UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Modelo de Sistema de Ciberseguridad para la Gestión de Riesgo de una Empresa de Matizados de Pintura de Lima, 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Ingeniería de Sistemas con mención en Tecnologías de la Información

AUTORA:

Calderon Aquiño, Cinthia Jeanette (orcid.org/0000-0002-3478-0581)

ASESOR:

Dr. Acuña Benites, Marlon Frank (orcid.org/0000-0001-5207-9353)

LÍNEA DE INVESTIGACIÓN:

Sistema de Información y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2022

Dedicatoria:

A mis Padres **José y Rosenda** por el apoyo incondicional y así demostrando ser el orgullo en casa, a mis hermanos que con sus consejos me ayudaron a superar diferentes pruebas en esta etapa de mi vida y al asesor Doc. Marlon Acuña por su enseñanza y dedicación para la elaboración de mi Tesis. MUCHAS GRACIAS A TODOS.

“Amado, yo deseo que tú seas prosperado en todas las cosas, y que tengas salud, así como prospera tu alma.” **(3 Juan 1: 2)**

Agradecimiento:

Este trabajo de investigación con arduo esforzó le agradezco a DIOS con todo mi corazón y le pido siempre sabiduría para desempeñarme en la carrera como profesional. También estoy muy agradecida por el apoyo incondicional y por la paciencia enorme a mi novio Lenny Fernandez.

“El principio de la sabiduría es el temor al Señor; Los insensatos desprecian la sabiduría y la enseñanza.” **(Proverbios 1:7)**

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Resumen

La presente investigación tiene el objetivo general de la presente investigación fue determinar cómo influye un guía para Modelo de Sistema de Ciberseguridad para la Gestión de Riesgo de una Empresa de Matizados de Pintura de Lima, 2022. El presente estudio fue de tipo aplicada, con un diseño pre experimental, la población elegida de 17 activos de información de la empresa. Se trabajo con la metodología de SGI y con el ISO 27001 con una mejora en el análisis descriptivo se concluye que en el indicador nivel de activos se obtuvo de 7.88% aplicado mediante la implementación se logró 13.53% dando con la prueba en T-Student, el nivel de riesgos se obtuvo de 9.5% aplicado mediante la implementación se logró 18.73% con la prueba en T-Student y número de controles aplicados se obtuvo de 89.38% no aplica y si aplica un 99.12% con Wilcoxon. Donde el resultado se rechaza la hipótesis nula con un nivel de significancia del 0.05 y se concluye que los activos informáticos de los 114 controles son por la aplicación de ISO 27001. Por lo cual se adoptó en la empresa fue el idóneo porque hay una mejora notable.

Palabras clave: *ciberseguridad, gestión de riesgos, nivel de riesgos, seguridad*

Abstract

The general objective of this research was to determine the influence of a guide for a Cybersecurity System Model for the Risk Management of a Paint Matting Company in Lima, 2022. The present study was of applied type, with a pre-experimental design, the chosen population of 17 information assets of the company. We worked with the methodology of SGI and ISO 27001 with an improvement in the descriptive analysis it is concluded that in the indicator level of assets was obtained 7.88% applied through the implementation was achieved 13.53% giving with the T-Student test, the level of risks was obtained 9.5% applied through the implementation was achieved 18.73% with the T-Student test and number of controls applied was obtained 89.38% does not apply and if it applies 99.12% with Wilcoxon. Where the result rejects the null hypothesis with a significance level of 0.05 and it is concluded that the IT assets of the 114 controls are by the application of ISO 27001. Therefore, it was adopted in the company was ideal because there is a significant improvement.

Keywords*: cybersecurity, risk management, risk level, security*

I. INTRODUCCIÓN

A nivel mundial se cuenta con diversas compañías globales una de ellas es Accenture cuya empresa de seguridad digital brinda servicios en consultoría, marketing, tecnología y operaciones inteligentes. El autor Sánchez (2022). Se realizó un informe sobre el ataque de ciberseguridad en Madrid el 04 de febrero del 2022 arrojando un 55% de ciberataques, detectan las debilidades rápidamente. Posteriormente se realizó otro estudio con el 81% encuestados se genera un ataque indefectible el año 2020. Dando un aumento contravenciones de aplicaciones, redes, servicios dando un porcentaje de 31% internacional causando dentro los 270 a MIPYMES. Con un reportaje ejecutado por más de 4.700 ejecutivos de diversos países.

Por otro lado, Machín y Gazapo (2016). En el siglo XX en España, la llegada de Internet ha revolucionado la sociedad sin precedentes en la historia humana. En Europa una estrategia de ciberseguridad es instrumentos que permitan una gestión de crisis alta y eficaz. El consumo depende de la ola en los ataques de sistema de información. Sin embargo, las amenazas son constantes. Esta situación afecta a la materia de gestión de riesgos y a la normalidad de seguridad. En Europa su plan de ciberseguridad para poder integrar verdaderamente los planes internacionales ya que se necesitan con urgencia decisiones difíciles y muchas mejores herramientas y aplicaciones para permitir que la congregación implemente la gestión de problemas en tiempo real y la prevención de ciber conflictos.

Así mismo según Taípe (2018), en la investigación el problema radica por la falta de seguridad y política en la empresa por lo cual se da un impacto en sus acciones afectando una vulnerabilidad en sus activos informáticos con alta demanda midiendo el porcentaje de protección se realizó un análisis de riesgos de test Ethical Hacking y políticas que consiste en una serie de pruebas técnicas de diversos ataques como un hacker, pero controlado. Teniendo como objetivo realizar una auditoría de seguridad. (Bernal et al. 2000).

El autor Jara (2018) con finalidad manifestar para un sistema de seguridad de información con un proceso de riesgo basado en un enfoque cuantitativo, con un método hipotético deductivo se desenrolló una investigación aplicada con una población sustituida por riesgo de los activos con un análisis de deficiente en el incumplimiento de la información documentada y controles de seguridad. Tomó como objetivo aplicar en gestión de seguridad. Se utilizó ISO 31001 para los activos de información se base funciones operativas en el sistema de control. Donde la población se consideró 31 activos y 114 controles por la norma señalada. Por lo cual para mejorar se aplicó la gestión de riesgos brindando la seguridad al gobierno local.

Ante la problemática la empresa se tiene diversos ataques, riesgos por sus clientes y competencia alrededor del local por lo cual se enfoca en brindar una excelente atención, aunque las diversidades se generan por la coyuntura de la pandemia COVID 19 dando una debilidad baja con un resultado de vulnerabilidad en el robo de información e integridad de información por los empleados, así también en los datos de cada distribuidor y productos en venta. Por ellos se demanda un modelo de ciberseguridad para el levantamiento de riesgo y su mejor rendimiento de seguridad. Con un porcentaje de pérdida de 48% el propósito es reducir el número e impacto de futuras incidencias de riesgos altos.

La justificación de metodología a través de la norma ISO 27001 evalúa los riesgos y controles prósperos en la 27002. Para el cálculo de conflicto se contienen en ISO/IEC TR 13335-3 en la tecnología e información. Con una contingencia de la alta amenaza y debilidad de activos de controles.

Por otro lado, la justificación teórica de ISO 31000-2009 dentro la causa de gestión de conflictos en el régimen local, afirmar el proceso de gestión de riesgo en una serie de labores, identificar riesgos, sus instrumentos y tomar discretas para comprimir a un nivel aprobado, para que los efectos de la búsqueda la suplan de instrucciones a la corporación científica cubierta en la seguridad de información.

Por último, se tiene la justificación práctica del ISO/IEC 27002 de las buenas prácticas con expectativa para sistemas de información. Por lo cual se puede reducir el impacto de riesgo y defender las habilidades. Con una certificación en la organización con una norma UNE-ISO/IEC 27001.

