información?

Evaluación periódica de vulnerabilidades

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Neutral	3	42,9	42,9	42,9
Poco efectiva	4	57,1	57,1	100,0
Total	7	100,0	100,0	

Fuente: Elaboración propia

De la tabla 18 se puede evidenciar que el 42,9% de los encuestados considera neutral la comunicación interna sobre temas de seguridad informática dentro de la Unidad de Tecnologías de la Información y el 57,1% como poca efectiva.

Tabla N° 19: Pregunta 9 En su experiencia, ¿se implementan actualizaciones de seguridad de manera oportuna en los sistemas y aplicaciones utilizados en la Unidad de Tecnologías de la Información?

Actualizaciones de seguridad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En su mayoría no oportuna	3	42,9	42,9	42,9
Nunca de manera oportuna	4	57,1	57,1	100,0
Total	7	100,0	100,0	

Fuente: Elaboración propia

De la tabla 19 se puede evidenciar que el 42,9% de los encuestados considera que en su mayoría no oportuna se implementan actualizaciones de seguridad de manera oportuna en los sistemas y aplicaciones utilizados en la Unidad de Tecnologías de la Información y el 57,1% nunca de manera oportuna.

- Pruebas técnicas

Tabla N° 20: Evaluación de pruebas técnicas

N°	Tipo de Prueba	Descripción	% Cumplimiento	Nivel de Criticidad
1	Escaneo de Vulnerabilidades	Evaluación de vulnerabilidades en la red y sistemas	75	Critico
2	Prueba de Penetración	Simulación de un ataque para evaluar la resistencia del sistema	60	Critico
3	Análisis de Logs	Revisión de registros de eventos para detectar posibles amenazas	80	Alto
4	Evaluación de Controles de Acceso	Verificación de la efectividad de los controles de acceso	90	Moderado
5	Revisión de Configuración de Firewall	Análisis de la configuración del firewall para posibles brechas	70	Moderado
6	Pruebas de Seguridad en Aplicaciones Web	Evaluación de vulnerabilidades en aplicaciones web	85	Alto
7	Análisis de Seguridad en Servidores	Evaluación de la seguridad en servidores y servicios críticos	100	Bajo
8	Evaluación de Políticas de Seguridad	Revisión de las políticas de seguridad y su implementación	90	Moderado
9	Monitoreo de Tráfico de Red	Análisis del tráfico de red para detectar actividades sospechosas	80	Alto
10	Evaluación de Respaldo y Recuperación de Datos	Verificación de la eficacia de los procedimientos de respaldo	95	Bajo

Fuente: Elaboración propia

Se identificaron 12 vulnerabilidades críticas, lo que sugiere la necesidad urgente de abordar y remediar estas vulnerabilidades. El cumplimiento se sitúa en el 75%, indicando áreas de mejora significativa.

Se logró acceso no autorizado en 3 instancias, lo cual es crítico. El cumplimiento se encuentra en el 60%, indicando deficiencias notables en la resistencia del sistema.

Se detectaron patrones de actividad sospechosa, con un cumplimiento del 80%. La criticidad es alta, sugiriendo que se deben tomar medidas adicionales para fortalecer la seguridad de los registros de eventos.

Fallos en la autenticación en 7 intentos, aunque el cumplimiento es del 90%. La criticidad es moderada, lo que indica áreas específicas que podrían necesitar mejoras.

Se encontraron 6 vulnerabilidades en la aplicación, pero el cumplimiento es relativamente alto (85%). La criticidad es alta, lo que destaca la importancia de abordar las vulnerabilidades identificadas.

Configuración segura en todos los servidores, con un cumplimiento del 100%. La criticidad es baja, indicando una buena postura de seguridad en esta área específica.

Cumplimiento del 90% de las políticas establecidas, con una criticidad moderada. Esto sugiere áreas de mejora para cumplir completamente con las políticas de seguridad.

Actividades anómalas detectadas en 14 casos, con un cumplimiento del 80%. La criticidad es alta, resaltando la importancia de mejorar la detección y respuesta a actividades sospechosas.

