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

ANÁLISIS DE RIESGOS EN LA INFRAESTRUCTURA INFORMÁTICA DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE BELÉN 2023

PARA OBTAR EL TITÚLO PROFESIONAL

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

- **BACH. VILDER ELÍ MONTALVÁN MONDRAGÓN**
- **BACH. RODOLFO RUIZ VÍLCHEZ**

ASESOR:

- **ING. LEE FRANK MENDOZA LÓPEZ, Dr.**

SAN JUAN BAUTISTA – MAYNAS – LORETO - PERÚ – 2024

UNIVERSIDAD CIENTÍFICA DEL PERÚ

"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:

"ANÁLISIS DE RIESGOS EN LA INFRAESTRUCTURA INFORMÁTICA DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE BELÉN 2023"

De los alumnos: **VILDER ELÍ MONTALVÁN MONDRAGÓN Y RODOLFO RUIZ VÍLCHEZ,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **17% de similitud**. Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 24 de mayo del 2024.

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

JLTF/ri-a
197-2024

UCP_ING.SISTEMASDEINFORMACION_2024_TESIS_VilderMo...

INFORME DE ORIGINALIDAD

17%	16%	2%	9%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repository.unad.edu.co Fuente de Internet	3%
2	www.grafiati.com Fuente de Internet	3%
3	alicia.concytec.gob.pe Fuente de Internet	2%
4	www.slideshare.net Fuente de Internet	1%
5	Submitted to Universidad Catolica de Avila Trabajo del estudiante	1%
6	repository.javeriana.edu.co Fuente de Internet	1%
7	repositorio.uta.edu.ec Fuente de Internet	1%
8	gdoc.tips Fuente de Internet	<1%
9	ruidera.uclm.es Fuente de Internet	<1%

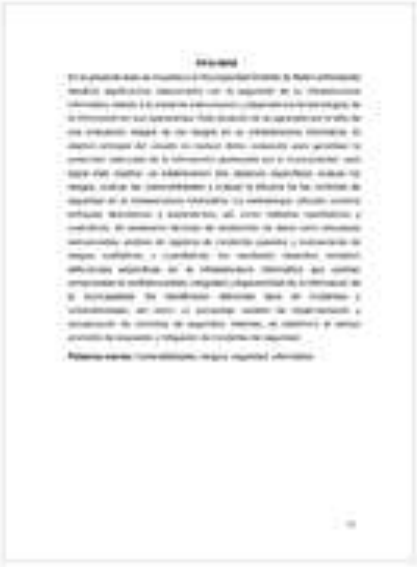
turnitin

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:	Vilder Elí Montalván Mondragón
Título del ejercicio:	Quick Submit
Título de la entrega:	UCP_ING.SISTEMASDEINFORMACION_2024_TESIS_VilderMon...
Nombre del archivo:	MONTALVAN-_RUIZ_INFORME_FINAL_EJECUTADO.pdf
Tamaño del archivo:	295.58K
Total páginas:	80
Total de palabras:	5,796
Total de caracteres:	34,028
Fecha de entrega:	28-may.-2024 11:11p. m. (UTC+0700)
Identificador de la entre...	2386500270



ACTA DE SUSTENTACIÓN

FACULTAD DE CIENCIAS E INGENIERÍA

UNIVERSIDAD CIENTÍFICA DEL PERÚ

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 130-2024-UCP-FCEI del 22 de febrero del 2024, 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 Asesor de la Tesis, Ing. Lee Frank Mendoza López, Mtro

En la ciudad de Iquitos, siendo las **08:00 am** del día **10 de junio 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 de la Tesis: ***ANALISIS DE RIESGOS EN LA INFRAESTRUCTURA INFORMATICA DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE BELEN 2023***

Presentado por las sustentantes

- RUIZ VILCHEZ RODOLFO

- MONTALVAN MONDRAGON VILDER ELÍ

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 APROBADA POR UNANIMIDAD

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

Ing. Jimmy Max Ramírez Villacorta, Mtro.
Presidente

Ing. Christian Alfredo Arévalo Jesús, Mtro.
Miembro

Ing. Tonny Eduardo Bardales Lozano, Mgr
Miembro

HOJA DE APROBACIÓN

UNIVERSIDAD CIENTÍFICA DEL PERÚ

HOJA DE APROBACIÓN

PROGRAMA ACADÉMICO INGENIERÍA DE SISTEMAS INFORMACIÓN
TESISTAS: RUIZ VILCHEZ RODOLFO y MONTALVAN MONDRAGON VILDER ELÍ

Tesis sustentada en acto publico el 10 de junio de 2024, a las 08:00 am en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ.

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

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

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

ING. LEE FRANK MENDOZA LOPEZ, MTRO.
ASESOR

DEDICATORIA

“Dedico este trabajo en primer lugar a mis padres que día a día siempre lucharon para formar un hijo de bien, a mis hermanos de sangre en especial a mi hermano Joel, a mis hermanos de carrera Rodolfo y José Carlos por el apoyo mutuo de inicio a fin”

BACH. VILDER ELÍ MONTALVÁN MONDRAGÓN

DEDICATORIA

"Dedico este trabajo a mi esposa Amarily, cuyo aliento y apoyo incondicional fue mi fuente invaluable de inspiración a lo largo de este proceso académico. A mi hijo por ser mi principal fuente de fortaleza en salir adelante. A Vilder y José Carlos, mis hermanos de carrera; por brindarme su ánimo y motivación en los momentos difíciles. Finalmente, a mi madre, su apoyo y consejos me hicieron fuerte para llegar hasta aquí. Este logro, es también de ustedes"

BACH. RODOLFO RUIZ VÍLCHEZ

AGRADECIMIENTO

“Empezar agradeciendo a mis padres que sin su apoyo llegar hasta este punto habría sido imposible, a mi hermano José que gracias a su aliento tirar la toalla nunca fue una opción, a mis docentes a lo largo de toda la carrera, a mi asesor de tesis por el apoyo constante en esta investigación y agradecer a cada personita que estuvo involucrada en este hermoso proceso de formación profesional**”**