Posteriormente, en el ISO 17799:2005. El objetivo de revisión y control de SGSI con información de resultados a través de Check. Generando una verificación tomando un proceso de audiencia.

Así mismo, esclarecer el contexto problemático, se exterioriza la enunciación de la problemática general: ¿Cómo impacta el modelo de sistema de ciberseguridad para la gestión del riesgo en la empresa matizado de pinturas, Lima 2022?

Contemporánea con la tesis es evidente en la asociación ocurrió un robo de información por unos de los trabajadores, cuya de sus funciones vulnero la confianza y respeto. Sumado la generalización de bienes que brinda la entidad y la manifestación del internet con cibernética de la tecnología de la era digital con una consecuencia de una alta crisis de la pandemia que arrasa y debilita a millones de empresa que caen como punto de eje principal a obtener miles de informaciones diariamente. Donde se demanda un modelo de ciberseguridad en la entidad y medir la seguridad de nivel de proceso de riesgos.

Con la destreza de solventar la problemática indicada se requiere el objetivo general: Determinar cómo se influye un guía de sistema de ciberseguridad para la gestión de riesgo de una empresa matizado de pinturas, Lima 2022.

En las siguientes hipótesis de trabajo, hipótesis general: La implementación de un modelo de sistema de ciberseguridad para la gestión de riesgo de una empresa de matizados de pintura de Lima, 2022, las hipótesis específica de la investigación es: (a) La implementación de modelo de sistema de ciberseguridad en el nivel de riesgos para la gestión de riesgo de una empresa

de matizados de pintura de Lima, 2022, (b) Además la hipótesis específica es, modelo de sistema de ciberseguridad en el nivel de activos para la gestión de riesgo de una empresa de matizados de pintura de Lima, 2022 y (c) La implementación de modelo de sistema de ciberseguridad en el números de control de aplicación para la gestión de riesgo de una empresa de matizados de pintura de Lima, 2022

II. MARCO TEÓRICO

Se tiene como antecedente nacional al autor Aliaga (2021) en su investigación el problema radicó por el impacto de la coyuntura de la pandemia COVID 19 por lo cual se descubrió en disminuir las aptitudes en la gente y responsabilidad en equipo. En 5 años consecutivos no tuvo un crecimiento. Sin embargo, su V1 es ciberseguridad y V2 la prevención de los ataques cibernéticos. En conclusión, se determinó por V1 el valor de la prueba T_Student es de -46.680 y V2 el valor de la prueba T_Student es de -24.961. De esta investigación de tesis se accede, fortaleciendo los conceptos de la metodología y los indicadores Nivel de activos.

Manifestó Huerta (2019) en su tema de investigación en la metodología de investigación ISO 27001:2013 y con la población de 24 activos de información, por lo tanto, con un resultado estadístico por T_Student con 4,614 con la diferencia en con la prueba Wilcoxon con 9,644. Inscrito a un nivel de valor = 0,000 y con un rechazo de hipótesis nula con una aceptación de hipótesis de investigación $p<0,05$. Conduciendo al rechazo de la hipótesis nula la implementación de sistema de gestión de seguridad de la información tiene un impacto positivo al incrementar la cantidad de controles aplicados en el proceso de gestión de riesgos por parte en Coopsol Consulting.

Álvarez y Honorio (2018), con la tesis de investigación ciberseguridad en la era digital con una problemática que por falta de proceso y gestión de riesgos generando un ataque encaminado sobre robos de virus troyanos bancarios. Con un resultado para generar un 79% de gastos operativos dando una mejora de era digital con un 85% de tiempo operación con un recurso de 99% de datos y con una reducción de 86% con un servicio básico. De esta investigación se utilizó la variable 2 para los conceptos metodológicos en la presente tesis de investigación.

El investigador Alama (2018), mociona en la atención de requerimientos de la organización de Software Enterprise Services en Lima con una problemática de ataques de riesgos con una sobrecarga de trabajo en las comunicaciones hacia el cliente que afine un incumplimiento de SLA’s que impacta en la factura

de cada mes. Obteniendo una escala de pérdida de recursos humanos con requerimientos de menos de 2 días para el proceso de área determinando la fecha de entrega. Con el resultado se obtuvo la reducción de tiempo enviando alertas de gestiones de proyectos en la empresa en cálculos de días hábiles. Dando un nivel de cumplimiento de requerimientos entregados un porcentaje un 90%.

El investigador Llontop (2018), con la línea de investigación en TI. El problema se tenía en la falta de práctica por administradores y la falla de arquitectura para poder incrementar y controlar los riesgos. Así mismo, el objetivo es comparar los resultados de forma numéricamente. Con un total de 21 empresas como población con el indicador de nivel de eficiencia dando un 83.9%. En la primera conclusión se enfrentó a una encuestados y comparación de servicios a 63.5% se observó en la falta de la política antes los desastres. En la segunda conclusión el riesgo de nivel eficiente de 60.7& y de comparación de servicios de 38.5% por falta de algunas políticas afecto a varias empresas de servicios y la tercera conclusión el riesgo del nivel eficiente con 55.4% encuestados con una diferencia de balance de servicios a 46.2% aquí la diferencia resalta sobre los riesgos a las empresas comerciales. Brindando capacitaciones para la gestión de riesgos y a los servicios con certificados en ITIL al personal.

Se tiene como antecedente Internacional Mitxelena, Dal Cin y Bissell (2022). En una encuesta anual de 4744 encuestados a nivel mundial sobre el estado actual de la resiliencia de la ciberseguridad, el 85 % de los CISO desarrollan estrategias de ciberseguridad con objetivos comerciales como el crecimiento y la participación de mercado en mente. Sin embargo, en comparación con el 69 % en 2020, el 81 % también dijo que “estar por delante de los atacantes es una lucha constante y los costos son insostenibles”. En el año 2020 hubo una media de 270 ataques empresariales, un aumento del 31% con una infracción de una cadena de valor en una extensión de 44% a 61%. Con una inversión más de 80% encuestados afirmaron el incremento de seguridad TI hasta un 15% de consumo. Cloud Security, la empresa número 32, afirma que la seguridad no ha

sido parte del debate sobre la nube desde el principio, pero se esfuerza por ponerse al día. Las preocupaciones de seguridad son la motivación para la adopción de la nube. Alrededor de un tercio de los encuestados tienen problemas con una gobernanza y una regulación deficientes, la seguridad en la nube es demasiado compleja y no tienen las habilidades internas para implementar un marco de seguridad en la nube de Estructura apropiado.

Tabla 1

Medidas clave de la ciberresiliencia

	Los ciberdefensores	**Los obstaculizadores del negocio**	**Los que asumen ciberriesgos**	**Los vulnerables**
Detienen más ataques: Número de ataques que violan la seguridad	1 de 6	1 de 4	1 de 2	1 de 2,3
Detienen violaciones más rápido: % de violaciones detectadas en <1 día	55%	50%	11%	15%
Remedian violaciones más rápido: % remediadas en 15 días o menos	100%	96%	30%	30%
Reducen el impacto de las violaciones: % violaciones sin impacto	72%	64%	23%	24%

Fuente: Accenture,Tecnologica.

Como se puede apreciar en la tabla 1 se muestra las medidas claves para el ataque en ciberseguridad donde se resalta los porcentajes alcanzado en cada etapa.

El autor Räni (2018). El problema surge a través en los analistas de gestión de riesgos de software porque no conocer las próximas puntuaciones de gravedad de las categorías de vulnerabilidad podría resultar en evaluaciones de nivel de riesgo menos precisas. Este proyecto de tesis proporciona un paquete R que aborda el problema. Eventualmente se usa para pronosticar puntajes CVSS mensuales medios del año 2018. MAE, RMSE, MAPE y MASE se utilizan para evaluar la precisión de los pronósticos para los años 2016 y 2017. Estas medidas ayudan a elegir entre los modelos. Se consideran trece tipos diferentes

de modelos al generar los pronósticos de 2018 para un subconjunto de 34 CWE. Según las previsiones puntuales, se espera que diez CWE tengan una alta gravedad.

