ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
PROGRAMA DE MAESTRÍA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN

Tesis

Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información de la Procesadora Tropical

Para optar el Grado Académico de Maestro en Ciencias con Mención en Tecnología de la Información

Autor:
Juan Ramos Estela
https://orcid.org/0009-0002-1117-1940

Asesor:
Ing. Dr. Alberto Alva Arévalo
https://orcid.org/0000-0002-8392-3542

Tarapoto, Perú

2023

ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
PROGRAMA DE MAESTRÍA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN

Tesis

Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información de la Procesadora Tropical

Para optar el Grado Académico de Maestro en Ciencias con Mención en Tecnología de la Información

Autor:
Juan Ramos Estela
https://orcid.org/0009-0005-9350-9635

Asesor:
Ing. Dr. Alberto Alva Arévalo
https://orcid.org/0000-0002-8392-3542

Tarapoto, Perú

2023

ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
PROGRAMA DE MAESTRÍA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN

Tesis

Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información de la Procesadora Tropical

Para optar el Grado Académico de Maestro en Ciencias con Mención en Tecnología de la Información

Autor:
Juan Ramos Estela

Sustentada y aprobado el 10 de noviembre de 2023, ante el honorable jurado:

Presidente de Jurado: Ing. Dr. Jorge Damián Valverde Iparraguirre	**Secretario de Jurado:** Ing. Dr. Juan Orlando Riascos Armas
Miembro de Jurado: Ing. Mg. Segundo Roger Ramírez Shupingahua	**Asesor:** Ing. Dr. Alberto Alva Arévalo

UNIVERSIDAD NACIONAL DE SAN MARTÍN

Escuela de Posgrado

ACTA DE SUSTENTACIÓN DE TESIS

Los Miembros del Jurado que suscriben, reunidos para estudiar y escuchar la sustentación y defensa del Trabajo de Tesis, modo presencial, presentado por:

Bach. Juan Ramos Estela

Con el asesoramiento del Ing. Dr. Alberto Alva Arévalo.

"Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical"

Teniendo en consideración los méritos del referido trabajo, así como los conocimientos demostrados por el sustentante, lo declaramos: APROBADO

MUY BUENO

Con el calificativo (*) DIECIOCHO (18)

En consecuencia, queda en condición de ser considerado APTO por el Consejo Universitario y recibir el Grado Académico de Maestro, de conformidad con lo estipulado en el Artículo 30° del Reglamento de Tesis de la Escuela de Posgrado de la UNSM.

Tarapoto, 10 de noviembre de 2023.

Ing. Dr. Jorge Damián Valverde Iparraguirre
Presidente

Ing. Dr. Juan Orlando Riascos Armas
Secretario

Ing. Mg. Segundo Roger Ramirez Shupingahua
Miembro

Ing. Dr. Alberto Alva Arévalo
Asesor

(*) De acuerdo con el Artículo 40° del Reglamento General de Ciencia, Tecnología e Innovación (RG - CTI) la Universidad Nacional de San Martín - Tarapoto, estas deberán ser calificadas con términos de: BUENO, MUY BUENO, EXCELENTE, también considerar la nota

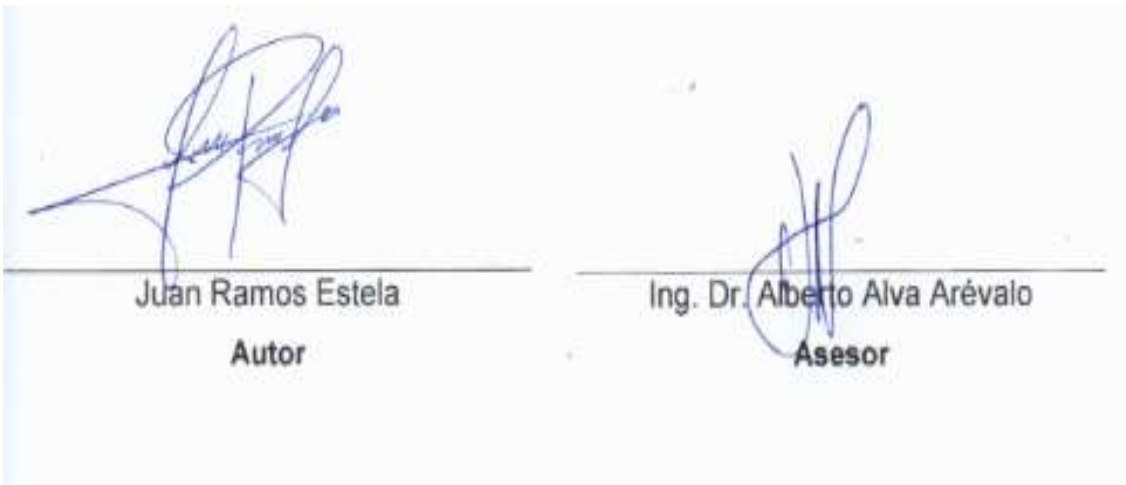
ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
PROGRAMA DE MAESTRÍA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN

Tesis

Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información de la Procesadora Tropical

Para optar el Grado Académico de Maestro en Ciencias con mención en Tecnología de la Información

El suscrito declara que el presente trabajo de tesis es original, en su contenido y forma



Tarapoto, Perú

2023

Declaratoria de autenticidad

Yo, Juan Ramos Estela, identificado con DNI N° 47094944, egresado de la Escuela de Posgrado de la Universidad Nacional de San Martín, Unidad de Posgrado de la Facultad de Ingeniería de Sistemas e Informática, Programa de Maestría en Ciencias con Mención en Tecnología de la Información, con la tesis titulada: **"**Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información de la Procesadora Tropical"

Declaro que:

Juro lo siguiente bajo pena de perjurio:

1. La tesis aportada es de nuestra autoría.
2. Las fuentes bibliográficas revisadas fueron debidamente citadas y referenciadas en la tesis.
3. La tesis no contiene material plagiado;
4. El material de esta investigación debe ser considerado como una contribución a la realidad investigada, ya que los datos ofrecidos en los resultados son auténticos y no han sido modificados ni copiados.

Por lo expuesto, acepto la responsabilidad por los resultados de mis actividades y me someto a las polticas vigentes de la Universidad Nacional San Martn-Tarapoto, as como a las leyes de mi nacin.

Tarapoto, 10 de noviembre de 2023.

Ficha de identificación

Título del proyecto Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical	**Área de investigación:** Ciencias de Sistemas e Informática **Línea de investigación:** Estrategias de tecnologías de información y comunicación (TIC) y sistemas constructivos convencionales y no convencionales para el desarrollo sostenible. **Sublínea de investigación:** No aplica **Grupo de investigación:** No aplica **Tipo de investigación:** Básica ☐ Aplicada ☒ Desarrollo experimental ☐

Autor: Juan, Ramos Estela	Facultad de Ingeniería de Sistemas e Informática Escuela Profesional de Ingeniería de Sistemas e Informática https://orcid.org/0009-0005-9350-9635

Asesor: Ing. Dr. Alberto Alva Arévalo	**Dependencia local de soporte:** Facultad de Ingeniería de Sistemas e Informática Escuela Profesional de Ingeniería de Sistemas e Informática Unidad o Laboratorio Ingeniería de Sistemas e Informática https://orcid.org/0000-0002-8392-3542

Dedicatoria

A Dios, en primer lugar, por concederme vida, salud y discernimiento para llegar a esta etapa crucial en mi desarrollo personal y profesional.

Siempre estaré agradecido a mis padres, Segundo Manuel Ramos Campos y María Yolanda Estela Alarcón, por ser la piedra angular de mi identidad personal y profesional y por su apoyo incondicional.

A mis hermanos, Leoncio y Cristian Max Ramos Estela, por su inquebrantable presencia y diversas formas de apoyo que me motivan a seguir adelante en cualquier circunstancia.

Agradecimiento

A Dios, que me concede la virtud de tener una familia unida, fuerte y ejemplar y poder vivir con su bendición.

Además de ser un tipo maravilloso y un profesional de excelencia, quiero agradecer personalmente al Ing. Dr. Alberto Alva Arévalo por ayudarme a culminar esta tesis.

Gracias a todo el cuerpo docente de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de San Martín (UNSM) por ser parte de mi formación profesional de posgrado.

A mis amigos y compañeros de formación académica, con quienes siempre he podido compartir mis conocimientos en la materia.

Índice general

Índice de tablas

Índice de figuras

RESUMEN

La presente investigación tuvo como objetivo estudiar los controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical. Correspondió a un estudio de tipo aplicada, enfoque cuantitativo, método deductivo, nivel descriptivo y diseño experimental de tipo preexperimental longitudinal. La población y muestra lo conformaron 36 trabajadores de la empresa. Como técnica de recolección de datos, se usó la encuesta y como instrumento fue el cuestionario. Los resultados muestran que, antes la usabilidad de la información era inadecuada con 61.1 %, después de los controles críticos pasó a ser adecuada con 88.9 %. Antes la seguridad era inadecuada con 69.4 %. Después, de los controles críticos pasó a ser adecuada con 88.9 %. Antes la fiabilidad era inadecuada con 55.6 %. Después de los controles críticos, pasó a ser adecuada con 86.1 %. Finalmente, se llegó a concluir que, los controles críticos de ciberseguridad generan un impacto significativo en el uso eficiente de la información en la procesadora tropical. Esto quedó demostrado tras aplicar la prueba estadística paramétrica *t – student* para muestras relacionadas. En donde, el valor p encontrado fue menor al nivel de significancia o margen de error permitido (0.000 < 0.05). De esta manera se comprobó que la gestión de los controles críticos de ciberseguridad tiene una influencia significativa en la eficiencia de la usabilidad de la información en la empresa.

Palabras clave: Gestión, controles críticos, ciberseguridad, información

ABSTRACT

The objective of this research was to study the critical cybersecurity controls and their impact on the efficient use of information at Procesadora Tropical. It corresponded to an applied study, with a quantitative approach, deductive method, descriptive level and longitudinal pre-experimental design. The population and sample consisted of 36 workers of the company. The survey was used as a data collection technique and the questionnaire as an instrument. The results show that, before the usability of the information was inadequate with 61.1 %, after the critical controls it became adequate with 88.9 %. Before, security was inadequate with 69.4 %, after the critical controls, it became adequate with 88.9 %. Previously, reliability was inadequate at 55.6 %, and after the critical controls, it became adequate at 86.1 %. Finally, it was concluded that critical cybersecurity controls have a significant impact on the efficient use of information in the tropical processor. This was demonstrated after applying the parametric statistical t - student test for related samples where the p-value found was lower than the permitted significance level or margin of error (0.000 < 0.05). Thus, it was proven that the management of critical cybersecurity controls has a significant influence on the efficiency of information usability in the company.

Keywords: Management, critical controls, cyber security, information

CAPÍTULO I
INTRODUCCIÓN A LA INVESTIGACIÓN

Al principio, toda la información quedaba como registro en documentos y memorias; sin embargo con el pasar del tiempo al ser tan extensa dicha información nace la necesidad de tener algún contenedor donde guardarlos, es aquí donde aparecieron los dispositivos de almacenamiento de memoria; y con el pasar de los años se ha implementado servidores de almacenamiento on premise y en la nube con el fin de soportar la gran cantidad de información que generan las empresas, estados, personas, instituciones, industrias y ahora también en la agricultura y otros sectores. Por tanto, es pertinente mencionar que actualmente existe abundante información y seguirá generándose en grandes cantidades; esta información puede ser tan valioso, tal es así que existen abundantes ataques informáticos, ingeniería social, phishing y demás técnicas que permiten vulnerar cualquier sistema y red para vender y traficar dicha información; en relación a lo mencionado es que ha desarrollado diversas técnicas, marcos y metodologías que permitan salvaguardar la información de forma adecuada.

La ISO 27001 es una norma estándar que respalda la Ciberseguridad mediante políticas, técnicas, y controles de seguridad; esta norma muestra el proceso completo a seguir si deseamos mantener una gestión adecuada de la información, esta ISO cuenta con 114 controles de seguridad; es aquí donde nace la pregunta ¿Cuánto impacta un control de seguridad en el uso de la información?; tratando de responder a esta pregunta clave como problema a razón de que la procesadora tropical genera información y como antecedente tuvo un incidente menor donde su información se vio comprometida y a manera de prevenir cualquier incidente de mayor magnitud, es que nos vemos en la necesidad de realizar una investigación que permita definir el impacto que genera los controles de seguridad considerando la los elementos de la triada CIA que son la privacidad, honestidad y accesibilidad en el uso de la información (Sandoval, 2020).

Foro Económico Mundial (2018), Los principales riesgos mundiales en 2017, según el informe sobre riesgos globales, estaban relacionados con la economía, la geopolítica, el medio ambiente, los ciberataques en curso y el robo de datos corporativos, que sigue siendo una amenaza importante a pesar de que los analistas informáticos advierten de que la frecuencia de estos ataques se ha duplicado en los últimos cinco años. El informe también señala que el impacto financiero de estos ciberataques podría aumentar, afectando potencialmente a particulares, empresas y entidades financieras. El ataque más grave de los cinco años anteriores se produjo en 2017, cuando el ransomware -software

infectado que compromete todos los datos y toma el control de la información almacenada lo que representó el 64 % de todos los correos electrónicos maliciosos.

WannaCry, que infectó 300.000 máquinas en 150 países, y NotPetya, que costó a las empresas afectadas 300 millones de dólares en pérdidas cada trimestre, fueron los ataques de ransomware más frecuentes. El uso de ciberataques para dañar infraestructuras vitales y sectores industriales importantes fue otra tendencia. (Pareja, 2020a), sin embargo, según el Informe de Seguridad de ESET, tres de cada cinco empresas en América Latina experimentaron al menos un problema de seguridad de red en 2017, y la mayoría de esos incidentes se produjeron en el nivel más alto de infección de códigos maliciosos. Además, el secuestro de información afectó al menos a una de cada cinco empresas (ESET, 2023).

Dada la importante evolución del ransomware, el Informe de Seguridad aconseja a las organizaciones estar constantemente atentas a las posibles debilidades importantes en su infraestructura TIC para evitar pérdidas imprevistas. Perú (25%), México (20%), Argentina (15%), Brasil (14%) y Colombia (10%) fueron los países latinoamericanos más afectados por estos ciberataques. Sin embargo, muchas empresas en América Latina y más allá optan por ignorar estos ciberataques y piensan que pueden resolverse pagando una extorsión, aunque la pérdida de datos sea un problema cada vez más peligroso que debemos evitar (Pareja, 2020b).

