Universidad Autónoma "Juan Misael Saracho"
Secretaría de Educación Continua

3

ARTICULO DE INVESTIGACIÓN

MODELO DE SEGURIDAD BASADO EN GESTIÓN DE RIESGOS PARA EL FORTALECIMIENTO DEL CONTROL DE ACTIVOS TECNOLÓGICOS

RISK MANAGEMENT-BASED SECURITY MODEL FOR STRENGTHENING THE CONTROL OF TECHNOLOGICAL ASSETS.

Fecha de recepción: 24/04/2026 | Fecha de aceptación: 11/05/2026

Autor(es):

* **Omar Amilkar Choque-Gonzales.**

* Carrera de Ingeniería Informática, Facultad de Ciencias y Tecnología Universidad Autónoma "Juan Misael Saracho"

* Correspondencia del autor(es): (+591) 60290002, ocho@correo.uajms.edu.bo

Modelo de seguridad basado en gestión de riesgos para el fortalecimiento del control de activos tecnológicos

Risk management-based security model for strengthening the control of technological assets.

Resumen

La presente investigación tiene como objetivo desarrollar un modelo de seguridad de inventarios de recursos tecnológicos basado en el análisis de riesgos, orientado a identificar, clasificar y valorar los activos tecnológicos de una institución empresaria, buscando fortalecer la seguridad de la información, optimizar la gestión de activos y garantizar la continuidad de las operaciones ante amenazas internas y externas, en concordancia con normas estándares de control y seguridad de recursos TI.

La metodología se basa en un enfoque cuanti-cualitativo, donde se utilizaron instrumentos como cuestionarios estructurados y revisión documental.

Los resultados arrojaron deficiencias en la infraestructura tecnológica, incluyendo hardware con bajo rendimiento, insuficiencia de software especializado y conectividad limitada. Además, se identificó una insatisfacción generalizada respecto a los recursos disponibles, como periféricos esenciales para desarrollar sus actividades laborales dentro de una organización.

El modelo propuesto integra fases como la clasificación de activos tecnológicos, el análisis de riesgos, la implementación de controles de seguridad y el desarrollo de un prototipo de sistema de gestión que permite registrar, clasificar y monitorear los recursos tecnológicos, alineándose con las normativas y estándares.

En conclusión, el modelo de seguridad de inventarios responde a las necesidades detectadas en el diagnóstico inicial, fortaleciendo la gestión de los recursos tecnológicos, mejorando su protección y garantizando la continuidad operativa.

Abstract

This research aims to develop a security model for inventories of technological resources based on risk analysis, oriented to identify, classify, and value the technological assets of a business institution. It seeks to strengthen information security, optimize asset management, and guarantee continuity of operations against internal and external threats, in accordance with standard control and IT resource security norms.

The methodology is based on a quantitative-qualitative approach, using instruments such as structured questionnaires and documentary review.

Palabras Claves: Seguridad de activos tecnológicos, inventario TI, modelo de seguridad TI.

Keywords: Technological asset security, IT inventory, IT security model

Results revealed deficiencies in technological infrastructure, including low-performance hardware, insufficient specialized software, and limited connectivity. In addition, a widespread dissatisfaction was identified regarding the available resources, such as essential peripherals needed to carry out work activities within the organization.

The proposed model integrates phases such as the classification of technological assets, risk analysis, implementation of security controls, and the development of a management system prototype that allows the registration, classification, and monitoring of technological resources, aligned with applicable standards and regulations.

In conclusion, the inventory security model addresses the needs detected in the initial diagnosis, strengthening the management of technological resources, improving their protection, and ensuring operational continuity.

1. Introducción

Este articulo examina el contexto evolutivo de las tecnologías de la información y comunicación en instituciones empresariales, destacando cómo la transformación digital ha incrementado la necesidad del control y la seguridad de los recursos tecnológicos debido a la complejidad y cantidad de activos tecnológicos inmersos en este tipo de organizaciones. Se enfatiza en la necesidad de sistemas de gestión adecuados que eviten pérdidas de información, riesgos operativos y de recursos tecnológicos lo que trae consigo nuevos desafíos en materia de seguridad de la información y control de activos tecnológicos (Whitman & Mattord, 2022).

Ante esta situación, se identificó a la falta de un inventario detallado y actualizado como un problema central, que expone a una institución a diversas vulnerabilidades; derivando en un problema de investigación central que es ¿Cómo garantizar el control y la seguridad de los activos tecnológicos en las instituciones empresarias ante la ausencia de un inventario preciso?", abordando las brechas en la gestión de recursos tecnológicos.