Tesis de autor Turac (2020). Mediante el enfoque de investigación abductivo, los riesgos con los procesos actuales de gestión de riesgos dentro de la industria de la construcción en Suecia serán investigado. Al involucrar a contratistas y desarrolladores; técnicas de gestión, percepción del riesgo y la propensión al riesgo, independientemente de la relación contractual convenio. Consultores con experiencia tanto desde la perspectiva del desarrollador como del contratista se han incluido para comprender la conexión entre cómo se gestionan los riesgos para el final producto: el edificio terminado. Este estudio exploratorio se investigó cuando se utilizando un estudio a través de semiestructurado entrevistas para identificar riesgos con el proceso de gestión de riesgos un enfoque de investigación abductivo fue elegido. Las conclusiones de la tesis servirán como base para resaltar los riesgos en la industria de construcción y proponer algunos procedimientos correctivos para mejorar aún más los beneficios de una de las industrias más grandes e importantes de Suecia. La selección de los entrevistados se basó en encontrar una mezcla de profesionales dentro del industria de la construcción que todos trabajan de alguna manera con la gestión de riesgos y que pueden hacer o tomar decisiones que impliquen riesgo.

Tabla 2
Lista de entrevistados

Interviewee	Actor	Years of experience
1	Contractor	5
2	Consultant	15
3	Developer	33
4	Contractor	20
5	Developer	22
6	Developer	25
7	Consultant	29
8	Contractor	23
9	Developer	14
10	Contractor	20

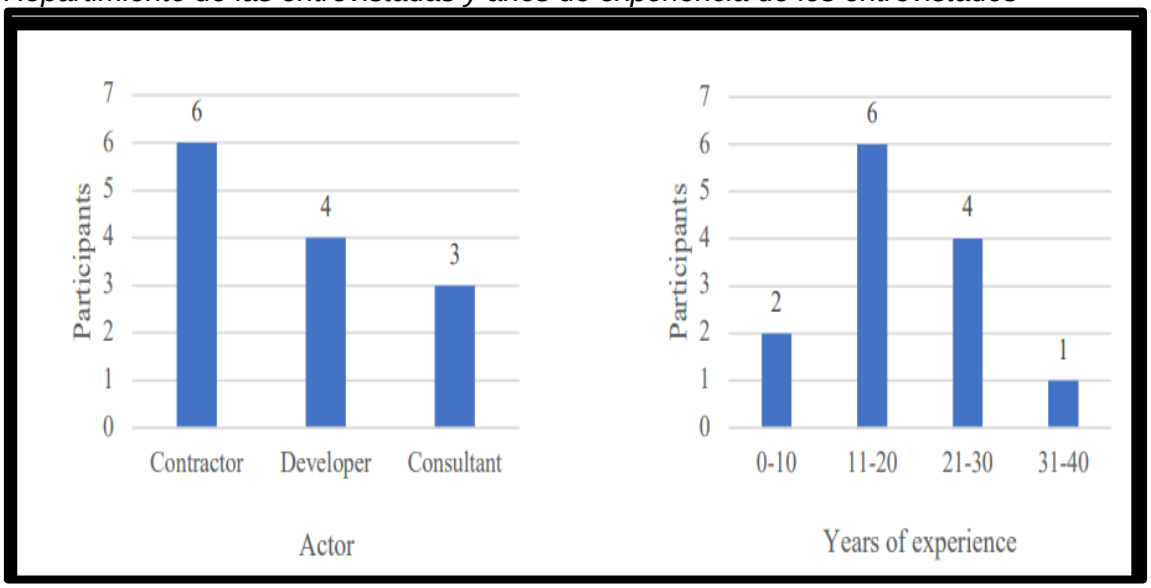
11	Contractor	0
12	Contractor	15
13	Consultant	19

Fuente: Jannis Turac.

Se puede apreciar en la tabla 02 que los participantes provenían de siete organizaciones diferentes en un total de 13 entrevistas. Se celebraron y los participantes procedían de siete organizaciones diferentes

Figura 1

Repartimiento de las entrevistadas y años de experiencia de los entrevistados



Fuente: Jannis Turac.

La tabla describe la lista de los entrevistados y las figuras 1 muestran la distribución y años de experiencia de los entrevistados.

Como autor Santiago (2020), con la tesis Aportes para la adecuación del marco jurídico de la ciberdefensa y la ciberseguridad en Argentina con la problemática se genera a través de los servidores, enrutadores y conexiones. Se genera un bloqueo de los servidores en diversas locaciones como EE. UU, Rusia y China creando edificios sutiles con una réplica de antecedentes con una mesura de seguridad. Las causas surgen por el derecho de internacionalidad de seguridad ya que se recibe severos ataques de virus. Con una conclusión de establecer diversos aportes de ciberdefensa y ciberseguridad.

Ramos, Arango y Tinoco (2020) según la empresa operadora de seguridad en Bogotá Colombia. Surge el planteamiento de la era mundial de la pandemia del Covid-19, con una economía y educación sin una tendencia de tecnología y con el crecimiento de infraestructura de la era digital con diversos aportes del Banco Interamericano -BID se generó unos los 3 meses con una aceleración que anticipó 3 años. Posteriormente se tiene un porcentaje de 74% de diversas áreas con el trabajo de remoto con la nueva normalidad. Con una crítica OT, servidores en la nueve, colaboradores en línea entre otros. Con unos resultados aplicando la medición de 128 colaboradores desempeña el rol analista de ciberseguridad y con la diferencia final 102 respuestas al nivel confianza del 100%.

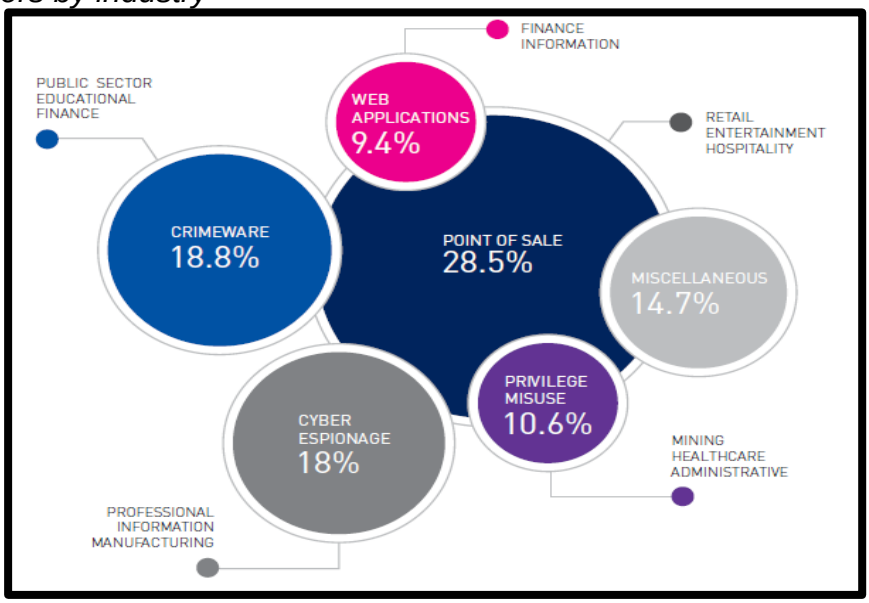
El autor Ferdinando (2016). Inicia la investigación en EE.UU en la nación necesita estar un paso adelante. Como demostrará el documento de los adversarios implacables. Ya han robado información sensible, y comprometido la privacidad de millones de estadounidenses. Con la infraestructura vulnerable, la seguridad nacional de una fuerte cultura cibernética. Para adelantarse a la amenaza, la seguridad cibernética debe estar arraigada en la conciencia nacional a través de la educación, mensajes sostenidos y una mayor cooperación entre las empresas y el gobierno. Las vulnerabilidades, cita estudios de casos, política nacional y análisis de expertos. Explorar los caminos a seguir, a partir de la información nacional. conversación y los desarrollos más recientes sobre el tema. La hipótesis es que necesitamos un cambio nacional en el pensamiento sobre ciberseguridad; necesitamos fortalecer la cultura cibernética. Para ese fin, miraré los cambios sociales usando los ejemplos de dos temas que son independientes entre sí, el tabaquismo y el uso del cinturón de seguridad. Con estos dos problemas, la sociedad cambió su comportamiento con el tiempo ante los peligros y las consecuencias.

