UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA INDUSTRIAL

Implementación de plan preventivo para disminuir riesgos tecnológicos en el área de tecnología e información en la empresa PROANCO, Sullana

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero Industrial

AUTORES:

Granda Perez, Víctor Joao (orcid.org/0009-0008-6677-0303)

Mora Gomez, Adrian Paul (orcid.org/0000-0001-6961-2601)

ASESORA:

Mg. Guerrero Carrasco, Mercedes Soledad (orcid.org/0000-0002-5622-8536)

LÍNEA DE INVESTIGACIÓN:

Sistema de Gestión de la Seguridad y Calidad

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

PIURA – PERÚ

2023

Dedicatoria

El presente proyecto de tesis realizada por Granda Pérez Víctor Joao y Mora Gómez Adrián Paul, hacemos esta dedicación de nuestra investigación principalmente a Dios, quien nos da vida, salud y fortaleza para poder seguir con nuestro futuro, y con responsabilidad para llegar a la meta.

De igual manera a nuestros padres, porque son el un gran soporte, dando consejos y ser una motivación constante e incentivar a que todo esfuerzo tiene su recompensa y así seguir adelante cada día. Y, por último, le dedico a los docentes de mi Escuela profesional que, por su enseñanza, su tiempo, paciencia y apoyo, así como la sabiduría que me transmitieron al momento de desarrollar sus asignaturas suman a mis saberes.

Agradecimiento

Hacemos un expresivo agradecimiento a nuestros padres por otorgarnos los estudios universitarios donde atribuimos los conocimientos necesarios para lograr desempeñarnos en un ambiente laboral.

Además, agradecemos a nuestra asesora Mg. Mercedes Carrasco Guerrero quien culminó su labor de manera satisfactoria al ofrecer su capacidad para guiarnos en las asesorías y así nuestro artículo de investigación sea eficaz y concreto.

Por último, a la Universidad César Vallejo por brindar páginas de alcances científicas para nuestro artículo de investigación.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA INDUSTRIAL

Declaratoria de Autenticidad del Asesor

Yo, GUERRERO CARRASCO MERCEDES SOLEDAD, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA INDUSTRIALde la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, asesor de Tesis titulada: "Implementación de plan preventivo para disminuir riesgos tecnológicos en el área de tecnología e información en la empresa PROANCO, Sullana", cuyos autores son MORA GOMEZ ADRIAN PAUL, GRANDA PEREZ VICTOR JOAO, constato que la investigación tiene un índice de similitud de 12%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por locual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

PIURA, 09 de Diciembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
GUERRERO CARRASCO MERCEDES SOLEDAD **DNI:** 02854299 **ORCID:** 0000-0002-5622-8536	Firmado electrónicamente por: MSGUERREROC el 09-12-2023 09:15:46

Código documento Trilce: TRI - 0689388

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA INDUSTRIAL

Declaratoria de Originalidad de los Autores

Nosotros, MORA GOMEZ ADRIAN PAUL, GRANDA PEREZ VICTOR JOAO estudiantes de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA INDUSTRIAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Implementación de plan preventivo para disminuir riesgos tecnológicos en el área de tecnología e información en la empresa PROANCO, Sullana", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. Hemos mencionado todas las fuentes empleadas, identificando correctamente todacita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro gradoacadémico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, nicopiados.

En tal sentido asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual nos sometemos a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
ADRIAN PAUL MORA GOMEZ **DNI:** 74690595 **ORCID:** 0000-0001-6961-2601	Firmado electrónicamente por: AMORAGOM el 09-12-2023 23:16:29
VICTOR JOAO GRANDA PEREZ **DNI:** 73087019 **ORCID:** 0009-0008-6677-0303	Firmado electrónicamente por: VGRANDA el 09-12-2023 07:18:56

Código documento Trilce: TRI - 0689390

INVESTIGA UCV

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La investigación se desarrolló con la finalidad de implementar un plan preventivo para disminuir riesgos tecnológicos en el área de Tecnología de la Información en la empresa PROANCO, Sullana 2023.

La investigación se desarrolló mediante un tipo de estudio cuantitativa, aplicada y nivel explicativo, y con un diseño pre experimental. La población y muestra estuvo constituida por 06 trabajadores que manejan computadoras de escritorio del área de tecnología e información en la empresa PROANCO. Para la recopilación de datos se utilizó como técnicas a dos entrevistas y un análisis documental y como instrumentos una matriz de identificación y evaluación de riesgos tecnológicos, guía de identificación de causas y ficha de análisis documental para las variables de estudio.

Según los resultados adquiridos, en el diagnóstico de los riesgos tecnológicos del área de Tecnología de la Información arroja que el 32% se encuentra en nivel alto, distribuyéndose en los riesgos con respecto a equipo, programas y personas con el 8%, 8% y 16%. Se diseñó de un plan de prevención para disminuir los riesgos tecnológicos. En conclusión, con la aplicación del plan preventivo se disminuyó los riesgos tecnológicos de nivel alto en 28%.

Palabras clave: plan preventivo, riesgos tecnológicos respecto a equipos, programas, personas.

Abstract

The research was developed with the purpose of implementing a preventive plan to reduce technological risks in the area of Information Technology in the company PROANCO, Sullana 2023.

The research was developed through a quantitative, applied and explanatory type of study, and with a pre-experimental design. The population and sample consisted of 06 workers who manage desktop computers in the technology and information area at the PROANCO company. For data collection, two interviews and a documentary analysis were used as techniques, and a technological risk identification and evaluation matrix, cause identification guide, and documentary analysis sheet for the study variables were used as instruments.

According to the results acquired, the diagnosis of technological risks in the Information Technology area shows that 32% are at a high level, distributed among the risks with respect to equipment, programs and people with 8%, 8% and 16%. A prevention plan was designed to reduce technological risks. In conclusion, with the application of the preventive plan, high-level technological risks were reduced by 28%.

Keywords: preventive plan, technological risks regarding equipment, programs, people.

I. INTRODUCCIÓN

En el ámbito mundial, en los últimos años el empleo de las tecnologías de la información (TI) es uno de los factores esenciales en el manejo exitoso de la Gestión empresarial; pero está sujeta a ciertos riesgos tecnológicos relacionados con el uso de TI, que pueden darse por malas manipulaciones de los empleados o por acciones intencionales de algún intruso para tener acceso en forma ilegal a información reservada (Bejarano y Merseguer, 2021), (Didraga, et al., 2019).

En el campo empresarial, gestionar los riesgos tecnológicos va más allá de dar protección a datos almacenados en algún dispositivo, red o algún medio en línea, sino que está obligada a emprender acciones de identificación, evaluación y clasificación de amanezcas previa priorización (Öbrand, et al., 2018), así como planificación de medidas para eliminar, disminuir o mitigar los peligros relacionados con uso de Ti dentro de las organizaciones (Barriga, 2019).

Todo el personal que integran el área de TI cumplen un rol esencial, pues dentro de esta área lo que se busca es estudiar, analizar, diseñar, elaborar, administrar e implementar sistemas informáticos internos que permitan resguardar la base de datos e información de la empresa (Brunner, 2020), asimismo se brinda el soporte técnico de los usuarios y del mantenimiento de los servicios electrónicos como computadoras, laptops, la red, los software, y la implementación de las nuevas tecnologías para alcanzar una mejora.(Pashchenko, 2023).

Las organizaciones que disponen de TI cuentan con un componente esencial para desarrollar las diversas acciones, pues facilita la operación de sus procesos, en tal sentido resulta fundamental su integración con los documentos de gestión de la organización (Smite et al. 2022), el análisis y gestión de riesgos de fallas es un reto al que cualquier enfrenta actualmente (Colina y Túa, 2020).

En el ámbito peruano, solo el 75% de las empresas que están operando formalmente cuentan con un plan de mantenimiento preventivo en sus diversas instalaciones y equipos (Andina, 2021). El país no está exento de sufrir riesgos de TI que produzcan ataques directos a la protección de los datos de las entidades, así como sobre equipos y sistemas que no disponen de protección (Barriga, 2019; Pazmiño, Serrano y Gonzáles, 2020).

En la empresa “Productora Andina de Congelados S.R.L” se adolece de un plan preventivo de riesgos, pues el área de Tecnología e Información (TI) está expuesta a riesgos que pueden surtir la base de datos, el sistema, los softwares o la propia red. Se adolece de una permanente identificación y análisis de riesgos de las actividades que se realiza, actuando con prontitud solo cuando ocurren fallas que impiden la recepción, almacenamiento y distribución de información. Asimismo, no hay un manejo eficiente de las credenciales de acceso a las maquinas que contienen información importante para a empresa. Asimismo, las normas de seguridad informática están desactualizados, no están acordó al desarrollo de la empresa y a las nuevas necesidades de protección de os equipos e información.

En ese contexto, fue necesario implementar un plan preventivo que busco disminuir esos riesgos en el área de TI, considerando como componentes los equipos, los programas y el personal que ejecuta las tareas. De tal forma se buscó generar en el empleador una visión más integral, generando más interés por brindar el soporte no solo a la maquinaria sino también brindarles la seguridad a sus trabajadores, es por ello que se consideró necesario que uno de los fines de dicho plan sea contar con medidas preventivas que permita disminuir los posibles riesgos y en caso de ocurrencia como accionar frente a ellos.

Teniendo en cuenta la realidad problemática se estableció como problema de investigación: ¿En qué medida la implementación de un plan preventivo disminuirá los riesgos tecnológicos en el área de tecnología e información en la empresa PROANCO, Sullana 2023? Las específicas: ¿Cuál el diagnóstico del estado actual de los riesgos tecnológicos del área de TI? ¿Cómo diseñar un plan preventivo para disminuir riesgos tecnológicos en el área de TI? ¿Cuál es la disminución de los riesgos tecnológicos en el área de TI?

En lo que respecta a la justificación de la investigación realizada se tuvo lo siguiente: como justificación teórica se emplearon teorías y conceptos que nos permitieron entender y conocer la realidad problemática que se viene suscitando en el área de Tecnología de la Información de la empresa en cuestión, a fin de demostrar el problema y con ello se implementó un plan preventivo que permitió disminuir los riesgos tecnológicos. Se tiene como justificación práctica, que la investigación sirvió para demostrar la importancia que trae consigo la

implementación de un plan preventivo a fin de lograr disminuir riesgos tecnológicos en el área de Tecnología de la Información, asimismo permitió brindarle mayor seguridad al personal que labora en dicha área En lo que respecta a la justificación metodológica fue necesario aplicar técnicas y herramientas que permitieron obtener datos que fueron debidamente recolectados y evaluados por medio de instrumentos elaborados para tal fin como es la entrevista, y análisis documental, lo cual fue procesado para conocer el diagnostico respectivo que sirvió de dalla para elaborar un plan preventivo orientado a disminuir los riesgos tecnológicos; que luego de su aplicación se determinó una variación de disminución en el área de aplicación.

Se tuvo como objetivo general: Implementar un plan preventivo para disminuir riesgos tecnológicos en el área de Tecnología de la Información en la empresa PROANCO, Sullana 2023; y como objetivos específicos tenemos: Diagnosticar el estado imperante de los riesgos tecnológicos del área de Tecnología de la Información de la empresa PROANCO; Diseñar el plan preventivo para disminuir riesgos tecnológicos en el área de Tecnología de la Información en la empresa PROANCO y Determinar la disminución de los riesgos tecnológicos en el área de Tecnología de la Información de la empresa PROANCO.

La hipótesis de la investigación fue: La implementación de un plan preventivo disminuye significativamente los riesgos tecnológicos en el área de tecnología e información en la empresa PROANCO, Sullana 2023.

II. MARCO TEÓRICO

Para el desarrollo de la investigación se consignaron antecedentes a nivel internacional y nacional, así como también teorías que permitieron analizar el tema con mayor amplitud.

A nivel internacional, Morales (2019) en su investigación realizada en Ecuador para diseñar un programa de mantenimiento preventivo para la maquinaria de una empresa. Concluyó que, el plan de mantenimiento preventivo es de gran importancia para la disminución de fallas en máquinas existentes. El aporte que proporciona el autor es que resulta necesario que cada empresa cuente con un plan preventivo ya sea para disminuir riesgos o para evitar los fallos en la maquinaria, lo que conlleva también a capacitar a los trabajadores del área con el propósito de que conozcan las normas y procedimientos para mantener la integridad de la información y la operatividad de las máquinas en general.

Patiño y Bedoya (2023), realizada en Colombia para la implementación de un plan para identificar riesgos y vulnerabilidad en la seguridad de la información de la data del personal de una organización. Concluyo que a evaluación de las probabilidades de ocurrencia y los impactos potenciales en la empresa permitió establecer una priorización de los riesgos y orientar las atenciones a los más relevantes, a partir de lo cual se elaboró un plan que abarca el tener identificado las amenazas, la valoración de riesgos y las acciones pertinentes para proteger la información de la data. El estudio aporta que es necesario para la elaboración eficaz de un plan preventivo de riesgos es actuar sobre las causas, para lo cual hay que identificarlas, valorarlas y evaluarlas.