Esta necesidad, genera una investigación que se justifica por su relevancia en la protección de información crítica, la optimización de recursos y el cumplimiento normativo en contextos tecnológicos; incluyendo los aspectos generales como los riesgos derivados de la transformación digital, los aspectos sociales como el fortalecimiento de la seguridad en instituciones, los económicos por la reducción de costos por pérdidas y de investigación por la necesidad de generar conocimiento sobre las vulnerabilidades y las mejores prácticas para su mitigación.

Con esta finalidad, la investigación persigue el objetivo general de desarrollar un modelo de seguridad para inventarios de recursos TI basado en análisis de riesgos, enfocado en un caso empresarial. Se incluyen aspectos como sintetizar conceptos teóricos sobre control y seguridad usando COBIT(Control de Objetivos de la Información y la Tecnología), identificar factores actuales de control, determinar estándares para evaluar riesgos y proponer un modelo lógico de catálogo de inventarios.

2. Marco teórico

Los elementos teórico conceptuales analizados parten de una revisión documental de literatura académica sobre seguridad de activos tecnológicos y análisis de riesgos, integrando componentes como la clasificación de información, evaluación de amenazas y selección de controles. Todo con la finalidad de establecer los componentes del modelo lógico propuesto. Se consideran:

a. Inventario de Recursos TI

Según Holded (2018) y FulfillMent (2023), hace referencia al listado de los productos, componentes tecnológicos, descritos de una forma ordenada, precisa y actualizada que permite a las empresas conocer en tiempo real la disponibilidad de productos, facilitando

decisiones informadas sobre reabastecimiento, planificación de producción y gestión de la demanda optimizando costos y recursos al evitar la falta de stock o el exceso de productos en la empresa.

b. **Recursos TI**

Los recursos de la Tecnología de Información (TI) son 5:

- **Datos:** Definidos como objetos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, números, caracteres y otros. Por lo cual los datos se pueden definir como representaciones de información que se formula de diferentes formas.
- **Aplicaciones:** Entendidos como la suma de los procedimientos manuales y programados; a los procedimientos programados se los puede entender como una aplicación o programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.
- **Tecnología:** Cubre los componentes de hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc.
- **Infraestructura:** Comprende los Recursos para alojar y dar soporte a los sistemas de información. Se define infraestructura como un conjunto de elementos que componen un lugar o un sistema.
- **Recursos humanos:** Compuesto por la gente o los recursos humanos de una organización, las mismas que tienen habilidades del personal, conocimiento, sensibilización y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

c. **COBIT – Seguridad de la información**

El marco de referencia de los Objetivos de Control para las Tecnologías de la Información y Comunicación (COBIT), centra sus normas y políticas para establecer los estándares de auditoria informática a nivel mundial, para ello establece recursos TI, criterios de la información, dominios, procesos y tareas a ser aplicadas como controles de prevención, detección y corrección de los riesgos tecnológicos (Villamizar, 2022).

d. Criterios de la información

Los siete criterios de Información que maneja COBIT son:

- **Eficacia:** Encargada de establecer que la información sea relevante y pertinente a los procesos del negocio, y que sea entregada de manera oportuna, correcta, consistente y utilizable.
- **Eficiencia:** Se refiere a que la información sea producida mediante el uso óptimo (más productivo y económico) de los recursos.
- **Confidencialidad:** Tiene que ver con la protección de la información sensible contra divulgación no autorizada.
- **Integridad:** Se refiere a la exactitud y totalidad de la información, así como a su validez según el conjunto de valores y expectativas del negocio.
- **Disponibilidad:** Tiene que ver con la disponibilidad de la información cada vez que lo requieran los procesos del negocio y, por lo tanto, también se relaciona con la salvaguarda de los recursos.
- **Cumplimiento:** Se refiere al cumplimiento de las leyes, regulaciones y arreglos contractuales a que están sujetos los procesos del negocio; tales como los criterios de negocios impuestos por terceros.
- **Confiabilidad de la información:** Se refiere a que los sistemas brinden información apropiada a la gerencia para el manejo institucional, provean información financiera a los usuarios

de la información financiera, y produzcan la información pertinente para las entidades reguladoras, respecto al cumplimiento de las leyes y regulaciones.