En América Latina a finales del 2018, los países más perjudicados por los ciberamenazas fueron: México (23,00%), Perú (14,00%) y Brasil (12,00%) (Pichihua, 2018). En base a ello, según el reporte de ESET (2020), indica que pasamos de las simples preocupaciones a los incidentes, los cuales ya son el reflejo de los ataques. Para ello, es fundamental comprender la frecuencia de los incidentes y gestionar adecuadamente los riesgos. Es con esta comprensión que podemos afirmar, basándonos en un análisis de los datos proporcionados por las organizaciones de toda América Latina, que el 60% de las empresas experimentaron al menos un incidente de seguridad informática, una cifra que se mantiene sin cambios desde el año anterior. La infección por código malicioso sigue manteniéndose como el suceso más frecuente, con 1 de cada 3 organizaciones reportando una infección por ransomware u otro código malicioso.

Cuando tanto el número de detecciones como la tasa de creación de nuevas variantes experimentaron un crecimiento exponencial en 2017, la actividad de la amenaza alcanzó un máximo histórico. Perú (25%) fue el país más afectado en la zona, con un tercio de las detecciones de ese año que se produjeron en ese continente. Andina (2018), reveló que, en términos de robo de información, a menudo conocido como ransomware o secuestro

de datos, Perú fue la nación blanco de más ataques de ransomware en América Latina en 2017 (ESET, 2019).

Los sistemas de Perú necesitan ser actualizados con frecuencia, lo que significa que tiene graves lagunas de ciberseguridad en sus TIC. Además, en la parte tecnológica de las normas de control aprobadas en 2006, tal como lo sugirió la (Contraloría General de la República [CGR], (2018), demuestra la necesidad de mejorar todas las herramientas de las TIC para eliminar riesgos; en consecuencia, los expertos en sistemas, informática y ciberseguridad deben adoptar medidas preventivas ante cualquier tipo de amenaza cibernética en entornos institucionales.

Como una de las naciones más impactadas por los ciberataques en 2019, Perú ocupa el puesto 40 a nivel mundial. Los archivos basura representan el 58,65% de estos ataques, seguidos de las amenazas web con el 43,60% y el correo infectado con el 22,32%. Según Kaspersky (2021), afirma que infecciones informáticas como Trojan Script Minergen, Trojan HTML Fraud gen y Analysis of Sender Attributes suelen estar dirigidas a empresas y organizaciones peruanas.

Analizando los datos presentados, es evidente que las empresas en los diversos países implementen controles de seguridad para la gestión y el uso adecuado de la información y contrarrestar los ataques informáticos, según ESET (2020) el Perú es el País que menos a implementado controles al año 2020, esto genera incertidumbre en las instituciones, que muy a menudo les cuesta invertir en seguridad.

De manera, que se llegó a formular el siguiente problema de investigación: ¿Cuánto impactan los controles críticos de ciberseguridad en el uso eficiente de la información en la procesadora tropical? De tal forma que este trabajo tuvo como objetivo general: Evaluar los controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical. Y como objetivos específicos: a) Analizar los controles críticos de ciberseguridad y su impacto en la usabilidad de la información en la Procesadora Tropical. b) Analizar los controles críticos de ciberseguridad y su impacto en la ciberseguridad de la Procesadora Tropical. c) Analizar los controles críticos de ciberseguridad y su impacto en la fiabilidad de la información en la Procesadora Tropical.

Después, la hipótesis general del estudio quedó definida como; Los controles críticos de ciberseguridad generan un efecto significativo en el uso eficiente de la información en la procesadora tropical. Mientras que las hipótesis específicas fueron; a) Los controles críticos de ciberseguridad generan un efecto significativo en la usabilidad de la información en la procesadora tropical. b) Los controles críticos de ciberseguridad generan un impacto

significativo en la ciberseguridad en la procesadora tropical. c) Los controles críticos de ciberseguridad generan un efecto significativo en la fiabilidad de la información en la procesadora tropical.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. A nivel internacional

Olivera (2019), dentro de su estudio el proceso de ejecución de un sistema de gestión de la ciberseguridad para mejorar la excelencia de la información proporcionada por los servicios de consultoría, aplicación en el CIGET Holguin. El objetivo era crear un proceso para implantar un sistema de gestión TI. Como tipo de metodología fue aplicada, su técnica de análisis fue la revisión documentaria, alineado con la ISO 27001; asimismo también usó la observación científica de procesos y resultados mediante entrevistas, observación directa aplicado a dos grupos. El autor concluye que los enfoques de ciberseguridad se encuentran implicados directamente con la excelencia de los servicios mediante los controles implementados; también menciona que mediante el procedimiento de ejecución del sistema de gestión de ciberseguridad se contribuye a la calidad de la información para esto especifica seis etapas importantes: dedicación, planificación, diagnóstico, diseño, documentación, manipulación, control y mejora; además este proceso permite demostrar la viabilidad y utilidad de la información elevando la cultura de la gestión de la ciberseguridad por parte de los trabajadores y que les ayude a desarrollar nuevas competencias y redefinir roles y responsabilidades de seguridad que permitiría además mantener un control e inventario de los activos de información de la organización.

Salazar (2018), en su tesis, el autor examina en qué medida los lideres de las empresas de la región citrícola de Nuevo León utilizan datos financieros para fundamentar sus decisiones. Su objetivo era conocer el grado y volumen de uso de los datos financieros en la toma de decisiones. La investigación utilizó una metodología cuantitativa, transversal, descriptiva y correlacional; aplica un muestreo no probabilístico por convivencia de la población de directivos, en su instrumento hace uso de una escala predeterminada y define que el uso de la información se da de acuerdo con las funciones y roles que se mantiene. El autor concluye que las evaluaciones de los gerentes sobre la aplicación de datos financieros y la toma de decisiones en la región citrícola de Nuevo León muestran una asociación distinta, fuerte, positiva y significativa, y que las percepciones de los gerentes sobre cómo se utiliza la información financiera están positivamente correlacionadas con el grado de toma de decisiones, muestra además que el grado de toma de decisiones percibido por los gerentes de las empresas de la región citrícola de Nuevo León fue influido

significativamente por la variable capacitación contable y financiera, lo que significa que quienes tienen capacitación toman mejores decisiones que quienes no la tienen.

Peñuela (2018), en su investigación tuvo el objetivo de proporcionar a las empresas colombianas un análisis global de la relevancia y las acciones requeridas para salvaguardar los activos de información, la investigación analiza e identifica el estado actual de la ciberseguridad, se centra en analizar el estado de la seguridad de las organizaciones en la actualidad. La información recopilada proviene de informes proporcionados por destacadas empresas de software de seguridad, revelando un aumento constante de los ataques cibernéticos, los cuales se ejecutan con mayor sofisticación y planificación. Esta situación pone de relieve lo vital que es educar al público en general sobre el valor de la seguridad, transformándola de una percepción de gasto a una comprensión más precisa, una inversión.

2.1.2. A nivel nacional

Jara (2018), en su investigación titulada “Sistema de gestión de la ciberseguridad para mejorar el procedimiento de gestión de riesgos de la administración local”. El objetivo principal era evaluar las repercusiones de la adopción de un sistema de gestión de la ciberseguridad en la gestión de los riesgos asociados a las TI. Su metodología de investigación es de tipo aplicada y mantiene un diseño cuasiexperimental, asimismo en esta investigación se toma un enfoque cuantitativo y la metodología aplicada es hipotético deductivo; Utilizando herramientas de observación directa para la recolección de información, el autor analiza y gestiona los riesgos según normas aceptadas e ISOS relacionados a la ciberseguridad, tal como la ISO 27001; El autor concluye afirmando que las comparaciones de grupos validan el procedimiento de Wilcoxon. Adicionalmente, el autor señala que la municipalidad distrital de Carabayllo en el 2018, el análisis y el cuidado del riesgo del gobierno local se ven significativamente impactados por la implementación de un sistema de gestión de la ciberseguridad

Vásquez (2023), en su búsqueda de la adecuación profesional Uso de plataformas OpenSource para ejecuctar el servicio de centro de operaciones de ciberseguridad (CYBERSOC) para instituciones financieras concluye que, como resultado de la introducción del (CyberSoc), mediante el uso de plataformas de código abierto en una entidad financiera, se logró abordar de manera efectiva la supervisión de plataformas, la gestión de vulnerabilidades, la respuesta a incidentes, la gestión y correlación de eventos, así como la gestión de análisis forense. En su investigación, descubrió que la mayoría de los casos denunciados se trataron el mismo día en que se envió el aviso. En conclusión, los clientes se benefician de una mayor seguridad de la plataforma mediante el uso del

servicio del centro de operaciones de ciberseguridad, que también ayuda a disminuir el riesgo de pérdida o corrupción de información al reducir la vulnerabilidad material.

Cáceda (2021), demuestra en su tesis, "Dynamic model for security management of information and communication technology infrastructure", cómo el uso de modelos en el ámbito de la seguridad ayuda a los responsables a tomar mejores decisiones, pues reduce el número de alertas generadas por diversas áreas, evidenciando su capacidad para proporcionar respuestas inmediatas ante posibles ataques y, lo que es aún más crucial, para prevenirlos. La evaluación de diferentes escenarios, respaldada por corridas y decisiones estratégicas, ha confirmado que la aplicación de este modelo, basado en la dinámica de sistemas, ha desempeñado un papel crucial en minimizar el número de vulnerabilidades, fortaleciendo así la postura de seguridad global.

2.1.3. Antecedentes locales

Ortiz (2018), en su informe de tesis “Controles de seguridad según ISO/IEC 27002:2013 para la mejora de la gestión de la seguridad de la información en la Universidad Nacional Agraria de la Selva (UNAS)”. Su objetivo fue mejorar la gestión de la ciberseguridad en la UNAS mediante la introducción de los controles de ciberseguridad descritos en la Norma ISO/IEC 27002:2013. Los controles fueron elegidos en base a un análisis situacional de la universidad en relación a la ciberseguridad, para posteriormente realizar una gestión de riesgos mediante el marco de trabajo MAGERIT, Emplea un diseño cuasiexperimental con una metodología de investigación aplicada, manteniendo un entorno controlado. Los instrumentos utilizados incluyen listas de control, escalas, hojas de observación, entrevistas y análisis estadístico no paramétrico. Los 24 controles se eligieron en función del diagnóstico realizado. Como resultado, se produjo un aumento global del 28 % al 34,0%, lo que, en resumen, representa un aumento del 6,0% en la implementación de controles de ciberseguridad. El autor concluye que el nivel de confianza en que la implantación de controles de seguridad conforme a la norma ISO/IEC 27002:2013 permite mejorar la gestión de la ciberseguridad. La implantación de controles estratégicos ha pasado del 12,0% inicial al 14,0%, y los controles operativos del 16,0% al 20%. En resumen, esto significa que se ha producido un incremento en la adopción de medidas de ciberseguridad del 6,0%, pasando del 0% al 20%; además, el enfoque MAGERIT permitió identificar y clasificar los activos de información en siete grupos, que son los siguientes: los procesos institucionales, los datos y la información, los sistemas y el software, el hardware y la infraestructura informática, los equipos auxiliares, el personal y la infraestructura física. También se dice que la detección de las vulnerabilidades de los activos de información permite identificar las debilidades internas que podrían ser

explotadas por las amenazas detectadas; El uso de sistemas operativos obsoletos, la falta de registros de acceso a zonas restringidas, el desconocimiento y formación del personal en cuestiones de seguridad de la información, la ausencia de un plan de mantenimiento de la infraestructura informática y el hardware, y la falta de políticas y procedimientos de seguridad fueron algunas de las vulnerabilidades detectadas con más frecuencia.

2.1.4. Fundamentos teóricos

2.1.5. Sector de estudio agricultura

La Agricultura, como parte de las industrias puede tener diversos enfoques, ya que cada producto puede tomar fines diferentes que finalmente son parte de la economía mundial, tal es así que (Grijpink et al., 2020), mencionan que la agricultura es parte de los dominios que mantienen un potencial significativo de la economía en el marco de la evolución de la conectividad global. Sin embargo, actualmente la agricultura se ha visto involucrada en la adopción de tecnologías de información para cumplir con diversas actividades en sus procesos, es por ello que actualmente se procesa información y se realiza una transformación digital organizacional.

Fiocco et al. (2021), mencionan que las empresas agrícolas participan en línea desde el principio y mantienen el compromiso durante todo el proceso de compra a través de canales digitales y físicos. Además, añaden que, por temas de comodidad de los mismos agricultores, los canales digitales han aumentado su uso con mayor énfasis desde aproximadamente el año 2018, provocando el uso de plataformas web, dispositivos móviles, equipos de TI, infraestructuras tecnológicas orientadas a la gestión y mejora de procesos que requieren automatización para el desarrollo de sus actividades y finalmente para la investigación y planificación.

2.1.6. Controles de Ciberseguridad

Los controles de ciberseguridad tienen como objetivo recomendar acciones a ejecutar a fin de que estas permiten salvaguardar la información dentro de cualquier organización, ya que actualmente la información es un activo muy potencial y valorado que permite en gran dimensión el crecimiento global.

La UNE-EN ISO/IEC 27002 (2017), describe detalladamente cómo se aplica un conjunto adecuado de controles para garantizar la ciberseguridad, incluidas las estructuras organizativas, los procesos, políticas, procedimientos y las funciones de hardware y software. Garantizar que la meta y la visión de la entidad están alineadas con la consecución de los objetivos empresariales y de seguridad específicos de la organización,

estos controles de seguridad deben desarrollarse, implantarse, supervisarse, revisarse y mejorarse según sea necesario.

La seguridad de la Información como tal, está enfocado en mantener la triada CIA dentro del flujo de trabajo y procesos organizacionales a fin de tener la certeza de que nuestros datos no sean expuestos a terceros.

Confidencialidad

Con esta expresión se designa la información a la que sólo tienen acceso las personas autorizadas; (Walkowski, 2019a), “La confidencialidad se refiere a los esfuerzos de una organización para mantener sus datos privados o secretos”. prever que sólo los usuarios autorizados puedan acceder a recursos específicos y que los usuarios no autorizados se mantengan activamente fuera del sistema o de la red constituye limitar el acceso a los datos para prevenir su divulgación no autorizada

Integridad

Es la capacidad de los datos para ser alterados sólo con permiso, (Walkowski, 2019b), es garantizar que la información es fidedigna y no ha sido alterada. Los clientes que compran por Internet, por ejemplo, esperan que la información sobre productos y precios sea correcta y que los datos sobre disponibilidad, cantidad y otros detalles no cambien una vez realizado el pedido. La integridad en su forma nos permite mantener la veracidad de la información ante cualquier petición o requerimiento.