BACH. VILDER ELÍ MONTALVÁN MONDRAGÓN

“Quiero empezar dando gracias a mis padres, que con su apoyo me han impulsado siempre a perseguir mis metas y nunca abandonar el estudio. Mi más sincero agradecimiento a mi Asesor de Tesis, por su orientación y apoyo constante a lo largo de este Proyecto. Agradezco a mis docentes, que me transmitieron los conocimientos necesarios durante mi camino universitario. A mis compañeros, por el tiempo compartido, los trabajos en grupos y las experiencias vividas. Además, quiero agradecer a mi Universidad, por tantas exigencias para impartir conocimientos y formarme como profesional competente. Su colaboración para la realización de este trabajo a sido invaluable"

BACH. RODOLFO RUIZ VÍLCHEZ

INDICE DE CONTENIDO

Página

INDICE DE TABLAS

RESUMEN

En la presente tesis se muestra a la Municipalidad Distrital de Belén enfrentando desafíos significativos relacionados con la seguridad de su infraestructura informática, debido a la creciente interconexión y dependencia de tecnologías de la información en sus operaciones. Esta situación se ve agravada por la falta de una evaluación integral de los riesgos en su infraestructura informática. El objetivo principal del estudio es realizar dicha evaluación para garantizar la protección adecuada de la información gestionada por la municipalidad, para lograr este objetivo, se establecieron tres objetivos específicos: evaluar los riesgos, evaluar las vulnerabilidades y evaluar la eficacia de los controles de seguridad en la infraestructura informática. La metodología utilizada combina enfoques descriptivos y exploratorios, así como métodos cuan titativos y cualitativos. Se emplearon técnicas de recolección de datos como encuestas estructuradas, análisis de registros de incidentes pasados y evaluaciones de riesgos cualitativas y cuantitativas, los resultados obtenidos revelaron deficiencias específicas en la infraestructura informática que podrían comprometer la confidencialidad, integridad y disponibilidad de la información de la municipalidad. Se identificaron diferentes tipos de incidentes y vulnerabilidades, así como un porcentaje variable de implementación y actualización de controles de seguridad. Además, se determinó el tiempo promedio de respuesta y mitigación de incidentes de seguridad.

Palabras claves: Vulnerabilidades, riesgos, seguridad, informática

ABSTRACT

In this thesis, the District Municipality of Belén is shown facing significant challenges related to the security of its IT infrastructure, due to the increasing interconnection and dependence on information technologies in its operations. This situation is exacerbated by the lack of a comprehensive risk assessment of its IT infrastructure. The main objective of the study is to conduct such an assessment to ensure the proper protection of the information managed by the municipality. To achieve this goal, three specific objectives were established: to assess risks, to evaluate vulnerabilities, and to assess the effectiveness of security controls in the IT infrastructure. The methodology used combines descriptive and exploratory approaches, as well as quantitative and qualitative methods. Data collection techniques such as structured surveys, analysis of past incident records, and qualitative and quantitative risk assessments were employed. The results obtained revealed specific deficiencies in the IT infrastructure th at could compromise the confidentiality, integrity, and availability of the municipality's information. Different types of incidents and vulnerabilities were identified, as well as a variable percentage of implementation and updating of security controls. Additionally, the average response and mitigation time for security incidents were determined.

Keywords: Vulnerabilities, risks, security, IT

CAPÍTULO I.- MARCO TEÓRICO:

1.1 Antecedentes de Estudio:

- Solarte, Mirian (2015), el propósito fundamental de este artículo es cultivar las habilidades de los ingenieros de sistemas, capacitándolos para liderar proyectos de diagnóstico, implementación e implantación de sistemas de seguridad de la información (SGSI). Estos esfuerzos se alinean con los estándares ISO/IEC 27001 y el sistema de control propuesto en la norma ISO/IEC 27002. Los resultados presentados derivan de una experiencia práctica que involucra las fases de auditoría y la metodología de análisis y evaluación de riesgos, para llevar a cabo este diagnóstico de seguridad, se emplearon diversos instrumentos, tales como cuestionarios dirigidos a los administradores, clave de seguridad, entrevistas con el personal del área informática y usuarios de los sistemas, pruebas de intrusión y testeo. Estas acciones permitieron establecer un diagnóstico preciso de la seguridad actual. Posteriormente, se aplicó una lista de chequeo basada en la norma, con el propósito de verificar la existencia de controles de seguridad en los procesos organizacionales, con base en los resultados obtenidos durante el análisis y evaluación de riesgos, se proponen controles de seguridad específicos. La idea es integrar estos controles en un SGSI futuro que se ajuste a las necesidades particulares de seguridad informática y de la información, respondiendo de manera efectiva a los requerimientos del entorno.

- Perfán, John, et al. (2014), El presente trabajo expone la necesidad imperante de la Institución Universitaria Colegio Mayor del Cauca de llevar a cabo un análisis de riesgos informáticos. Este análisis se basa en la metodología MAGERIT, la cual es una herramienta desarrollada por el Consejo Superior de Administración Electrónica para la

evaluación y gestión de riesgos en sistemas de información . El objetivo principal es minimizar los riesgos asociados con la implementación y uso de tecnologías de la información, especialmente dirigido a instituciones educativas. La metodología MAGERIT busca clasificar de manera precisa los riesgos, y los resultados obtenidos se utilizarán para generar recomendaciones específicas. Estas recomendaciones incluirán la selección e implementación de controles diseñados para mitigar los riesgos más altos o críticos, adicionalmente, se propone la creación de políticas de seguridad de la información como parte integral de este proceso. Estas políticas podrían ser posteriormente integradas en un Sistema de Gestión de Seguridad de la Información (SGSI) para la institución, fortaleciendo así la postura de seguridad global y asegurando una gestión integral de los riesgos informáticos.