e. Seguridad informática

Según Kissel (2012), la seguridad, la seguridad informática se define como la protección de información y sistemas de información de acceso no autorizado, se vincula con tres elementos básicos: la informaci6n que, como activo intangible, representa quizá el elemento más sensible y vulnerable; el software, cuya pérdida o modificación mal intencionada puede representar daños económicos y operativos severos a los usuarios y a una institución; por último el hardware, que al fallar provoca retrasos en la operación diaria y la consecuente pérdida de tiempo y costos elevados. Incluye:

- La protección de datos, referida a "los derechos de las personas e instituciones cuyos datos se recogen, se mantienen y se procesan; considerando las obligaciones legales y éticas con respecto a compartir los datos" (CEPAL: Comisión Económica para América Latina y el Caribe, 2021).
- La evaluación de impacto en la protección de datos, "es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos en función de las actividades de tratamiento que se llevan a cabo con los mismos" (AGPD: Agencia Española de protección de datos, 2018).

f. Gestión de riesgos

Un riesgo se define como la posibilidad (probabilidad) de que un acontecimiento ocurra y afecte (consecuencia o impacto) negativamente a la consecución de los objetivos. Según Sommerville (2005), la gestión de riesgos se fundamenta en las siguientes etapas:

- La **identificación de riesgos**, determina los posibles riesgos del proyecto que se obtienen de estudiar distintos aspectos contextuales del proyecto, como el producto y los negocios. El resultado de esta etapa es obtener el listado de riesgos potenciales
- El **análisis de riesgos**, donde se considera un análisis por separado de cada riesgo identificado definiendo la probabilidad y el efecto de su impacto en la organización, valorados como catastrófico, serio, tolerable o insignificante. El resultado de este proceso es una lista ordenada de los riesgos priorizado por el efecto o incidencia.
- **Planeación de riesgos**, este proceso considera cada uno de los riesgos clave identificados y las estrategias para administrarlo en tres categorías; las estrategias de anulación que son destinadas a reducir la probabilidad de que el riesgo surja; las estrategias de minimización destinadas reducir el impacto del riesgo y los planes de contingencia que contienen acciones a seguir sí el riesgo se materializa con tareas estratégicas para abordarlo.
- La **supervisión de riesgos**, que establece un conjunto de indicadores que podrían mostrar los cambios en cada riesgo.

3. Métodos

Los métodos empleados en la investigación, fueron importantes para obtener un diagnóstico de los factores que inciden en el control y la seguridad del inventario de recursos TI, siendo estos los siguientes:

- El enfoque de la investigación empleado fue mixto cuanti-cualitativo, con predominio cuantitativo, por el grado de análisis requerido a nivel de control y seguridad de activos tecnológicos en una organización empresarial, per-

mitiendo crear una propuesta basada en datos empíricos y teóricos (Ramirez, 2015).

- El tipo de investigación es aplicada y descriptiva, utilizando métodos teóricos (revisión documental y causal) y empíricos (observación y medición) para recopilar y analizar datos sobre riesgos y seguridad.
- Se aplicaron técnicas como la revisión documental para marco teórico, encuestas (cuestionarios estructurados) e entrevistas para las percepciones de usuarios, facilitando la recolección de datos sobre control y seguridad de activos tecnológicos.
- Se operacionalizaron variables dependientes a nivel de control y seguridad e independientes como los factores de riesgo, utilizando instrumentos como cuestionarios y entrevistas para medir percepciones y recopilar datos cuantitativos y cualitativos de manera sistemática.

4. Resultados

4.1. Aspectos relevantes del diagnóstico

Entre los hallazgos principales, se revelan deficiencias en la infraestructura tecnológica empresarial, como bajo rendimiento de hardware, limitada diversidad de software y problemas de conectividad, con hallazgos demográficos (mayor predominio masculino) y de uso (bajo empleo de bases de datos), identificando áreas críticas para mejora en el control de activos TI.

Entre las deficiencias identificadas, destacan la escasez de periféricos, problemas de ergonomía, insuficiencia en almacenamiento y conectividad, junto con insatisfacción general de usuarios respecto a la infraestructura del laboratorio, y los servicios informáticos lo que incrementa vulnerabilidades en la seguridad informática.

De este estudio, surgen algunas fortalezas como espacios adecuados y niveles aceptables de limpieza en instalaciones, así como la existencia de un marco para análisis de riesgos, que sirven de base para propuestas de mejora en la gestión de activos tecnológicos.

4.2. Modelo propuesto

El modelo propuesto -Figura 1- genera un inventario completo de recursos TI, identificando amenazas y vulnerabilidades clave; se proponen controles de seguridad específicos para mitigar riesgos, junto con un prototipo de sistema de gestión que facilita la monitorización y actualización de activos, mejorando la integridad, disponibilidad y confidencialidad de los recursos tecnológicos.