Priyatna, et al. (2021), en su estudio realizado en Indonesia para orientar la mejora de recolección datos de los resultados preventivos haciendo uso de Microsoft Excel, para lo cual se creó una aplicación de mantenimiento preventivo enfocado en la web. Concluyó que el sistema mejoró la recolección de la data de máquinas y herramientas, la base de datos respecto a los resultados y la práctica del mantenimiento preventivo, por lo cual está disponible con eficacia y eficiencia. En consecuencia, un sistema que recopile y brinde información sobre el mantenimiento preventivo es de gran utilidad para la toma de decisiones en base a información

real y disponible. El estudio aporta que la utilización de aplicaciones web contribuya al manteamiento preventivo de los componentes de la Tecnología de la Información (TI).

Llanos y Campoverde (2021), en su investigación realizada en Ecuador para analizar riesgos en el área de las TI de una entidad registradora de propiedades. Concluye que se identificó una alta criticidad de riesgos para lo cual se definió controles y recomendaciones de auditoría con el propósito de disminuir el impacto en los procesos de la organización; ojeteo que se logró disminuyendo los riesgos en un 66%. El estudio aporta que cuando existe un alto nivel de riesgos relacionados con las TI al implementar controles se mejora la eficiencia y efectividad de los procesos de la organización en los que interviene datos, pero debe ser un proceso continuo con el propósito de evitar dificultades para contar con una información integra, confidencial y disponible.

Gómez (2022), en su estudio realizado en Cuba orientada a gestionar y prevenir riesgos con uso de las TI en una organización. Encontró como resultados tres variables principales a tener en cuenta, el contexto (C), la evaluación (E) y el monitoreo (M), a partir de lo cual fue diseñado y aplicado a un procedimiento para la gestión de riesgos de TI en la organización a través de la web, realizando la identificación, clasificación y valoración hasta reducirlos totalmente en forma progresiva y sostenida en el tiempo. La investigación aporta que el uso de las TI facilita el análisis para la toma de decisiones en beneficio de la disponibilidad eficaz de la información.

A nivel nacional, Aquino y Atalaya (2020) en su estudio realizado para diseñar un plan preventivo para la mejora de la disponibilidad de equipos en la organización. Concluyó que, al implementar el plan preventivo diseñado acorde a la necesidad, ha generado que el 90% de las maquinarias mejoren su disponibilidad. El aporte del estudio es que, el contar con dicho instrumento es fundamental debido a que tiene el propósito de reducir los riesgos que surgen en los diferentes equipos tecnológicos, incluyendo la integridad del personal de dicha área.

Montoya (2020), en su tesis para la mitigación de riesgos ante amenazas que afectan a la información, áreas y procesos de la empresa. Concluyó que dentro de

una organización es necesario y fundamental identificar, clasificar y establecer el nivel de los riesgos que tiene la información y los procesos internos; dicha data debe estar a disposición de los directivos de la empresa para la toma de decisiones y la aplicación de diversas estrategias de seguridad, así como implementar controles pertinentes. El estudio aporta que la mitigación de riesgos es fundamental para neutralizar las amenazas a lo que esta expuestos la información de la organización y el área de TI.

Torres (2023), en su estudio analizó los riesgos y desafíos que enfrenta el personal por el uso de la inteligencia artificial en el centro de labores. Concluyo que, usando la inteligencia artificial en el centro de labores se crean tantos riesgos como desafíos para el personal. Los riesgos incluyen las pérdidas de puestos de trabajo por automatización, no se producen datos personales; así como los desafíos es adaptarse y capacitarse en forma constante para poder desenvolverse con tecnología moderna, de la misma forma garantizar que lo que decida la inteligencia artificial sea justa y ética. El estudio aporta que el avance tecnológico implica asumir riesgos, pero tiene que asumir el reto de enfrentarlos y disminuirlos.

Flores (2023) en su estado relaciono la Ciberseguridad y la Gestión de Riesgos de TI. Concluyo que ambas variables están relacionadas de manera directa ($P < 0.05$; Rho= :0.833), lo que indica que hay una relación de dependencia. Además, se determinó que es casi nula la gestión de Riesgos de TI, pues el 23.3% de trabajadores manifiesta que casi nunca lo realizan, constituyéndose en un punto débil de la organización. El autor aporta que la gestión de riesgos tecnológicos puede convertirse en una debilidad o fortaleza, dependido del grado de interés y esfuerzo que ponga por desarrollarla.

Pizarro (2022), en su estudio para establecer un modelo de gestión de riesgos en la seguridad de la información de una entidad. Concluyó que el modelo para gestionar riesgos incide en un 47.70% en la seguridad de información de la entidad. El estudio aporta que es importante la implementación de modelos de gestión de riesgos teniendo en cuenta que mejoran la seguridad de los datos internos de la organización; sin embargo, es necesario aplicar otras acciones simultáneas como un plan preventivo que asegure la disponibilidad y confiabilidad de la información.

En cuanto a la conceptualización de riesgos tecnológicos se tiene a Lee (2018), quien lo entiende como la pérdida potencial por algún daño, interrupción, alteración o falla que derivan de la utilización del hardware, software, sistema, aplicación, red y los diversos canales de distribución de Información que la organización dispone para operar.

Por su parte Bernaldo (2018) los considera como aquellos que se generan con el incremento de herramientas y aplicaciones tecnológicas que no disponen de gestiones adecuada respecto a la seguridad, encontrándose desprotegidas por los constantes cambios.

Contreras y Medina (2019) lo conciben como la probabilidad que objetos, equipos, materiales, procesos, sustancias o fenómeno interaccionen y lleguen a ocasionar una cantidad determinada de consecuencias principalmente en la salud, económica y medio ambiente.

Por último, Klus (2021) lo considera como la contingencia de que las interrupciones, alteraciones, o fallas de una infraestructura, sistema de información, bases de datos y procesos de TI, provoquen pérdidas económicas en la organización.

Para la evaluación de la variable riesgos tecnológicos se ha considerado las dimensiones tomadas por Tiznado (2019) quien distingue cuatro aspectos a evaluación, respecto al equipo, respecto a los programas, respecto a las personas y los relacionados con el trabajo. Sin embrago, para efectos de la investigación se ha considerado las tres primeras por ser las que más se ajustan al contexto de estudio:

El primero, hace referencia a los riesgos en equipos en los que destaca, origen desconocido de equipos, durante, inexistencia de respaldo a equipo, desastre natural, etc. (Tiznado, 2019).

El segundo, hace referencia a los riesgos en los que destaca: fraudes o desfalcos a través de la afectación de los activos e información de la organización, susurración o copias de programa, nula posibilidad de recuperar y reiniciar un proceso o la comunicación de una data importante, realización de modificaciones sin autorización, datos no validados, etc. (Tiznado, 2019).

El tercero, hace referencia a los riesgos que se entrelazan con la protección para el combate de otros riesgos, también incluye la concientización en la formación y carteles de seguridad, así como practicar valores para actuar en forma segura y no en forma irresponsable. El personal tiene responsabilidad de cumplir las normas de seguridad (Tiznado, 2019).

En cuanto, a la teoría en que se fundamenta la variable se sustenta en la teoría de gestión de riesgos de TI, la cual está enfocada en el monitoreo y administración de elementos relacionados con las TI en una entidad, principalmente hardware, software y redes (IBM, 2020). Es decir, la preocupación se centra en cómo lograr que los sistemas de información y sus componentes alcancen un funcionamiento eficiente y contribuye a que los trabajadores realicen sus actividades en forma eficiente (Masso, 2020).

En cuanto a la conceptualización de la variable implementación de un plan preventivo, se tiene a Murillo (2017) considera que son acciones que se ponen en práctica una vez planificadas destinadas a conservar los equipos haciendo revisiones y mantenimientos para mantenerles operativos.

Blanco, Molina y Sánchez (2018) manifiestan que son acciones implementadas que disminuyen en gran porcentaje la frecuencia de mantenimientos correctivos en las organizaciones, lo cual, a la vez, disminuye los costos, toda vez que las acciones de prevención cuestan menos que las correctivas.

Asimismo, Arango, Rosero y Montoya (2020) lo conciben como un grupo de acciones puestas en práctica que se programan mediante un cronograma, estableciendo las actividades que permiten realizar el mantenimiento a efectuarse a cada equipo, máquina o instrumento; asimismo, se considera los recursos requeridos, lo cual conlleva a reducir costos e incrementar la operatividad en la organización.

Robayo (2020) considera que tiene por propósito la conservación de equipos en un estado adecuado; para ello, prioritariamente se planifican y programan, tareas a efectuarse a los equipos por individual con la previsión del tiempo antes que presenten fallas.

Y, por último, para Pérez (2021) es la implementación de acción la cual contiene que, define fechas, hora, duración y ubicación referencial de las acciones que cautelan los equipos, información y la seguridad del personal previamente identificadas.

Para la evaluación de la variable implementación de un plan preventivo se ha considerado los aspectos tomados por López, et al. (2022), quien plateo tres componentes a tomar en cuenta: Diagnostico, planeación e inversión.

La primera, hace referencia a lo que debe tenerse como principio: las actividades que se deseen mejorar, primero hay que comenzar por conocer cuál es su estado en la actualidad; estableciéndose para ello, el mecanismo adecuado para hacer mediciones, lo cual se conoce como diagnóstico. Es un conjunto de actividades consecutivas que permiten analizar el estado actual de equipos, redes, sistemas, etc. (Marrero, Vilalta y Martínez, 2019).

La segunda, hace referencia al conjunto de tareas con su programación respectiva para ejecutarse en una organización, permitiendo el aseguramiento de disponibilidad de los recursos tecnológicos establecidos (Arroyo y Obando, 2022). También se planifica con qué frecuencia se realizará, que duración tendrá, que materiales insumos se utilizará. Es un conjunto de actividades que se deben ejecutar con el propósito de realizar el mantenimiento que permita la operatividad, evitando paralizaciones (Arroyo y Obando, 2022).

El tercero, se refiere a las actividades de mantenimiento que son costos fijos que no están en función de la producción, requiere personal, materiales e insumos, que constituye una inversión porque asegura la operatividad, tenemos que si se disminuye el presupuesto se disminuye también las acciones preventivas, lo cual conlleva a incrementar las paralizaciones por fallas (Orehek y Petrič, 2021). Por lo que el supuesto ahorro, genera incertidumbre sobre el estado de las instalaciones y de la capacidad de producción de la organización (Cruz, et al. 2020).

El riesgo tecnológico puede verse desde tres aspectos, primero a nivel de la infraestructura tecnológica (hardware o nivel físico), en segundo lugar, a nivel lógico (riesgos asociados a software, sistemas de información e información) y por último

los riesgos derivados del mal uso de los anteriores factores, que corresponde al factor humano como un tercer nivel (Rao, et al., 2021).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

Investigación de enfoque cuantitativa, considerando que se buscó obtener datos cuantitativos al aplicar matrices de identificación y evaluación de riesgos tecnológicos antes y después de implementación del plan de prevención, cuya data fue registrada cuantificada y analizada para determinar y comprobar la disminución de los riesgos (Ansari, et al. 2022).

Aplicada, porque buscó contribuir a la solución de la problemática identificada con la Implementación de un plan preventivo para disminuir riesgos tecnológicos (Leavy, 2022). Es consecuencia, no solo se brindó información del estado actual, sino que aporto a la solución de la problemática mediante la implementación de un plan.

Nivel explicativo, porque busco explicar de forma clara sobre la disminución de riesgos que ejerció el plan preventivo en el área de tecnología, respondiendo a las deficiencias identificadas en el diagnóstico que se realizó (Arias y Covinos, 2020).

Diseño de investigación

El diseño es experimental, porque se manipulo la variable dependiente, considerando que los ejecutores del estudio realizaron una implementación de un plan preventivo sin sujetos de control con el propósito de disminuir los riesgos tecnológicos, y, por consiguiente, se modificó el estado inicial de la variable dependiente (Mulisa, 2022). Sin embargo, se considera pre experimental porque los investigadores no tuvieron el medio control suficiente (Cohen, et al., 2018). La representación del diseño es el siguiente:

$$G: O_1 - X - O_2$$

Dónde:

G: Muestra de equipos de área de tecnología.

O1: Diagnóstico de riesgos tecnológicos.

X: Plan preventivo.

O2: Evaluación de la disminución de riesgos.

3.2. Variables y operacionalización

Variable dependiente: Riesgos tecnológicos

Definición conceptual:

La contingencia de que las interrupciones, alteraciones, o fallas de una infraestructura, sistema de información, bases de datos y procesos de TI, provoquen pérdidas económicas en la organización. (Klus, 2021).

Definición operacional:

Se evaluó equipos, programas y personas del área de tecnología mediante una ficha de análisis y evaluación de riesgos tecnológicos.

Indicadores:

Dimensión 1 respecto a los equipos equipo: riesgos en equipos en los que destaca, origen desconocido de equipos, durante, inexistencia de respaldo a equipo, desastre natural, etc. (Tiznado, 2019). Cuenta con tres indicadores, Resguardo de información, Protección de seguridad y Desastre natural.

Dimensión 2 respecto a los programas: riesgos en los que destaca los fraudes o desfalcos a través de la afectación de los activos e información de la organización, susurración o copias de programa, nula posibilidad de recuperar y reiniciar un proceso o la comunicación de una data importante, realización de modificaciones sin autorización, datos no validados, etc. (Tiznado, 2019). Cuenta con tres indicadores, Fuentes desconocidas, Afectación viral a la información y Restricciones de acceso.

Dimensión 3 respecto a las personas: riesgos que se entrelazan con la protección para el combate de otros riesgos; los trabajadores independientemente de su rango deben conocer y cumplir las reglas de seguridad, así como practicar valores para actuar en forma segura y no en forma irresponsable. El personal tiene

responsabilidad de cumplir las normas de seguridad (Tiznado, 2019). Cuenta con tres indicadores, Normas de seguridad, Medidas preventivas y Practica de valores.