Disponibilidad

Puesto que la información está disponible, las partes autorizadas deben poder acceder a ella, (Walkowski, 2019c) “la accesibilidad significa que las redes, los sistemas y las aplicaciones están en su pleno funcionamiento cotidiano, garantiza que los usuarios que se encuentra autorizados tengan acceso oportuno y fiable a los recursos cuando los necesiten”.

Según la (CNSS, 2015), al existir tantos controles de seguridad, estos en referencia al (NIST, 2014) menciona que, por la diversidad de controles de seguridad ya mencionados, se puede dividir en tres categorías siendo un total de 20 controles críticos de seguridad, sin embargo, también menciona que cada ejecutor de los controles los puede realizar según criterio establecido.

Controles de administración

Estos controles incluyen las medidas adoptadas para supervisar la creación, el mantenimiento y la aplicación de los sistemas; incluyen las políticas y los procesos que permiten el uso más eficaz de los recursos.

Controles operativos

Para asegurar los sistemas operativos y su entorno, estos controles ponen en práctica procedimientos y procesos estándar como la formación de concienciación, la gestión de la configuración y la respuesta a incidentes.

Controles técnicos

se centra en las salvaguardias de hardware y software utilizadas para preservar los sistemas informáticos TI y los datos a lo largo de su procesamiento, transmisión y almacenamiento. Por ejemplo, cifrado, métodos de autenticación y controles de acceso.

La definición de estos controles viene dada por numerosos organismos reguladores y normas, y aplicarlos todos es sumamente difícil. Como lo demuestra la norma ISO/IEC 27001:2013 (Indecopi, 2014), la norma NIST 800-53 revisión 4 (National Institute of Standards and Technology, 2014) describe 114 controles organizados en 35 objetivos de control, y el Center for Internet Security (CIS, Centro para la Seguridad en Internet) (CIS, 2021) describe los 20 controles críticos de seguridad con 171 subcontroles, es evidente que implementar adecuadamente los controles de ciberseguridad es un proceso complejo y multifacético. En relación con esto, el NIST recomienda 20 controles de ciberseguridad que podemos adoptar de forma centralizada, y se dividen tres categorías según criterio propio tal como lo recomiendan.

Controles de prevención y protección

En relación con el mismo nombre, refiere a los controles que podemos aplicar para prevenir riesgos, ataques y a través de ellos brindar seguridad y protección a nuestra red, sistemas e infraestructura de TIC que manejamos dentro de nuestra organización.

1. Inventario de Dispositivos y software Autorizados y no Autorizados
2. Configuración segura de hardware y software para ordenadores, portátiles, de sobremesa y servidores
3. El proceso continuo de identificar vulnerabilidades y corregirlas
4. Utilizar cuidadosamente los derechos administrativos
5. Cuidado, Monitorización y Análisis de LOGs de Auditoría
6. Protección del correo electrónico y los navegadores

7. Defensas Contra el Malware Avanzado de Correo Electrónico y del Navegador
8. Limitar y Controlar los Puertos de Red, Protocolos y Servicios
9. Capacidad de Recuperación de Datos
10. Configuraciones Seguras de Dispositivos de Red (Firewalls, Routers y Switches)
11. Defensa perimetral
12. Defensa de los Datos
13. Ingreso Basado en la Necesidad de Conocer (Need to Know)

Controles de Detección y monitorización

Son aquellos controles que permiten monitorear y detectar anomalías o posibles incidentes dentro de nuestra infraestructura y sistemas, estos controles trabajan en relación con los controles de prevención y los de recuperación.

14. Control de ingreso Wireless
15. Control y Monitorización de Cuentas de Sistema

Controles de recuperación y respuesta

Son aquellos controles que permiten mantener la continuidad de trabajo dentro de la organización y no vernos afectados de manera radical o por lo menos tener ventanas pequeñas de cortes de los servicios.

16. Verificación de las Habilidades de Seguridad y Formación Adecuada
17. Seguridad en el Ciclo de Vida de las Aplicaciones
18. Gestión y Respuesta a Incidentes
19. Realizar Test de Penetración y Ejercicios de Ataque

Por otra parte, según (Montesino, Fenz y Baluja, 2012) hace un troubleshooting de ese problema de seleccionar tantos controles, por lo que define algunos que son adaptables de forma que podamos automatizarlos:

- Inventario de activos (hardware y software)
- Gestión de cuentas y logs
- Monitoreo de sistemas y Protección contra malware
- Gestión de actualizaciones y escaneo de vulnerabilidades
- Verificación del cumplimiento y evaluación de seguridad
- Backup de información
- Seguridad física
- Gestión de incidentes

Coincidiendo con el NIST también existen muchas otras organizaciones, autores y diversos libros que se adaptan a dichos controles críticos para reforzar la ciberseguridad dentro de las organizaciones, sin embargo, el hecho de saber cuáles controles se debe implementar dependerá del ejecutor.

Manage Engine (2021), Los ataques más potentes y generalizados pueden evitarse con la ayuda de los Controles Críticos de Seguridad CIS, un conjunto priorizado y prescriptivo de mejores prácticas de ciberseguridad y medidas defensivas que también apoyan el cumplimiento en un mundo de marcos múltiples. Un equipo de especialistas en TIC desarrolló estas prácticas recomendadas para la ciberdefensa analizando datos de asaltos reales y sus contramedidas exitosas que solucionaron los puntos débiles. Los controles CIS proporcionan a las empresas una dirección precisa y una ruta bien definida para cumplir las metas y objetivos delineados por diversos marcos legales, reglamentarios y normativos.

Adaptar estos controles CIS puede ayudar directamente a:

- Formule un fundamento básico tanto para su programa de Ciberseguridad como para su estrategia general de seguridad.
- Concéntrese en aplicar las medidas técnicas más específicas y eficaces posibles para reforzar la postura defensiva de su empresa.
- Adhiérase a una estrategia de gestión de riesgos probada para la ciberseguridad que ha demostrado funcionar en el mundo real.
- Ajustarse fácilmente a otros marcos y regulaciones, incluidos NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, serie ISO 27000, PCI DSS, HIPAA, NERC CIP, y FISMA.

El uso eficiente de la información

Se refiere a la utilidad de la información como parte de la organización, la UNE-EN ISO/IEC 27002 (2017), demuestra que la información es más valiosa que las palabras escritas, las estadísticas y las imágenes. Los tipos intangibles de información incluyen conocimientos, conceptos, ideas y marcas. La información, junto con los sistemas, redes e infraestructuras tecnológicas que la soportan, así como las personas que la gestionan, operan y salvaguardan, son activos vitales para las operaciones de una organización y, como tales, deben protegerse frente a diversos riesgos. Esto es especialmente cierto en un mundo interconectado.

La información es un recurso muy importante dentro de cualquier organización, por ello el uso de la misma debe ser con tal seguridad. (Ortega, 2013), sostiene que el conocimiento

es una propiedad válida de cualquier mente razonable, incluso frente a limitaciones específicas como los secretos de Estado y los tipos tradicionales de conocimiento esotérico, y que esto no entra en conflicto con la necesidad de salvaguardar la propiedad intelectual. En cambio, En un mercado donde el valor depende de la escasez, la información puede comprarse y venderse como cualquier otra mercancía. El excesivo énfasis puesto en la información en lugar del conocimiento demuestra hasta qué punto el desarrollo de los modelos de la economía del conocimiento ha alterado nuestra relación con el conocimiento.

Usabilidad

se refiere al proceso de desarrollo de las operaciones organizativas internas mediante la utilización de la información, según la RAE se considera la facultad de obrar y las operaciones o tareas propias de una persona o entidad; a partir de ello definimos como actividades a la producción agrícola, transformación de alimentos, distribución y facturación. (ISO 9241-11, 1998), explica que la usabilidad es la eficacia, eficiencia y nivel de satisfacción con que un producto permite alcanzar determinados objetivos en relación con determinados usuarios en un contexto de uso concreto.

Seguridad

Los trabajadores son el capital humano de la organización; según la RAE “se define Persona que realiza una labor socialmente útil” por lo que se define como el uso de la información en los trabajadores de la procesadora tropical mediante sus roles o funciones Gerencia, Administración, Agricultores, Extensionistas, Empleados. (ISO/IEC 27000, 2018), Los protocolos de ciberseguridad incluyen esfuerzos continuos para detener el acceso ilegal, el uso, la divulgación, la perturbación, el cambio o la destrucción de datos y sistemas de información, mejores prácticas, técnicas ágiles y resistentes, así mismo la seguridad está relacionada directamente con la triada CIA.

Fiabilidad

Las acciones o secuencias de acciones emprendidas para alcanzar un objetivo se denominan procesos, según la RAE son “el conjunto de fases sucesivas de un fenómeno natural o de una operación artificial”, por lo que para este caso se refiere a los procesos a nivel Estratégico, Técnico y Operacional. Según la (ISO/IEC 27000, 2018) es la propiedad relacionada con el comportamiento y los resultados esperados y consistentes, esto nos quiere decir que debemos obtener los resultados requeridos.

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1. Ámbito de la investigación

3.1.1. Ubicación experimental

Esta investigación se realizó en:

País: Perú

Departamento: Ucayali

Provincia: Padre Abad

Distrito: Padre Abad.

3.2. Sistema de variables

Tras la identificación, conceptualización de las variables de estudio a la luz de los objetivos de la investigación, se obtuvieron los siguientes resultados:

- Causa: VI = Gestión de Controles críticos de ciberseguridad
- Efecto: VD= Uso eficiente de la información

Variable Independiente:

- X: Gestión de Controles críticos de ciberseguridad.

Variable Dependiente:

- Y: Uso eficiente de la información.

Tabla 1

Explicación de variables por objetivo específico 1

Objetivo específico N.º 1: Analizar los controles críticos de ciberseguridad y su impacto en la usabilidad de la información en la Procesadora Tropical.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Gestión de controles críticos de ciberseguridad	• Controles de prevención y protección • Controles de detección y monitorización • Controles de recuperación y respuesta	Ficha de observación	Cualitativa
Uso eficiente de la información	Usabilidad	Encuesta	Cuantitativa

Fuente: elaboración propia.

Tabla 2

Explicación de variables por objetivo específico 2

Objetivo específico N.º 2: Analizar los controles críticos de ciberseguridad y su impacto en la seguridad de la información de la Procesadora Tropical.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Gestión de controles críticos de ciberseguridad	• Controles de prevención y protección • Controles de detección y monitorización • Controles de recuperación y respuesta	Ficha de observación	Cualitativa
Uso eficiente de la información	Seguridad	Encuesta	Cuantitativa

Fuente: elaboración propia.

Tabla 3

Expliación de variables por objetivo específico 3

Objetivo específico N.º 3: Analizar los controles críticos de ciberseguridad y su impacto en la fiabilidad de la información en la Procesadora Tropical.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Gestión de controles críticos de ciberseguridad	• Controles de prevención y protección • Controles de detección y monitorización • Controles de recuperación y respuesta	Ficha de observación	Cualitativa
Uso eficiente de la información	Fiabilidad	Encuesta	Cuantitativa

Fuente: Propio del estudio.

3.3. Diseño de la investigación

3.3.1. Tipo y nivel de la investigación

El estudio se desarrolló de forma aplicada ya que viene ser el tipo de estudio en donde el personal investigador conoce la problemática y lo utiliza para responder a formulaciones plateadas de forma específica (Rodríguez, 2019). Mediante medidas cruciales de ciberseguridad, la investigación ofreció una solución al reto de la institución. El nivel de investigación fue descriptivo porque las variables se midieron dentro de la misma unidad de estudio (Sampieri et al., 2014).

3.3.2. Población y muestra

Población

En el ámbito del estudio a realizar, es la recopilación de todos los agentes o casos que se relacionan y mantienen características y otra serie de caracterizaciones. Todos ellos son empleados de la Tropical (Sampieri, 2014).

Muestra

Es un subconjunto o la esencia del universo poblacional; dicho de otro modo, es un subconjunto de la población que se caracteriza por una serie de características poblacionales y se corresponde con el conjunto (Sampieri, 2014). El tamaño de la muestra fueron 36 trabajadores, y para esta investigación fue determinado por muestreo no probabilístico, similar al tamaño población, por cuanto es una cantidad reducida. La selección de las

personas fue por juicio, ya que corresponde a quienes conocen el tema y manejan información, ya que no todos los usuarios pueden participar siempre en la investigación por su misma naturaleza de trabajo o según se haya evaluado previamente.

3.3.3. Diseño analítico, muestral y experimental

Experimental: De carácter pre - experimental haciendo uso del pretest y el post-test de un solo grupo experimental, mediante la cual se trabajó a la variable independiente para buscar en la variable dependiente un efecto o un comportamiento.

Para el análisis de los datos:

Los programas informáticos utilizados como tratamiento, observación de los datos fueron Microsoft Excel 2021 (estadística descriptiva) y SPSS v. 27 (estadística inferencial), la información fue presentada en tablas para su mejor interpretación.

Encontrar el contenido de los datos:

La media o promedio aritmético: Es la tendencia central más significativo y puede utilizarse para variables de cualquier nivel de medida, aunque las medidas de intervalo y de razón son las que más se benefician de él.

Dónde: X, media aritmética; X1, X2, X3, Xn conjunto de observaciones y n número total de los valores considerados.

$$\bar{X} = \frac{\sum_{i=1}^{n} x_i}{n}$$

La desviación estándar (S) es: Permite medir el grado de homogeneidad o heterogeneidad de los datos de la población estudiada. Es la media de las desviaciones o dispersiones de la puntuación respecto a la media o promedio. A medida que aumenta el grado de dispersión de los datos respecto a la media, aumenta también la desviación estándar, lo que indica un aumento de la heterogeneidad de la medición. Para hallar la desviación típica de una muestra de observaciones de datos, puede utilizarse la siguiente formula:

$$\mathbf{S} = \sqrt{\frac{\sum_{\mathbf{i=1}}^{\mathbf{n}} (\mathbf{X}_i - \bar{\mathbf{X}})^2}{\mathbf{n} - \mathbf{1}}}$$

Dónde: Xi, enésimo dato; $\bar{X}$, valor medio o media de la muestra, n, número de datos (de 1, 2, 3,…, n).

La varianza: Se define como la elevación al cuadrado de la desviación estándar, S2.

$$S^2 = \frac{\sum_{j=1}^{n} (X_j - \overline{X})^2}{n-1}$$

Para describir las diferencias entre grupos y variables:

Prueba *T-student* para datos apareados: Este tipo de prueba es ideal cuando se desea comparar las medidas de dos grupos con datos apareados.

$$t = \frac{\overline{X}_D - \mu_0}{s_D/\sqrt{n}}.$$

Dónde:

t = *T-student* calculada para datos apareados

$\bar{X}d$ = Media de las diferencias de las muestras apareadas.