El modelo propuesto, se inició con la **clasificación de la información** sobre el inventario de los recursos TI, donde se logró identificar y categorizar los activos de información, registrada en cuadernos, archivadores y en sistema de información obsoleto sin clasificar.

Algunos de los aspectos comunes en el personal de una empresa muestran resultados relevantes del diagnóstico del inventario de recursos tecnológicos, siendo estos los siguientes:

Dispositivos y Hardware

Los teléfonos inteligentes son los dispositivos más uti-

lizados (46%), lo que sugiere la necesidad de evaluar la disponibilidad y el estado de otros dispositivos esenciales como computadoras y laptops.

Un 89% de los encuestados señaló insuficiencias en la capacidad de procesamiento y memoria RAM, indicando la urgencia de actualizar o adquirir nuevos equipos.

Software

El 54% calificó el software como "Nada adecuado", y el 43% expresó desacuerdo con la variedad disponible. Esto resalta la importancia de inventariar el software actual y considerar la adquisición de licencias más adecuadas para las necesidades académicas.

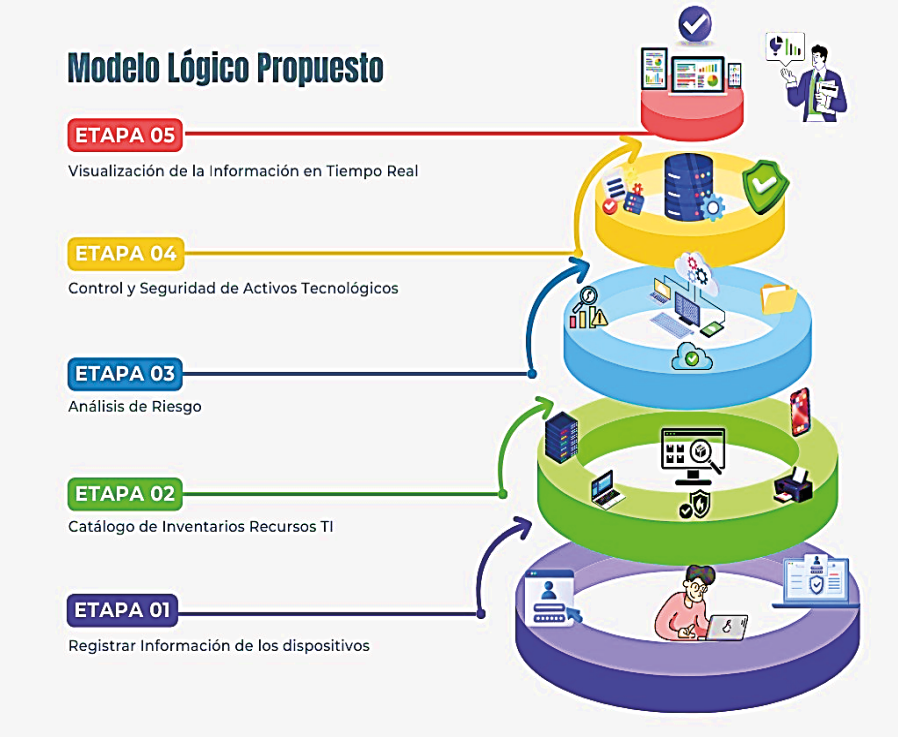
Conectividad a Internet

Con un 49% reportando acceso "Ocasional" y problemas constantes de conectividad, es crucial evaluar la infraestructura de red y asegurar que los recursos de conectividad sean suficientes y confiables.

Recursos Tecnológicos y Periféricos

La carencia de periféricos y recursos tecnológicos clave fue afirmada por el 87% de los encuestados. Un inventario detallado ayudaría a identificar y priorizar la adquisición de estos recursos.

Figura 1: Modelo lógico Propuesto



Fuente: Elaboración Propia.

Servidores y Mantenimiento

Con el 48% describiendo los servidores como "Muy lentos" y el 40% experimentando interrupciones, es fundamental revisar el estado de los servidores y planificar un mantenimiento más frecuente.

Personal Técnico

La disponibilidad "Intermitente" del personal técnico (45%) y la calidad de atención "Regular" (36%) sugieren la necesidad de evaluar y posiblemente aumentar el personal técnico para mejorar el soporte y mantenimiento de los recursos tecnológicos.