Escala de medición:

Respecto al impacto del riesgo tecnológico: Alto, Medio y Bajo.

Variable independiente: Plan preventivo

Definición conceptual:

Implementación de acción que define fechas, hora, duración y ubicación referencial de las acciones que cautelan los equipos, información y la seguridad del personal previamente identificadas (Pérez, 2021).

Definición operacional:

Se realizó el diagnóstico, planearon e inversión del plan preventivo mediante diagramas, fichas técnicas y guías de entrevista

Indicadores:

Dimensión 1 Diagnostico: conjunto de actividades consecutivas que permiten analizar el estado actual de equipos, redes, sistemas, etc. (Marrero, Vilalta y Martínez, 2019). Cuenta con dos indicadores, Historial de fallas y Numero de causas.

Dimensión 2 planeación: conjunto de tareas de mantenimiento con su programación respectiva para ejecutarse en una organización, permitiendo el aseguramiento de disponibilidad de los recursos tecnológicos establecidos (Arroyo y Obando, 2022). Cuenta con dos indicadores, Tareas a realizar y Programación de tareas.

Dimensión 3 inversión: actividades de mantenimiento que son costos fijos que no están en función de la producción, requiere personal, materiales e insumos, que constituye una inversión porque asegura la operatividad (Cruz, et al. 2020). Cuenta con un indicador, Costo- beneficio.

Escala de medición:

Se tomó en cuenta el nivel de reducción de riesgos tecnológicos: Bueno, Regular, Malo.

3.3. Población, muestra, muestreo y unidad de análisis

Población

Estuvo compuesta por 06 trabajadores del área de tecnología e información en la empresa PROANCO, Sullana.

Criterios de inclusión:

Trabajadores con al menos 01 de servicio.

Trabajadores presupuestos a colaborar.

Criterios de exclusión:

Trabajadores con menos de 01 de servicio.

Trabajadores no presupuestos a colaborar

Muestra

Se tomó a la totalidad de la población, es decir, 06 trabajadores del área de tecnología e información en la empresa PROANCO, Sullana.

Muestreo

La técnica que se utilizo fue el muestreo no probabilístico en consecuencia ningún elemento fue elegido al azar.

Unidad de análisis

Trabajadores que manejan las computadoras del área de tecnología e información en la empresa PROANCO, Sullana.

3.4. Técnicas e instrumentos de recolección de datos

Para la realización del presente estudio se tomó en cuenta las técnicas e instrumentos acorde con las variables que se analizaron con sus respetivas fuentes de información.

Tabla 1. *Técnicas e instrumentos de obtención de información*

VARIABLE	TÉCNICA	INSTRUMENTOS	FUENTE
Riesgos tecnológicos	Entrevista	• Matriz de identificación y evaluación de riesgos tecnológicos	Trabajadores del área y técnico de mantenimiento.
	Entrevista	• Guía de identificación de causas	Trabajadores del área y técnico de mantenimiento.
Plan Preventivo	Análisis documental	• Ficha de análisis documental	Documentos relacionados con el mantenimiento de equipos.

Fuente: elaboración propia

3.5. Procedimientos

Para la realización del estudio se aplicó mediante una entrevista para la identificación y evaluación de riesgos tecnológicos con el propósito de determinar su nivel (Ver Anexo 2, instrumento 1). Identificados los riesgos tecnológicos en sus niveles Alto, Medio y Bajo se aplicó una entrevista para identificar y evaluar las causas de los riegos tecnológicos, especialmente los de nivel Altos (ver Anexo 2, instrumento 2), Identificadas las causas se elaboró el diagrama de causa – efecto y el diagrama de Pareto con el cual se determinó las causas principales de los riesgos tecnológicos. Asimismo, realizó un análisis documental (Ver anexo 2, instrumento 3). Asimismo, se elaboró el plan preventivo en función de las causas principales identificadas con el propósito de disminuir los riesgos tecnológicos (Ver anexo 3), el mismo que posteriormente fue aplicado para determinar el porcentaje de disminución de riesgos tecnológicos.

3.6. Método de análisis de datos

La ejecución de la investigación se realizó utilizando un enfoque cuantitativo, a partir de la identificación y valoración de los riesgos tecnológicos del área de

tecnología e información en la empresa PROANCO, Sullana para lo cual se elaboró una base de datos utilizando el programa Excel y el programa SPSS v 25, en el cual se registró los resultados del diagnóstico de los riesgos tecnológicas identificados y evaluados en su respectivo nivel Alto, Medio y Bajo. Después de aplicar el plan preventivo se evaluó por segunda vez los riesgos tecnológicos para determinar la disolución, especialmente en el nivel alto (% después de aplicar - %antes de aplicar)

3.7. Aspectos éticos

Se obtuvo la información de la empresa PROANCO, Sullana., respetando la confiabilidad y confidenciales de la data, toda vez que fueron usados únicamente para la realización del estudio y mejorar la disponibilidad operativa de las máquinas del área de tecnología. Además, se respetó la autonomía de los trabajadores del área de participar en el estudio. Asimismo, toda la información y plan preventivo fue de conocimiento de la gerencia de la empresa para verificación de la transparencia y principios éticos aplicados en dicho proceso. Asimismo, los ejecutores cumplieron ligeramente las disposiciones establecidas en las normas en referencia a los derechos de autor.

IV. RESULTADOS

Respecto a objetivo específico 1: Diagnosticar el estado imperante de los riesgos tecnológicos del área de Tecnología de la Información de la empresa PROANCO

Tabla 2. *Riesgos tecnológicos respecto a los equipos*

Indicador	Riesgo Identificado	NIVEL DE RIESGO			
		BAJO	MEDIO	ALTO	MUY ALTO
		<24	32-40	48-64	80-100
Resguardó de información.	Falta de mantenimiento a UPS.		32		
	Falla física imprevista de equipo.			48	
	No contar con sistemas de copias de seguridad.		40		
Protección de seguridad.	Acceso libre a usuarios de equipo.	16			
	Acceso libre a BIOS o UEFI.	24			
	Falta de equipo regulador de voltaje.	16			
Desastre natural	Deterioro por humedad o filtrado de agua de lluvia.			64	
	Temblores de alta intensidad.		38		

Fuente: Matrices de identificación y evaluación de riesgos tecnológicos

La Tabla 2 muestra la identificación y análisis de riesgos respecto a los equipos, observándose que destaca con nivel alto los riegos, falla física imprevista de los equipos y filtrado de agua de lluvia en área de trabajo.

Tabla 3: *Riesgos tecnológicos respecto a los programas*

Indicador	Riesgo Identificado	NIVEL DE RIESGO			
		BAJO	MEDIO	ALTO	MUY ALTO
		<24	32-40	48-64	80-100
Fuentes desconocidas	Uso de páginas web desconocidas.	**16**			
	Instalaciones de programas sin permisos de administrador.	**16**			
Afectación viral a la información	Permitir conectar dispositivos USB externos a la PC.	**16**			
	Descargar archivos ejecutables de páginas no confiables.	**16**			
	Instalar programas craqueados.		**36**		
	No contar con antivirus licenciados.		**40**		
	Filtrado de clave de usuario.		**32**		
Restricciones de acceso	Rotación de credenciales de acceso			**48**	
	Credenciales de acceso almacenadas o guardadas en equipos.			**48**	

Fuente: Matrices de identificación y evaluación de riesgos tecnológicos.

La Tabla 3 muestra la identificación y análisis de riesgos respecto a los programas, observándose que destaca con nivel alto los riegos, rotación de credenciales y las credenciales almacenadas o guardadas en equipos.

Tabla 4: *Riesgos tecnológicos respecto a personas*

Indicador	Riesgo Identificado	NIVEL DE RIESGO			
		BAJO <24	MEDIO 32-40	ALTO 48-64	MUY ALTO 80-100
Normas de seguridad	Incumplimiento de las normas de seguridad.			48	
	Falta de señalización de zonas de peligro en el área	32			
	Desconocimiento de las normas de seguridad en trabajadores nuevos.	16			
Medidas preventivas	Falta de registro de fallas.	32			
	Falta de identificación de riesgos.			48	
	Falta de conciencia de prevención.			64	
Práctica de valores	Actuación irresponsable.			64	
	Conductas no éticas.	32			

Fuente: Matrices de identificación y evaluación de riesgos tecnológicos

La Tabla 4 muestra la identificación y análisis de riesgos respecto a las personas, observándose que destaca con nivel alto los riegos, falta de políticas de seguridad actualizadas, falta de difusión de normas de seguridad, incumplimiento de las normas de seguridad, falta de actualización de normas de seguridad, falta de identificación de riesgos y falta de conciencia de prevención.

Asimismo, se registró la información consensuada con los trabajadores y técnicos del área de Tecnología de la Información en la empresa PROANCO respecto a las causas de los riesgos tecnológicos, con lo cual se ha tenido una visión más amplia sobre las reales causas del problema con el propósito de contribuir a disminuirlos.

Tabla 5: *Consolidado de los riesgos tecnológicos identificados por nivel*

Dimensiones/ variable	Bajo		Medio		Alto		Total	
	n	%	n	%	n	%	n	%
Respecto a equipos	3	12.00	3	12.00	2	8.00	8	32
Respecto a programas	4	16.00	3	12.00	2	8.00	9	36
Respecto a personas	4	16.00	0	0.00	4	16.00	8	32
Total	11	44.00	6	24.00	8	32.00	25	100

Fuente: Riesgos tecnológicos identificados Tabla 2, 3 y 4.

Para calcular la frecuencia en cada una de las dimensiones de la varíale riesgos tecnológicos y su total se realizó un conteo de la cantidad de riesgos identificados en cada una de las dimensiones (tablas 2, 3 y 4), aplicado para cada nivel las siguientes fórmulas:

- ✓ % Nivel Alto= (Cantidad de riesgos en nivel Alto) x100
  Cantidad total de riesgos
- ✓ %nivel Medio= (Cantidad de riesgos en nivel Medio) x100
  Cantidad total de riesgos
- ✓ % % nivel Bajo = (Cantidad de riesgos en nivel Bajo) x100
  Cantidad total de riesgos

La Tabla 5 muestra el consolidado de los riesgos tecnológicos por nivel, destacando el nivel alto con el 32%, distribuyéndose en los riesgos respecto a equipos, programas y personas con el 8%, 8% y 16%, por lo cual se requiere una intervención con el fin de disminuir este nivel alto de riesgos.

Los resultados de los análisis documentales indican que documental arroja que los registros de fallas y averías, de actividades realizadas y en general del plan de mantenimiento se encuentran desactualizados, así como las normas de seguridad informática del área.

Respecto a objetivo específico 2: Diseñar el plan preventivo para disminuir riesgos tecnológicos en el área de Tecnología de la Información en la empresa PROANCO

Se elaboro un diagrama causa efecto mismo que se puede observar en anexo 3: Diagrama Causa-Efecto, identificándose las causas principales: Maquinas:

inexistencia de plan preventivo, Inexistencia de registros de fallas, Ineficiente inspección; Mano de obra: Ausencia de capacitación técnica, No practica de valores institucionales, Deficiente coordinación interna, Deficiente supervisión; Métodos: Desactualizado plan de mantenimiento, Imprecisión de funciones en el área, Deficiente gestión de mantenimiento, Desactualizado plan de seguridad informática e Imprecisión de responsabilidades en el área. Posterior a ello se elaboró la matriz de identificación de causas.

Tabla 6: *Identificación y evaluación de las causas de riesgos tocológicos*

Ítem	Causa	f	i	e	a	%
A	Ausencia de capacitación técnica	5	12	60	60	21.90%
M	Desactualizado plan de mantenimiento	5	12	60	120	43.80%
G	Inexistencia de registros de fallas	5	12	60	180	65.69%
N	Desactualizado plan de seguridad informática	3	12	36	216	78.83%
H	Ineficiente inspección	3	9	27	243	88.69%
B	No practica de valores institucionales	1	9	9	252	91.97%
Q	Deficiente gestión de mantenimiento	1	9	9	261	95.26%
E	Deficiente supervisión	1	3	3	264	96.35%
F	Inexistencia de mantenimiento preventivo	1	3	3	267	97.45%
O	Imprecisión de funciones en el área	1	3	3	270	98.54%
P	Imprecisión de responsabilidades en el área	1	3	3	273	99.64%

Ítem	Causa	f	i	e	a	%
D	Deficiente coordinación interna	1	1	1	274	100.00%

Fuente: Matriz de identificación y evaluación de causas de riesgos tecnológicos

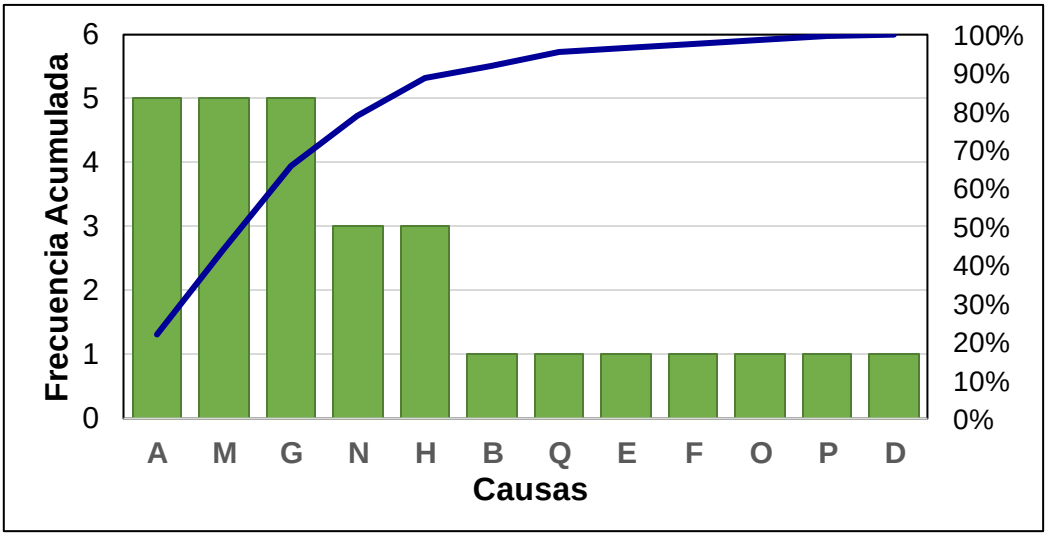


Figura 1: *Diagrama de Pareto de los riesgos tecnológicos*

Fuente: Tabla 6.