- Garavito, Hina, et al. (2015), esta tesis se enfoca en realizar un análisis de riesgos utilizando la metodología MAGERIT en una entidad gubernamental no especificada por razones de seguridad. El análisis incluye la valoración de los activos de información, la evaluación de amenazas que pueden afectar dichos activos, un examen de las salvaguardas existentes (controles implementados actualmente en la entidad) y el análisis del riesgo efectivo. Para evaluar las amenazas, se emplearon entrevistas con los administradores de seguridad en la entidad, los resultados de un estudio de Ethical Hacking, y los datos recopilados de encuestas realizadas a todos los funcionarios con el fin de evaluar el adecuado u so de las tecnologías de información, los resultados de este análisis de riesgo proporcionan una comprensión del riesgo efectivo al que se enfrenta la entidad, junto con una propuesta de controles y recomendaciones. El objetivo es reducir los riesgos identificados y mejorar la fiabilidad, integridad y disponibilidad de la información en la entidad.

Vílchez, Denisse (2021), El propósito principal de la tesis consiste en realizar un análisis de riesgos dirigido a los activos de información, con el objetivo de permitir a la municipalidad identificar sus riesgos y vulnerabilidades. Esto posibilitará la adopción de medidas preventivas oportunas para evitar amenazas latentes en el entorno, la metodología empleada abarca enfoques cualitativos y cuantitativos, incorporando una ficha detallada de activos que el personal valoró para estimar el grado de riesgo. Además, se implementó una encuesta entregada a los colaboradores responsables, lo que facilitó la identificación y comprensión de la situación actual de los activos de información en la municipalidad, el análisis resultante permitirá que la municipalidad dirija y gestione las evaluaciones de riesgo de manera autónoma, tomando decisiones informadas mediante la comparación del análisis inicial con los resultados obtenidos. Esto facilitará la determinación de la aceptabilidad del riesgo. La implementación de buenas prácticas durante la investigación incluirá un control periódico de los activos, con el objetivo de mitigar los riesgos potenciales. En resumen, el Análisis de Riesgos busca reducir la probabilidad de incidentes. Es importante tener en cuenta que, si bien no es posible reducir la amenaza en sí misma, se puede eliminar la vulnerabilidad y minimizar el impacto de su ocurrencia.

Mamani, Wilber (2020), en este artículo, se investiga la estructura organizacional de la municipalidad distrital de Asillo con el propósito de mejorar la circulación de la información y el conocimiento relacionados con la seguridad de su infraestructura. Con este objetivo, se llevaron a cabo estudios descriptivos para detectar problemas en la municipalidad. Los resultados obtenidos permitieron identificar las debilidades existentes, que serán empleadas en investigaciones futuras para diseñar un plan de tratamiento de riesgos. Este plan incluirá la adquisición de habilidades necesarias para gestionar de manera más efectiva el riesgo, así como la implementación de buenas

prácticas gerenciales adaptadas a los desafíos contemporáneos, la información recopilada aborda diversos aspectos, como los elementos de la política de seguridad del municipio, la administración de activos, la organización de la seguridad de los recursos humanos, la seguridad física, la gestión de comunicaciones y operaciones, el control de acceso, el mantenimiento de sistemas, y la gestión de incidencias. Se sugiere la implementación de sistemas robustos basados en la norma ISO 27001:2013, haciendo uso de tecnologías modernas que se ajusten adecuadamente a las necesidades de la comunidad y salvaguarden sus activos de información más críticos.

Correa, Renzo (2019), este proyecto tiene como propósito principal diseñar un plan de continuidad de servicios críticos de tecnología de la información para la empresa constructora JJC Contratistas Generales
S.A. Se basa principalmente en la norma ISO/IEC 27031:2011 y otras guías pertinentes. El objetivo es mejorar la capacidad de respuesta ante posibles interrupciones parciales o totales de los servicios, garantizando una alta disponibilidad con tiempos de recuperación relativamente cortos para mantener la continuidad del negocio, la estructura del trabajo se divide en cinco puntos que facilitarán la comprensión del diseño propuesto. En el primer punto, se abordarán aspectos introductorios, como la situación problemática, los objetivos del proyecto y el estado del arte. En el segundo punto, se detallará el marco teórico, proporcionando información sobre los conceptos clave del plan de continuidad de servicios de TI, su importancia y las fases involucradas. El tercer punto se centrará en la definición del problema, el alcance de la solución, y la realización de análisis de riesgos, amenazas y vulnerabilidades, en el cuarto punto, se llevará a cabo la elaboración de la política de continuidad, la evaluación del riesgo junto con el análisis de impacto en el negocio, el desarrollo de estrategias de continuidad para diferentes escenarios, y la presentación detallada de

las alternativas de continuidad. Finalmente, en el quinto punto, se abordarán aspectos prácticos como el plan de pruebas, la ejecución, y la revisión y validación de los resultados de las pruebas. Como conclusión, se presentarán las conclusiones y recomendaciones para futuros proyectos.

1.2 Bases Teóricas:

Análisis de riesgos informático:

Para Whitman, M. E., & Mattord, H. J.; El análisis de riesgos informáticos constituye un procedimiento que implica la identificación y evaluación de los activos de información, así como el estudio de las amenazas y vulnerabilidades relacionadas. Su propósito fundamental radica en cuantificar el impacto potencial de eventos adversos y en la determinación de las medidas requeridas para mitigar estos riesgos.

Según la ISO/IEC 27001:2013; El análisis de riesgos informáticos se caracteriza por ser una evaluación sistemática y estructurada de los riesgos que impactan la confidencialidad, integridad y disponibilidad de la información. Este proceso conlleva la identificación de activos, amenazas y vulnerabilidades, así como la determinación de controles destinados a reducir o mitigar dichos riesgos.

Harris, S.; El análisis de riesgos informáticos constituye el procedimiento mediante el cual se identifican, evalúan y gestionan las amenazas y vulnerabilidades que pueden incidir en la seguridad de la información de una organización. Este proceso abarca la evaluación de la probabilidad y el impacto de eventos adversos, junto con la implementación de controles destinados a mitigar dichos riesgos.