Se tiene diversos conceptos para la variable ciberseguridad. Según el Instituto Nacional de Ciberseguridad INC (2020). El uso en redes de telecomunicaciones y dispositivos inteligentes para apoyar el teletrabajo, que contiene consejos simples y prácticos para promover la limpieza cibernética de

los puntos de conexión utilizados para el teletrabajo y originar la ciberseguridad de las personas y organizaciones.

Figura 2

Threat vectors by industry



Para la revista Defense One, 2015, los jefes de inteligencia de Estados Unidos dicen que los datos que se pierden pueden convertirse en la menor preocupación cibernética.

El autor Tucher Patrick, 2015. Los grandes ataques que se han dado a conocer en 2015 involucraron el robo de datos, y mucho. Unos 21 millones de registros de personal fueron sustraídos de la Oficina de Administración de personal en China con 4000 registros, algunos con información “sensible”, fueron robados del sistema de correo electrónico civil del estado mayor Conjunto, un robo que se atribuye a Rusia, pero los principales espías de Estados Unidos dicen que los ataques que les preocupan no implican el robo de datos, sino la manipulación directa de los mismos, cambiando las percepciones de lo que es real y lo que no lo es.

Según Corletti (2017) encuentra ocho procesos que abarca la importancia de la ciberseguridad ingreso en la producción, gestión de cambios, gestión de

accesos, configuración e inventario, gestión de Backup, gestión de incidencias, supervisión y monitorización y gestión de Logs.

El presidente Castro. (2019) El Desafío del riesgo cibernético en el Sector Financiero de Colombia y América Latina es el primer libro publicado entre la asociación en banqueros y la institución financiera colombiana Asobancaria y la Secretaría de la Organización Americana (OEA). Este documento es una compilación de una serie de estudios y publicaciones profesionales sobre la relación entre la vanguardia de la ciberseguridad y el sistema financiero de América Latina y Global, especialmente Colombia.

Finalmente, el autor Clive (2016). Dado a la amenaza de virus y malware de la informática, la seguridad y integridad de los datos, por lo que la exposición de tantas máquinas en la web proporcionó un verdadero campo de juego para hackers para poner a prueba sus habilidades, trayendo desactivar sitios web, robar datos o cometiendo fraude. es algo que nosotros ahora llámese ciberdelincuencia. Desde entonces el internet global alcanzó un estimado 3.400 millones de usuarios (aproximadamente 46% de la población mundial 2), las oportunidades para el delito cibernético se han hinchado exponencialmente.

Diferentes procesos V.D. gestión de riesgos y cambios en el riesgo del tomador de decisiones que fueron identificados en la literatura seguida por la consulta de profesionales de la industria para desarrollar más la pregunta de investigación. Un enfoque de investigación abductivo es adecuado cuando se mueve ida y vuelta entre la inducción y la deducción, para poder desarrollar inductivo inferencias y ser probado deductivo a lo largo del proceso de investigación (Saunders Lewis, y Thorn Hill, 2015).

Así mismo el autor Szymański (2017) afirma que la gestión de riesgos consta de seis etapas: riesgo sistema de identificación y alerta temprana, análisis de riesgos y formulación de variantes, evaluación de riesgos, decisiones y acciones en materia de riesgos y control seguimiento y evaluación de actividades emprendidas. En esta tesis de maestría, en los cuatro pasos iterativos de

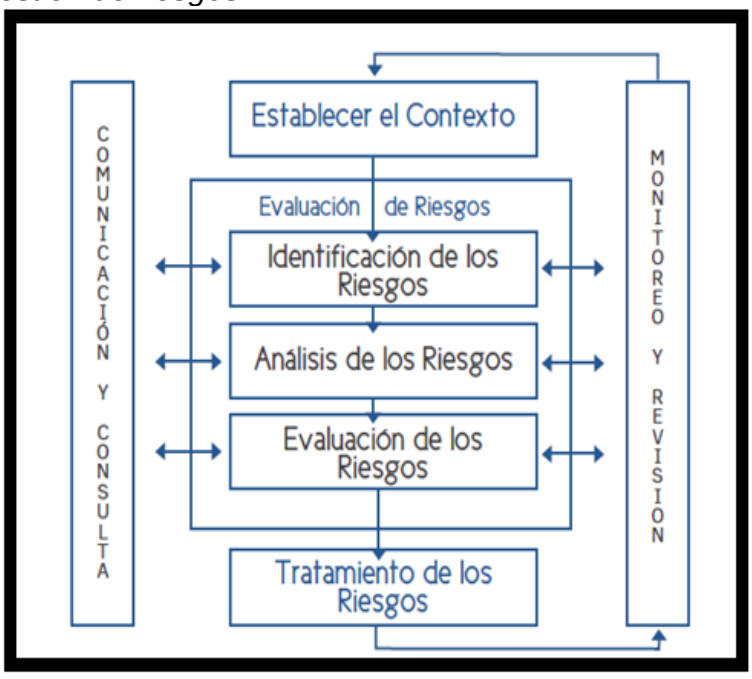
identificación de riesgos se utilizará la evaluación de análisis, la respuesta al riesgo y el control del riesgo.

Por otro lado, el autor Castro (2010). En el proceso de gestión de riesgos es una porción de integral del gobierno debe adaptarse a los procesos comerciales de la organización, reflejando la cultura y las costumbres.

La gestión de los riesgos debe ser una parte integral de la gestión y debe estar en línea con el plan de negocios de la distribución, reflejando la cultura y las prácticas. Con 5 aspectos de la creación de una situación: evaluación de riesgos y evaluación, análisis y análisis de riesgos cualitativos y cuantitativos; gestión de riesgos para la adquisición de decisiones; comunicación y asesoramiento; monitoreo y evaluación. (Casares y Lizarzaburu, 2016).

Figura 3

Proceso de gestión de riesgos



Fuente: UNE-ISO 31000 (2009): Gestión del riesgo. Principios y directrices

Se puede apreciar en la figura 03 con la causa de gestión de riesgos en la escala de evaluaciones que se demostrará a continuación para su descripción dada.

Se utilizó los Indicadores nivel de riesgos, nivel de activos y número de control aplicado, por lo cual se establecerá con la V.D. para dar solución al problema que radica la empresa en la ciberseguridad.

Manifestó el autor de Casares (2016) El proceso de gestión de riesgos es uno de los tres pilares básicos de la norma ISO 31000. La suma importancia es porque solo se puede gestionar en la práctica el riesgo que surge en el contexto de la empresa. Se establece la causa de la gestión de riesgos de los cuales son:

Establecimiento del contexto: Se inicia con los objetivos y responsabilidad por proceso con una definición de actividades con respetos alcance en reconocer la relación de diversos proyectos sanos una metodología de valor en riesgo y estableciendo críticos análisis de decisiones a su vez con reconocer estudios específicos.

Contexto externo: Se establece por el ambiente social, cultural, político, legal con reglamento, económico con financiero y tecnológico. Con relaciones de varios grupos (stakeholders) externos. Con un objetivo impactante a las organizaciones.