Restauración exitosa del 95% de los datos, con un cumplimiento del 95%. La criticidad es baja, indicando un buen rendimiento en la gestión de respaldo y recuperación de datos.

4. Fase de Análisis de Datos:

❖ Comparación con Estándares de COBIT 5:

- Dominio "Evaluar, Dirigir y Supervisar" (EDM):
  - Objetivo: Evaluación de Riesgos y Controles.

    La identificación de riesgos y la evaluación de la efectividad de los controles se alinea con este dominio. Las matrices de análisis de riesgos presentadas son coherentes con el enfoque de COBIT 5 para la gestión de riesgos.

- Dominio "Adquirir, Implementar, y Gestionar" (AIE):
  - Objetivo: Políticas, Planes y Procesos de Seguridad.

    Las recomendaciones sobre la creación de políticas adicionales, manuales de procedimientos y documentación de sistemas se alinean con los requisitos de este dominio. Se sugiere mejorar la documentación de políticas y procedimientos.

  - Objetivo: Gestión de Riesgos de TI.

    Las recomendaciones relacionadas con la evaluación de riesgos y la implementación de medidas adicionales para mitigar riesgos se alinean con este objetivo.

  - Objetivo: Educación y Concientización.

    La necesidad de mejorar la conciencia y la capacitación del personal coincide con los requisitos de este dominio. Se sugiere un programa de formación regular y simulacros.

- Dominio "Monitorear, Evaluar y Valorar" (MEA):
  - Objetivo: Monitoreo de Controles Internos.

Las recomendaciones sobre auditorías y monitoreo de logs se alinean con la necesidad de monitorear continuamente los controles internos, tal como se describe en COBIT 5.

- ❖ Objetivo: Evaluación de Cumplimiento.
  Las pruebas técnicas y la evaluación continua se relacionan con el objetivo de evaluar el cumplimiento con las políticas y procedimientos establecidos.

- ❖ Objetivo: Evaluación de Rendimiento y Conformidad.
  La evaluación periódica de vulnerabilidades y la implementación oportuna de actualizaciones de seguridad se alinean con la necesidad de evaluar el rendimiento y la conformidad.

- ➢ Dominio "Construir, Entregar y Ejecutar" (BAE):
  - ❖ Objetivo: Gestión de Cambios.
    Las recomendaciones sobre la falta de documentación, como manuales de procedimientos, y la falta de políticas en algunos aspectos, sugieren la necesidad de mejorar la gestión de cambios.

  - ❖ Objetivo: Gestión de la Seguridad de la Información.
    Las recomendaciones para mejorar la seguridad de la información, incluida la gestión de incidentes y la concientización del personal, se alinean con este objetivo.

- ➢ Dominio "Entregar, Servicios y Soporte" (DSS):
  - ❖ Objetivo: Gestión de Servicios.
    Las recomendaciones sobre la necesidad de mejorar la comunicación interna, la respuesta a incidentes y la implementación de actualizaciones de seguridad se relacionan con la gestión efectiva de servicios.

5. Presentación de Resultados:

- Revisión y Mejora de Documentación:

  Considerando las políticas de seguridad, se sugiere desarrollar y documentar políticas adicionales, especialmente aquellas relacionadas con la seguridad física, gestión de incidentes, educación y concientización en seguridad, entre otras.

  La falta de manuales de procedimientos y documentación en varias áreas es un área crítica que requiere atención. Se recomienda desarrollar manuales de procedimientos para cubrir aspectos importantes como gestión de incidentes, gestión de accesos, respaldo y recuperación, seguridad de la información, entre otros.

  Se debe trabajar en la creación de registros y documentación de sistemas faltantes, como diagramas de arquitectura del sistema, procedimientos de respaldo y recuperación, planes de continuidad del negocio, entre otros.

- Gestión de Riesgos:

  Dada la alta probabilidad de riesgos identificados en el Data Center y los servidores, se recomienda implementar medidas adicionales para mitigar estos riesgos. Esto puede incluir mejoras en la infraestructura, medidas de seguridad física y protocolos de respuesta a incidentes.