Para la NIST SP 800-30, El análisis de riesgos informáticos se desenvuelve como un procedimiento que abarca desde la identificación de activos, amenazas y vulnerabilidades hasta la evaluación de las posibles consecuencias. Este proceso culmina con la determinación de medidas de seguridad destinadas a gestionar y reducir los riesgos vinculados a la información y los sistemas de información.

Metodologías para el análisis de riesgo informático

Según el Consejo Superior de Administración Electrónica, MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) representa un enfoque desarrollado por el Consejo Superior de Administración Electrónica de España. Su principal objetivo es dirigirse al análisis y gestión de riesgos específicamente en el ámbito de los sistemas de información.

Según la CERT Coordination Center, Universidad Carnegie Mellon, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) se configura como una metodología concebida por el CERT Coordination Center de la Universidad Carnegie Mellon. Su orientación se centra específicamente en la identificación y evaluación de riesgos tanto a nivel organizativo como técnico. El desarrollo de esta metodología lleva la autoría del CERT Coordination Center, perteneciente a la Universidad Carnegie Mellon.

Para la National Institute of Standards and Technology (NIST), La metodología NIST SP 800-30, suministrada por el National Institute of Standards and Technology (NIST) de Estados Unidos, se especializa en la gestión de riesgos asociados con tecnologías de la información y sistemas de información.

Para la Agencia Central de Telecomunicaciones y la Agencia de Suministros del Gobierno (CCTA) del Reino Unido, CRAMM (CCTA Risk Analysis and Management Method) es una metodología desarrollada por la Agencia Central de Telecomunicaciones y la Agencia de Suministros del Gobierno (CCTA) del Reino Unido. Se enfoca en el análisis y gestión de riesgos de tecnologías de la información.

Infraestructura informática

La infraestructura informática abarca el conjunto integral de recursos físicos, software, redes y servicios que constituyen la fundamentación tecnológica para llevar a cabo el procesamiento, almacenamiento, transmisión y gestión de información dentro de un entorno organizacional.

Gartner (2019), La infraestructura informática comprende la totalidad de elementos físicos y lógicos esenciales para el desempeño de los sistemas de información dentro de una organización. Este conjunto abarca hardware, software, redes, servicios y recursos afines que facilitan las operaciones de procesamiento, almacenamiento, transmisión y gestión de la información.

1.3 Definición de Términos Básicos:

- Seguridad: La seguridad implica encontrarse en un estado exento de peligros, daños o riesgos, y se logra mediante la aplicación de medidas preventivas y de protección frente a amenazas potenciales.
- Virtualización: es la generación de representaciones virtuales de recursos informáticos, como servidores, redes o almacenamiento. Esta práctica optimiza el aprovechamiento de la infraestructura, mejorando su flexibilidad y escalabilidad.
- Cloud Computing: se refiere a la entrega de servicios informáticos, como almacenamiento, procesamiento y software, a través de internet. Este enfoque reduce la dependencia de la infraestructura física local.
- Redes Definidas por Software (SDN): es una estrategia que desvincula el control de las redes del flujo de datos, permitiendo una gestión dinámica y programable de la infraestructura de red.
- Almacenamiento Definido por Software (SDS): separa la gestión de almacenamiento del software del hardware, brindando una

administración más adaptable y eficiente de los recursos de almacenamiento.

- Internet de las Cosas (IoT): abarca la conexión de dispositivos físicos a través de internet, utilizando sensores y actuadores para recopilar y compartir datos.

CAPÍTULO II.- PLANTEAMIENTO DEL PROBLEMA:

2.1 Descripción del Problema:

La creciente interconexión y dependencia de las tecnologías de la información en las entidades gubernamentales ha elevado la exposición a amenazas cibernéticas de carácter global. La creciente sofisticación de los ciberataques y la aparición de amenazas transnacionales generan riesgos significativos para la integridad, confidencialidad y disponibilidad de la información manejada por las instituciones gubernamentales, la Municipalidad Distrital de Belén, ubicada en el departamento de Loreto, Provincia de Maynas y distrito de Belén, quien es responsable de la administración y gobierno local en el distrito de Belén, sus funciones abarcan aspectos como planificación territorial, desarrollo urbano, gestión ambiental y servicios públicos locales, la municipalidad opera dentro del marco legal establecido por el gobierno central y se coordina con otras entidades gubernamentales para garantizar la coherencia y alineación de sus acciones con políticas nacionales y regionales, actualmente se enfrenta a desafíos específicos relacionados con la seguridad de su infraestructura informática. El aumento de incidentes cibernéticos a nivel nacional y las regulaciones gubernamentales cada vez más estrictas respecto a la protección de datos imponen la necesidad urgente de evaluar y gestionar los riesgos en la infraestructura informática. Además, la interconexión de sistemas a nivel nacional amplifica las amenazas potenciales a los activos de información de la municipalidad, la Oficina de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Belén enfrenta desafíos específicos derivados de la creciente digitalización de los servicios gubernamentales a nivel local. La demanda de servicios electrónicos y la gestión de información sensible de los ciudadanos aumentan la importancia de salvaguardar la infraestructura informática. Además, la infraestructura local puede verse afectada por amenazas

específicas, como ataques dirigidos a nivel comunitario o intentos de acceso no autorizado a datos locales.

2.2 Formulación del Problema:

2.2.1 Problema General:

- ✓ ¿En qué medida la ausencia de una evaluación integral de los riesgos de en la infraestructura informática puede afectar la gestión de la información en la municipalidad distrital de Belén?

2.2.2 Problemas Específicos:

- ✓ ¿Cuáles son los riesgos de la infraestructura informática que podrían comprometer la información de la municipalidad distrital de Belén?
- ✓ ¿Cuáles son las vulnerabilidades de la infraestructura informática que podrían comprometer la información de la municipalidad distrital de Belén?
- ✓ ¿Cuál es la eficacia de los controles de seguridad de la infraestructura informática que podrían comprometer la información de la municipalidad distrital de Belén?