μo= Media hipotética de la población para las diferencias.

SD= Desviación estándar de la muestra para las diferencias de las muestras apareadas.

n = Tamaño de la muestra.

No obstante, si los grupos a evaluar se distribuyen de acuerdo con la Ley Normal (criterio de Normalidad), también puede aplicarse a muestras mayores (n>100).

Pruebas de normalidad: Para utilizar la prueba t de Student, la variable cuantitativa de cada uno de los grupos que se comparan debe distribuirse de acuerdo con la Ley Normal. La significación estadística "p" se obtiene a partir de la prueba "Shapiro-Wilk", que fue la prueba de normalidad que se empleó. Esto significa que:

Si p >=0.05, p es no significativo, Se asume Normalidad.

Si p < 0.05, p es significativo, No se asume Normalidad.

3.4. Procedimientos de la investigación

3.4.1. Actividades del objetivo específico 1.

Objetivo específico 1: Analizar los controles críticos de ciberseguridad y su impacto en la usabilidad de la información en la Procesadora Tropical.

- Se evaluó en pretest el nivel de la percepción de los trabajadores con respecto a la usabilidad de la información en la Procesadora Tropical.
- Se implementó los controles críticos de ciberseguridad en la empresa Procesadora Tropical. (Evidencia de la implementación en Anexos).
- S evaluó en post test el nivel de la percepción de los trabajadores con respecto a la usabilidad de la información en la empresa procesadora Tropical.

3.4.2. Actividades del objetivo específico 2.

Objetivo específico 2: Analizar los controles críticos de ciberseguridad y su impacto en la seguridad de la información de la Procesadora Tropical.

- Se evaluó en pretest el nivel de la percepción de los trabajadores con respecto a la seguridad de la información en la Procesadora Tropical.
- Se incorporó los controles críticos de ciberseguridad en la empresa Procesadora Tropical. (Evidencia de la implementación en Anexos).
- S evaluó en post test el nivel de la percepción de los trabajadores con respecto a la seguridad de la información en la empresa procesadora Tropical.

3.4.3. Actividades del objetivo específico 3.

Objetivo específico 3: Analizar los controles críticos de ciberseguridad y su impacto en la fiabilidad de la información en la Procesadora Tropical.

- Se evaluó en pretest el nivel de la percepción de los trabajadores con respecto a la fiabilidad de la información en la Procesadora Tropical.
- Se implementó los controles críticos de ciberseguridad en la empresa Procesadora Tropical. (Evidencia de la implementación en Anexos).
- Se evaluó en post test el nivel de la percepción de los trabajadores con respecto a la fiabilidad de la información en la empresa procesadora Tropical.

3.5. Autorizaciones y permisos

Consentimiento informado de los trabajadores de la procesadora tropical. Y autorización de la alta dirección para la ejecución de la investigación.

3.6. Control ambiental y protocolos de bioseguridad

No aplicó.

3.7. Aplicación de principios éticos internacionales

La calidad ética de la investigación quedó garantizada por nuestro compromiso con las normas éticas nacionales e internacionales, y los datos se manejaron con responsabilidad.

Nos comportamos de forma ética y profesional. La información se mantuvo fiel a su integridad original. Se respetó la autonomía de los participantes y no se les perjudicó, ya que los resultados sólo se utilizaron por motivos académicos y los autores fueron referenciados y citados conforme a los acuerdos internacionales normales de la APA.

3.8. Nivel de implementación de controles

Se realizó inicialmente un análisis del estado de implementación de los controles, esto a través de una ficha de observación; asimismo después de gestionar e implementar a gran medida los controles se vuelve a tener la ficha del estado de implementación de los controles; cabe mencionar que va relacionado con el Pretest y el Post-test. El análisis realizado se trabajó en una escala de 0 a 5; donde el Nivel de Implementación varía según lo observado (1= no implementado, 2=implementación básica, 3=Implementación intermedia, 4=Implementación avanzada, 5=Implementación completada).

Tabla 4

Nivel de implementación de controles

Control	Pre-test	Pos-test
01	3	5
02	1	5
03	3	4
04	2	4
05	4	5
06	2	4
07	1	4
08	4	4
09	2	5
10	1	3
11	3	4
12	2	4
13	2	5
14	2	4
15	2	4
16	2	4
17	3	5
18	3	4
19	2	4
20	1	3

Fuente: Según resultados de observación de nivel de implementación de controles.

Interpretación

La Tabla 4 muestra la como se observa el nivel de implementación de controles para el pretest y en el post-test, donde la media del pretest des de 2.25 y en el post-test se tiene una media de 4.20

3.9. Gestión de controles

Se ha realizado el proceso de diagnóstico, implementación y gestión de los controles críticos de ciberseguridad según los recursos y la infraestructura que se tienen en la organización. A continuación, se presentan los 20 controles críticos desplegados para el uso eficiente de la información en la Procesadora Tropical. Los controles críticos están bajo la NIST (Instituto Nacional de Estándares y Tecnología), según las dimensiones identificadas.

Control 1: Inventario de Dispositivos Autorizados y no Autorizados

Se ha realizado el inventario de los equipos relacionados al área de TIC, mediante registros y usando herramientas en consola para obtener información de los equipos en red.

Dispositivos de red

- ✓ Router
- ✓ Switch L2/L3
- ✓ Access Point
- ✓ Radioenlaces
- ✓ Repetidor de radio

Hosts

- ✓ Desktop
- ✓ Laptop
- ✓ Teléfonos móviles
- ✓ Servidores
- ✓ Cámaras IP
- ✓ NVR/DVR
- ✓ Controladores de Balanza
- ✓ Controladores de Sistema de Panel Solar
- ✓ Repetidora
- ✓ Radio de comunicación
- ✓ Impresoras

Control 2: Inventario de Software autorizado y no autorizado

Se ha verificado mediante observación y mediante herramientas de consola las aplicaciones instaladas en los equipos, asimismo en los servidores.

- ✓ Registro de todos los software, sistemas y software
- ✓ Navegadores Web (Chrome, Brave y Mozilla)
- ✓ ERP Web
- ✓ Suite Ofimática
- ✓ Antivirus
- ✓ Sistema de control de peso
- ✓ Sistemas operativos (Windows, Windows Server, Ubuntu Server, CentOs)
- ✓ Sistemas de Facturación y Guías de remisión
- ✓ Aplicaciones de repositorio de archivos y transferencia: Dropbox
- ✓ Aplicaciones de planos: Google Heart, AutoCAD, ArcGIS
- ✓ Aplicaciones desktops de trabajo Open Source: Lectores de pdf, compresor de archivos, Visualizadores, software de asistencia remota.
- ✓ Gestión del software aprobado
- ✓ Gestión del software no aprobado
- ✓ Validar soporte de fabricante

Control 3: Configuraciones seguras de software y hardware para dispositivos móviles, portátiles, equipos de escritorio y servidores

- ✓ Inhabilitación de acceso remoto
- ✓ Configuración de usuarios estándar y usuario administrador
- ✓ Uso de Windows defender
- ✓ Acceso a todo dispositivo por credenciales
- ✓ Mantener imágenes seguras

Control 4: Proceso continuo de Identificación y remediación de Vulnerabilidades

- ✓ Configuración de controlador de dominio local
- ✓ Gestión de conexiones VPN adecuado con protocolo ptp
- ✓ Escaneo de puertos y vulnerabilidades
- ✓ Uso de certificados SSL/TLS locales y en la nube
- ✓ Parches y actualizaciones de Fimware y versiones

Control 5: Uso controlado de privilegios administrativos

- ✓ Uso de políticas de la suite de ofimática para usuarios administrativos
- ✓ Usuario administrador es el único que puede instalar aplicaciones
- ✓ Privilegios restringidos en usuarios administrativos, logs
- ✓ Contraseñas únicas y validas
- ✓ Separación de cuentas administrativas
- ✓ Uso de equipos dedicados
- ✓ Gestionar grupos administrativos y operativos

Control 6: Protección del correo electrónico y del navegador

- ✓ Gestión de Spam y bloqueo en los navegadores
- ✓ Uso de navegadores con soporte activo
- ✓ Gestión adecuada de pluggins en navegador y cliente correo
- ✓ Deshabilitar lenguajes de scripting en navegadores y cliente correo
- ✓ Bloqueo de URL's a nivel de resolución de DNS
- ✓ Configuración para evitar correos de orígenes ya identificados como no admisibles.
- ✓ Registros de las URL's y DNS
- ✓ Uso de técnicas Sandbox para archivos sospechosos

Control 7: Defensas contra el Malware avanzado de correo electrónico y del navegador

- ✓ Gestión para implementación de Harmony Email & Collaboration (Checkpoint)

Control 8: Seguridad en el ciclo de vida de las aplicaciones

- ✓ Actualizaciones de versiones
- ✓ Inclusión al equipo de desarrollo (Pruebas unitarias estática y dinámica y DevSecOps)
- ✓ Validación de soporte de aplicaciones
- ✓ Usar aplicaciones actualizadas y de confianza
- ✓ Uso de algoritmos de cifrado
- ✓ Entorno PreProd, y Prod (En futuro Certificación)
- ✓ Uso de plantillas seguras en el desarrollo

Control 9: Configuraciones seguras de dispositivos de red (Firewalls, Routers y Switches)

- ✓ Configuración de VLAN’s
- ✓ Configuración de red jerárquica
- ✓ Encriptado de tráfico de contraseñas
- ✓ Actualizaciones de Fimware
- ✓ Uso de equipo dedicado

Control 10: Defensa perimetral

- ✓ Firewall a nivel de capa 7 (Reglas, ACL)
- ✓ Segmentación de red (LAN, WAN, DMZ)
- ✓ Bloqueo de direcciones IP
- ✓ Uso de IDS
- ✓ Uso de Proxy
- ✓ Gestión de dispositivos remotos

Control 11: Protección de los datos

- ✓ Acceso por credenciales
- ✓ Inventario de información sensible
- ✓ Acceso controlado en red
- ✓ Uso de BitLocker
- ✓ Gestión controlada de dispositivos de memoria externa
- ✓ Gestionar permisos de escritura y lectura

Control 12: Acceso basado en la necesidad de conocer (Need to Know)

- ✓ Uso de políticas para autenticación de doble factor
- ✓ Listas de control de acceso

Control 13: Control de acceso Wireless

- ✓ Uso de Wireless LAN Controller
- ✓ Autenticación a redes Wi-Fi por contraseñas y red oculta
- ✓ Registro y control mediante ARP, DHCP.
- ✓ Puntos de acceso gestionados
- ✓ Uso de protocolos WPA2

Control 14: Limitar y controlar los puertos de red, protocolos y servicios

- ✓ Inhabilitación de puertos por defecto
- ✓ Cambio de puertos (Uso de puertos no conocidos)
- ✓ Configuración y uso de protocolos y servicios seguros

Control 15: Mantenimiento, monitorización y análisis de LOGs de auditoría

- ✓ Uso de Wireshark para analizar monitorear tráfico
- ✓ Uso de dude para monitorear equipos
- ✓ Logs en los dispositivos
- ✓ Visualización de eventos en PowerShell
- ✓ Uso de protocolo SNMP y Syslog para monitoreo
- ✓ Documentación de políticas

Control 16: Gestión y respuesta a incidentes

- ✓ Concientizar el reportar eventos fuera de rutina
- ✓ Bloqueo de salida por el ISP en caso de infección por Malware
- ✓ Uso de la nube (Según nivel del incidente) para dar continuidad de trabajo
- ✓ Documentación de incidentes y remediación
- ✓ Asignación de responsabilidades ante incidentes

Control 17: Capacidad de recuperación de datos

- ✓ Backup de archivos
- ✓ Backup de configuraciones
- ✓ Backup de DB
- ✓ Puntos de restauración
- ✓ Gestión de Imágenes
- ✓ Uso de la nube sincronizado

Control 18: Control y monitorización de cuentas de sistema

- ✓ Privilegios de usuarios
- ✓ Accesos según rol de usuarios, logs
- ✓ Inventario de autenticaciones
- ✓ Autenticación multi factor
- ✓ Deshabilitar cuentas de usuarios retirados
- ✓ Bloqueo de sesiones de trabajo por inactividad
- ✓ Restringir intentos de acceso

Control 19: Verificación de habilidades de seguridad y formación adecuada

- ✓ Gestión de acceso por lectores de huellas a las instalaciones
- ✓ Charlas en seguridad informática básica e ingeniería social
- ✓ Concientizar el reportar eventos fuera de rutina
- ✓ Incentivar al uso adecuado de datos sensibles

Control 20: Realizar Test de penetración y ejercicios de ataque

- ✓ Pruebas de acceso
- ✓ Escaneo de puertos
- ✓ Realizar explotado de vulnerabilidades

CAPÍTULO IV
RESULTADO Y DISCUSIÓN

4.1. Resultado objetivo específico 1

Objetivo: estudiar los controles críticos de ciberseguridad y su impacto en la usabilidad de la información en la Procesadora Tropical.

Tabla 5

Usabilidad de la información antes y después de la gestión de controles críticos.

Calificación	Antes		Después	
	Cantidad	Porcentaje	Cantidad	Porcentaje
Deficiente	22	61.1	0	0.00
Regular	14	38.9	4	11.1
Eficiente	0	0	32	88.9
Total	**36**	**100 %**	**36**	**100 %**

Fuente: Según resultados del cuestionario.

Interpretación

En la tabla 5 compara la usabilidad de la información sin gestión de controles críticos y con gestión de controles críticos según la percepción de los trabajadores de la procesadora tropical. Antes, la usabilidad era deficiente, representada por la opinión del 61.1 % (22) de los trabajadores, seguido de un nivel regular, la cual estaba representada por el 38.9 % (14) de los trabajadores, ninguno de ellos (trabajadores) vieron al proceso de usabilidad de la información como eficiente. En tanto, después de la gestión de los controles críticos de ciberseguridad que se desarrolló, mejoró la percepción de los trabajadores con respecto al proceso de usabilidad de la información, ya que para el 88.9 % (32) de los trabajadores pasó a ser percibido como eficiente, en tanto, para el 11.1 % (4) lo vieron como regular todavía.

4.2. Resultado objetivo específico 2

Objetivo 2: Analizar los controles críticos de ciberseguridad y su impacto en la seguridad de la información de la Procesadora Tropical.