Contexto interno: Se encuentra con estructura organizacional con funciones y responsabilidad, políticas obteniendo el objetivo y estrategias implementadas de alcance, capacidad con intuición de recursos humanos, grupos de interés stakeholders internos.

Análisis de riesgos: Su implementación consigue variar ampliamente dependiendo de factores tales como amenazas, objetivos e información de la investigación, datos, recursos disponibles, etc. Logra ser cuantitativo los resultados con los factores de riesgo están determinados por los resultados de los estudios de exploración y pueden tener efectos tanto visibles como invisibles.

Evaluación de Riesgos: El objetivo principal es apoyar las decisiones para determinar los riesgos que deben abordarse y priorizarse en los resultados de la estimación. Esto puede llevar a la decisión de no ver la amenaza de otra manera que no sea la gestión real. Las decisiones son reglas, regulaciones y otros.

Tratamiento de riesgos: Se tiene los riesgos, caso de oportunidad, toma de riesgos o incremento, fuentes de riesgo con la probabilidad transfiriendo o mitigando, retener el riesgo con una toma de información y compartir el riesgo activo.

Comunicación y consulta: Contactar y discutir con las partes interesadas en el proceso de las etapas para identificar el proceso y las partes interesadas.

Monitoreo y revisión: Se resalta algunos aspectos de riesgos que garanticen una gestión eficaz y eficiente mediante el seguimiento del rendimiento y la recepción de información adicional para mejorar la evaluación de riesgos. Analiza eventos, cambios, tendencias, éxitos y fracasos y cuéntale a tu organización lo mejor de ellos. Reconocer cambios en contextos internos y externos, revisar y priorizar el procesamiento de riesgos e identificar nuevos riesgos

Teoría de decisión

Peñaloza (2010). En la investigación del autor se dio como criterio en la información utilizable, las decisiones se pueden clasificar en tres tipos:

Tabla 3:

Clasificación de los tipos de decisiones

TIPO DE DECISIÓN	INFORMACIÓN	RIESGO
Contextos de Certeza	Clara, exacta y complete	Bajo
Contextos de Riesgo	Con probabilidad de dicho	Medio
Contextos de Vacilación	Muy insuficiente o nula	Alto

Fuente: Elaboración Propia

Por la norma internacional ISO 3100 Se tienen los principios para la gestión del riesgo tomado de los cuales son: La creación y protección del valor de una organización, la integralidad organizativa, la estructurada con oportuna,

la dinámica y receptiva al cambio, se basa en mejorar la información disponible, la toma de los factores humanos y adaptada a la organización.

Por Calle Juan (2020) Nos dice que la organización tiene diferentes objetivos estratégicos y la muestra al riesgo varía de una organización a otra. Sin embargo, ese tiene un proceso de gestión de riesgos. Por lo cual se tiene cinco fases elementales que establecen la madurez de la gestión de riesgos dentro de una organización.

Primera etapa:

Base tradicional: En una etapa que no existe una estructura formal para hacer frente al riesgo. De esta forma, el riesgo siempre está presente y los gestores de riesgos actúan de forma independiente.

Segunda etapa:

Concientización: En esta etapa para el proceso de gestión de riesgos operacionales la llevan a cabo empresas que establecen capacidades de gestión de riesgos dedicadas. Definen lineamientos, responsabilidades y herramientas de apoyo.

Tercera etapa:

Monitoreo: Una vez que se han reconocido todos los riesgos, es trascendental al descifrar el embudo de los procesos comerciales. Esta fase del proceso de gestión del riesgo operativo controla el nivel de riesgo actual y la eficacia de las funciones de gestión del riesgo.

Cuarta etapa:

Cuantificación: Es una fase del proceso para la gestión del riesgo operacional en la que una organización se vuelve más madura. En esta etapa, las instituciones financieras ya tienen una mejor comprensión de la situación del riesgo operativo.

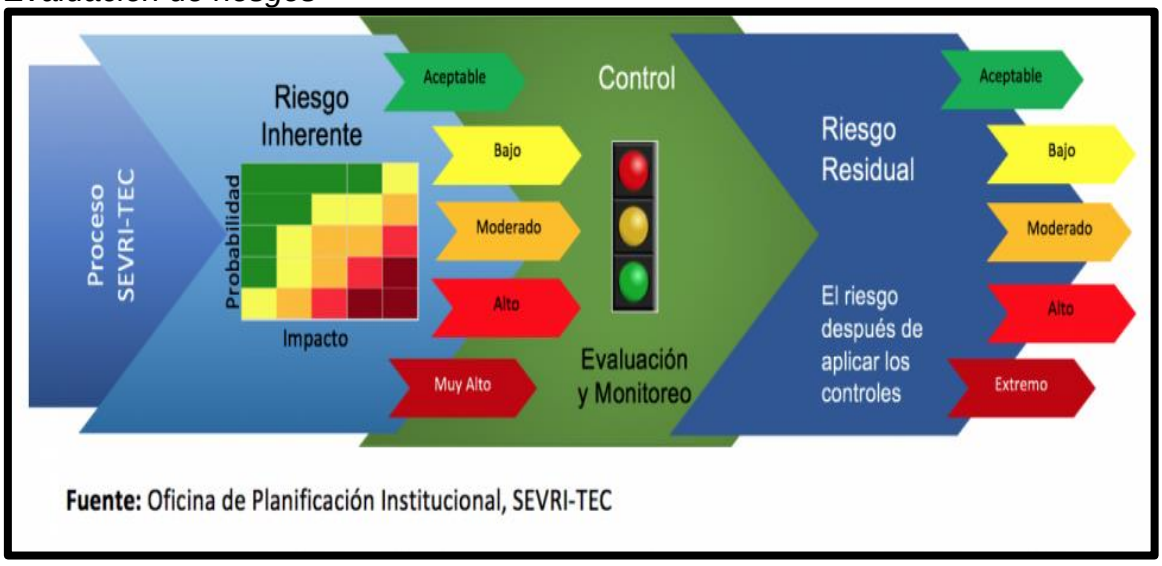
Quinta etapa:

Integración: Es la importancia de gestionar el riesgo operacional es examinada por las áreas de negocio involucradas en la plena integración del

parámetro de los riesgos en una empresa y no se limita a considerar el riesgo operacional. En este sentido, la cuantificación se aplica a la planificación estratégica ya la mejora de la calidad de los procesos.

La gestión de riesgos del TEC se basa en tres fases: evaluación del riesgo, definición de la respuesta al riesgo e implementación de las acciones de respuesta.

Figura 4
Evaluación de riesgos



Fuente: Oficina de Planificación Institucional, SEVRI-TEC

Se aprecia en la figura 04 por SEVRI-TEC el proceso de evaluaciones de riesgos inherentes y riesgos residuales.

Según Carrasco (2021) Se manifestó en el nivel de activos, se refieren a los bienes y derechos que se poseen. Analizar qué es un activo, cómo se clasifica y cómo se explica su depreciación.

Así mismo en instituto nacional de defensa civil - INDC (2006), Nos manifiesta que en el nivel de riesgo son vulnerabilidades en un rango de crítica de lo bajo a un porcentaje de alto.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Mostró Baena (2014) El objetivo es aportar hechos nuevos que se pueda confiar en los hechos revelados y evaluable para la teoría. Puesto que un problema es concreto y no puede resolverse aplicando el principio abstracto.

Por otro lado, el autor Caballero (2014). Se llama estudio práctico o empírico. Este tipo de investigación se caracteriza por considerar la finalidad práctica del conocimiento. El propósito de este tipo de investigación es desarrollar el conocimiento técnico que se puede aplicar de inmediato para resolver una situación particular. Sucede como una serie de actividades diseñadas para aprovechar los resultados.