2.3 Objetivos:

2.3.1 Objetivo General:

- ✓ Realizar una evaluación integral de la seguridad de la infraestructura informática de la municipalidad distrital de Belén en el año 2023

2.3.2 Objetivos Específicos:

- ✓ Evaluar los riesgos de la infraestructura informática en la munici palidad distrital de Belén.
- ✓ Evaluar las vulnerabilidades de la infraestructura informática en la municipalidad distrital de Belén.

- ✓ Evaluar la eficacia de los controles de la infraestructura informática respecto a la protección de la disponibilidad de la in formación en la municipalidad distrital de Belén.

2.4 Hipótesis:

- No Aplica.

2.5 Variables:

2.5.1 Identificación de Variables:

- **Variable:** Riesgo de la infraestructura informática

2.5.1.1 Definición conceptual:

Tabla 1.- Definición conceptual de la variable

Variable	Definición Conceptual	Definición Operacional
Riesgo de la infraestructura informática	Comprende las potenciales amenazas y vulnerabilidades que podrían comprometer la seguridad informática, así como las consecuencias asociadas, incluyendo pérdida de datos, interrupciones en los servicios y perjuicios a la reputación de la entidad.	Es la cuantificación mediante métodos específicos de evaluación, como el análisis de vulnerabilidades y la identificación de amenazas. Se emplearán indicadores clave, como la frecuencia de incidentes y la eficacia de los controles de seguridad, para medir y gestionar el riesgo de manera efectiva. La prontitud en la restauración de servicios tras interrupciones y la conformidad con estándares de seguridad reconocidos serán consideradas en la evaluación operacional del riesgo.

Fuente: Elaboración Propia

2.5.1.2 Operacionalización de las Variables:

Tabla 2.- Operacionalización de variables

Variables	Dimensiones	Indicadores	Instrumento de Recolección de Datos
Riesgo de la infraestructura informática	Evaluación del riesgo	% de frecuencia de incidentes	Fichas de Observación Fichas de registro Cuestionario
		% de Ocurrencia	
	Evaluación de vulnerabilidades	% de vulnerabilidades identificadas	
		% de vulnerabilidades corregidas	
	Eficacia de los controles	% de controles de seguridad implementados y actualizados	
		Tiempo con la que se responden y mitigan los incidentes de seguridad	

Fuente: Elaboración Propia

CAPÍTULO III.- METODOLOGÍA:

3.1 Tipo y Diseño de Investigación:

El tipo de investigación para el estudio "Análisis de Riesgos en la Infraestructura Informática de la Oficina de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Belén 2023" es principalmente descriptivo y exploratorio, y se complementa con un enfoque mixto, el enfoque descriptivo es fundamental para proporcionar un panorama claro de la situación actual de los riesgos en la infraestructura informática, el enfoque exploratorio permite identificar factores y aspectos que podrían no haber sido considerados previamente, contribuyendo a una comprensión más completa, la combinación de métodos cuantitativos y cualitativos permite una evaluación integral, proporcionando datos numéricos y percepciones subyacentes.

3.2 Población y Muestra:

- **Población:**

  Personal de la Oficina de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Belén.

- **Muestra:**

  El muestreo será por conveniencia y estará compuesta de la siguiente manera

Tabla 3.- Cuadro de personal de la oficina de tecnologías de la información y comunicaciones de la municipalidad distrital de Belén

Cargo	Cantidad
Jefe de Oficina	01
Analista Programador	01
Soporte Técnico	02
Total	04

3.3 Técnicas, instrumentos y procedimientos de recolección de datos:

- **Técnica de Recolección de Datos:**

- Encuestas estructuradas sobre riesgos de la infraestructura informática.
- Análisis de registros y datos de incidentes de seguridad pasados.

- **Instrumento de Recolección de Datos:**

- Cuestionarios estructurados sobre riesgos de la infraestructura informática.
- Fichas de registros y datos de incidentes de seguridad pasados.

- **Procedimiento de Recolección de Datos:**

- Matrices de riesgos cualitativas y cuantitativas.
- Evaluación de los riesgos identificados.

3.4 Procesamiento y análisis de datos:

- La Información será procesada en software estadístico, cuyos resultados serán clasificados en cuadros y gráficos estadísticos.
- Integración de hallazgos cualitativos y cuantitativos para obtener una visión completa de los riesgos en la infraestructura informática.

CAPÍTULO IV.- RESULTADOS:

Objetivo 1. Evaluar los riesgos de la infraestructura informática respecto a la protección de la confidencialidad de la información en la municipalidad distrital de Belén.

Dimensión: Evaluación del riesgo

Indicador: Porcentaje de frecuencia de incidentes

Tabla 4.- Porcentaje de frecuencia de incidentes – 2023

Mes	Tipo de incidente	Número de incidente registrado	Total de días trabajados	Porcentaje de frecuencia
Enero	Acceso no autorizado	2	22	22%
	Pérdida de datos	1		
	Fallo del sistema de dominio	2		
	Virus/Malware	5		
Febrero	Virus/Malware	5	20	45%
	Fallo de sistema de rentas	2		
	Acceso no autorizado	2		
Marzo	Acceso no autorizado	2	24	21%
	Fallo de sistema de rentas	3		
Abril	Pérdida de datos	1	20	45%
	Acceso no autorizado	1		
	Virus/Malware	7		
Mayo	Sin incidentes	0	20	0%
Junio	Virus/Malware	8	20	50%
	Acceso no autorizado	1		
	Pérdida de datos	1		
Julio	Acceso no autorizado	1	20	35%
	Virus/Malware	3		
	Fallo del sistema SIGA	2		
Agosto	Acceso no autorizado	1	22	5%
Setiembre	Fallo del sistema de tramite documentario	2	22	23%
	Acceso no autorizado	1		
	Fallo de sistema SIAF	2		
Octubre	Acceso no autorizado	1	22	27%
	Virus/Malware	2		
	Fallo del sistema de tramite documentario	3		
Noviembre	Acceso no autorizado	1	22	41%
	Virus/Malware	6		
	Fallo de sistema de rentas	2		
Diciembre	Fallo del sistema de rentas	1	22	23%
	Virus/Malware	4		