Tabla 6

Seguridad de la información antes y después de la gestión de controles críticos.

Calificación	Antes		Después	
	Cantidad	Porcentaje	Cantidad	Porcentaje
Deficiente	25	69.4	0	0.00
Regular	11	30.6	4	11.1
Eficiente	0	0	32	88.9
Total	**36**	**100 %**	**36**	**100 %**

Fuente: Según resultados del cuestionario.

Interpretación

Los datos de la tabla 6 compara la seguridad de la información sin gestión de controles críticos y con gestión de controles críticos según la percepción de los trabajadores de la procesadora tropical. Antes, la seguridad era deficiente, representada por la opinión del 69.4 % (25) de los trabajadores, seguido de un nivel regular, la cual estaba representada por el 30.6 % (11) de los trabajadores, ninguno de ellos (trabajadores) vieron a la ciberseguridad como eficiente. En tanto, después de la gestión de los controles críticos de ciberseguridad que se desarrolló, mejoró la percepción de los trabajadores con respecto a la seguridad de la información en la empresa, ya que para el 88.9 % (32) de los trabajadores pasó a ser percibido como eficiente, en tanto, para el 11.1 % (4) lo vieron como regular todavía. En este caso, no hubo ningún trabajador que consideró a la seguridad como inadecuada o deficiente. Lo que demuestra que tras aplicar de manera adecuada la gestión de los controles críticos hubo una mejora positiva en el pensar de los trabajadores, pasando a tener mayor confianza sobre la seguridad de la información en la empresa.

4.3. Resultado objetivo específico 3

Objetivo 3: Analizar los controles críticos de ciberseguridad y su impacto en la fiabilidad de la información en la Procesadora Tropical.

Tabla 7

Fiabilidad de la información antes y después de la gestión de controles críticos.

Calificación	Antes		Después	
	Cantidad	Porcentaje	Cantidad	Porcentaje
Deficiente	20	55.6	0	0.00
Regular	16	44.4	5	13.9
Eficiente	0	0	31	86.1
Total	**36**	**100.00%**	**36**	**100.00%**

Fuente: Según datos procesados en SPSS v27

Interpretación

En la tabla 7 compara la fiabilidad de la información sin gestión de controles críticos y con gestión de controles críticos según la percepción de los trabajadores de la procesadora tropical. Antes, la fiabilidad era visto como deficiente, representada por la opinión del 55.6 % (20) de los trabajadores, seguido de un nivel regular, la cual estaba representada por el 44.4 % (16) de los trabajadores, ninguno de ellos (trabajadores) vieron a la fiabilidad de la información como adecuada o eficiente. En tanto, después de la gestión de los controles críticos de ciberseguridad que se desarrolló, mejoró la percepción de los trabajadores con respecto a la fiabilidad de la información en la empresa, ya que para el 86.1 % (31) de los trabajadores pasó a ser percibido como eficiente, en tanto, el 13.9 % (5) lo vieron como regular todavía. En este caso, no hubo ningún trabajador que consideró a la fiabilidad como inadecuada o deficiente. Lo que demuestra que tras aplicar de manera adecuada la gestión de los controles críticos hubo una mejora positiva en el pensar de los trabajadores, pasando a tener mayor confianza sobre la fiabilidad de la información en la empresa.

4.4. Resultado objetivo general.

Objetivo general: Estudiar los controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical.

Descriptivos de la usabilidad de la información

Tabla 8

Usabilidad de la información antes y después de la gestión de controles críticos

Calificación	Antes		Después	
	Cantidad	Porcentaje	Cantidad	Porcentaje
Deficiente	35	97.2	0	0.00
Regular	1	2.8	4	11.1
Eficiente	0	0	32	88.9
Total	**36**	**100 %**	**36**	**100 %**

Fuente: Datos propios del estudio

Interpretación

Los datos de la tabla 8 muestran los descriptivos de cómo era la usabilidad de la información antes y después de la gestión de controles críticos de ciberseguridad en la procesadora Tropical vista o entendida desde la percepción de los trabajadores. Antes, los trabajadores lo vieron como deficiente con 97.2 % (35), seguido de regular con 2.8 % (1). Después, para mejora de la empresa, la percepción de los trabajadores mejoró considerablemente, ya que la usabilidad pasó a ser eficiente con 88.9 % (32), mientras que un pequeño grupo de trabajadores todavía opinaba que la usabilidad de la información es regular con 11.1 % (4).

Tabla 9

Prueba de normalidad.

Variable	Shapiro-Wilk		
	Estadístico	gl	Sig.
Diferencia (Uso eficiente después – Uso eficiente antes)	,975	36	,562

Fuente: Según datos procesados en SPSS v27.

Interpretación

En la tabla 9, el nivel de significancia para la variable generada de la diferencia entre los valores encontrados de la variable uso eficiente de la información después menos el uso eficiente antes, es igual a 0.562, valor superior a 0.05, por lo tanto, se demuestra que los datos tienen distribución normal, por lo que se hace aplicable la prueba paramétrica *t – student* para comparar la media de ambos casos.

Prueba de hipótesis:

Ho: Los controles críticos de ciberseguridad generan un impacto significativo en el uso eficiente de la información en la procesadora tropical.

Ha: Los controles críticos de ciberseguridad generan un impacto significativo en el uso eficiente de la información en la procesadora tropical.

Nivel de significación:

El nivel de significancia teórica es α = 0,05, correspondiente al nivel de confiabilidad del 95%.

Regla de decisión

Si Valor p > 0.05, se acepta la Hipótesis Nula (Ho)

Si Valor p < 0.05, se acepta la hipótesis alterna (Ha).

Tabla 10

Prueba t – student para muestras emparejadas.

		Diferencias emparejadas					t	gl	Sig. (p - valor)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior	Superior			
Par 1	Uso eficiente de la información (Después) - Uso eficiente de la información	24,778	3,457	,576	23,608	25,947	43,007	35	,000

Fuente: Datos procesados por el software SPSS v27

Interpretación

Los datos de la tabla 10 muestra que existió una diferencia de 24.778 puntos entre la valoración del uso eficiente de la información después y el uso eficiente antes, además, No hay ningún cero en los datos desde el límite inferior hasta el límite superior, por lo que es evidente que ambas muestras no son iguales, es decir, son diferentes. Ahora, al comparar el nivel de significancia encontrado, la cual es igual a 0.000 con el margen de error 5 % (0.05), nos damos cuenta que es menor, es decir, (0.000 < 0.05) por consiguiente, cumpliendo con la regla de decisión, queda negada la hipótesis nula y aceptada la hipótesis del estudio, en donde, se puede afirmar que hay evidencias estadísticas suficientes que demuestran que los controles críticos de ciberseguridad generan un impacto significativo en el uso eficiente de la información en la procesadora tropical.

Para contextualizar, los resultados estadísticos del estudio indicaron que el material de Procesadora Tropical era más utilizable cuando los controles cruciales de ciberseguridad se gestionaban adecuadamente. Antes, según la percepción de los trabajadores de dicha empresa, tuvieron niveles muy bajos en cuanto a la eficiencia del uso de la información según sus dimensiones de usabilidad, seguridad y fiabilidad. En todos, la opinión de los trabajadores era negativa. La usabilidad de la información era inadecuada con 61.1 %, después de eso, era regular con 38.6 %. Ningún trabajador llegó a considerar como bueno o adecuado a la usabilidad de la información en la empresa. De la misma manera sucedió con la seguridad, en la que se observó un problema gigante al demostrar que la percepción de los trabajadores era negativa, predominando una seguridad de nivel bajo con 69.4 %, seguida de un nivel regular con 30.6 %. Finalmente, la dimensión fiabilidad corrió con la misma tendencia, el nivel era muy bajo, más de la mitad de los trabajadores lo evaluaron como inadecuada (55.6 %), seguida de un nivel regular con 44.4 %. Durante este periodo, se evidenció claridad en la descripción del problema, ya que, a nivel general, la usabilidad de la información fue inadecuada, llegando a ser representado por el 97.2 % de los trabajadores, solo el 2.8 % pensó que era regular.

Después de todo esto, se implementó la gestión de los controles críticos de ciberseguridad en la empresa, la cual fue desarrollado justamente para mejorar los niveles bajos de usabilidad, seguridad y fiabilidad, y de esta manera, los trabajadores tengan un mejor panorama y seguridad al momento de trabajar con los datos que se generan en la empresa. Al respecto de esto, Mercado (2016), autor que tuvo que elaborar un modelo de gestión de ciberseguridad. El citado autor identificó 8 modelos, de las cuales pudo identificar 8 elementos importantes para generar un modelo que pudiese gestionar de manera eficiente la información, además, de la selección adecuada de los controles críticos para mitigar los riesgos existentes en una organización.

Tras volver a evaluar, los resultados tuvieron una mejora significativa en las tres dimensiones. En donde, a nivel de la usabilidad, la mayoría de los trabajadores 88.9 % lo calificaron como adecuada, mientras que solo el 11.1 % lo calificaron como regular. Sucedió algo similar con la dimensión seguridad, pues, la mayoría de los trabajadores tuvieron una percepción positiva, ya que el 88.9 % de los trabajadores evaluaron a la seguridad como adecuada, igual que con la anterior dimensión, el 11.1 % calificaron como regular. Finalmente, la fiabilidad no se quedó atrás y también mejoró considerablemente, ya que el 86.1 % de los trabajadores lo evaluaron como adecuada, llegando a haber solo el 13.9 % quienes lo evaluaron como regular. En términos generales, la usabilidad de la información en la empresa fue adecuada, llegando a percibirlo así el 88.9 % de los trabajadores, mientras que para el 11.1 % todavía era regular.

Después de presentar los descriptivos, en lo inferencial y de acuerdo a la prueba estadística paramétrica *t – student*, se demostró que existió evidencia científica en el estudio con lo que no quedó más que confirmar y aceptar la hipótesis del estudio, con lo que finalmente se infiere que la gestión de los controles críticos de ciberseguridad influyó de manera significativa en el uso eficiente de la información en la empresa Procesadora Tropical en el año. Esto después de que, al procesar los datos, el valor p estuvo por debajo del nivel de significa, es decir, (0.000 < 0.05). Resultados que guardan relación con la investigación de Olivera (2019), quien estudio el efecto de la gestión de la ciberseguridad en la calidad de la información en una empresa consultora, el autor llegó a concluir que la gestión de los enfoques de la ciberseguridad influyó positivamente en la calidad de la información, lo explicó basándose en los hallazgos positivos encontrados sobre la mejora del compromiso, diagnóstico, operación, control y mejora. Con esto, el autor demostró viabilidad y utilidad de la información consiguiendo elevar la cultura de la gestión de la ciberseguridad en los trabajadores y así en la organización.

Salazar (2018), que realizó una investigación sobre el impacto de la utilidad de la información en la toma de decisiones de las empresas. El autor llegó a la conclusión de que la toma de decisiones se ve influida por la utilidad de la información, llegando a justificar que, a mayor eficiencia en el uso de la información, incrementa la probabilidad de que la decisión adoptada por los usuarios o tomadores de decisiones sea la correcta y ayude a la organización a generar mayores beneficios. Al respecto, en el estudio de Jara (2018), autor que tuvo la responsabilidad de evaluar la influencia de un sistema de gestión de ciberseguridad en el proceso de la gestión del riesgo en una institución gubernamental. Después de haber realizado las activades correspondientes a la implementación del sistema de gestión de seguridad, estudió su impacto en la evaluación de los riesgos, llegando a concluir que a través de la estadística inferencial no paramétrica denominada Wilcoxon, que definitivamente, existe influencia significativa, con esto, pudo demostrar que el sistema de gestión de ciberseguridadd es un activo clave y muy trascendental para que se gestione de manera correcta los riesgos existentes en una organización.

CONCLUSIONES

Las medidas importantes de ciberseguridad tienen una gran influencia en el buen uso de la información por parte del procesador tropical. Tras utilizar la prueba estadística paramétrica t-student para muestras relacionadas, esto quedó demostrado. El valor p descubierto fue inferior al margen de error o nivel de significación permitido (0,000 < 0,05). Así, se estableció que la efectividad de la usabilidad de la información dentro de la organización se ve significativamente impactada por la administración de importantes controles de ciberseguridad.

Antes de la gestión de controles críticos de ciberseguridad la usabilidad de la información en la empresa procesadora Tropical era inadecuada, valorada así por el 61.1 % de los trabajadores, seguido de una percepción regular por el 38.9 % (14) trabajadores. Después, hubo una mejora significativa, ya que la mayoría de los trabajadores tuvieron una percepción positiva sobre la usabilidad, ya que para el 88.9 % (32) pasó a ser adecuada, mientras que para el 11.1 % regular. De esta manera si hubo un impacto positivo en la usabilidad a causa de la gestión de los controles críticos.

Antes de la gestión de controles críticos de ciberseguridad la seguridad de la información en la empresa procesadora Tropical era inadecuada, valorada así por el 69.4 % de los trabajadores, seguido de una percepción regular por el 30.6 % (11) trabajadores. Después, hubo una mejora significativa, ya que la mayoría de los trabajadores tuvieron una percepción positiva sobre la seguridad, ya que para el 88.9 % (32) pasó a ser adecuada, mientras que para el 11.1 % regular. De esta manera si hubo un impacto positivo en la seguridad de la información, a causa de la gestión eficiente de los controles críticos.

Antes de la gestión de controles críticos de ciberseguridad la fiabilidad de la información en la empresa procesadora Tropical era inadecuada, valorada así por el 55.6 % de los trabajadores, seguido de una percepción regular por el 44.4 %. Después, la mayoría de los trabajadores tuvieron una percepción positiva sobre la fiabilidad, ya que para el 86.1 % (31) pasó a ser adecuada, mientras que para el 13.9 % regular. De esta manera si hubo un impacto positivo en la fiabilidad de la información, a causa de la gestión eficiente de los controles críticos.

RECOMENDACIONES

Al gerente general de la empresa Procesadora Tropical se le recomienda desarrollar e implementar nuevas estrategias de seguridad de la información conforme los riesgos vayan aumentando y la tecnología vaya transformándose también. Esto para que la empresa siempre esté protegida ante cualquier eventualidad o suceso negativo que pudiera poner en riesgo la funcionalidad normal de sus operaciones y causar grandes pérdidas económicas.

A los trabajadores del departamento de tecnología de la información de la empresa Procesadora Tropical, se le recomienda la realización constante y continua del análisis de riesgo en la empresa, esto con la finalidad de tener indicadores reales que permitan la toma de decisiones oportunas para el uso adecuado de los datos en la organización.