- Controles Actuales:

  Aunque las políticas de seguridad están bien documentadas y comunicadas, la baja efectividad en auditorías y monitoreo de logs es preocupante. Se sugiere mejorar la implementación de auditorías y monitoreo constante para identificar y responder rápidamente a eventos de seguridad.

- Entrenamiento y Concientización:

  Dado que un porcentaje significativo de encuestados indica que no se realizan simulacros o pruebas de seguridad informática con regularidad, se recomienda aumentar la frecuencia de estos ejercicios y proporcionar capacitación adicional al personal.

  La falta de recursos y conciencia entre el personal son desafíos identificados. Se puede abordar esta situación mediante la asignación adecuada de recursos y la implementación de programas de concientización y capacitación regulares.

- Pruebas Técnicas y Evaluación Continua:

  La identificación de vulnerabilidades críticas y acceso no autorizado durante las pruebas técnicas subraya la necesidad de un enfoque más proactivo hacia la seguridad informática. Se recomienda realizar pruebas técnicas de manera regular y llevar a cabo evaluaciones de seguridad continuas.

- Implementación Oportuna de Actualizaciones de Seguridad:

  Dado que una proporción significativa de encuestados considera que las actualizaciones de seguridad no se implementan de manera oportuna, se sugiere mejorar los procesos para garantizar la aplicación oportuna de parches y actualizaciones.

- Comunicación Interna:

  La percepción de que la comunicación interna sobre temas de seguridad informática es neutral o poco efectiva destaca la necesidad de mejorar la comunicación y concientización dentro del equipo. Se pueden implementar estrategias para mejorar la

comunicación y compartir regularmente información relevante sobre seguridad.

- ❖ Respuesta a Incidentes:

  Dado que la mayoría de los encuestados califican como neutral la respuesta de la unidad ante incidentes de seguridad, se sugiere revisar y mejorar los procedimientos de respuesta a incidentes para garantizar una respuesta rápida y eficaz.

- ❖ Evaluación Periódica de Vulnerabilidades:

  La evaluación periódica de vulnerabilidades debería ser una práctica estándar. Se recomienda establecer un programa regular de evaluación de vulnerabilidades y realizar las correcciones necesarias de manera oportuna.

- ❖ Monitoreo y Mejora Continua:

  Implementar un sistema de monitoreo continuo de seguridad para detectar y responder a amenazas de manera proactiva. Además, establecer un ciclo de mejora continua para abordar los hallazgos de las auditorías y pruebas técnicas.

Objetivo 2. Elaborar planes para mejorar la seguridad informática para la unidad de tecnologías de la información de la municipalidad distrital de Punchana

1. Fase de Planificación y Preparación:

Actividades:

1.1. **Revisión de Documentación Existente:**

- Actualizar las políticas de seguridad que no están documentadas.
- Crear manuales de procedimientos faltantes, especialmente en gestión de incidentes, auditoría informática y desarrollo de software.

- Mejorar la documentación de los registros de incidentes y amenazas detectadas.

1.2. **Entrenamiento del Personal:**

- Proporcionar formación adicional sobre las políticas actualizadas y nuevos procedimientos.
- Implementar sesiones periódicas de concientización en seguridad para el personal.

2. Fase de Evaluación de Riesgos y Controles:

Actividades:

2.1. **Análisis de Riesgos:**

- Implementar medidas de mitigación para las amenazas identificadas, especialmente en el Data Center y equipos servidores.
- Actualizar y fortalecer los controles de seguridad según las recomendaciones.

2.2. **Evaluación de Controles Actuales:**

- Reforzar la implementación de auditorías y monitoreo de logs.
- Mejorar la gestión de identidad y acceso, implementando procedimientos más efectivos.
- Realizar simulacros regulares y pruebas de seguridad informática.

3. Fase de Ejecución: Recopilación de Datos y Pruebas:

Actividades:

3.1. **Entrevistas y Encuestas:**

- Recopilar feedback del personal sobre la claridad de las políticas y procedimientos.
- Mejorar la comunicación interna sobre temas de seguridad informática.