Se tiene por parte del autor Barbour (2013) sobre la investigación cuantifica que es este estudio el que recopila y luego interpreta información que no se puede cuantificar en función de las observaciones del comportamiento. Su propósito es explicar las características de los hechos o fenómenos. La investigación cualitativa está interesada en hacer accesibles experiencias, interacciones y documentos en un contexto natural.

Como señala el autor Kerlinger (1979). En los estudios no experimentales son aquellos que se llevan a cabo fuera de manipular intencionalmente las variables. Como es una tesis que no cambia intencionalmente la V1 Los estudios no experimentales observan y analizan fenómenos que ocurren en situaciones naturales.

3.2. Variables y operacionalización

Variable Independiente (V1):

Sistema de ciberseguridad

Martínez y Fernández (2020). La ciberseguridad surge para eliminar las diversas amenazas que generalmente en referencia a la capacidad de administrar de acceso en la red, integra una aplicación de todo el sistema para la observación y la gestión de inseguridades relacionadas con ella. El uso,

proceso de almacenar y entrega de información o antecedentes en el proceso y procedimientos utilizados sobre la base de estándares internacionalmente aceptados, y debe desarrollarse como un proceso continuo.

Se manifestó Cybersecurity y Infrastructure Security Agency (CISA) (2019) La ciberseguridad es una tecnología que protege las redes, los dispositivos y los datos del acceso no autorizado o el uso delictivo, y mantiene la confiabilidad, integridad y disponibilidad de la información. En años recientes, la ciberseguridad se ha vuelto más prioritaria en los negocios ya que los usuarios y las empresas son más conscientes de las amenazas que afectan a sus datos privados. Además, con esfuerzos de regulación específicos como el reglamento general de protección de datos (GDPR) en 2016 y la ley de protección de datos (DPA) en 2018, ahora hay instrucciones claras y consecuencias para motivar a las organizaciones a establecer una adecuada ciberseguridad infraestructura y gestión.

Variable Dependiente (V2):

Gestión de riesgos:

Para Peltier (2014), Las estrategias en gestión de riesgos incluyen identificación de riesgos, evaluación que pueden hacer y la adopción de medidas para minimizar todos los riesgos y niveles aceptables. Todos los sistemas de análisis de amenazas utilizan el mismo método. Encuentra los tesoros que quieres explorar. Identificar amenazas, problemas o debilidades.

Operacionalización de Variables:

Nos indica el autor Arias (2022). El propósito principal de esta tesis científica es desarrollar una guía para el desarrollo de la manipulación de variables, dirigida a docentes, investigadores, estudiantes y doctorandos que se dedican a la investigación científica de manera cuantitativa. Pretende brindar una herramienta para que estudiantes e investigadores conozcan los criterios básicos y los pasos a seguir para crear una tabla de manipulación de variables tanto desde la parte teórica como desde la práctica. Esta guía se divide en seis

partes básicas: variables, definiciones conceptuales de variables, definiciones operativas, dimensiones, indicadores y escalas de medición. (Ver Anexo 02).

Según la autora Mercedes (2019). El proceso de manipular variables es el proceso de reemplazar algunas variables con variables más específicas que representan las variables reemplazadas. Un ejemplo de este proceso son las calificaciones escolares. Sirve como un indicador necesario para calcular la escala del éxito de la exploración.

3.3. Población, muestra, muestreo

En el ISO 27001 los controles identificados son aquellos que se utilizan en las organizaciones con un análisis de riesgos por un método. El valor de riesgos es puesto de tener medidas de seguridad que disminuyen en el impacto de la vulnerabilidad del activo que incidente de seguridad.

Por tanto, si la población alcanza la plena accesibilidad considerando el número de unidades que la componen, no es necesario realizar una muestra. A que se consideraron 17 activos en informática y 114 controles. La muestra según Castro (2003). La población es menor a 50% del individuo es igual a la muestra. Por lo consiguiente la empresa no se aplicó la muestra por la cantidad aplicada.

Menciona el autor Hernández (2014). La investigación es que no definen claramente la identidad de las personas ni piensan que la muestra la representa automáticamente. Es frecuente que algunos estudios se basen únicamente en la muestra de los alumnos universitarios (puesto que es más posible poner medidas ya que están a la mano) haciendo calientes generalizaciones acerca de que estos adolescentes pueden tener otras características sociales. Por lo tanto, es mejor crear una identidad clara de los habitantes, para definir cuál será el tamaño de la muestra.

Lepkowski (2008) Una vez definido el apartado de evaluación de análisis, se cuantifica el número de estudios a estudiar y se consideran los resultados globales. Así, la población es toda una función del sistema legal.

3.4. Técnicas e instrumentos de recolección de datos

Técnica

Mejía, Sanchez y llanes (2018) Es un conjunto de equipos y medios por los cuales se ejecuta un método. La diferencia entre métodos y técnicas es que los métodos son una serie de pasos y fases que debe seguir la investigación, lo cual se aplica a algunas ciencias.

La información se recopila mediante una técnica utilizando indicadores en cada dimensión para generar ítems que son cuestionarios para medir variables**.**

Instrumento

Se utiliza ficha de observación según Diaz (2021). Mostró que en la estructura con un nivel de crítico y registrar cada uno presentando en una tabla con valores mostrando el puntaje adecuado.

Manifestó Rojas (2021). La ficha de observación es un instrumento de recolección de información que determina el comportamiento y brinda el resultado de la investigación.

Se aplicará para los usuarios en la organización, Por ello, la recolección, procesamiento e interpretación de datos se realizan cumpliendo el protocolo de bioseguridad y utilizando tecnologías de la información.

3.5. Procedimientos

El procedimiento de este estudio es el siguiente. Se tiene para la gestión de riesgos, se coordinó con la dueña de la empresa para brindar una buena solución ante el problema. Luego aplicó una encuesta virtual generando una herramienta de medición variable. En el modelo de sistema de ciberseguridad será como plantación al ISO 31000-2009 gestionado el régimen local, la norma del ISO 27001 para evaluar el riesgos y control de ISO 27002. para su análisis. De esta manera ISO/IEC TR 13335-3, se evaluaron las fichas derivados fueron integrados por el software IBM SPSS Statistics 25, para posteriormente el análisis. Además, se evaluaron las hipótesis generadas en la investigación. Finalmente, un ISO 17799:2005 por lo que se tiene la revisión de SGSI con resultados.

3.6. Método de análisis de datos

Descriptiva

Espinoza (2018). Una característica del dispositivo para lograr medidas que pertenezcan al contexto. El dispositivo es confiable si los datos obtenidos son los mismos cuando se aplican al mismo sujeto en dos ocasiones diferentes.

Por otro lado, Rendon y Villasis (2016). Las estadísticas descriptivas es una rama de las estadísticas que formulan recomendaciones sobre cómo resumir los datos de la encuesta de una manera clara y sencilla con diagramas, tablas, diagramas o gráficos.

Enfoque Cuantitativo

Manifestó Torres (2014). El enfoque cuantitativo es reconocido por la recolección de información como un conjunto de procesos para la aprobación de la hipótesis mediante los análisis estadísticos y define el comportamiento dado.

Inferencial

De mismo modo, Andale (2014). Las estadísticas de inferencia le permiten hacer predicciones ("inferencias") a partir de estos datos. La estadística inferencial toma identificaciones de una muestra y los generaliza a una población.

3.7. Aspectos éticos

En la actual la investigación es de mi autoría, ya que los datos fueron recolectados, procesados e interpretados por el autor. La información bibliográfica utilizada en el estudio está correctamente referenciada como estándares de asociación americana de psicología (APA) 7ª Edición. Además, este trabajo de investigación será evaluado en el programa de Turnitin y producirá un informe único basado en la Resolución de Investigación del Vicepresidente Ejecutivo N° 020-2022-VI/UCV. Además, cumple con los lineamientos exigidos por la UCV. de acuerdo con la Resolución Administrativa N° 110-2022-VI/UCV a recopilar los datos.