A los trabajadores del departamento de tecnología de la información de la empresa Procesadora Tropical, se les recomienda desarrollar e implementar nuevas estrategias de seguridad que estén alineadas a la misión y visión de la empresa, garantizando en todo momento la disponibilidad de los datos, así como también su confidencialidad y no menos importante su integridad de los mismos, además de esto, deberá existir registro de todas las operaciones que se realicen, para que la empresa esté preparada para hacer los seguimientos de los casos o eventos fortuitos que se llegaran a presentar.

A los trabajadores administrativos de la empresa Procesadora Tropical, se les recomienda estar alertas a los distintos tipos de estrategias malintencionadas que pudieran generar alto riesgo en la continuidad de las operaciones, para ello, todos los trabajadores deberán ser capacitados en temas de interés organizacional sobre la seguridad digital, para que no cometan errores o sean cómplices de engaños para que los datos sean vulnerados.

REFERENCIAS BIBLIOGRÁFICAS

Ariganello, E. (2014). *REDES CISCO Guía de estudio para la certificación CCNA Routing y Switching.* Madrid-España: Ra-Ma S.A Editorial y Publicaciones.

Cáceda Rodríguez, C. R. (2021). *Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/16013/Caceda_rc.pdf?sequence=3&isAllowed=y*

Cantli, J. R. (1997). *CONECTIVIDAD DE REDES DE COMPUTADORAS.*

Castillo Velázquez, J. I. (2019). *REDES DE DATOS Contexto y evolución.* México: Samsara.

Castillo Velázquez, J., Cobos Panduro, V., & Marchand Niño, W. (2018). IPV6 Connectivity and Management Emulation for REUNA, the Chilean Advanced Network. *IEEE.*

Centeno, C. M. (2014). Controladores SDN, elementos para su selección y evaluación. *Telem@tica*.

CGR. (2018). *Ataques de ransomware (secuestro de datos) en Latinoamérica 2017.*

CIS. (2021). *Center for Internet Security*. Obtenido de https://www.cisecurity.org/

Cisco. (2010). *REDES CISCO.* aRGENTINA: Redes Cisco / coordinado por Daniel Benchimol. - 1a ed. - Banfield - Lomas de Zamora : Gradi.

CNSS. (2015). *Committee on National Security Systems*. Obtenido de https://doi.org/10.1016/0020-7292(88)90192-0

De Cusatis, C. (2013). *HandBook of Fiber Optic Data Conmunication: A Practical Guide to Optical Networking.* Academic Press.

EcuRed. (25 de Marzo de 2015). *EcuRed (Conocimiento con todos y para todos)*. Obtenido de https://www.ecured.cu/Protocolos_de_red

ESET. (2020). *Security Report Latino Amércia 2020.*

ESET. (2019). *ESET SECURITY REPORT Latinoamérica 2019*. https://web-assets.esetstatic.com/wls/2019/07/ESET-security-report-LATAM-2019.pdf

ESET. (2023). *El 69% de las organizaciones de Latinoamérica sufrió algún incidente de*

seguridad durante el último año. https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/el-69-de-las-organizaciones-de-latinoamrica-sufrio-algun-incidente-de-seguridad-durante-el-ultimom-a/

Fiocco, D., Ganesan, V., Harrison, L., & Pawlowski, J. (2021). Farmers value digital engagement, but want suppliers to step up their game. *Mckinsey*, 8.

Gonzales, M. V. (1999). *Análisis de los factores de retardo de red que afectan el transporte de la voz sobre redes públicas frame relay.* San Nicolás de los Garza, N.L.

Grijpink, F., Kutcher, E., Ménard, A., Ramaswamy, S., Schiavotto, D., Manyika, J., . . . Okan, E. (2020). Connected world: An evolution in connectivity beyond the 5G revolution. *Mc Kinsey*, 100.

Hernández Sampieri, R. (2014). *METODOLOGIA DE LA INVESTIGACION.* Mexico: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Hidalgo, D. A. (2014). *Diseño e implementación de una aplicación de red bajo la arquitectura SDN.*

IBM. (09 de Fecbrero de 2020). *Rendimiento de red*. Obtenido de Rendimiento de red: https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_73/rzahx/rzahxebusnet.htm

Icaza, J. A. (2016). *DISEÑO DE ESCENARIOS VIRTUALES DE DISTRIBUCION DE CONTENIDO MULTIMEDIA CON SOPORTE DE REDES DEFINIDAS POR SOFTWARE.*

Indecopi. (2014). *Norma Técnica Peruana NTP-ISO/IEC 27001-2014. Tecnología de la nformación.* Lima.

ISO 9241-11. (1998). *OBP Online Browsing Platform (OBP)*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-1:v1:en:sec:D

ISO/IEC 27000. (2018). *ISO*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:fr

Jara Mendoza, O. Y. (2018). *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018.* Lima.

Jianqing, W., Yan , H., Jiaming, K., Qin, T., & Xin, H. (2015). *A Study on the Dependability of Software Defined Networks.* China. 42

Kaspersky. (2021). *CIBERAMENAZA MAPA EN TIEMPO REAL*. Obtenido de https://cybermap.kaspersky.com/es

Kayssi, O. S. (2018). QoS Guarantee over Hybrid SDN/non-SDN Networks. *IEEE.*

Linares Columbié, R., Patterson Hernández, M., & Viciedo Tijera, L. (2000). SECCIÓN HISTÓRICA La información a través del tiempo. *Scielo*, 11.

Maistre, R. L. (23 de 10 de 2012). *LIGHT READING*. Obtenido de https://www.lightreading.com/carrier-sdn/sdn-architectures/google-sdn-works-for-us/d/d-id/699197

Mamamta, T. T. (2017). CORAL-SDN: A Software-Defined Networking Solution for the Internet of Things. *IEEE.*

Manage Engine. (2021). *Recursos y controles CIS*. Obtenido de https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Manzanares López, P., Muñoz Gea, J., Malgosa Sanahuja, J., & Flores de la Cruz, A. (2019). A virtualized infrastructure to offer network mapping functionality in SDN networks. *WILEY*, 1-10.

Mazza, N. h. (2014). *Gestión Estratégica de Recursos Informáticos.*

Mejía Fajardo, Á. M. (2004). Redes Convergentes. *CIBERTEC*.

Mercado Rojas, J. E. (2016). *Modelo de gestión de seguridad de la información para el E-Gobierno.* Lima.

Minh, P., & Doan B, H. (2016). SDN applications - the intent-based Northbound interface realisation for extended applications. *IEEE*, 372-377.

Muro, Y. A. (2016). *Plataforma de pruebas para evaluar el desempeño de las redes definidas por software basadas en el protocolo openflow.*

National Institute of Standards and Technology. (2014). *Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations. Sp-800-53Ar4, 462.* Obtenido de https://doi.org/10.6028/NIST.SP.800-53Ar4

NIST. (2014). *Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations. Sp-800-53Ar4, 462*. Obtenido de https://doi.org/10.6028/NIST.SP.800-53Ar4

Olivera Argota, Y. (2019). *PROCEDIMIENTO PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN COMO CONTRIBUCIÓN A* 43 *LA CALIDAD DE LA INFORMACIÓN DE LOS SERVICIOS DE CONSULTORÍA. APLICACIÓN EN EL CIGET DE HOLGUÍN.* Holguin - Cuba.

Ortiz Morales, E. A. (2018). *CONTROLES DE SEGURIDAD SEGÚN LA NORMA ISO/IEC.*

Pareja, D. (2020a). *Seguridad informática, entre los peores riesgos del mundo*. Piranirisk. https://www.piranirisk.com/es/blog/seguridad-informatica-uno-de-los-peores-riesgos-del-mundo

Pareja, D. (2020b). *Una de cada cinco empresas es víctima de "secuestro" de información*. Piranirisk. https://www.piranirisk.com/es/blog/una-de-cada-cinco-empresas-es-victima-de-secuestro-de-informacion

Peñuela Vasquez, Y. D. (2018). Monografía de investigación para optar el título de especialista en seguridad informática. Colombia. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/17260/35254395.pdf?sequence=1&isAllowed=y

Pichihua, S. (2018). *Dispositivos conectados en riesgo de ciberataques*. El Peruano. https://elperuano.pe/noticia/70191-dispositivos-conectados-en-riesgo-de-ciberataques

Poma Vargas, A. E., & Vargas Vásquez, R. L. (2019). Problemática enCiberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. *SCIENDO*, 8.

Quinteros Basantes, J. B. (2017). *Elaboración de las Políticas de Seguridad de la Información para el Consejo Nacional Electoral del Ecuador.* CUENCA - ECUADOR.

Ramos de Santiago, F. J. (2010). *Análisis e implementación de un sistema real de medida de ancho de banda.* Madrid.

RFC 793. (Septiembre de 1981). *PROTOCOLO DE CONTROL DE TRANSMISIÓN*. Obtenido de RFC: 793: https://www.rfc-es.org/rfc/rfc0793-es.txt

Ríos Ortega, J. (2013). The concept of information in Library Science, Sociology and Cognitive Science. *Scielo*, 35.

Salazar Sánchez, A. d. (2018). *GRADO DE USO DE LA INFORMACIÓN FINANCIERA EN EL PROCESO DE TOMA DE DECISIONES POR DIRECTIVOS DE EMPRESAS EN LA REGIÓN CITRÍCOLA DE NUEVO LEÓN, MÉXICO.* México.

Salinas Rodríguez, M. S., & Valencia Moncada, J. A. (2017). *Sistema de Gestión de Seguridad de la Información y Riesgos de Información en seis sedes de una entidad bancaria del Perú.* Trujillo.

Sampieri, R. H. (2014). *Metodología de la Investigación.* México.

Sandoval, Y. (2020). *ISO 27001: de qué se trata y cómo implementarla*. Piranisk. https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

Serrano, C. D. (2015). *REDES DEFINIDAS POR SFOTWARE (SDN): OPENFLOW.*

Stalings, W. (2004). *COMUNICACIONES Y REDES DE COMPUTADORAS Séptima edición.* Madrid: PEARSON EDUCACIÓN S.A.

Tanenbaum, A. S. (2003). *Redes de computadoras.* Pearson Educación México.

Tatang, D., Quinkert, F., Frank, J., Ropke, C., & Holz, T. (2017). SDN-GUARD: Protecting SDN Controllers Against SDN Rootkits. *IEEE*, 297-302. 44 UNE-EN ISO/IEC 27002. (2017). *Tecnología de la Información Técnicas de seguridad Código de prácticas para los controles de seguridad de la Información.* ESPAÑA: AENOR INTERNACIONAL S.A.U.

Vásquez Barzola, W.F. (2023). *Implementación de servicio de Centro de Operaciones de Ciberseguridad (CYBERSOC) con plataformas OpenSource a una entidad financiera. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/19755/Vasquez_bw.pdf?sequence=3&isAllowed=y*

Walkowski, D. (2019). ¿Qué es la tríada de la CIA? *SearchDataCenter.*

Wireshark. (2020). *Wireshark*. Obtenido de Sobre Wireshark: https://www.wireshark.org/

World Economic Forum. (2018). *The Global Risks Report 2018 13th Edition.* Geneva: World Economic Forum.

ANEXOS

Anexo 1. Matriz de consistencia

Título: Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical

Formulación del problema

General

¿Cuánto impactan los controles críticos de ciberseguridad en el uso eficiente de la información en la procesadora tropical?

Objetivo

General

Evaluar los controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical.

Específicos

a) Analizar los controles críticos de ciberseguridad y su impacto en la usabilidad de la información en la Procesadora Tropical.

b) Analizar los controles críticos de ciberseguridad y su impacto en la seguridad de la información de la Procesadora Tropical.

c) Analizar los controles críticos de ciberseguridad y su impacto en la fiabilidad de la información en la Procesadora Tropical.

Hipótesis

General

Los controles críticos de ciberseguridad generan un impacto significativo en el uso eficiente de la información en la procesadora tropical.

Tipo, nivel y diseño de investigación

El tipo de investigación es aplicada

Diseño preexperimental

Nivel de investigación descriptivo

Población y muestra

Población

36 trabajadores de la empresa procesadora Tropical.

Muestra:

Correspondió al total de la población.

Variable de estudio

Variable	Dimensiones
Controles críticos de ciberseguridad	Controles de prevención y protección
	Controles de detección y monitorización
	Controles de recuperación y respuesta
Uso eficiente de la información	Usabilidad
	Seguridad
	Fiabilidad

Técnicas e instrumentos

Técnica: Encuesta

Instrumento: Cuestionario

Anexo 2. Instrumento de recolección de datos

UNIVERSIDAD NACIONAL DE SAN MARTIN – TARAPOTO
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E

TEMA: **"Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical"**

CUESTIONARIO "Uso eficiente de la información"

Estimado(a) participante, marcar con una equis (X) en cada recuadro la respuesta que mejor represente su opinión.

Niveles de la escala:
1=Totalmente en desacuerdo; 2=En desacuerdo; 3=Indiferente; 4=De acuerdo; 5=Totalmente de acuerdo

Nro.	Preguntas	1	2	3	4	5
1	¿Con que frecuencia genera información asociada a la empresa?					
2	¿Con que frecuencia comparte Información de manera interna y externa de la empresa?					
3	¿La Información generada es reutilizada para nuevas actividades?					
4	¿La Información generada es clasificada para dar mejor uso?					
5	¿La información que utiliza es protegida con accesos de credenciales a las plataformas?					
6	¿La información generada al interior de la empresa es tratada de manera confidencial?					
7	¿La información que se usa es modificada por cualquier usuario?					
8	¿La información está disponible para todos?					
9	¿Existe una trazabilidad o rastreo de la información?					
10	¿La información está disponible cuando Ud. ¿La necesita?					
11	¿La información que recibida corresponde a la solicitada?					
12	¿La información que ha sido alterada o perdida ha sido posible recuperar?					

Anexo 3. Confiabilidad del instrumento

Cuestionario “Uso eficiente de la información”

La confiabilidad del instrumento se calculó a través del Índice de confiabilidad - Alfa de Cronbach, teniendo como muestra piloto a 30 sujetos; y del análisis de los 12 ítems del instrumento de evaluación se obtuvo como resultado un índice de **0,809** que se encuentra dentro del rango “Muy bueno” de confiabilidad, por lo tanto, el instrumento de medición es muy confiable para su aplicación.