Fuente: Elaboración propia

Para calcular el porcentaje de frecuencia de incidentes, se siguió los siguientes pasos:

1. Determina el número de incidentes registrados: Este es el número total de incidentes que ocurrieron en un período específico, que puede ser mensual, trimestral o anual, según la frecuencia de tus registros.
2. Calcula el total de días trabajados: Esto representa el número total de días en los que la infraestructura informática estuvo en funcionamiento durante el mismo período que estás analizando. Esto puede incluir días laborables y días festivos, dependiendo de la disponibilidad y la operatividad de los sistemas.
3. Aplica la fórmula del porcentaje de frecuencia: Utiliza la siguiente fórmula para calcular el porcentaje de frecuencia de incidentes:

$$\text{Porcentaje de Frecuencia} = \frac{\text{Número de Incidentes Registrados}}{\text{Total de Días Trabajados}} \times 100$$

4. Interpreta el resultado: El porcentaje de frecuencia de incidentes te dará una medida de la frecuencia relativa de incidentes en relación con el tiempo operativo de la infraestructura informática. Cuanto mayor sea el porcentaje, más frecuentes son los incidentes en relación con el tiempo trabajado.

   Para cada mes, simplemente aplicas esta fórmula utilizando el número de incidentes registrados en ese mes y el total de días trabajados en ese mes. Luego, multiplicas el resultado por 100 para obtener el porcentaje. Este proceso se repite para cada mes del año o el período que estés analizando.

Interpretación: La tabla 04 presenta un resumen detallado de los incidentes registrados en la infraestructura informática de la Oficina de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Belén a lo largo del año 2023. Se observa una variedad de incidentes, como acceso no autorizado, virus/malware, pérdida de datos y fallos en sistemas específicos. Los meses con mayor frecuencia de incidentes fueron febrero,

abril, junio y noviembre, mientras que mayo fue el único mes sin incidentes registrados.

Dimensión: Evaluación del riesgo Indicador:

Porcentaje de Ocurrencia

Tabla 5.- Porcentaje de ocurrencia de incidentes – 2023

Tipo de incidente	Número de incidente registrado	Porcentaje de ocurrencia
Acceso no autorizado	19	24.68%
Virus/Malware	47	61.04%
Pérdida de datos	5	6.49%
Fallo del sistema de dominio	2	2.60%
Fallo de sistema de rentas	9	11.69%
Fallo del sistema SIGA	2	2.60%
Fallo del sistema de tramite documentario	6	7.79%
Fallo del sistema SIAF	2	2.60%
Sin incidentes	1	1.30%
Total de incidentes	77	100%

Fuente: Elaboración propia

Para calcular el porcentaje de ocurrencia de un tipo de incidente específico, dividimos el número de incidentes registrados de ese tipo por el total de incidentes registrados y luego multiplica por 100 para obtener el resultado en porcentaje.

La fórmula es la siguiente:

$$\text{Porcentaje de Ocurrencia} = \left(\frac{\text{Número de Incidentes Registrados de un Tipo}}{\text{Total de Incidentes Registrados}} \right) \times 100$$

Interpretación: La tabla 05 muestra el porcentaje de ocurrencia de distintos tipos de incidentes en la infraestructura informática de la Oficina de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Belén durante el período 2023. Se observa que los virus/malware son los incidentes más frecuentes, representando el 61.04% del total de incidentes registrados, seguidos por los accesos no autorizados

con un 24.68%. Los otros tipos de incidentes tienen un porcentaje de ocurrencia menor en comparación.

Objetivo 2. Evaluar las vulnerabilidades de la infraestructura informática en la municipalidad distrital de Belén.

Dimensión: Vulnerabilidades identificadas

Indicador: Porcentaje de vulnerabilidades identificadas

Tabla 6.- Porcentaje de vulnerabilidades identificadas – 2023

Mes	Tipo	Número de vulnerabilidades identificadas	Total de activos evaluados	Porcentaje de vulnerabilidades identificadas
Enero	Fallos de seguridad de software	20	100	20%
	Errores de configuración			
	Vulnerabilidades de red			
	Problemas de autenticación			
Febrero	Errores de configuración	15	110	13.64%
	Vulnerabilidades de aplicaciones			
Marzo	Fallos de seguridad de software	25	105	23.81%
	Errores de configuración			
	Vulnerabilidades de red			
Abril	Vulnerabilidades de aplicaciones	18	112	16.07%
	Problemas de autenticación			
Mayo	Errores de configuración	10	115	8.70%
Junio	Fallos de seguridad de software	22	120	18.33%
	Vulnerabilidades de aplicaciones			
Julio	Vulnerabilidades de red	28	118	23.73%
	Problemas de autenticación			
Agosto	Fallos de seguridad de software	14	122	11.48%
	Vulnerabilidades de aplicaciones			
Setiembre	Errores de configuración	20	125	16.00%
	Problemas de autenticación			
Octubre	Vulnerabilidades de red	16	130	12.31%
	Problemas de autenticación			
Noviembre	Fallos de seguridad de software	24	135	17.78%
	Errores de configuración			
Diciembre	Vulnerabilidades de aplicaciones	19	140	13.57%
	Problemas de autenticación			
Total de vulnerabilidades		231	1372	16.84%

Fuente: Elaboración propia

Para calcular el porcentaje de vulnerabilidades identificadas, primero necesitas conocer el número total de vulnerabilidades identificadas y el total de activos evaluados en un determinado período de tiempo, usando la siguiente fórmula:

$$\text{Porcentaje de Vulnerabilidades Identificadas} = \left(\frac{\text{Número de Vulnerabilidades Identificadas}}{\text{Total de Activos Evaluados}}\right) \times 100$$

Interpretación: La tabla 06 muestra el número de vulnerabilidades identificadas en la infraestructura informática de la Oficina de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Belén para cada mes del año. Al especificar los tipos de vulnerabilidades, proporciona una visión detallada de las áreas de riesgo dentro de la infraestructura. El porcentaje de vulnerabilidades identificadas indica la proporción de activos evaluados que presentan vulnerabilidades en cada mes.