En la figura 1 se observa que las causas más determinantes de los riesgos tecnológicos son: A= Ausencia de capacitación técnica. M= Desactualizado plan de mantenimiento. G=Inexistencia de registros de fallas. N= Desactualizado plan de seguridad informática. H=Ineficiente inspección.

Después de esta identificación de riesgos, se implementó un programa integral que comprende un conjunto de tres talleres estratégicos. Estos talleres fueron diseñados para abordar de manera específica las cinco causas previamente identificadas en relación con equipos, programas y personas. El enfoque principal de estos talleres era mitigar y reducir los riesgos tecnológicos asociados.

Cada taller dentro del programa se centró en aspectos clave, desde la seguridad de los equipos hasta la eficiencia de los programas y la capacitación adecuada de las personas involucradas. Se llevó a cabo un análisis exhaustivo de las vulnerabilidades existentes en los sistemas, evaluando tanto la infraestructura física como la virtual.

El primer taller se enfocó en optimizar el rendimiento de los equipos, asegurando su integridad y funcionamiento eficiente. Se implementaron medidas de seguridad avanzadas para proteger contra posibles amenazas. El segundo taller se dedicó a mejorar la robustez y la seguridad de los programas utilizados en la organización. Se llevaron a cabo actualizaciones y parches necesarios, y se implementaron prácticas de desarrollo seguro para prevenir posibles brechas de seguridad. Además, se establecieron procedimientos de monitoreo continuo para detectar y abordar rápidamente cualquier anomalía. El tercer taller se centró en el recurso humano, proporcionando programas de capacitación detallados y personalizados. Esto incluyó la concienciación sobre seguridad cibernética, buenas prácticas en el uso de sistemas tecnológicos y la promoción de una cultura organizacional que valore la seguridad en todos los niveles.

En conjunto, estos talleres formaron un programa integral que no solo abordó las causas fundamentales de los riesgos tecnológicos, sino que también fortaleció la resiliencia de la organización ante posibles desafíos futuros. La implementación de este programa marcó un hito significativo en la gestión proactiva de la seguridad tecnológica y sentó las bases para un entorno más seguro y eficiente.

1. Actividades y tareas

Tabla 7: *Actividades y tareas realizadas*

			Semanas			
ACTIVIDAD	**N°**	**TAREAS**	Septiembre -2023			
			1	**2**	**3**	**4**
Taller 1						
Evento 1: “Mantenimiento preventivo”	1	Empoderamiento de habilidades en análisis de riesgos y planes de mantenimiento.				
	2	Empoderamiento de habilidades en registro de fallas y utilización de data.				
	3	Empoderamiento de habilidades para realizar inspecciones a procesos y procedimientos.				
Taller 2						

ACTIVIDAD	N°	TAREAS	Semanas Septiembre -2023 1	2	3	4
“Seguridad informática	1	Empoderamiento de habilidades en análisis de riegos y planes de seguridad informática.				
	2	Empoderamiento de habilidades en implementación de planes de seguridad informática.				
Taller 3. Evento 3: “Prevención de la calidad ambiental”	1	Empoderamiento de habilidades para cumplimiento de normas de seguridad.				
	2	Empoderamiento de habilidades prácticas de valores institucionales en centro laboral.				

Fuente: Elaboración propia.

Objetivo específico 3: Determinar la disminución de los riesgos tecnológicos en el área de Tecnología de la Información de la empresa PROANCO

Tabla 8: *Variación de porcentaje de los riesgos tecnológicos antes y después de la aplicación del plan de prevención*

Dimensiones / Variable	Nivel Bajo (%)			Medio (%)			Alto (%)		
	Antes	Después	Variación	Antes	Después	Variación	Antes	Después	Variación
Riesgos tecnológicos	44.0	56.0	12.0	24.0	40.0	16.0	32.0	4.0	-28.0
Respecto a equipos	12.0	16.0	4.0	12.0	12.0	0.0	8.0	4.0	-4.0
Respecto a programas	16.0	24.0	8.0	12.0	12.0	0.0	8.0	0.0	-8.0
Respecto a personas	16.0	16.0	0.0	0.0	16.0	16.0	16.0	0.0	-16.0

Fuente: Matriz de evaluación de riesgos.

La tabla 9 muestra la variación de los resultados del porcentaje de riesgos tecnológicos antes y después de la aplicación del plan preventivo, aplicado el indicador y formulas establecidas en la Tabla, observándose como valor más relevante los presentados en el nivel alto con una variación negativa (disminución)

de -28%. Asimismo, los riesgos respecto a equipos, programas y personas del nivel alto tuvieron una variación negativa (disminución) en -4,0%, -8.0% y -16.0%.

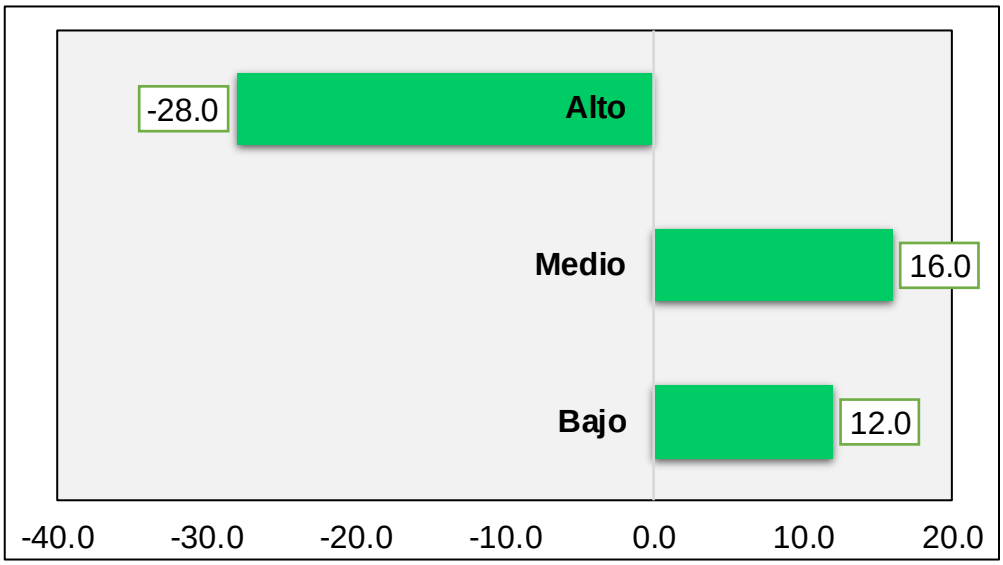


Figura 2: *Variación del nivel de Riesgos tecnológicos*

Fuente. Anexo 4, Medidas de control

La Figura 2, muestra la variación de los riesgos tecnólogos, en el nivel alto es negativo (descuido) en -28%. el nivel medio y bajo es positivo (aumentado) en 16 y 12% respectivamente.

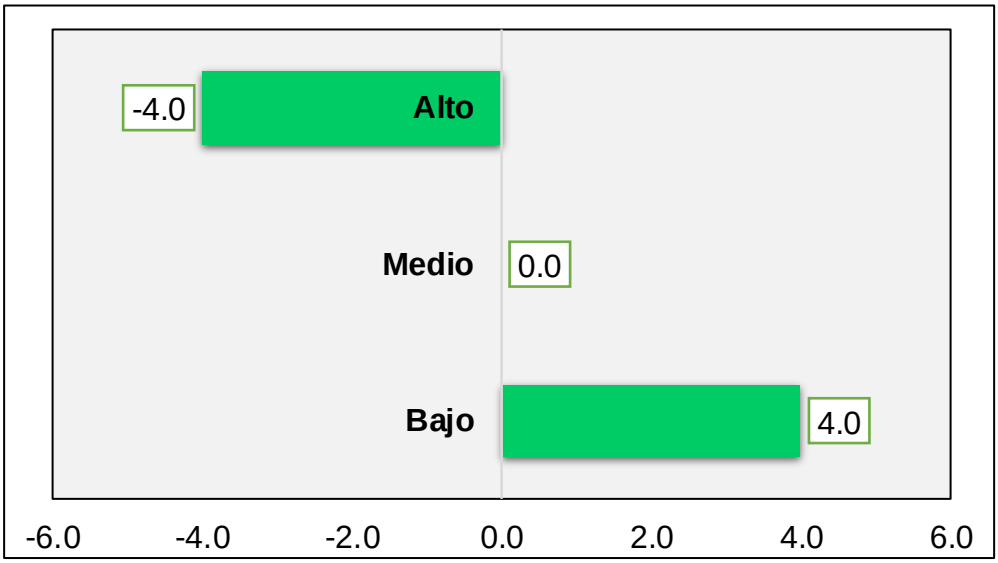


Figura 3: *Variación del nivel de Riesgos tecnológicos respecto a equipos*

Fuente. Anexo 4, Medidas de control

La Figura 3, muestra la variación de los riesgos tecnólogos respecto a equipos, en el nivel alto es negativo (disminuido) en -4.0%, el nivel bajo y medio es positivo (aumentado) en 4% y 0%, respectivamente.

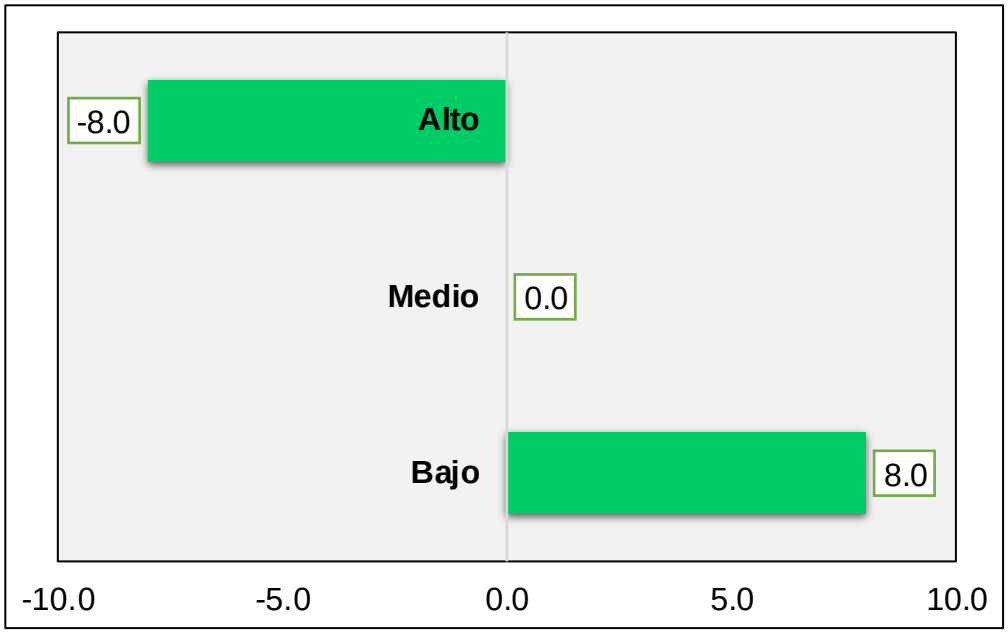


Figura 4: *Variación del nivel de Riesgos tecnológicos respecto a programas*

Fuente. Anexo 4, Medidas de control

La Figura 4, muestra la variación de los riesgos tecnólogos respecto a programas, el nivel alto es negativo (disminuido) en -8.0%, el nivel bajo y medio es positivo (aumento) con 8% y 0%, respectivamente.