A través del Alfa de Cronbach

$$\alpha = \frac{K}{K-1}\left[1-\frac{\sum S_i^2}{S_T^2}\right]$$

Nivel de confiabilidad del coeficiente alfa de Cronbach

Rango	Nivel
0,9 – 1,0	Excelente
0,8 – 0,9	Muy bueno
0,7 – 0,8	Aceptable
0,6 – 0,7	Cuestionable
0,5 – 0,6	Pobre
0,0 – 0,5	No aceptable

Fuente: George y Mallery (2003).

Resumen del procesamiento de los casos

		N	%
Casos	Válido	30	100,0
	Excluido[a]	0	,0
	Total	30	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Fuente: SPSS ver 27.

Estadísticas de total de elemento				
	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
item1	34,30	63,321	,696	,771
item2	34,00	73,103	,442	,798
item3	34,10	71,541	,478	,794
item4	33,87	67,706	,626	,781
item5	34,47	67,637	,532	,788
item6	34,30	64,148	,684	,773
item7	34,13	65,775	,630	,779
item8	34,47	71,913	,357	,805
Item9	34,03	69,964	,455	,796
item10	34,10	77,817	,156	,818
item11	34,13	73,913	,281	,811
item12	34,03	75,689	,171	,823

Fuente: SPSS 27

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,809	12

Fuente: SPSS 27

Bibliografía de Referencia:

George, D., & Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference. 11.0 update (4th ed.). Boston: Allyn & Bacon.

Datos de la prueba de confiabilidad

Sujetos/ítems	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	4	4	5	2	2	2	2	3
2	4	3	4	4	2	4	2	5	4	4	4	5
3	2	2	1	1	1	1	1	4	2	3	2	2
4	4	4	4	5	5	5	4	4	5	5	2	2
5	2	3	2	4	2	2	3	2	1	2	5	5
6	4	5	4	4	5	5	5	5	5	1	2	1
7	2	2	1	2	1	2	1	4	3	3	2	4
8	2	2	3	2	4	3	2	2	2	4	5	1
9	1	5	4	5	1	1	1	1	4	1	1	1
10	2	3	1	2	2	2	4	2	3	2	3	3
11	3	2	1	3	4	3	3	4	5	4	4	4
12	5	4	4	5	5	5	5	2	2	1	1	2
13	1	3	3	3	1	1	1	2	1	3	3	2
14	1	2	2	2	2	2	2	1	5	4	4	5
15	4	4	4	3	2	4	4	1	3	4	2	2
16	1	3	4	3	4	2	2	3	2	4	3	4
17	5	5	4	5	1	1	5	5	4	4	5	5
18	4	2	2	2	2	3	3	3	3	3	3	2
19	5	4	4	5	4	5	4	1	5	4	5	5
20	3	4	4	3	2	2	4	2	3	3	3	2
21	3	2	4	3	4	3	3	4	5	4	4	4
22	5	4	4	5	5	5	5	2	2	1	2	3
23	1	3	3	3	1	1	1	2	1	3	1	5
24	1	2	2	2	2	2	2	1	5	4	5	5
25	4	4	4	3	2	4	4	2	3	4	2	2
26	1	3	4	3	4	2	2	3	2	4	3	4
27	5	5	4	5	4	5	5	5	4	4	5	5
28	4	2	2	2	2	3	3	3	3	3	3	2
29	5	4	4	5	4	5	4	5	5	4	5	5
30	3	4	4	3	2	2	4	2	3	3	3	2

Anexo 4. Validación del instrumento

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Wilson Torres Delgado
Institución donde labora : Universidad Nacional de San Martín - Tarapoto
Especialidad : Licenciado en estadística – COESPE 380
Instrumento de evaluación : Cuestionario: Uso eficiente de la información
Autor (s) del instrumento (s) : Juan Ramos Estela

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.					X
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.					X
ACTUALIDAD	El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Uso eficiente de la información.				X	
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación.					X
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.				X	
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Uso eficiente de la información				X	
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento permitirá analizar, describir y explicar la realidad, motivo de la investigación.				X	
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Uso eficiente de la información					X
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL		46				

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 “Excelente”; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

III. OPINIÓN DE APLICABILIDAD

Establecido los valores de aplicabilidad se llegó a determinar que el instrumento de recolección de datos se encuentra listo para su ejecución con validación obtenida de “Excelente”

IV. PROMEDIO DE VALORACIÓN: **46**

Tarapoto 26 de marzo de 2023

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Andi Lozano Chung
Institución donde labora : Universidad Nacional de San Martín
Especialidad : Docente en la Universidad Nacional de San Martín
Instrumento de evaluación : Cuestionario: Uso eficiente de la información
Autor (s) del instrumento (s) : Juan Ramos Estela

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.				X	
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.					X
ACTUALIDAD	El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Uso eficiente de la información.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación.					X
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.					X
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Uso eficiente de la información				X	
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento permitirá analizar, describir y explicar la realidad, motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Uso eficiente de la información				X	
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL		**47**				

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 “Excelente”; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

III. OPINIÓN DE APLICABILIDAD

Aplicable y Coherente.

IV. PROMEDIO DE VALORACIÓN: **47**

Tarapoto 26 de marzo de 2023

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto : Ing. MBA. Ángel Cárdenas García
Institución donde labora : Universidad Nacional de San Martín
Especialidad : Docente en Metodología - UNSM
Instrumento de evaluación : Cuestionario: Uso eficiente de la información
Autor (s) del instrumento (s) : Juan Ramos Estela

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.				X	
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.				X	
ACTUALIDAD	El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Uso eficiente de la información.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación.				X	
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.					X
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Uso eficiente de la información					X
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Uso eficiente de la información.					X
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.				X	
PUNTAJE TOTAL		**46**				

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 “Excelente”; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

III. OPINIÓN DE APLICABILIDAD

Excelente para su aplicación.

IV. PROMEDIO DE VALORACIÓN: **46**

Tarapoto 26 de marzo de 2023

Anexo 5. Controles críticos de ciberseguridad

A continuación, se presentan los 20 controles críticos desplegados para el uso eficiente de la información en la Procesadora Tropical. Los controles críticos están bajo la NIST (Instituto Nacional de Estándares y Tecnología).

Figura 1. Script para realizar inventario de equipos y software (Control 1 y Control 2)

Figura 2. Inhabilitación de acceso remoto (Control 3)

Figura 3. Configuración de usuarios (Control 3)

Figura 4. Uso de Windows defender (Control 3)

Figura 5. Acceso al dispositivo por credenciales (Control 3)

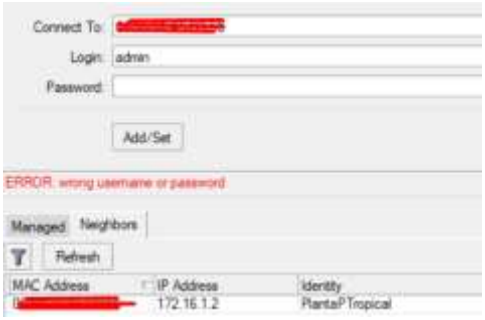


Figura 6. Acceso al dispositivo por credenciales 2 (Control 3)

Figura 7. Inhabilitación de usuarios por defecto (Control 4)

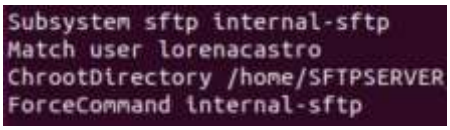


Figura 8. Conexiones seguras SFTP

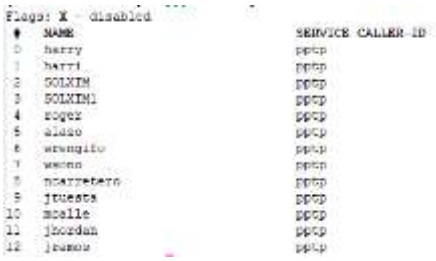


Figura 9. Configuración de VPN (Control 4)

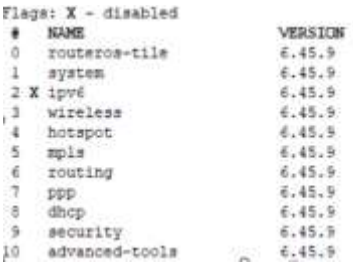


Figura 10. Actualización de versions (Control 4)

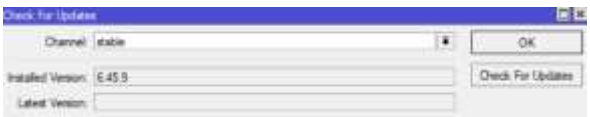


Figura 11. Actualización de Firmware (Control 4)

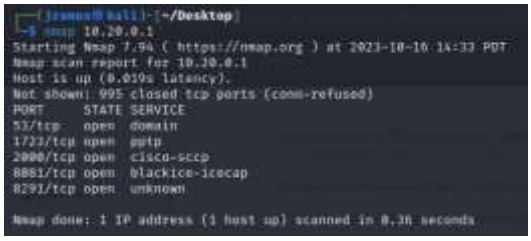


Figura 12. Escaneo de puertos (Control 4)

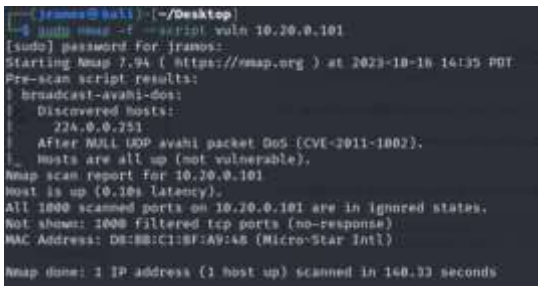


Figura 13. Escaneo de vulnerabilidades (Control 4)

Figura 14. Uso controlado de privilegios administrativos (Control 5)

Figura 15. *Privilegios restringidos en usuarios administrativos (Control 5)*

Figura 16. Gestión de spam, bloqueo de navegadores (Control 6)

Figura 17. Bloqueo de urls de phishing a nivel de resolución de DNS (Control 6)

Figura 18. Gestión para implementar CheckPoint (Control 7)

Figura 19. Entorno Preprod

Figura 20. Configuración de VLAN's 1 (Control 9)

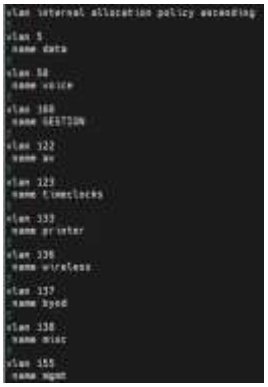


Figura 21. Configuración de VLAN's 2 (Control 9)

Figura 22. Encriptado de contraseñas (Control 9)

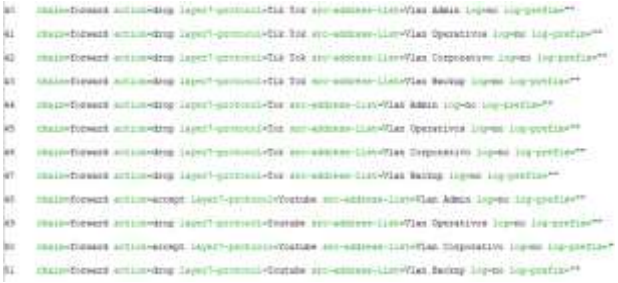


Figura 23. Firewall a nivel de capa 7 (Reglas, ACL) (Control 10)

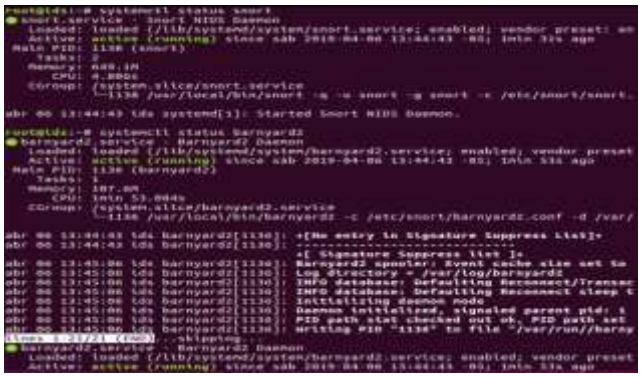


Figura 24. Configuración de IDS

Figura 25. Segmentación de red (LAN, WAN, DMZ) (Control 10)

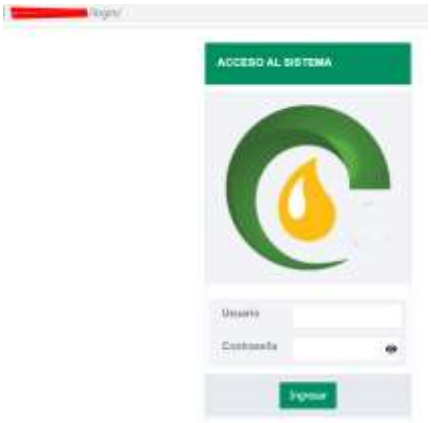


Figura 26. Acceso por credenciales (Control 11)

Figura 27. Uso de BitLocker

```
root@storage:~# chmod 700 /home/SFTPSERVER/
```

Figura 28. Permisos de escritura y lectura (Control 11)

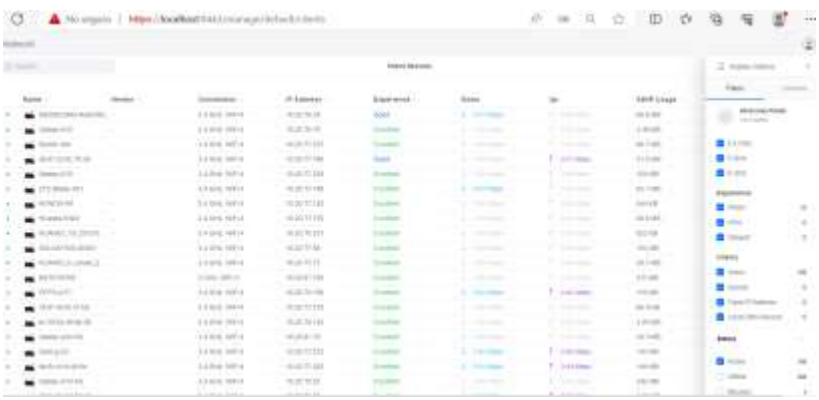


Figura 29. Uso de un Wirelles Controller Local (Control 13)

Figura 30. Autenticación por contraseñas (Control 13)

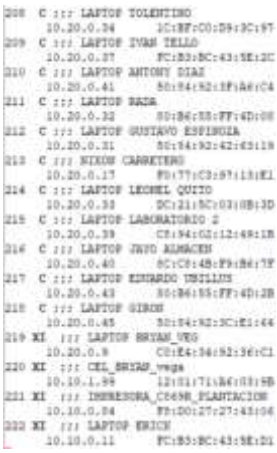


Figura 31. Registros de IP amarrado a MAC para soluciones ARP, DHCP (Control 13)