Dimensión: Vulnerabilidades identificadas

Indicador: Porcentaje de vulnerabilidades corregidas

Tabla 7.- Porcentaje de vulnerabilidades corregidas – 2023

Mes	Número de vulnerabilidades identificadas	Número de vulnerabilidades corregidas	Porcentaje de vulnerabilidades corregidas
Enero	20	15	75.00%
Febrero	15	10	66.67%
Marzo	25	20	80.00%
Abril	18	15	83.33%
Mayo	10	8	80.00%
Junio	22	18	81.82%
Julio	28	24	85.71%
Agosto	14	12	85.71%
Setiembre	20	18	90.00%
Octubre	16	13	81.25%
Noviembre	24	20	83.33%
Diciembre	19	16	84.21%
Total	231	189	81.82%

Fuente: Elaboración propia

Para calcular el porcentaje de vulnerabilidades corregidas, dividimos el número de vulnerabilidades corregidas entre el total de vulnerabilidades identificadas y luego se multiplica por 100 para obtener el porcentaje.

La fórmula es la siguiente:

$$\text{Vulnerabilidades Corregidas} = \left(\frac{\text{Número de Vulnerabilidades Corregidas}}{\text{Total de Vulnerabilidades Identificadas}}\right) \times 100$$

Interpretación: La tabla 07 muestra el progreso de la corrección de vulnerabilidades en la infraestructura informática de la Oficina de

Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Belén durante el año 2023. Cada fila representa un mes del año, indicando el número de vulnerabilidades corregidas, el total de vulnerabilidades identificadas en ese mes y el porcentaje de vulnerabilidades corregidas en relación con el total identificado.

Objetivo 3. Evaluar la eficacia de los controles de la infraestructura informática respecto a la protección de la disponibilidad de la información en la municipalidad distrital de Belén.

Dimensión: Eficacia de los controles

Indicador: Porcentaje de controles de seguridad implementados y actualizados

Tabla 8.- Porcentaje de controles de seguridad implementados y actualizados – 2023

Mes	Tipo de controles	Número de controles planificados	Total de controles implementados	Porcentaje de controles implementados
Enero	Mantenimiento de Hardware y Software	28	30	92%
	Revisión de Antivirus	2		
	Actualizaciones de software sistema operativo	2		
Febrero	Actualización de usuarios de los sistemas	25	28	100%
	Revisión de Antivirus	3		
Marzo	Revisión del cableado de red	30	30	100%
Abril	Mantenimiento de servidores	29	27	95%
	Revisión de Antivirus	3		
Mayo	Revisión de Firewall	26	25	99%
Junio	Actualización de software	32	28	95%
	Revisión de Antivirus	3		
Julio	Mantenimiento de los equipos de red	31	31	100%
Agosto	Actualización de software ofimático	27	30	100%
	Revisión de Antivirus	3		
Setiembre	Auditoria a los sistemas informáticos	30	25	83%
Octubre	Mantenimiento de Hardware y Software	28	28	100%
Noviembre	Revisión de Firewall	29	32	100%
	Revisión de Antivirus	3		
Diciembre	Inventario de hardware y software	200	200	100%

Fuente: Elaboración propia

Interpretación: La tabla 08 muestra el progreso de implementación de diferentes tipos de controles de seguridad en la infraestructura informática de la Oficina de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Belén durante el año 2023.

Dimensión: Eficacia de los controles

Indicador: Tiempo con la que se responden y mitigan los incidentes de seguridad

Tabla 9.- Tiempo con la que se responden y mitigan los incidentes de seguridad- 2023

Mes	Tipo de controles	Tiempo Promedio de Respuesta y Mitigación de Incidentes (horas)
Enero	Mantenimiento de Hardware y Software	2
	Revisión de Antivirus	1
	Actualizaciones de software sistema operativo	3
Febrero	Actualización de usuarios de los sistemas	5
	Revisión de Antivirus	1
Marzo	Revisión del cableado de red	8
Abril	Mantenimiento de servidores	6
	Revisión de Antivirus	2
Mayo	Revisión de Firewall	2
Junio	Actualización de software	3
	Revisión de Antivirus	3
Julio	Mantenimiento de los equipos de red	5
Agosto	Actualización de software ofimático	5
	Revisión de Antivirus	5
Setiembre	Auditoria a los sistemas informáticos	5
Octubre	Mantenimiento de Hardware y Software	4
Noviembre	Revisión de Firewall	3
	Revisión de Antivirus	2
Diciembre	Inventario de hardware y software	12

Fuente: Elaboración propia

Interpretación: La tabla 08 muestra el tiempo promedio de respuesta y mitigación de incidentes de seguridad para cada tipo de control durante cada mes del año.

CAPÍTULO V.- DISCUSIÓN:

Solarte, Mirian (2015), los resultados presentados en las tablas reflejan una implementación efectiva de controles de seguridad informática y un tiempo de respuesta y mitigación de incidentes que está en línea con las buenas prácticas recomendadas por los estándares ISO/IEC 27001 y 27002. Esto sugiere que la Municipalidad Distrital de Belén está avanzando hacia la adopción de un SGSI efectivo, en línea con los esfuerzos liderados por los ingenieros de sistemas capacitados en seguridad de la información.

Perfán, John, et al. (2014), los resultados de las tablas indican que la implementación de controles de seguridad y los tiempos de respuesta y mitigación de incidentes están siendo gestionados de manera efectiva en la Municipalidad Distrital de Belén, lo que contribuye a la minimización de riesgos asociados con el uso de tecnologías de la información, tal como se propone en la metodología MAGERIT. Además, las recomendaciones específicas derivadas de los resultados podrían fortalecer aún más la postura de seguridad de la institución.