IV. RESULTADOS

Análisis Descriptivo

Se realizó el estudio del impacto del tema de investigación originada con el indicador de nivel de riesgo y la aplicación con medidas de control en el proceso de gestión de la empresa.

INDICADOR 01 Y 02: Resultados descriptivos de los indicadores nivel de activos, nivel de riesgos y número de control de aplicada en antes y después de implementar el sistema con la metodología de SGSI.

Tabla 4

Estadísticos descriptivos de nivel de activos, nivel de conocimiento riesgo y número de control de aplicada en Pre Test y Post Test

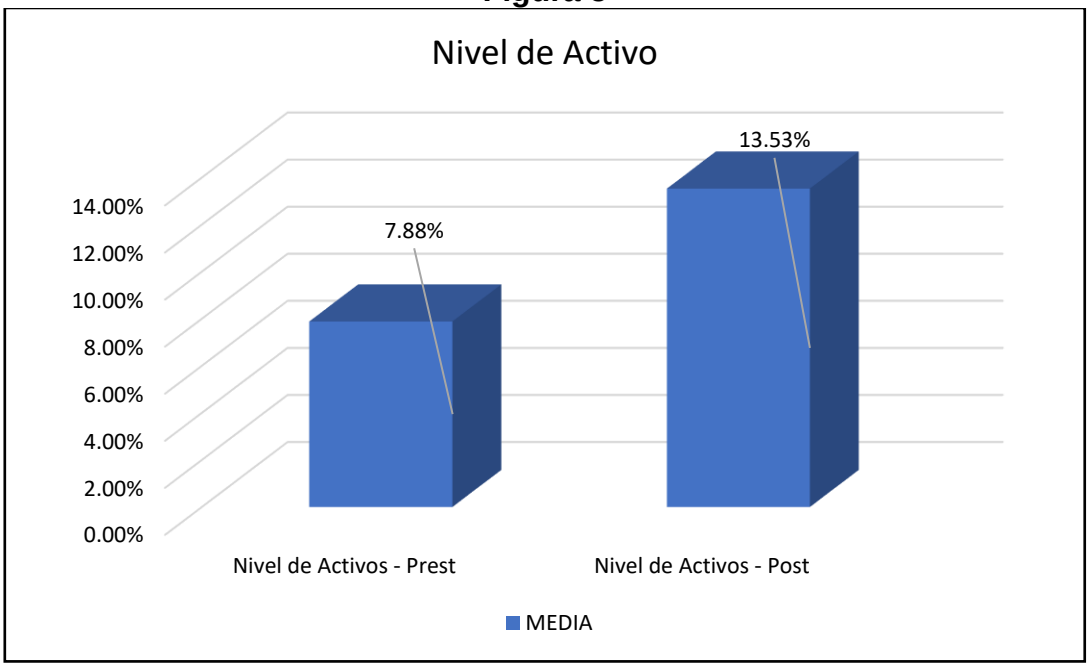
Estadísticos descriptivos

	N	Rango	Mínimo	Máximo	Media	Desv. Desviación
PreT_Nivel_Riesgos	17	11,00	4,00	15,00	9,5147	3,27212
PosT_Nivel_Riesgos	17	10,00	15,00	25,00	18,7353	3,11307
PreT_Nivel_Activos	17	8,00	4,00	12,00	7,8824	1,83311
PosT_Nivel_Activos	17	14,00	6,00	20,00	13,5294	4,17010
Prest Numero Control A.	114	1	1	2	1.13	,340
Post Numero Control A.	114	1	1	2	1.04	,185

Fuente: Elaboración Propia

Se muestra en la tabla 04 para el primer indicador nivel de riesgo para la variable gestión de riesgo, se obtuvo un valor de 9.5% a 18.74% en cuanto a la dispersión se tuvo una desviación de 3,27%; posteriormente a 3,11% en el segundo indicador nivel de activos, se obtuvo un valor de 7,88%, a 13,53%. En cuanto a la dispersión se asumió una desviación de 1,83%; y subsiguientemente de 4,17%. En el tercer indicador número de controles, se obtuvo un valor de 1,13%, a 1,04%. En cuanto a la dispersión se poseyó una desviación de 0,340%; y se asumió de 0,185%. de aplicados.

Figura 5

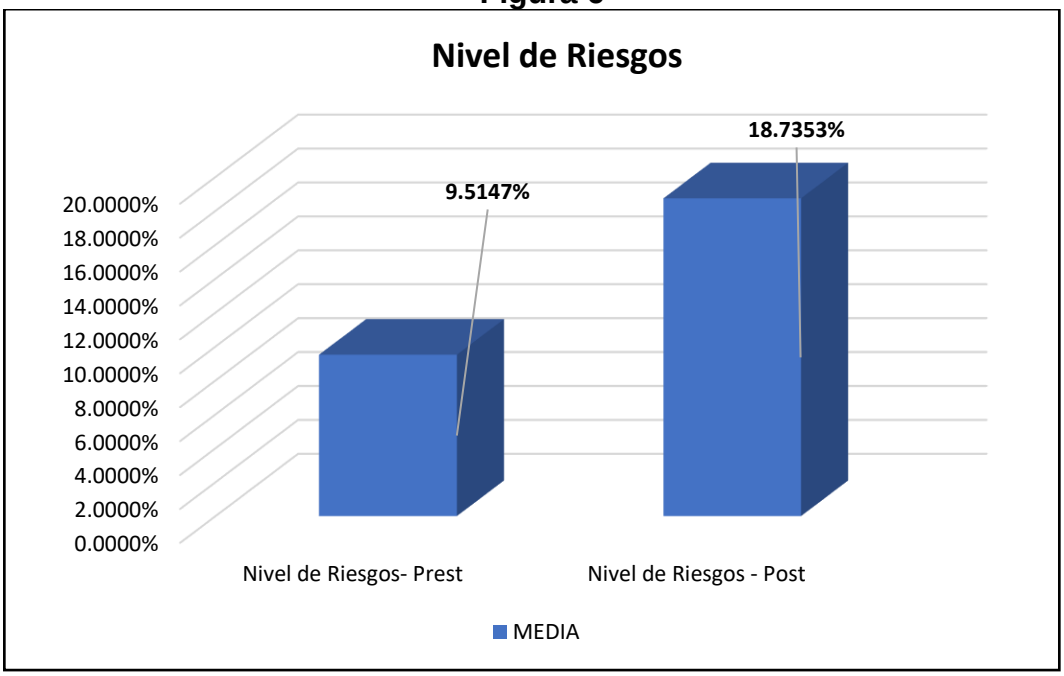


Fuente: Elaboración Propia

PreTest y PostTest niveles de activos

Como se observa en la figura 05, se tiene el pretest de 7.88% aplicado mediante la implementación se logró 13.53%. Entonces existe una diferencia antes y después de la aplicación de modelo de sistema ciberseguridad.

Figura 6



Fuente: Elaboración Propia

PreTest y PostTest niveles de activos

Como se observa en la figura 06, se tiene el pretest de 9.5% aplicado mediante la implementación se logró 18.73%. Entonces existe una diferencia antes y después de la aplicación de modelo de sistema ciberseguridad.

INDICADOR 3: Resultados descriptivo de Número de controles aplicados en un antes y después.