3.2. **Pruebas Técnicas:**

- Abordar las vulnerabilidades críticas identificadas en el escaneo de vulnerabilidades y la prueba de penetración.
- Fortalecer la seguridad de las aplicaciones web y servidores.

4. Fase de Monitoreo Continuo y Evaluación:

Actividades:

4.1. **Implementación de Herramientas de Monitoreo:**

- Instalar herramientas de monitoreo de tráfico de red para detectar actividades sospechosas.

4.2. **Auditorías Periódicas:**

- Realizar auditorías periódicas de la implementación de políticas y controles.

5. Fase de Documentación y Mejora Continua:

Actividades:

5.1. **Documentación de Procesos:**

- Continuar mejorando y actualizando la documentación de políticas y procedimientos.

5.2. **Análisis de Resultados:**

- Evaluar regularmente los resultados de las pruebas técnicas y encuestas.
- Ajustar y mejorar los controles y procedimientos según sea necesario.

Recursos Necesarios:

- Capacitadores para la formación del personal.
- Herramientas de seguridad informática.

- Personal técnico para implementar medidas de mitigación.
- Herramientas de monitoreo de red.

Indicadores de Éxito:

1. Reducción del número de vulnerabilidades críticas.
2. Aumento en la efectividad de los controles según las pruebas técnicas.
3. Mejora en la percepción del personal sobre la claridad de las políticas y procedimientos.
4. Incremento en la frecuencia de simulacros y pruebas de seguridad.

CAPÍTULO V.- DISCUSIÓN:

Cuasapaz Narvaez y Landázuri Narvaez (2023): aborda la mitigación de riesgos tecnológicos en el GAD Municipal de Montúfar mediante COBIT 5. La evaluación revela deficiencias que podrían comprometer la seguridad de activos informáticos. La metodología cuali-cuantitativa y encuestas ofrecen una visión holística, y el plan de acción propuesto señala un impacto positivo potencial en la seguridad de la información.

Barreto Merino (2022): señala que el enfoque de auditoría informática en la Cooperativa de Transportes Patria destaca la importancia de COBIT 5 en seguridad de la información. Aunque se mencionan deficiencias, una exploración más profunda de las recomendaciones y su implementación podría proporcionar una comprensión más completa de cómo COBIT 5 contribuye a mejorar la seguridad informática.

Vargas García (2019): la investigación resalta el enfoque prioritario de las instituciones financieras ecuatorianas en la mejora de canales de atención digital. La propuesta de una metodología específica para evaluar el Control de Calidad de Software en bancos medianos, respaldada por COBIT, refuerza la validez y aporta un enfoque estructurado a la mejora de la calidad del software en el contexto bancario.

Machado Lloreda (2018): La auditoría en seguridad informática en la Institución Educativa Escuela Normal Superior de Quibdó, utilizando COBIT, destaca la aplicación del marco en entornos educativos. La metodología MAGERIT para el análisis de riesgos complementa el enfoque de COBIT, proporcionando una evaluación integral. Más detalles sobre las recomendaciones y acciones resultantes serían valiosos para comprender mejor el impacto en la cultura de seguridad informática.

Encarnacion Nuñez (2020): La auditoría informática en la Sub Gerencia de Administración Tributaria de la Municipalidad Distrital de Hualmay, basada en COBIT, destaca la correlación positiva entre la implementación de la auditoría y la mejora en la seguridad informática. Detalles adicionales sobre

cómo esta mejora impactó las operaciones específicas de la Sub Gerencia serían esclarecedores.

Bautista Ushiñahua (2020): La auditoría informática con COBIT 4.5 en la Universidad Nacional de Ucayali destaca la aplicabilidad del marco en el registro de software y hardware en el área de patrimonio. Más detalles sobre fases de auditoría y el impacto de las recomendaciones en la gestión de software y hardware enriquecerían la comprensión de la aplicación de COBIT 4.5 en el contexto universitario.