Luego, se definió los niveles de sensibilidad y vulnerabilidad para cada categoría mediante la aplicación de los principios del sistema de Administración de Bienes y Servicios dentro de la Ley No. 1178. Esto permitió establecer políticas y procedimientos para el manejo de la información según su clasificación, que fue la base para los planes y manuales de manejo de recurso tecnológicos.

Se logro etiquetar la información de acuerdo con su clasificación, mostrando las características y componentes tecnológicos de cada recurso TI.

Los resultados obtenidos de esta etapa fueron los siguientes:

- Información para un mayor control sobre los datos sensibles.
- Listado de recursos con alto riesgo de acceso no autorizado.
- Cumplimiento con normas de administración de bienes y servicios sobre los recursos tecnológicos que maneja la institución.
- Información para establecer recomendaciones sobre las regulaciones de privacidad y protección de datos.
- Conciencia de los empleados sobre la importancia de la seguridad de la información.

En una etapa 2, se elaboró el **catálogo del inventario tecnológico,** integrado la descripción detallada de todos los dispositivos tecnológicos utilizados por la organización, incluyendo computadoras, servidores, periféricos, equipos de red, dispositivos móviles y cualquier otro equipo electrónico de trabajo. Se aplica a todas las áreas y departamentos, considerando tanto los equipos en uso como los almacenados o en reparación.

La etapa 3, **análisis de riesgo,** permitió identificar, evaluar y priorizar los riesgos asociados a activos tecnológicos; aspectos relevantes para la etapa 4, denominada **establecimiento de controles,** permitió establecer controles de seguridad, manuales y guías fundamentales para estandarizar procedimientos, mitigar riesgos y garantizar el uso adecuado de los recursos TI, protegiendo la integridad y continuidad de los activos tecnológicos. Siendo estos:

a. **Manual de gestión de inventario de hardware**, elaborado con el propósito de mantener un registro preciso y actualizado de todos los dispositivos tecnológicos de la organización. Esto facilita la gestión de los activos, la toma de decisiones estratégicas y asegura que los equipos se utilicen de manera adecuada, además de cumplir con normativas legales y auditorías. Contempla la periodicidad de actualización del inventario, las tareas de protección física de los equipos, el proceso de baja de equipos, la entrada de nuevos equipos, el registro en el sistema de inventario, la asignación de equipos, el mantenimiento y actualización y la baja de equipos o activos tecnológicos.

b. **Guía de gestión de software y licencias**, orientada a garantizar un control eficiente y transparente de todo el software instalado y las licencias asociadas. Asegura el cumplimiento legal, optimiza los costos de adquisición y renovación de licencias, y promueve el uso ade-

cuado de los recursos tecnológicos.

c. **Protocolo de Seguridad de Recursos IT**, con el propósito de establecer las medidas de seguridad necesarias para proteger los recursos tecnológicos inventariados, garantizando que la información, hardware y software estén seguros frente a robos, pérdidas y ataques cibernéticos, de esta manera, este protocolo asegura que todos los recursos se gestionen de manera segura, minimizando riesgos y vulnerabilidades.

d. **Manual de Mantenimiento de Equipos**: integra procedimientos de mantenimiento preventivo y correctivo para el hardware, asegurando su correcto funcionamiento y maximizando su vida útil, además de garantizar su disponibilidad para su uso. La vinculación con el inventario permite un seguimiento efectivo del historial de mantenimiento de cada equipo.

e. **Guía de Asignación y Uso de Recursos Tecnológicos**, cuya finalidad es establecer un marco claro para la asignación y el uso de los recursos tecnológicos al personal de la organización. define responsabilidades y normas de uso, con el fin de asegurar un manejo eficiente de los recursos, optimizar su utilización y prevenir el uso indebido.

f. **Guía de respaldo y recuperación de datos,** orientado a establecer procedimientos claros y efectivos para realizar copias de seguridad (backups) y asegurar la recuperación de datos en caso de desastre o pérdida de información. Esta guía garantiza la protección de los datos críticos de la organización y asegura la continuidad de las operaciones en situaciones adversas.

g. **Protocolo de reciclaje y disposición de equipos,** destinado a establecer los procedimientos para la disposición segura, controlada y ambientalmente responsable de los equipos tecnológicos obsoletos, incluyendo computadoras, servidores, periféricos y dispositivos electrónicos. También busca garantizar la correcta baja en el inventario de los equipos retirados y documentar su destino final.