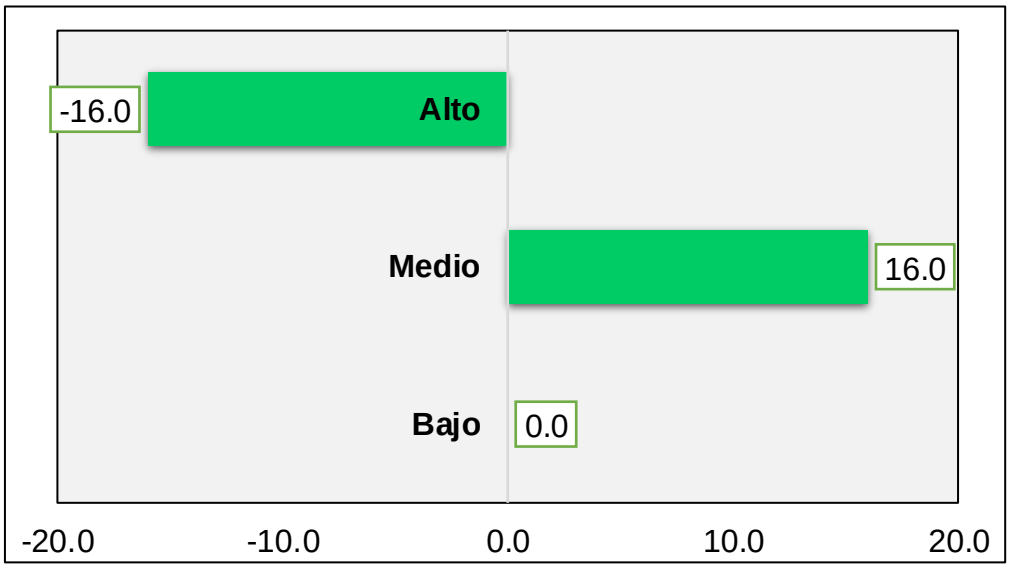


Figura 5: *Variación del nivel de Riesgos tecnológicos respecto a personas*

Fuente. Anexo 4, Medidas de control

La Figura 5, muestra la variación de los riesgos tecnólogos respecto a personas, el nivel alto es negativo (disminuido) en -16.0%, el nivel medio y bajo es positivo (aumentado) en 16% y 0%, respectivamente.

V. DISCUSIÓN

Respecto al objetivo específico 1, diagnosticar el estado imperante de los riesgos tecnológicos, los hallazgos previos indican que destaca el nivel alto con el 32%, lo cual indica que existe un grupo de riesgos que al mantenerse van a tener un impacto en el área de Tecnología de la Información por lo que amerita una intervención orientado a disminuirlos; toda vez, que la contingencia de que las interrupciones, alteraciones, o fallas de una infraestructura, sistema de información, bases de datos y procesos de TI, provocan pérdidas económicas (Klus, 2021). En la organización los riegos tecnológicos se generan con el incremento de herramientas y aplicaciones tecnológicas que no disponen de gestiones adecuada respecto a la seguridad, encontrándose desprotegidas por los constantes cambios (Bernaldo, 2018).

Los resultados encontrados se asocian a los de Montoya (2020) quien determino que dentro de una organización es necesario y fundamental identificar, clasificar y establecer el nivel de los riesgos que tiene la información y los procesos internos; dicha data debe estar a disposición de los directivos de la empresa para la toma de decisiones y la aplicación de diversas estrategias de seguridad, así como implementar controles pertinentes; aportando que la mitigación de riesgos es fundamental para neutralizar las amenazas a lo que esta expuestos la información de la organización y el área de TI. Asimismo, los resultados se asocian a los de Llanos y Campoverde (2021), quienes identificaron una alta criticidad, de riesgos para lo cual se definió controles y recomendaciones de auditoría con el propósito de disminuir el impacto en los procesos de la organización; la mitigación mediante controles mejora la eficiencia y efectividad de los procesos de la organización en los que interviene las TI, pero debe ser un proceso continuo con el propósito de evitar dificultades para contar con una información integra, confidencial y disponible. De la misma forma se relacionan con los resultados de Torres (2023), quien concluyó que los riesgos incluyen los desafíos es adaptarse y capacitarse en forma constante para poder desenvolverse con tecnología moderna; aportando que el avance tecnológico implica asumir riesgos, pero tiene que asumir el reto de enfrentarlos y disminuirlos.

Respecto al objetivo específico 2, diseñar el plan preventivo para disminuir riesgos tecnológicos, teniendo como fundamento el actuar sobre las causas y no sobre los efectos del problema, se diseñó un plan preventivo basado en las 5 causas principales obtenidas mediante el diagrama de Pareto: A= Ausencia de capacitación técnica. M= Desactualizado plan de mantenimiento. G=Inexistencia de registros de fallas. N= Desactualizado plan de seguridad informática. H=Ineficiente inspección. El actuar sobre las causas identificadas, garantiza que el plan preventivo actuó de manera directa sobre el problema de riesgos tecnológicos, cconsiderando que un plan preventivo se concibe como la implementación de acciones que cautelan principalmente los equipos y la información en una organización (Pérez, 2021).

El diseño del plan preventivo se relaciona con planteado por Aquino y Atalaya (2020) quien concluye que, al implementar el plan preventivo diseñado acorde a la necesidad, ha generado que el 90% de las maquinarias mejore su disponibilidad; contar con dicho instrumento es fundamental debido a que tiene el propósito de reducir los riesgos que surgen en los diferentes equipos tecnológicos, incluyendo algún tipo de riesgo electrónico en salvaguardar la integridad del personal de dicha área. Asimismo, el plan diseñado se asocia al planteado por Morales (2019) quien concluyó que el plan preventivo es de gran importancia para la disminución de fallas en máquinas existentes; por consiguiente resulta necesario que cada empresa cuente con un plan preventivo ya sea para disminuir riesgos o para evitar los fallos en la maquinaria, lo que conlleva también a capacitar a los trabajadores del área con el propósito de que conozcan las normas y procedimientos para mantener la integridad de la información y la operatividad de las máquinas en general. Así también se relaciona con lo que consiguió Patiño y Bedoya (2023) quienes concluyeron que la evaluación de las probabilidades de ocurrencia y los impactos potenciales en la empresa permiten establecer una priorización de los riesgos y orientar las atenciones en los más relevantes, a partir de lo cual se elaboró un plan que abarca el tener identificado las amenazas, la valoración de riesgos y las acciones pertinentes para proteger la información de la data: esto aporta que es necesario para la elaboración eficaz de un plan preventivo de riesgos es actuar sobre las causas, para lo cual hay que identificarlas, valorarlas y evaluarlas.

Respecto al objetivo específico 3**,** determinar la disminución de los riesgos tecnológicos en base a la implementación del plan preventivo; al realizar la comparación de los resultados obtenidos con la evaluación diagnosticada y la evaluación después de la intervención, observándose que el nivel alto disminuyó en -28% y en cuanto a los riesgos respecto a equipos, programas y personas, el nivel alto tuvo disminución en -4,0%, -8.0% y -16.0% respectivamente, esto implica que la aplicación del plan preventivo fue positivo. La implementación de un plan preventivo disminuye en gran porcentaje la frecuencia de mantenimientos correctivos en las organizaciones, lo cual, a la vez, disminuye los costos, toda vez que las acciones de prevención cuestan menos que las correctivas (Molina y Sánchez, 2018).

Los hallazgos obtenidos se relacionan con los de Gómez (2022) quien concluye que encontró como resultados tres variables principales a tener en cuenta, el contexto (C), la evaluación (E) y el monitoreo (M), a partir de lo cual fue diseñado y aplicado a un procedimiento para la gestión de riesgos de TI en la organización a través de la web, realizando la identificación, clasificación y valoración hasta reducirlos totalmente en forma progresiva y sostenida en el tiempo. La investigación aporta que el uso de las TI facilita el análisis para la toma de decisiones en beneficio de la disponibilidad eficaz de la información.

Asimismo, se relacionan con los encontrados por Pizarro (2022), quien concluyó que la implementación de un modelo para gestionar riesgos incide en un 47.70% en la seguridad de información de la entidad; aportando que es importante la implementación de modelos de gestión de riesgos teniendo en cuenta que mejoran la seguridad de los datos internos de la organización; sin embargo, es necesario aplicar otras acciones simultáneas como un plan preventivo que asegure la disponibilidad y confiabilidad de la información.

En síntesis, se ha comprobado que el diseño y aplicación de un plan preventivo a partir de la identificación de las causas del problema resulta eficaz, pues enfrenta el problema actuando sobre la raíz del problema y no desperdiciando los esfuerzos y recurso actuando sobre los efectos, por solo resulta algo temporal; en cambió la actuación sobre las causas resulta duradera y es eficaz. Bajo esta lógica, el plan

preventivo aplicado para disminuir riesgos tecnológicos resulto efectivo, teniendo en cuenta que disminuyó en un 28% los riesgos con el calificativo alto.

La fortaleza del estudio es haber implementado una propuesta diseñada a partir del análisis de una realidad evaluada conjuntamente con los trabajadores del área en estudio, considerando que son los trabajadores quienes conocen mejor la realidad del entorno de trabajo, los procesos y procedimientos que se realizan cotidianamente y por ende, pueden identificar y evaluar los riesgos tecnológicos con mayor conocimiento y criterio; lo cual le dio la validez necesaria para su aplicación y evaluación de los resultados con los respectivas medidas de control establecidas en el plan. Asimismo, se tuvo como debilidad, el hecho de no contar con instrumentos estandarizadas para realizar la investigación, pero fue superada con el diseño respectivo de instrumentos acorde a los objetivos y la empresa objeto de estudio.

VI. CONCLUSIONES

De acuerdo al trabajo de investigación se deduce que:

1. El diagnóstico de los riesgos tecnológicos del área de Tecnología de la Información arroja que el 32% se encuentra en nivel alto, distribuyéndose en los riesgos con respecto a equipo, programas y personas con el 8%, 8% y 16% respectivamente. Lo que indica que aproximadamente la tercera parte de los riesgos identificados de no tenerse ningunas medidas tendrán un impacto negativo en la operatividad del área.
2. El diseño de un plan de prevención para disminuir los riesgos tecnológicos se diseñó a partir de la identificación de las causas más relevantes del problema obtenidas mediante el diagrama de Pareto y a la vez, se asoció estas dimensiones (referente a equipos, programas y persona) de la variable.
3. Con la aplicación del plan preventivo se disminuyó los riesgos tecnológicos de nivel alto en 28%. Lo que indica que la aplicación del plan resulto eficaz, pues disminuyó los riesgos de mayor impacto negativo para la operatividad del área de Tecnología de la Información.

VII. RECOMENDACIONES

A los directivos de la empresa PROANCO, Sullana identificar y evaluar los riegos tecnológicos en todas las áreas, utilizando la matriz aportada con el propósito de tener una base de datos y utilizarlas en la toma de decisiones.

A los directivos de la empresa PROANCO diseñar planes preventivos de prevención de riesgos tecnológicos en las diversas áreas de la empresa con el propósito de tener un plan integral de prevención.

A los trabajadores del área de Tecnología de la Información continuar en forma identificando y evaluando la causa de los riesgos tecnológicos, teniendo en cuenta que, con los cambios de métodos, implementación de nuevos proceso o procedimientos surgen nuevos riesgos y por ende nuevas causas.

REFERENCIAS

ANDINA, 2021. Sector mantenimiento mueve alrededor de S/250 millones anuales en el Perú. Sector mantenimiento mueve alrededor de S/250 millones anuales en el Perú. Andina. 2 de febrero, p. 1. [en línea]. Disponible en: https://andina.pe/agencia/noticia-sectormantenimiento-mueve-alrededor-s250-millones-anuales-el-peru-834935.aspx

ANSARI, Mohd, RAHIM, Kazi, BHOJE, Rohaan y BHOSALE, Sumit (2022). A study on research design and its types. International Research Journal of Engineering and Technology (IRJET). 9(7). Disponible en: https://www.irjet.net/archives/V9/i7/IRJET-V9I7216.pdf

AQUINO, Wilder. y ATALAYA, Steve, 2020. Diseño de un plan de mantenimiento preventivo para mejorar la disponibilidad de equipos de la empresa Globaltruck E.I.R.L- 2018-2019 [en línea]. Tesis de licenciatura. Cajamarca: Universidad Privada del Norte. Disponible en: https://hdl.handle.net/11537/26312

ARANGO, Jaime., ROSERO, Silvio. y MONTOYA, Mario, 2020. Programación de mantenimiento preventivo usando algoritmos genéticos. Lámpsakos [en línea]. Colombia: núm, 23, pp. 37-44 [consulta: junio de 2023]. Disponible en: https://doi.org/10.21501/21454086.3112

ARIAS, José. y COVINOS, Mitsuo, 2020. Metodología y diseño de investigación. 1ra ed. Perú: Enfoques Consulting. ISBN: 978-612-48444-2-3. Disponible en: https://www.researchgate.net/publication/352157132_DISENO_Y_METODOLOGIA_DE_LA_INVESTIGACION

ARROYO, Cristian. y OBANDO, Romel, 2022. Importance of implementing preventive maintenance in production plants to optimize processes. E-IDEA Journal of Engineering Science [en línea]. Ecuador: vol. 4, núm, 10, pp. 59- 69 [consulta: julio de 2023]. Disponible en: https://doi.org/10.53734/esci.vol4.id240

BARRIGA, Gabriela, 2019. Gestión integral de riesgos y Antisoborno: un enfoque operacional desde la perspectiva ISO 31000 e ISO 37001. Revista Universidad y Empresa [en línea]. Bogotá: vol. 21, núm, 36. Pp. 79-118 [consulta junio 2023]. Disponible en: https://doi.org/10.12804/revistas.urosario.edu.co/empresa/a.6089

BEJARANO, Miguel y MERSEGUER, José. 2021. A Vision For Improving Business Continuity Through Cyber-Resilience Mechanisms And Frameworks. Iberian Conference On Information Systems And Technologies, Cisti. Cisti. Disponible en: https://doi.org/https://doi.org/10.23919/Cisti52073.2021.9476324

BERNALDO, Natividad. 2018. Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC. San Borja. Lima 2016 [en línea]. Tesis Maestría. Lima: Universidad Cesar Vallejo. Disponible en: http://repositorio.ucv.edu.pe/handle/UCV/12657

BLANCO, Francys., MOLINA, Rosa. y SÁNCHEZ, Ingris, 2018. Propuesta de un plan de gestión de mantenimiento preventivo total para los tornos de la empresa Torno Pineda de la ciudad de Estelí, en el segundo semestre 2017 [en línea]. Tesis grado. Nicaragua: Universidad Nacional Autónoma de Nicaragua]. Disponible en: https://repositorio.unan.edu.ni/8926/1/18782.pdf

BRUNNER, Michael (2020). Risk management practices in information security: Exploring the status quo in the DACH region. Computers & Security. Volume 92, 2020, 101776, ISSN 0167-4048. Retrieved from. Disponible en: https://doi.org/10.1016/j.cose.2020.101776

COHEN, Louis, MANION, Lawrence y MORRISON, Keith (2018). Research methods in education (8th ed.). Routledge, Taylor and Francis Group.