Chávez Ángeles (2020): La implementación de COBIT 5 en el proceso de transferencia de datos contables, financieros y administrativos en la Empresa DATCO S&H resalta la versatilidad del marco en áreas críticas de organizaciones. Aunque se destaca la alineación con estrategias empresariales, más detalles sobre la implementación específica y su impacto práctico en la gestión de la información serían esenciales para comprender completamente los beneficios obtenidos.

CAPÍTULO VI. - CONCLUSIONES:

Sobre la Revisión de Documentación Existente:
La evaluación de la documentación existente revela deficiencias en la cobertura de políticas de seguridad, manuales de procedimientos y registros de incidentes. Se destaca la necesidad de mejorar la documentación en áreas críticas como seguridad física, gestión de incidentes y políticas específicas.

Sobre la Fase de Evaluación de Riesgos y Controles:
El análisis de riesgos identifica áreas de preocupación, especialmente en el Data Center y los servidores, donde se registró una alta probabilidad de riesgos críticos. Se recomienda implementar medidas adicionales para mitigar estos riesgos y fortalecer la seguridad física.

Sobre la Evaluación de Controles Actuales:
Aunque las políticas de seguridad están bien comunicadas, la baja efectividad en auditorías y monitoreo de logs plantea preocupaciones. Se sugiere mejorar la implementación de auditorías y monitoreo constante para una respuesta más rápida a eventos de seguridad.

Sobre la Fase de Ejecución: Recopilación de Datos y Pruebas:
Los resultados de las entrevistas y encuestas revelan áreas de mejora en la comunicación interna, la frecuencia de simulacros y pruebas de seguridad informática, y la concientización del personal. La falta de recursos y conciencia entre el personal son desafíos que deben abordarse mediante asignación adecuada de recursos y programas de capacitación regulares.

Sobre las Pruebas Técnicas y Evaluación Continua:
Las pruebas técnicas identificaron vulnerabilidades críticas y acceso no autorizado, subrayando la necesidad de un enfoque proactivo hacia la

seguridad informática. Se recomienda realizar pruebas técnicas regulares y evaluaciones continuas de seguridad.

Sobre la Implementación Oportuna de Actualizaciones de Seguridad:
La percepción de que las actualizaciones de seguridad no se implementan de manera oportuna destaca la necesidad de mejorar los procesos para garantizar la aplicación puntual de parches y actualizaciones.

CAPÍTULO VII.- RECOMENDACIONES:

- Desarrollar políticas adicionales, especialmente en áreas críticas como seguridad física, gestión de incidentes, y concientización en seguridad.
- Crear manuales de procedimientos que aborden aspectos esenciales, tales como gestión de incidentes, gestión de accesos, respaldo y recuperación, seguridad de la información, entre otros.
- Elaborar la documentación y registros faltantes, como diagramas de arquitectura del sistema, procedimientos de respaldo y recuperación, y planes de continuidad del negocio.
- Garantizar la completa representación de políticas, manuales y registros para una cobertura integral de aspectos de seguridad informática.
- Implementar medidas adicionales para mitigar riesgos identificados en el Data Center y servidores, incluyendo mejoras en infraestructura, seguridad física y protocolos de respuesta a incidentes.
- Realizar evaluaciones periódicas de vulnerabilidades y controles de acceso para fortalecer la seguridad de los activos críticos.
- Mejorar la efectividad de auditorías y monitoreo constante para identificar y responder rápidamente a eventos de seguridad.
- Implementar herramientas de detección de amenazas y establecer procedimientos para la revisión regular de registros de eventos.
- Aumentar la frecuencia de simulacros y pruebas de seguridad informática para mejorar la preparación del personal ante posibles incidentes.
- Desarrollar programas regulares de capacitación y concientización en seguridad informática para abordar la falta de recursos y conciencia entre el personal.

CAPÍTULO VIII.- REFERENCIAS BIBLIOGRÁFICAS:

Barreto Merino, L. J. (2022). Auditoría informática mediante COBIT 5 a la Cooperativa de Transportes Patria, Período 2020 (Bachelor's thesis). Universidad Nacional de Chimborazo, Riobamba.