Todos los resultados de etapas anteriores, se registran en forma digital dentro de un modelo de sistema de información destinado a la **visualización de la información en tiempo real**, contribuyendo a:

- **La protección de activos:** Salvaguardando los recursos tecnológicos críticos para el funcionamiento dentro de una institución.
- **Apoyando al cumplimiento normativo**: Que asegura el cumplimiento de normativas y estándares de seguridad de la información.
- **La optimización de recursos:** Mejora la gestión y asignación de recursos tecnológicos, reduciendo costos y desperdicios.
- **Prevención de Incidentes:** Minimiza el riesgo de incidentes de seguridad mediante la identificación proactiva de amenazas.

Este prototipo permite reducir los riesgos, vulnerabilidades y amenazas en la inversión tecnológica; permite mejorar la eficiencia de la gestión de activos, con tiempos de respuesta rápidos ante los incidentes, mostrando transparencia y control en la gestión de recursos TI. Esto permite crear una cultura de mejora continua basado en el análisis de datos y la retroalimentación.

De todo este análisis, se puede concluir que el modelo propuesto contribuye con un enfoque integral a la clasificación, valoración y control de inventarios TI, basado en estándares como COBIT, ofreciendo herramientas prácticas para mitigar riesgos en contextos institucionales, con aportes en la generación de políticas y procedimientos para una gestión segura y eficiente en la gestión de recursos TI.

5. Conclusiones y recomendaciones

La investigación concluye que la ausencia de un inventario detallado expone a instituciones empresarias a riesgos significativos, pero el modelo propuesto, validado mediante encuestas, ofrece una solución efectiva para mejorar el control y seguridad de activos TI, contribuyendo a la línea de investigación esencial de la seguridad de activos tecnológicos y al análisis de riesgo.

Todo cambio o transformación parte de la importancia de hacer un diagnóstico de la situación actual, en su contenido resalta el alto nivel de insatisfacción entre los usuarios respecto a la infraestructura tecnológica, los servicios de gestión tecnológica, el rendimiento del hardware, las deficiencias en equipamiento tecnológico y la calidad del servicio técnico impactan negativamente en la satisfacción y productividad de los usuarios.

A partir de la situación real, se hace necesario aplicar técnicas de análisis de riesgo para identificar los factores de control y seguridad de activos tecnológicos, que permitan establecer estándares de control integrados en un catálogo de inventarios TI que mejore la gestión de recursos tecnológicos,

El seguimiento y supervisión de los activos tecnológicos requiere de un análisis de riesgos continuo, que permita contar con una comprensión clara de las amenazas potenciales y su impacto.

Estas conclusiones reflejan un enfoque integral para mejorar la seguridad y gestión de inventarios de recursos TI, asegurando la protección y eficiencia operativa de la institución.

Ante esta necesidad, es recomendable implementar sistemas de control de activos tecnológicos apoyados con una capacitación continua, con la actualización de inventarios periódicamente y con adoptar estándares internacionales para mitigar riesgos, además de difundir resultados para que otras instituciones fortalezcan sus sistemas de control, promoviendo un uso responsable de recursos tecnológicos.

6. Referencias

- AGPD: Agencia Española de protección de datos. (2018). *Guía práctica para las evaluaciones de impacto en la protección de datos.* Madrid: AGPD: Agencia Española de protección de datos.
- CEPAL: Comisión Económica para América Latina y el Caribe. (15 de 08 de 2021). *Biblioteca de la CEPAL* . Obtenido de Gestión de datos de investigación: Sobre la protección de los datos: https://biblioguias.cepal.org/c.php?g=495473&p=4398118
- FulfillMent. (4 de mayo de 2023). *La importancia de mantener un inventario preciso y actualizado en el almacén.* Obtenido de Fulfill Ment Hub Usa: https://fulfillmenthubusa.com/la-importancia-de-mantener-un-inventario-preciso-y-actualizado-en-el-almacen/
- Holded. (28 de octubre de 2018). *La importancia de tener un inventario actualizado*. Obtenido de Holded: https://www.holded.com/es/blog/la-importancia-de-tener-un-inventario-actualizado
- Kissel, R. (2012). *Glossary of Key Information Security Terms, National Institute of Standards and Technology.* Chicago: National Institute of Standards and Technology.
- Ramirez, I. (2015). *Apuntes de metodología de la investigación: Un enfoque crítico.* Sucre: Rayo del sur.
- Sommerville, I. (2005). *Ingeniería de Software* . México: Pearson Educación.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security, 7th Edition.* New York: Cengage.