COLINA, Alejandra. y TÚA, José, 2020. Activos informáticos: un referente en la caracterización de procesos de la gestión riesgos de TI. INNOVA Research Journal [en línea]. Ecuador: vol.5, núm, 3.2, pp. 196–213. [consultado julio 2023]. Disponible en: https://doi.org/10.33890/innova.v5.n3.2.2020.1608

CONTRERAS, Aristides. y MEDINA, Gladys, 2019. Gestión de riesgo en seguridad digital en el sector privado y mixto-contexto general. La seguridad en el ciberespacio: un desafío para Colombia [en línea]. Colombia: pp. 169-199. Disponible en: https://www.researchgate.net/publication/333153536_Gestion_de_riesgo_en_Seguridad_Digital_en_el_sector_privado_y_mixto_-_contexto_general

CRUZ, Alexander. IPARRAGUIRRE, Deylin. LOZANO, Eduardo. PARIMANGO, Leydi. y CASTILLO, Rafael, 2020. Diseño de plan de mantenimiento preventivo,

KARDEX, VSM y balance de línea para reducir costos. Rev. Ingeniería: Ciencia, Tecnología e Innovación [en línea]. Perú: vol. 7, núm, 2, pp. 142-151. [consulta en julio 2023]. ISSN: 2313-1926. Disponible en: https://doi.org/10.26495/icti.v7i2.1498

DIDRAGA, Otniel, BRANDAS, Claudiu, BATAGAN, Lorena y ALECU, Felician (2019). Characteristic of effective It project risk management romanian it companies. Economic Computation and Economic Cybernetics Studies and Research, Issue 4/2019; Vol. 53. Retrieved from. Disponible en: http://ecocyb.ase.ro/nr2019_4/11.%20DIDRAGA%20Otniel,%20Lorena%20Batagan.pdf

FLORES, Robinson. 2023. Ciberseguridad para el Proceso de Gestión de Riesgos de TI en una Empresa Transnacional, Lima 2023. [en línea]. Tesis Maestría. Lima, Perú: Universidad Cesar Vallejo. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/107946

GÓMEZ, Rafael, 2022. Gestión y prevención de riesgos con tecnologías de información y comunicaciones. Gestión y prevención de riesgos con tecnologías de información y comunicaciones Ciencias Holguín [en línea]. Cuba: Vol. 28, núm. 2 [consulta junio 2023]. ISSN: 1027-2127. Disponible en: https://www.redalyc.org/articulo.oa?id=181571550007

IBM (2020). Informe sobre el coste de una brecha de datos. Madrid, España: Editorial IBMSecurity. Disponible en: https://www.ibm.com/downloads/cas/D4YK8Q86

KLUS, Javier, 2021. Riesgos tecnológicos. Auditoria. 23 de mayo, p.1. [en línea]. Disponible en: https://auditgroup.org/2021/05/23/riesgos-tecnologicos-tips-1-obsolecencia/

LEAVY, Patricia, 2022. Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches. New York: Second Edition. – ISBN 978-1-4625-2999-5 (hard). Disponible en: https://www.guilford.com/books/Research-Design/Patricia-Leavy/9781462548972

LEE, Seongkee, 2018. Resiliency Of Mobile Os Security For Secure Personal Ubiquitous Computing. Personal And Ubiquitous Computing [en línea]. New york:

Vol. 22 [consulta junio 2023]. Issue 1. Disponible en: https://doi.org/https://doi.org/10.1007/S00779-017-1098-X

LLANOS, Cristian. y CAMPOVERDE, Milton, 2021. Análisis de riesgos del departamento de Tecnologías de la Información y Comunicación del Registro de la Propiedad de la ciudad de Cuenca, Ecuador. Pol. Con [en línea]. Ecuado: vol. 6, núm. 11, pp. 1168-1185 [consulta agosto 2023]. ISSN: 2550 - 682X. Disponible en: 10.23857/pc.v6i11.3320.
https://dialnet.unirioja.es/servlet/articulo?codigo=8219383

LÓPEZ, Rosario. BENITES, Elmer. RODRÍGUEZ, Lino. GUTIÉRREZ, Jaime. ITURRIZAGA, Johan. y MARTÍNEZ, Juan, 2022. Application of the Crystal Ball in Preventive Maintenance Management and its influence on productivity in a cardboard manufacturing company. Digital Object Identifier [en línea]. Perú: [consulta agosto 2023]. ISBN: 978-628-95207-0-5. Disponible en: http://dx.doi.org/10.18687/LACCEI2022.1.1.691

MARRERO, Rogej. VILALTA, José. y MARTÍNEZ, Edith, 2019. Modelo de diagnóstico-planificación y control del mantenimiento. Ingeniería Industrial [en línea]. Cuba: vol. XL, núm. 2. pp. 148-160. [consulta julio 2023]. /ISSN 1815-5936. Disponible en: http://scielo.sld.cu/pdf/rii/v40n2/1815-5936-rii-40-02-148.pdf

MASSO, Jhon (2020). Risk management in the software life cycle: A systematic literature review. Computer Standards & Interfaces, 10. Retrieved from. Disponible en: https://www.researchgate.net/publication/339747572_Risk_management_in_the_software_life_cycle_A_systematic_literature_review

MONTOYA, Martin, 2020. Evaluación de riesgo de seguridad de información según ISO 27005, OGITT – Instituto Nacional de Salud [en línea]. Tesis Maestría, Lima: Universidad Cesar Vallejo. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/42553/Montoya_OME.pdf?sequence=1&isAllowed=y

MORALES, Carlos, 2019. Desarrollar un plan de mantenimiento preventivo para la maquinaria de la empresa Imprenta “Morales” de la ciudad de Ambato. Tesis de pregrado [en línea]. Ecuador: Universidad Técnica de Ambato Ecuador. Disponible en: http://repositorio.uta.edu.ec/jspui/handle/123456789/29867

MULISA, Feyisa (2022). When does a researcher choose a quantitative, qualitative, or mixed research approach? Interchange, 53(1), 113–131. Disponible en: https://doi.org/10.1007/s10780-021-09447-z

MURILLO, I, 2017. Propuesta de mejoras a los procesos de mantenimiento preventivo de equipos portuarios [en línea]. Título de Tecnólogo en Administración de Empresa. Ecuador: Instituto Superior Tecnológico Bolivariano de Tecnología. Disponible en: https://repositorio.itb.edu.ec/bitstream/123456789/154/1/PROYECTO%20DE%20GRADO%20DE%20MURILLO%20VELIZ.pdf

ÖBRAND, Lars, HOLMSTRÖMA, Jonny y NEWMANB, Michael (2018). Navigating Rumsfeld's quadrants: A performative perspective on IT risk management. Technology in Society, Volume 53, 1-8. Retrieved from. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S0160791X15300634?via%3Dihub

OREHEK, Špela y PETRIČ, Gregor (2021). A systematic review of scales for measuring information security culture. Emerald insight - ISSN: 2056-4961. Retrieved from. Disponible en: https://www.emerald.com/insight/content/doi/10.1108/ICS-12-2019-0140/full/html

PASHCHENKO, Denis. 2023. Empresas competitivas de alta tecnología en la industria de tecnología de la información. Revista De Investigación En Tecnologías De La Información, 11(24), 37–49. Disponible en: https://doi.org/10.36825/RITI.11.24.004

PATIÑO, Javier y BEDOYA, Josed. 2023. Plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales en una empresa. Tesis grado. Colombia: Tecnológico de Antioquia - Institución Universitaria. Disponible en: https://dspace.tdea.edu.co/handle/tdea/3576

PAZMIÑO, César. SERRANO, Anita. y GONZÁLEZ, Martha, 2020. Las Tics como herramienta para la gestión de riesgos. RECIMUNDO [en línea], España: vol. 4, núm. 1, pp. 173- 181 [consulta agosto 2023]. Disponible en: https://www.recimundo.com/index.php/es/article/view/793

PÉREZ, Félix, 2021. Conceptos generales en la gestión del mantenimiento industrial. Colombia: Ediciones USTA. Pp. 107. ISBN: 9789588477923. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/33276/9789588477923.pdf?sequence=4&isAllowed=y

PIZARRO, Ivan, 2022. Modelo de Gestión de riesgos de TI para la seguridad de la información de una institución del estado, Lima 2022 [en línea]. Tesis Maestría. Lima: Universidad Cesar Vallejo. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/97613/Pizarro_CIMA-SD.pdf?sequence=4&isAllowed=y

Priyatna, Bayu. Trianto, Topan. Manurung, Julifer. Heryana, Nono. y Solehudin, Arip, 2021. Sistem Preventive Maintenance Berbasis Web dengan Menggunakan Algoritma Priority Scheduling pada PT. Beta Pharmacon. INTERNAL (Information System Journal) [en línea]. Indonesia: vol. 3, núm. 2, pp. 41–53 [consulta julio 2023]. E-ISSN. 2656-0259. Disponible en: https://doi.org/10.32627/internal.v3i2.294

RAO, Faizan, DOMINIC P., AZHAR, Syed, REHMAN, Mobashar y SOHAIL, Abid (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic literature review for identifying the transformation process from noncompliance to compliance. Advanced Technologies in Data and Information Security, 8-11. Retrieved from. Disponible en: https://www.mdpi.com/2076-3417/11/8/3383

ROBAYO, Nelson, 2020. Diseño y programación de un plan de mantenimiento preventivo para los equipos e instalaciones de una institución de educación superior de la ciudad de Quito [en línea]. Tesis grado. Quito: Escuela Politécnica Nacional. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/20704

TIZNADO, José, 2019. Riesgo y Seguridad en los Dispositivos Móviles en Estudiantes de la Carrera de Desarrollo de Software en el SENATI, 2019. [en línea]. Tesis Maestría. Lima: Universidad Cesar Vallejo. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/34448/Tiznado_UJA.pdf?sequence=1&isAllowed=y

ANEXOS

Anexo 1 Tabla de operacionalización de variables.

Variables	Definición conceptual	Definición operación al	Dimensiones	Indicadores	Escala de medición
Variable Dependiente: Riesgos tecnológicos	La contingencia de que las interrupciones, alteraciones, o fallas de una infraestructura, sistema de información, bases de datos y procesos de TI, provoquen pérdidas económicas en la organización. (Klus, 2021).	Se evaluará equipos, programas y personas del área de tecnología mediante una ficha de análisis y evaluación de riesgos tecnológicos.	Respecto a los equipos	– Resguardo de información. – Protección de seguridad. – Desastre natural.	Ordinal
			Respecto a los programas	– Fuentes desconocidas. – Afectación viral a la información. – Restricciones de acceso.	
			Respecto a personas	– Normas de seguridad. – Medidas preventivas – Practica de valores.	
Variable Independiente: Plan preventivo	Implementación de acción que, define fechas, hora, duración y ubicación referencial de las acciones que cautelan los equipos, información y la seguridad del personal previamente identificadas (Pérez, 2021).	Se realizará el diagnóstico, planeación e inversión del plan preventivo mediante diagramas, fichas técnicas y guías de entrevista	Diagnostico	– Historial de fallas. – Numero de causas.	Plan preventivo
			Planeación	– Tareas a realizar. – Programación de tareas.	
			Inversión	– Costo- beneficio.	

Anexo 2 Instrumento de recolección de datos.