Bautista Ushiñahua, M. A. (2020). Auditoría informática con metodología COBIT 4.5 para el registro de software y hardware del área de patrimonio de la Universidad Nacional de Ucayali: 2017.

Cuasapaz Narvaez, K. A., & Landázuri Narvaez, K. D. (2023). AUDITORIA INFORMÁTICA USANDO EL MARCO DE REFERENCIA COBIT 5 PARA EL DEPARTAMENTO DE TIC DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE MONTÚFAR. UPEC.

Chavez Angeles, E. E. (2020). Aplicación de la metodología COBIT 5 para la mejora de procesos de auditoría y seguridad informática en la empresa DATCO S&H, Huaraz.

Encarnacion Nuñez, E. F. (2020). Auditoría Informática aplicando la metodología COBIT en la subgerencia de administración tributaria de la Municipalidad Distrital de Hualmay-Provincia de Huaura, 2018.

ISACA. (2021). COBIT Framework. Retrieved from https://www.isaca.org/resources/cobit

IT Governance Institute. (2019). COBIT 2019 Framework. Retrieved from https://www.isaca.org/resources/cobit

Machado Lloreda, B. J. Auditoría informática a la infraestructura tecnológica y sistema de información bajo el estándar COBIT a la Institución Educativa Escuela Normal Superior de Quibdó.

Vargas García, H. H. (2019). Metodología de auditoría informática para evaluar el área de control de calidad de software en bancos privados medianos del Ecuador, basada en el marco de referencia COBIT.

ANEXOS:

Anexo 1.- Documento de aceptación de la evaluación:

CARTA DE AUTORIZACIÓN

AUDITORÍA INFORMÁTICA CON LA METODOLOGIA COBIT 5 DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA – 2023

El que suscribe, Ing. ERIKA VANESA RAMOS FERNANDEZ, jefe de la unidad de tecnología de la información de la Municipalidad Distrital de Punchana, autoriza a los Bachilleres LUZ ANGELA GORDON DOZA y ALEXANDER REYES MOZOMBITE, para realizar una auditoria informática, como parte del desarrollo de su tesis titulada "**AUDITORÍA INFORMÁTICA CON LA METODOLOGIA COBIT 5 DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA – 2023**", en la facultad de Ciencias e Ingeniería, programa académico de Ingeniería de Sistemas de Información.

San Juan Bautista, 11 de Noviembre del 2023

Atentamente,

_____
Ing. Erika Vanesa Ramos Fernández
Jefe de Unidad

Anexo 2.- Cuestionario para evaluar la eficiencia y eficacia de los controles de seguridad informática implementados en la unidad de TI de la municipalidad distrital de Punchana

Cuestionario para evaluar la eficiencia y eficacia de los controles de seguridad informática implementados en la unidad de TI de la municipalidad distrital de Punchana

Por favor, indique su rol o posición en la Unidad de Tecnologías de la Información: _____

Responda las siguientes preguntas:

N°	PREGUNTA	ESCALA LIKERT				
		1	2	3	4	5
1	¿Considera que las políticas de seguridad informática en la Unidad de Tecnologías de la Información son claras y comprensibles?					
2	¿Con qué frecuencia se llevan a cabo simulacros o pruebas de seguridad informática en la unidad?					
3	¿Cómo evaluaría la eficacia de los controles de acceso físico a los recursos informáticos en su área de trabajo?					
4	¿Ha recibido capacitación sobre buenas prácticas de seguridad informática en el último año?					
5	En su opinión, ¿cuál es el mayor desafío actual en términos de seguridad informática en la Unidad de Tecnologías de la Información?					
6	¿Cómo calificaría la respuesta de la unidad ante incidentes de seguridad informática?					
7	¿Se realiza una evaluación periódica de vulnerabilidades en los sistemas de la Unidad de Tecnologías de la Información?					
8	¿Cómo considera la comunicación interna sobre temas de seguridad informática dentro de la Unidad de Tecnologías de la Información?					
9	En su experiencia, ¿se implementan actualizaciones de seguridad de manera oportuna en los sistemas y aplicaciones utilizados en la Unidad de Tecnologías de la Información?					