Garavito, Hina, et al. (2015), las tablas presentan resultados que reflejan un análisis de riesgos integral, similar al enfoque propuesto en la metodología MAGERIT. Los tiempos de respuesta y mitigación de incidentes, junto con la implementación de controles de seguridad, sugieren un esfuerzo concertado para reducir los riesgos identificados y mejorar la fiabilidad, integridad y disponibilidad de la información en la Municipalidad Distrital de Belén.

Vílchez, Denisse (2021), los resultados presentados en las tablas respaldan los esfuerzos de la Municipalidad Distrital de Belén para identificar y gestionar los riesgos y vulnerabilidades de sus activos de información. La implementación de buenas prácticas de análisis de riesgos, junto con la adopción de medidas preventivas oportunas, sugiere un enfoque proactivo hacia la gestión de la seguridad de la información.

Mamani, Wilber (2020) , las tablas proporcionan datos concretos sobre los controles de seguridad implementados y los tiempos de respuesta y mitigación de incidentes en la Municipalidad Distrital de Belén. Estos resultados pueden ser utilizados para mejorar la circulación de información y el conocimiento relacionados con la seguridad de la infraestructura, como se sugiere en la investigación realizada en la municipalidad distrital de Asillo.

CAPÍTULO VI. - CONCLUSIONES:

- Se identificaron múltiples tipos de incidentes, como accesos no autorizados, pérdida de datos y fallos del sistema, que representan riesgos significativos para la seguridad de la información, la frecuencia y diversidad de los incidentes resaltan la necesidad urgente de mejorar los controles de seguridad y la gestión de riesgos en la infraestructura informática de la municipalidad.
- Las vulnerabilidades identificadas, como accesos no autorizados y fallos del sistema, revelan áreas críticas que requieren atención inmediata para mitigar los riesgos asociados, la diversidad y persistencia de las vulnerabilidades resaltan la importancia de implementar medidas proactivas de seguridad para proteger los activos de información de la municipalidad.
- La variabilidad en el porcentaje de controles implementados y actualizados a lo largo del año indica la necesidad de mejorar la consistencia y eficacia de los controles de seguridad, la implementación inconsistente de controles podría afectar la disponibilidad de la información y la capacidad de respuesta ante incidentes, subrayando la importancia de una gestión proactiva de la seguridad informática.

CAPÍTULO VII.- RECOMENDACIONES:

- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI):
  Establecer un SGSI basado en estándares reconocidos, como ISO/IEC 27001, para garantizar una gestión integral de la seguridad de la información en la municipalidad.
  El SGSI proporcionará un marco estructurado para identificar, evaluar y gestionar los riesgos de seguridad de manera sistemática, asegurando una respuesta proactiva ante posibles amenazas.

- Fortalecer los controles de seguridad existentes:
  Mejorar la implementación y actualización de los controles de seguridad, incluyendo el mantenimiento de hardware y software, revisiones de antivirus y actualizaciones de sistemas operativos.
  Establecer procedimientos claros y periódicos para mantener los controles de seguridad actualizados y garantizar su eficacia en la protección de la infraestructura informática.

- Realizar auditorías periódicas de seguridad:
  Programar auditorías regulares de seguridad informática para identificar posibles vulnerabilidades y evaluar la efectividad de los controles de seguridad implementados.
  Estas auditorías proporcionarán una visión actualizada de la postura de seguridad de la municipalidad y permitirán la implementación de medidas correctivas de manera oportuna.

- Brindar formación en concienciación sobre seguridad:
  Ofrecer programas de formación y concienciación en seguridad de la información para todo el personal de la municipalidad, destacando la importancia de prácticas seguras en el manejo de datos y sistemas.
  La formación ayudará a crear una cultura de seguridad sólida en toda la organización, reduciendo el riesgo de incidentes causados por errores humanos o prácticas inseguras.

CAPÍTULO VIII.- REFERENCIAS BIBLIOGRÁFICAS:

- Ashton, K. (2009). "That 'Internet of Things' Thing." RFID Journal.
- CORREA SALAZAR, Renzo Giancarlo. Diseño de un plan de continuidad para los servicios críticos del área de Tecnología de la Información de la empresa JJC Contratistas Generales SA basado principalmente en la norma ISO/IEC 27031: 2011. 2019.
- Gartner. (2019). "Gartner Glossary: IT Infrastructure." Gartner, Inc.
- GARAVITO ROBLES, Hina Luz, et al. Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información. 2015.
- Guía MAGERIT v3.1, Consejo Superior de Administración Electrónica de España.
- Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). "Software-Defined Networking: A Comprehensive Survey." IEEE Communications Surveys & Tutorials.
- OCTAVE Allegro: Systematic Security Risk Assessment at Small Organizations, Carnegie Mellon University.
- PERAFÁN RUIZ, John Jairo, et al. Análisis de riesgos de la seguridad de la información para la institución universitaria Colegio Mayor del Cauca. 2014.
- NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments, NIST.
- MAMANI VENTURA, Wilber. Análisis de riesgo de la información según la norma iso 27001: 2013: previo a una implementación. 2020.
- Mell, P., & Grance, T. (2011). "The NIST Definition of Cloud Computing." National Institute of Standards and Technology.
- Smith, J., & Nair, R. (2005). "Virtual Machines: Versatile Platforms for Systems and Processes." Elsevier.
- SOLARTE, Francisco Nicolás Solarte; ROSERO, Edgar Rodrigo Enriquez; DEL CARMEN BENAVIDES, Mirian. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica-ESPOL, 2015, vol. 28, no 5.

- VILCHEZ MORANTE, Denisse Katherine. Análisis de riesgos a los activos de información aplicado a la gerencia de administración y finanzas de la Municipalidad Provincial de San Martín-Tarapoto. 2021.
- Webster, F. (2014). "Software-Defined Storage: An Introduction." O'Reilly Media.