INSTRUMENTO 1: MATRICES DE IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS TECNOLÓGICOS

UNIVERSIDAD CÉSAR VALLEJO

DIMENSIÓN: RESPECTO A LOS EQUIPOS

IDENTIFICACIÓN		EVALUACION												
INDICAD.	RIESGO IDENTIFICADO	PROBALIDAD(P)				IMPACTO(I)				Px I	NIVEL DE RIESGO			
		BAJO	MEDIO	ALTO	MUY ALTO	BAJO	MEDIO	ALTO	MUY ALTO		BAJO	MEDIO	ALTO	MUY ALTO
		4	6	8	10	4	6	8	10		<24	32-40	48-64	80-100
Resguardó de información.														
Protección de seguridad.														
Desastre natural														

UNIVERSIDAD CÉSAR VALLEJO

DIMENSIÓN: RESPECTO A LOS PROGRAMAS

IDENTIFICACIÓN		EVALAUACION												
INDICAD.	RIESGO IDENTIFICADO	PROBALIDAD(P)				IMPACTO(I)				Px I	NIVEL DE RIESGO			
		BAJO	MEDIO	ALTO	MUY ALTO	BAJO	MEDIO	ALTO	MUY ALTO		BAJO	MEDIO	ALTO	MUY ALTO
		4	6	8	10	4	6	8	10		<24	32-40	48-64	80-100
Fuentes desconocidas														
Afectación viral a la información														
Restricciones de acceso														

UNIVERSIDAD CÉSAR VALLEJO

DIMENSIÓN: RESPECTO A PERSONAS

IDENTIFICACIÓN		EVALAUCION												
INDICAD.	RIESGO IDENTIFICADO	PROBALIDAD(P)				IMPACTO(I)				Px I	NIVEL DE RIESGO			
		BAJO	MEDIO	ALTO	MUY ALTO	BAJO	MEDIO	ALTO	MUY ALTO		BAJO	MEDIO	ALTO	MUY ALTO
		4	6	8	10	4	6	8	10		<24	32-40	48-64	80-100
Normas de seguridad														
Medidas preventivas														
Practica de valores														

INSTRUMENTO N° 02

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE IDENTIFICACIÓN Y EVALAUACION DE CAUSAS DE LOS RIESGOS TECNOLOGICOS

ÍTEMS	CAUSAS	IDENTIFICACION		EVALUACION							
				FRECUENCIA (F)			IMPACTO(I)				EFECTO
		SI	NO	A veces	Casi siempre	Siempre	Bajo	Moderado	Alto	Muy alto	F x I
				1	3	5	1	3	9	12	
A	Ausencia de capacitación técnica.										
B	No practica de valores institucionales.										
G	Incumplimiento de funciones.										
D	Deficiente coordinación interna.										
E	Deficiente supervisión.										
F	Inexistencia de mantenimiento preventivo.										
G	Inexistencia de registros de fallas.										

H	Ineficiente inspección.										
I	Sobrecarga de horas de trabajo.										
J	Inexistencia de restricciones de acceso a equipos.										
K	Inexistencia de restricciones de acceso a programas.										
L	Inseguridad de ambiente físico.										
M	Desactualizado plan de mantenimiento										
N	Desactualizado plan de seguridad informática										
O	Imprecisión de funciones en el área.										
P	Imprecisión responsabilidades en el área.										
Q	Deficiente gestión de mantenimiento										

INSTRUMENTO N° 03

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE ANÁLISIS DOCUMENTAL

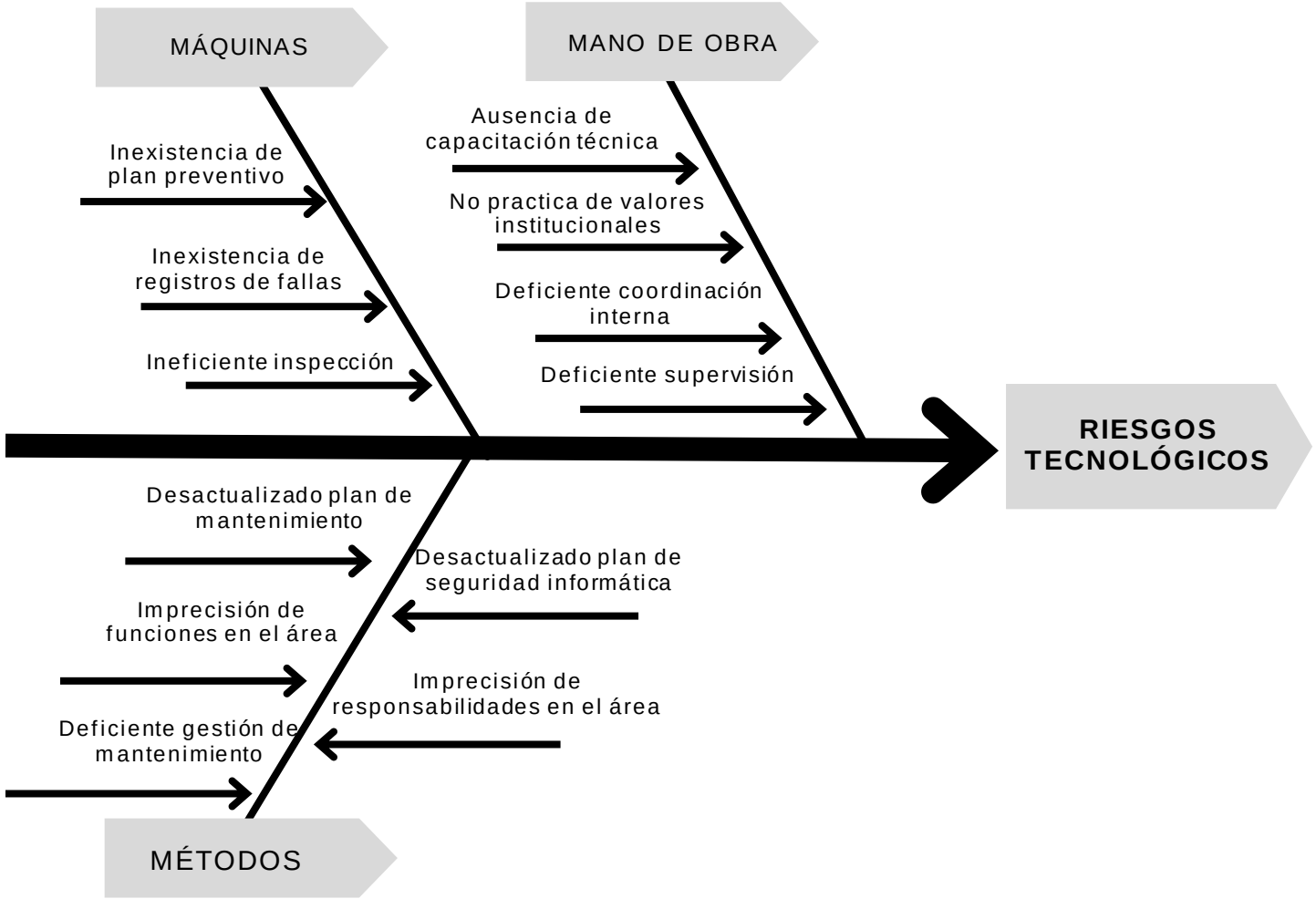
Objetivo: Evaluar la existencia y condición de documentos relacionados con el mantenimiento de equipos en el área de Tecnología de la Información en la empresa PROANCO

Fecha: …….

DOCUMENTO	EXISTENCIA/ CONDICIÓN			OBSERVACIONES
	NO	SI		
		DESACTUALIZADO	ACTUALIZADO	
Registro de fallas y averías.				
Registro de actividades de mantenimiento.				
Plan de mantenimiento.				
Normas de seguridad informática del área.				

Anexo 3: Diagrama Causa-Efecto

Diagrama Causa-Efecto de riesgos tecnológicos



Fuente. Diagrama Causa Efecto de riesgos tecnológicos

Anexo 4: Plan de prevención

1. **Denominación del plan:**

   Plan preventivo para disminuir riesgos tecnológicos.

2. **Justificación:**

   El plan de prevención fue planteado teniendo en consideración las 05 causas identificadas de mayor relevancia de los riesgos tecnológicos y las dimensiones consideradas. La intervención realizada se basó en 03 talleres de capacitación que buscó disminuir los riesgos tecnológicos actuando sobre las causas principales identificadas en relación con el tipo de riesgos o dimensiones respectivas: Bajo esas consideraciones, los talleres actuaron sobre las causas de los riesgos tecnológicos.

   Los riesgos respecto a equipos presentan las causas M, G, H.

   Los riesgos respecto a programas presentan la causa N.

   Los riegos respecto a personas presentan la causa A.

   De acuerdo a lo descrito, cada taller está orientado a cada uno de las dimensiones y a la vez, a las causas de los riesgos. Cada taller tuvo la duración promedio de 5 horas y fue dirigido al jefe del y trabajadores del área, así como al personal de mantenimiento.

Propósito:

3.1. Objetivos

3.1.1. General

Disminuir riesgos tecnológicos en el área de tecnología e información en la empresa PROANCO, Sullana.

Específicos

a. Disminuir riesgos tecnológicos respecto a los equipos.

b. Disminuir riesgos tecnológicos respecto a los programas.

c. Disminuir riesgos tecnológicos respecto a las personas.

3. Medidas de control

Indicador y formulas por objetivo planificado

Objetivo	Indicador	Forma de cálculo	Fuente de verificación
a	Disminución (%) de riesgos (DR)	% DR **Alto** = (%rRN Alto después) – (% NR Alto antes)	Matriz de identificación y evaluación de riesgos antes después
b		% DR **Medio**= (%rRN Medio después) – (% NR Medio antes)	
c		% DR **Bajo**= (%rRN Bajo después) – (% NR Bajo antes)	

4. Diseño de propuesta

4.1 Contenidos

Actividades	**CONTENIDOS**	**Horas**
Taller 1: "Mantenimiento preventivo"	- Análisis de riesgos. - Fundamentos. - Identificación y evaluación de riesgos de mantenimiento. - Identificación de causas de riesgos. - Planes de mantenimiento. - Prevención de riesgos. - Registro de fallas. - Inspección a procesos y procedimientos. - Utilización de data de fallas e inspecciones.	6

Taller 2: "Seguridad informática"	- Identificación y evaluación de riesgos de seguridad informática. - Identificación de causas de riesgos. - Planes de seguridad informática. - Implementación y supervisión de planes de seguridad.	5
Taller3: "Prevención de la calidad ambiental"	- Normas de seguridad personal en el trabajo. - Valores instituciones. - Práctica de valores institucionales.	4

4.2 Productos

Actividades	Productos
Taller 1: "Mantenimiento preventivo"	Jefe y trabajadores del área con habilidades empoderadas en análisis de riesgos, planes de mantenimiento, registro de fallas y utilización de data, así como inspecciones a procesos y procedimientos.
Taller 2: "Seguridad informática"	Jefe y trabajadores del área con habilidades empoderadas en análisis de riesgos, diseño, implementación y supervisión de planes de seguridad informática.
Taller3: "Prevención de la calidad ambiental"	Jefe y trabajadores del área con habilidades empoderadas para cumplir normas de seguridad y poner practica valores institucionales en el centro laboral (honestidad, respeto, lealtad, etc.).

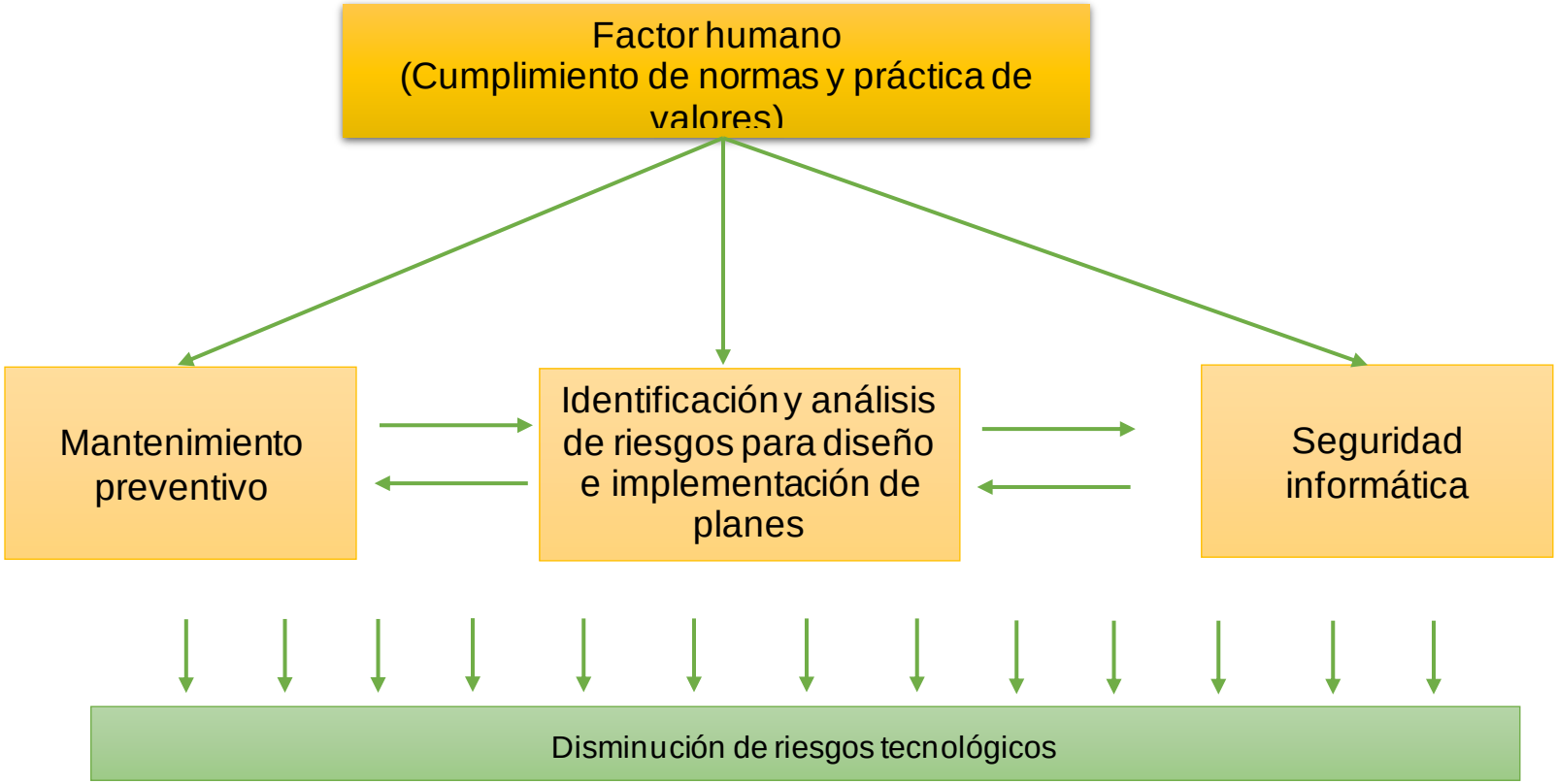
5. Actividades y tareas

Actividades y tareas realizadas

ACTIVIDAD	N°	TAREAS	Semanas Septiembre -2023 1 2 3 4
Taller 1			
	1	Empoderamiento de habilidades en análisis de riesgos y planes de mantenimiento.	
Evento 1: "Mantenimiento preventivo"	2	Empoderamiento de habilidades para registro de fallas y utilización de data.	
	3	Empoderamiento de habilidades para Inspecciones a procesos y procedimientos.	
Taller 2			
"Seguridad informática	1	Empoderamiento de habilidades en análisis de riesgos y planes de seguridad informática.	
	2	Empoderamiento de habilidades en implementación y supervisión de planes de seguridad informática.	
habilidades			
Evento 3: "Prevención de la calidad ambiental"	1	Empoderamiento de habilidades para cumplimiento de normas de seguridad, previo análisis de riesgos.	
	2	Empoderamiento de habilidades prácticas de valores institucionales en centro laboral.	