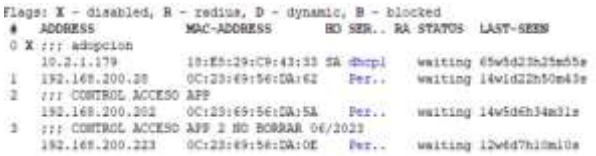


Figura 32. Registros de IP amarrado a MAC para soluciones ARP, DHCP – 2 (Control 13)

Figura 33. Inhabilitación de puertos por default (Control 14)

Figura 34. Cambio de puertos (no uso de puertos conocidos) (Control 14)

Figura 35. Uso de protocolos seguros (Control 14)

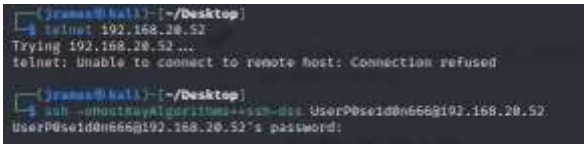


Figura 36. Protocolos seguros (Control 14)

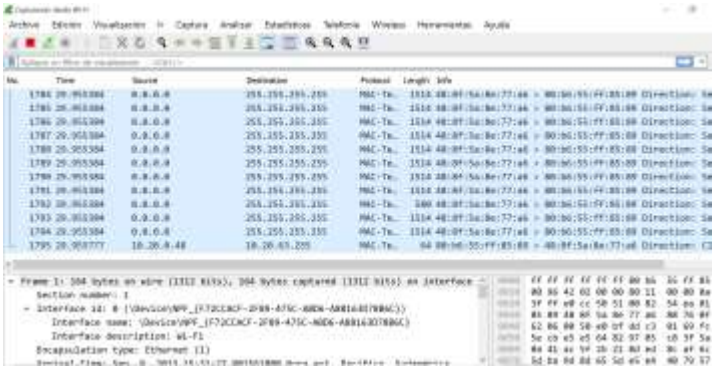


Figura 37. Uso de Wireshark para monitorear tráfico (Control 15)

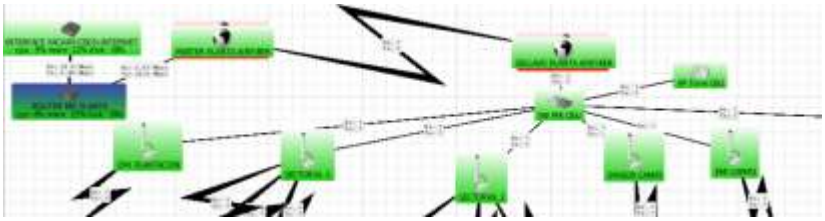


Figura 38. Uso de Dude para monitorear equipos (Control 15)

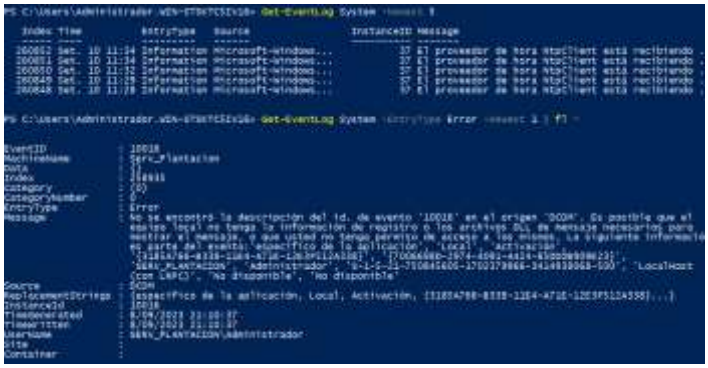


Figura 39. Visualización de eventos en PowerShell (Control 15)

Figura 40. Uso de snmp, syslog (Control 15)

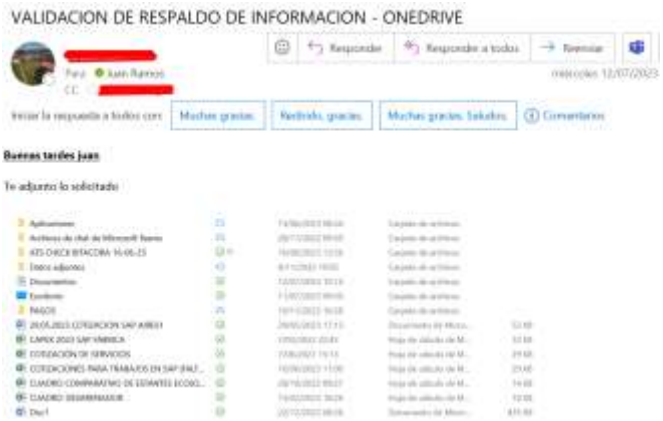


Figura 41. Backups de archivos (Control 17)

Figura 42. Backups de configuraciones (Control 17)

Figura 43. Script de Backup de DB (Control 17)

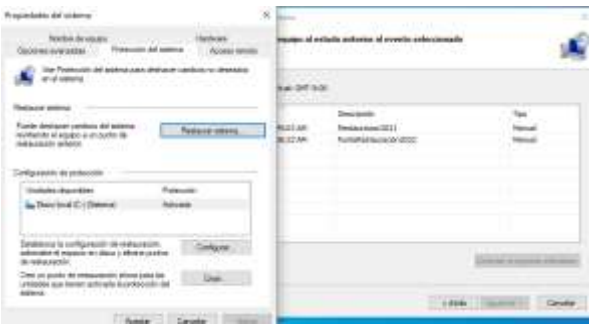


Figura 44. Puntos de restauración (Control 17)

Figura 45. Privilegios de usuarios (Control 18)

Figura 46. Acceso según su rol de usuario (Control 18)

Nota: Usuarios generalmente clasificados según el sistema que se maneja y los usuarios que lo utilizan.

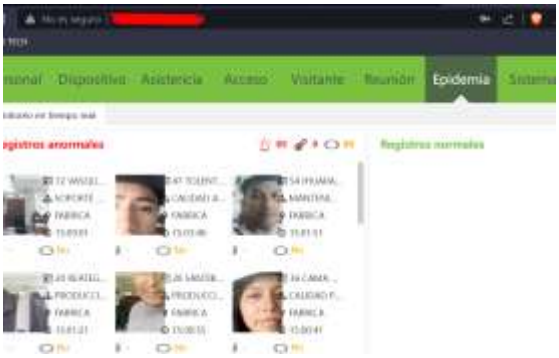


Figura 47. Acceso con lectores de huellas (Control 19)

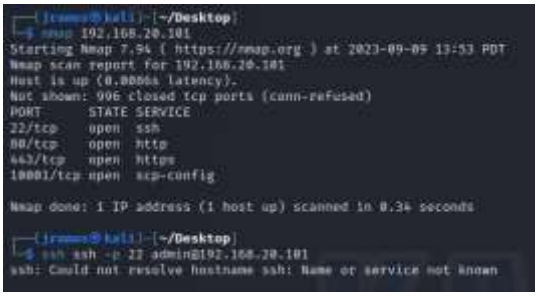


Figura 48. Pruebas de acceso (Control 20)

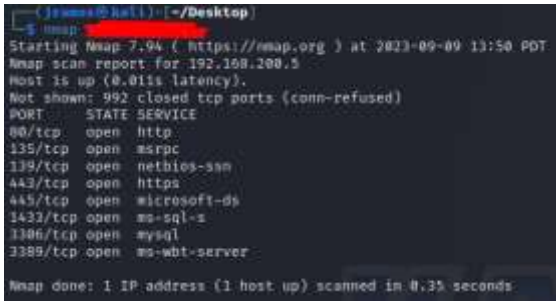


Figura 49. Escaneo de puertos (Control 20)

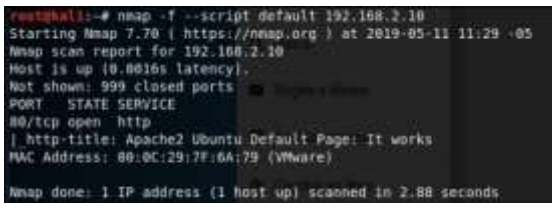


Figura 50. Explotado de Vulnerabilidades (Control 20)

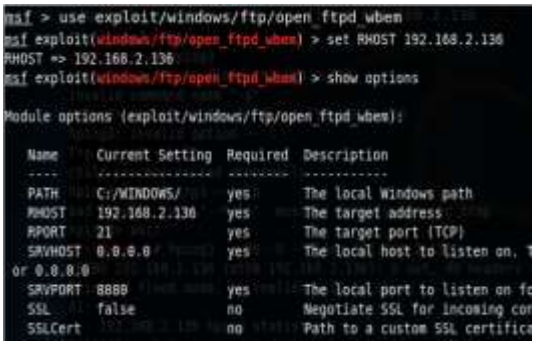


Figura 51. Exploit Lanzado (Control 20)

Implementación de controles críticos – imágenes

- Dispositivos centralizados.

- Encuestas y charlas

UNIVERSIDAD NACIONAL DE SAN MARTIN – TARAPOTO
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E

TEMA: **"Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical, 2022"**

CUESTIONARIO "Uso eficiente de la información"

Estimado(a) participante, marcar con una equis (X) en cada recuadro la respuesta que mejor represente su opinión.

Niveles de la escala:
1=Totalmente en desacuerdo; 2=En desacuerdo; 3=Indiferente; 4=De acuerdo; 5=Totalmente de acuerdo

Nro.	Preguntas	1	2	3	4	5
1	¿Con que frecuencia genera información asociada a la empresa?			X		
2	¿Con que frecuencia comparte Información de manera interna y externa de la empresa?		X			
3	¿La Información generada es reutilizada para nuevas actividades?		X			
4	¿La Información generada es clasificada para dar mejor uso?	X				
5	¿La información que utiliza es protegida con accesos de credenciales a las plataformas?		X			
6	¿La información generada al interior de la empresa es tratada de manera confidencial?		X			
7	¿La información que se usa es modificada por cualquier usuario?		X			
8	¿La información está disponible para todos?		X			
9	¿Existe una trazabilidad o rastreo de la información?	X				
10	¿La información está disponible cuando Ud. ¿La necesita?		X			
11	¿La información que recibida corresponde a la solicitada?		X			
12	¿La información que ha sido alterada o perdida ha sido posible recuperar?	X				

UNIVERSIDAD NACIONAL DE SAN MARTIN – TARAPOTO
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E

TEMA: **"Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información en la Procesadora Tropical, 2022"**

CUESTIONARIO "Uso eficiente de la información"

Estimado(a) participante, marcar con una equis (X) en cada recuadro la respuesta que mejor represente su opinión.

Niveles de la escala:
1=Totalmente en desacuerdo; 2=En desacuerdo; 3=Indiferente; 4=De acuerdo; 5=Totalmente de acuerdo

Nro.	Preguntas	1	2	3	4	5
1	¿Considera Ud. que genera con frecuencia información asociada a la empresa?				X	
2	¿Considera Ud. que comparte con frecuencia Información de manera interna y externa de la empresa?				X	
3	¿La Información generada es reutilizada para nuevas actividades?				X	
4	¿La Información generada es clasificada para dar mejor uso?				X	
5	¿La información que utiliza es protegida con accesos de credenciales a las plataformas?				X	
6	¿La información generada al interior de la empresa es tratada de manera confidencial?					X
7	¿La información que se usa es modificada por cualquier usuario?					X
8	¿La información está disponible para todos?				X	
9	¿Existe una trazabilidad o rastreo de la información?				X	
10	¿La información está disponible cuando Ud. ¿La necesita?				X	
11	¿La información que recibida corresponde a la solicitada?				X	
12	¿La información que ha sido alterada o perdida ha sido posible recuperar?					X

Base de datos estadísticos

N.º	Usabilidad	Seguridad	Fiabilidad	**Uso eficiente de la información**	Usabilidad después	Seguridad después	Fiabilidad después	**Uso eficiente de la información (Después)**
1	8	10	9	27	18	19	17	54
2	10	5	8	23	15	13	15	43
3	8	8	9	25	19	16	18	53
4	9	7	8	24	14	13	16	43
5	8	9	6	23	16	18	16	50
6	10	7	7	24	17	20	16	53
7	8	8	10	26	16	18	17	51
8	10	9	8	27	17	18	17	52
9	6	8	10	24	16	18	17	51
10	8	8	7	23	17	17	15	49
11	6	9	9	24	15	18	18	51
12	7	7	10	24	17	17	16	50
13	9	7	8	24	16	15	15	46
14	7	8	6	21	19	16	15	50
15	7	8	10	25	16	16	16	48
16	10	8	6	24	17	15	15	47
17	11	5	6	22	14	16	17	47
18	10	9	8	27	16	16	19	51
19	6	6	9	21	15	16	16	47
20	8	9	9	26	16	18	14	48
21	10	11	9	30	18	16	15	49
22	7	10	8	25	16	15	14	45
23	9	8	10	27	17	18	15	50
24	8	7	6	21	17	18	16	51
25	7	9	7	23	16	16	19	51

26	7	7	6	20	15	15	13	43
27	9	10	6	25	15	16	16	47
28	5	8	10	23	17	16	17	50
29	10	4	7	21	17	14	15	46
30	8	8	10	26	13	18	13	44
31	8	9	5	22	17	17	19	53
32	7	7	10	24	16	17	15	48
33	8	8	6	22	17	19	17	53
34	9	8	9	26	16	14	18	48
35	9	4	9	22	17	18	15	50
36	8	7	6	21	13	15	14	42

Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información de la Procesadora Tropical

por Juan Ramos Estela

Fecha de entrega: 30-nov-2023 11:17a.m. (UTC-0500)
Identificador de la entrega: 2243170253
Nombre del archivo: Tesis-Maestria-TI-JuanRamosEstela_2.docx (8.58M)
Total de palabras: 16457
Total de caracteres: 89129

Gestión de controles críticos de ciberseguridad y su impacto en el uso eficiente de la información de la Procesadora Tropical

INFORME DE ORIGINALIDAD

20%	20%	2%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	tesis.unsm.edu.pe Fuente de Internet	3%
2	repositorio.unsm.edu.pe Fuente de Internet	3%
3	hdl.handle.net Fuente de Internet	2%
4	repositorio.ucv.edu.pe Fuente de Internet	1%
5	www.gitltda.com Fuente de Internet	1%
6	Submitted to Universidad Nacional de San Martín Trabajo del estudiante	1%
7	server-die.alc.upv.es Fuente de Internet	1%
8	revistas.ulima.edu.pe Fuente de Internet	1%