4.1 Síntesis gráfica del plan de prevención

Figura 7. Plan de prevención



Anexo 6: Evaluación por juicio de expertos

UNIVERSIDAD CÉSAR VALLEJO

Anexo 2

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "1: Matrices de identificación y evaluación de riesgos tecnológicos", "2: Matriz de identificación y evaluación de causas de los riesgos tecnológicos", "3: Ficha de análisis documental". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Walter Antenor del Carmen; Rosas Quintero
Grado profesional:	Maestría (x) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (x)
Áreas de experiencia profesional:	Producción; Mantenimiento; Logística; Distribución y Comercial
Institución donde labora:	Universidad César Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

Datos de la escala (Colocar nombre de la escala, cuestionario o inventario)

Nombre de la Prueba:	1. Matrices de identificación y evaluación de riesgos tecnológicos 2. Matriz de identificación y evaluación de causas de los riesgos tecnológicos 3. Ficha de análisis documental
Autora:	Local
Procedencia:	Local
Administración:	Local

INVESTIGA UCV

Tiempo de aplicación:	Continua
Ámbito de aplicación:	Local
Significación:	Matrices de identificación para identificar los riesgos tecnológicos.

3. Soporte teórico

(describir en función al modelo teórico)

Escala/ÁREA	Subescala (dimensiones)	Definición
Plan de mantenimiento preventivo	Diagnostico Planeación Inversión	Se realizará el diagnóstico, planearon e inversión del plan de mantenimiento mediante diagramas, fichas técnicas y guías de entrevista
Riesgos tecnológicos	Provenientes de equipos Provenientes de los programas Respecto a personas	Se evaluará equipos, programas y personas del área de tecnología mediante una ficha de análisis y evaluación de riesgos tecnológicos.

4. Presentación de instrucciones para el juez:

A continuación, a usted le presento los instrumentos 1.- Matriz de identificación y evaluación de riesgos tecnológicos provenientes de equipos, 2.- Matriz de identificación y evaluación de riesgos tecnológicos provenientes de programas. 3.- Matriz de identificación y evaluación de riesgos tecnológicos respecto a personas, 4.- Matriz de identificación y evaluación de causas de los riesgos tecnológicos, 5.- Ficha de análisis documental; elaborado por Víctor Joao Granda Pérez y Adrián Mora Gómez. en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.

COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento: 1.- Matrices de identificación y evaluación de riesgos tecnológicos, 2.- Matriz de identificación y evaluación de causas de los riesgos tecnológicos, 3.- Ficha de análisis documental

- Primera dimensión: Provenientes de Equipos
- Objetivos de la Dimensión: Identificar los riesgos provenientes de equipos

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Resguardo de información		4	4	4	-
Protección de seguridad		4	4	4	-
Desastre natural		4	4	4	-

- Segunda dimensión: Provenientes de los programas
- Objetivos de la Dimensión: Identificar los riesgos provenientes de programas

INDICADORES	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Fuentes desconocidas		4	4	4	-
Afectación viral a la información		4	4	4	-
Restricciones de acceso		4	4	4	-

- Tercera dimensión: Respecto a personas
- Objetivos de la Dimensión: Identificar los riesgos hacia las personas

INDICADORES	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones

Políticas de seguridad.		4	4	4	-
Normas de seguridad.		4	4	4	-
Medidas preventivas		4	4	4	-

Firma del Evaluador
DNI 02635722

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2 hasta 20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

UNIVERSIDAD CÉSAR VALLEJO

Anexo 2

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "1: Matrices de identificación y evaluación de riesgos tecnológicos", "2: Matriz de identificación y evaluación de causas de los riesgos tecnológicos", "3: Ficha de análisis documental". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Jelitza Airam Guerrero Purizaga
Grado profesional:	Maestría ( ) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Servicios, seguridad, calidad, docencia
Institución donde labora:	Universidad César Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	No

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

Datos de la escala (Colocar nombre de la escala, cuestionario o inventario)

Nombre de la Prueba:	1. Matrices de identificación y evaluación de riesgos tecnológicos 2. Matriz de identificación y evaluación de causas de los riesgos tecnológicos 3. Ficha de análisis documental
Autora:	Local
Procedencia:	Local
Administración:	Local

INVESTIGA UCV

Tiempo de aplicación:	Continua
Ámbito de aplicación:	Local
Significación:	Matrices de identificación para identificar los riesgos tecnológicos.

3. **Soporte teórico**

(describir en función al modelo teórico)

Escala/ÁREA	Subescala (dimensiones)	Definición
Plan de mantenimiento preventivo	Diagnostico Planeación Inversión	Se realizará el diagnóstico, planearon e inversión del plan de mantenimiento mediante diagramas, fichas técnicas y guías de entrevista
Riesgos tecnológicos	Provenientes de equipos Provenientes de los programas Respecto a personas	Se evaluará equipos, programas y personas del área de tecnología mediante una ficha de análisis y evaluación de riesgos tecnológicos.

4. **Presentación de instrucciones para el juez:**

A continuación, a usted le presento los instrumentos 1.- Matriz de identificación y evaluación de riesgos tecnológicos provenientes de equipos. 2.- Matriz de identificación y evaluación de riesgos tecnológicos provenientes de programas. 3.- Matriz de identificación y evaluación de riesgos tecnológicos respecto a personas, 4.- Matriz de identificación y evaluación de causas de los riesgos tecnológicos, 5.- Ficha de análisis documental; elaborado por Víctor Joao Granda Pérez y Adrián Mora Gómez, en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.

El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitemos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del Instrumento: 1.- Matrices de identificación y evaluación de riesgos tecnológicos, 2.- Matriz de identificación y evaluación de causas de los riesgos tecnológicos, 3.- Ficha de análisis documental

- Primera dimensión: Provenientes de Equipos
- Objetivos de la Dimensión: Identificar los riesgos provenientes de equipos

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Resguardo de información		4	4	4	-
Protección de seguridad		4	4	4	-
Desastre natural		4	4	4	-

- Segunda dimensión: Provenientes de los programas
- Objetivos de la Dimensión: Identificar los riesgos provenientes de programas

INDICADORES	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Fuentes desconocidas		4	4	4	-
Afectación viral a la información		4	4	4	-
Restricciones de acceso		4	4	4	-

- Tercera dimensión: Respecto a personas
- Objetivos de la Dimensión: Identificar los riesgos hacia las personas

INDICADORES	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Políticas de seguridad.		4	4	4	-

Normas de seguridad		4	4	4	-
Medidas preventivas		4	4	4	-

Firma del evaluador
DNI 72314886
CIP N° 311981

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

UNIVERSIDAD CÉSAR VALLEJO

Anexo 2

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "1: Matrices de identificación y evaluación de riesgos tecnológicos", "2: Matriz de identificación y evaluación de causas de los riesgos tecnológicos", "3: Ficha de análisis documental". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Sandy Xiomara Ramos Timaná.
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Sistemas de Gestión de Calidad Gestión Administrativa.
Institución donde labora:	UCV – Caña Brava
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	No

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

Datos de la escala (Colocar nombre de la escala, cuestionario o inventario)

Nombre de la Prueba:	1. Matrices de identificación y evaluación de riesgos tecnológicos 2. Matriz de identificación y evaluación de causas de los riesgos tecnológicos 3. Ficha de análisis documental
Autora:	Local
Procedencia:	Local
Administración:	Local
Tiempo de aplicación:	Continua

INVESTIGA UCV

Ámbito de aplicación:	Local
Significación:	Matrices de identificación para identificar los riesgos tecnológicos.

3. **Soporte teórico**

(describir en función al modelo teórico)

Escala/ÁREA	Subescala (dimensiones)	Definición
Plan de mantenimiento preventivo	Diagnostico Planeación Inversión	Se realizará el diagnóstico, planearon e inversión del plan de mantenimiento mediante diagramas, fichas técnicas y guías de entrevista
Riesgos tecnológicos	Provenientes de equipos Provenientes de los programas Respecto a personas	Se evaluará equipos, programas y personas del área de tecnología mediante una ficha de análisis y evaluación de riesgos tecnológicos.

4. **Presentación de instrucciones para el juez:**

A continuación, a usted le presento los instrumentos 1.- Matriz de identificación y evaluación de riesgos tecnológicos provenientes de equipos, 2.- Matriz de identificación y evaluación de riesgos tecnológicos provenientes de programas. 3.- Matriz de identificación y evaluación de riesgos tecnológicos respecto a personas, 4.- 2. Matriz de identificación y evaluación de causas de los riesgos tecnológicos, 5.- Ficha de análisis documental; elaborado por Víctor Joao Granda Pérez y Adrián Mora Gómez. en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.

	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento: 1.- Matrices de identificación y evaluación de riesgos tecnológicos, 2.- Matriz de identificación y evaluación de causas de los riesgos tecnológicos, 3.- Ficha de análisis documental

- Primera dimensión: Provenientes de Equipos
- Objetivos de la Dimensión: Identificar los riesgos provenientes de equipos

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Resguardo de información		4	4	4	—
Protección de seguridad		4	4	4	—
Desastre natural		4	4	4	—

- Segunda dimensión: Provenientes de los programas
- Objetivos de la Dimensión: Identificar los riesgos provenientes de programas

INDICADORES	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Fuentes desconocidas		4	4	4	—
Afectación viral a la información		4	4	4	—
Restricciones de acceso		4	4	4	—

- Tercera dimensión: Respecto a personas
- Objetivos de la Dimensión: Identificar los riesgos hacia las personas

INDICADORES	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Políticas de seguridad.		4	4	4	—

Políticas de seguridad.		4	4	4	
Normas de seguridad.		4	4	4	
Medidas preventivas		4	4	4	

Firma del evaluador
DNI 46773587
CIP 176911
Ing. Sandy Perez Tinoco

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/a18v39n02/18390217.pdf entre otra bibliografía.

Anexo 7: Constancia de Autorización de la empresa PROANCO

PROANCO

Sullana, 07 de Agosto de 2023

Señores
UNIVERSIDAD CESAR VALLEJO-FILIAL PIURA.
Facultad de Ingeniería y Arquitectura
Escuela Profesional de Ingeniería Industrial.

Yo, Bruno Sernaque Miguel Angel, identificado con DNI Nº 42826300, en mi calidad de Jefe del área de Tecnología de la Información de la empresa PROANCO SRL, autorizo al Sr. Granda Perez Victor Joao identificado con DNI N° 73087019, estudiante de la Universidad Cesar Vallejo, a utilizar el contenido recopilado de las matrices de identificación de riesgo para el desarrollo del Trabajo de Investigación denominado: "IMPLMENTACION DE PLAN PREVENTIVO PARA DISMINUIR RIESGOS TECNOLOGICOS EN EL AREA DE TECNOLOGIA DE LA INFORMACION EN LA EMPRESA PROANCO, SULLANA 2023"

Como condiciones contractuales, el estudiante se obliga a (1) no divulgar ni usar para fines personales la información (documentos, expedientes, escritos, artículos, contratos, y demás materiales) que, con objeto de la relación de trabajo, le fue suministrada, (2) no proporcionar a terceras personas, verbalmente o por escrito, directa o indirectamente, información alguna de las actividades y/o procesos de cualquier clase que fuesen observadas en la empresa durante la duración del proyecto y (3) no utilizar completa o parcialmente ninguno de los productos (documentos, metodología, procesos y demás) relacionados con el proyecto. El estudiante asume que toda información y el resultado del proyecto serán de uso exclusivamente académico.

El material suministrado por la empresa será la base para la construcción del estudio. La información y resultado que se obtenga del mismo podrían llegar a convertirse en una herramienta didáctica que apoye la formación de los estudiantes de la Escuela.

En caso de que alguna(s) de las condiciones anteriores sea(n) infringida(s), el estudiante queda sujeto a la responsabilidad por daños y perjuicios que cause.

Atentamente,

Miguel Angel Bruno Sernaque
DNI: 42826300
Jefe del área de Tecnología
de la Información