Tabla 5:

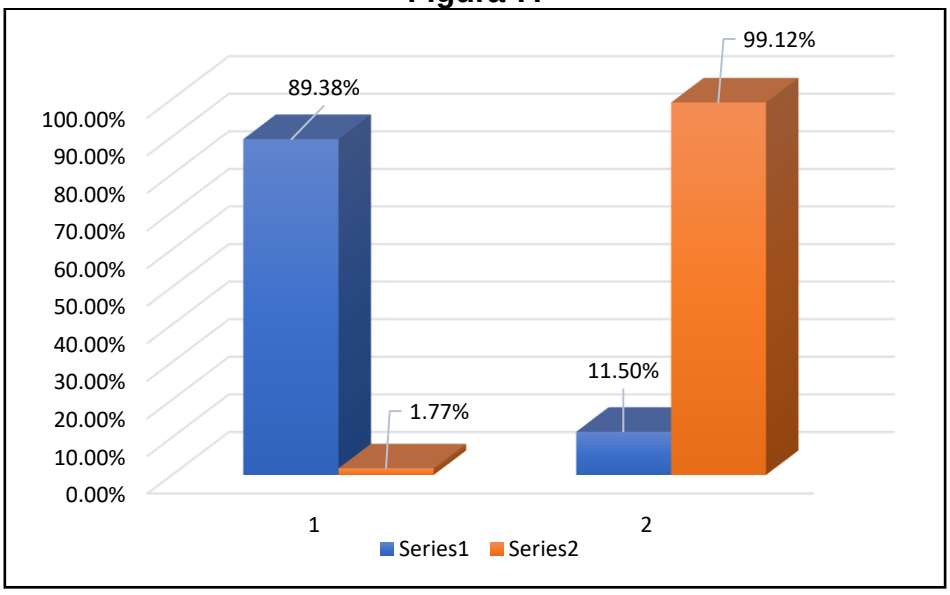
Resultados descriptivos de la prueba cruzada para números de controles aplicados con la metodología SGSI

Tabla cruzada Existencia de controles por Tipo de prueba

			TIPO DE PRUEBA	
			Pre Test	**Post Test**
Existencia del control	**No aplica**	Recuentro	101	13
		% dentro de Tipo de prueba	89.38%	11.50%
	Si aplica	Recuentro	2	112
		% dentro de tipo de prueba	1.77%	99.12%
Total		Recuento	114	114
		% dentro de tipo de prueba	100%	100%

Fuente: Elaboración Propia

Figura 7:



Existencia del control

En la tabla 05 y figura 7 por el indicador número de controles trabajadores, no se aplican en el 89.38% en el Pre_Test, sin embargo, el 99.12% (114), se utilizan en el Post_Test. De esta manera, solo se emplean 2 controles (1.77%), al inicio del proceso (pretest). Por la metodología de SGSI se alcanzó el objetivo en la variable 2.

ANÁLISIS INFERENCIAL:

Pruebas de Normalidad

En la toma de los indicadores debido al tamaño de la muestra que está conformado por 17 activos de información y es < 50. Se considera que los datos son cuantitativos con la prueba no paramétrica la distribución es no normal aplicando Shapiro-Wilk, de lo cual se obtuvieron los siguientes resultados a continuación.

Si: Sig. < 0.05 adopta una distribución no normal.

Sig. ≥ 0.05 adopta una distribución normal.

Dónde:

Sig.: P-valor o nivel crítico del contraste

Prueba de normalidad del indicador nivel de riesgos y nivel de activos de antes pretest y después de implementar el sistema de ciberseguridad.

Tabla 6:

Prueba de normalidad del nivel de riesgos, nivel de activos y números de controles aplicado

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
	Estadístico	gl	Sig.	**Estadístico**	**gl**	**Sig.**
PreT_Nivel_Riesgos	,132	17	,200*	**,964**	**17**	**,712**
PosT_Nivel_Riesgos	,182	17	,139	**,898**	**17**	**,064**
PreT_Nivel_Activos	,231	17	,016	**,900**	**17**	**,067**
PosT_Nivel_Activos	,194	17	,089	**,920**	**17**	**,146**
Prest Numero Control A.	,519	114	,000	**,398**	**114**	,000
Post Numero Control A.	,540	114	,000	**,178**	**114**	,000

Fuente: Elaboración Propia

Interpretación: Obteniendo resultado en la Tabla 6 de la prueba en el primer indicador nivel de riesgos de 0.712, es >0.05. Por lo tanto, un después de 0.064, cuyo nivel de sig. es >0.05. En el segundo indicador nivel de activos con un antes de 0.067, cuyo valor es >0.05. Por lo tanto, después de 0.146, cuyo nivel de sig. es >0.05. En el tercer indicador el número de controles aplicados con un antes de 0.000, cuyo valor es <0.05. Por lo tanto, después de 0.000, cuyo valor es <0.05. Dando como ejemplo la distribución que es no normal en ambos datos de la muestra, por lo siguiente la hipótesis se utilizó la prueba no paramétrica de Wilcoxon.

PRUEBA DE HIPÓTESIS

Se procederá a realizar la prueba de hipótesis para cada indicador. Por lo consiguiente se muestra los tipos de caso.

HIPÓTESIS GENERAL

H0: La implementación de un modelo de sistema de ciberseguridad para la gestión de riesgo que mejora una empresa de matizados de pintura de Lima, 2022.

H0: u2 = u1

H1: La implementación de un modelo de sistema de ciberseguridad para la gestión de riesgo que no mejora una empresa de matizados de pintura de Lima, 2022.

H1: u2 > u1

Nivel de Significación

Se ha considerado α= 0.05 en nivel de confianza del 95%

Regla de decisión:

Si p ≥ α, se acepta la hipótesis nula H0

Si p < α, se rechaza la hipótesis nula H1

Resultados de Prueba de T-Student de muestra relacionada de los indicadores Nivel de Activo y Nivel de Riesgos

Tabla 7:

Resultados de muestra relacionada en los indicadores Nivel de Activo y Nivel de Riesgos

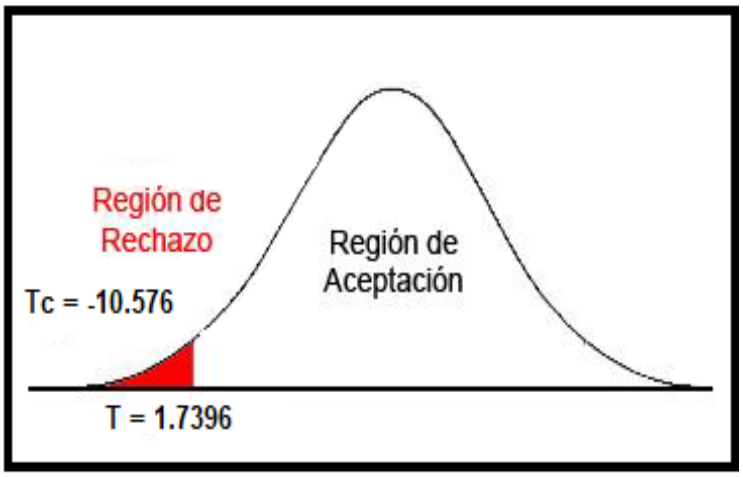
Prueba de muestras emparejadas

		Diferencias emparejadas					T	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior			
Par 1	PreT_Nivel_Riesgos PosT_Nivel_Riesgos	-9,22059	3,59457	,87181	-11,06875	-7,37243	-10,576	16	,000
Par 2	PreT_Nivel_Activos PosT_Nivel_Activos	-5,64706	4,07647	,98869	-7,74299	-3,55113	-5,712	16	,000

Fuente: Elaboración Propia

Reemplazando entonces en T en Nivel de Riesgos:

Figura 8:



Estadísticos de tabla T-Student NG

$$Tc = \frac{-9,22059}{3,59457 / \sqrt{17}}$$

$$Tc = \frac{-9,22059}{\frac{1}{3,59457}}$$

$$4.12310563$$

$$Tc = \frac{-38.017467}{3.59457}$$

$$Tc = -10,576$$

Reemplazando entonces en T en Nivel de Activos:

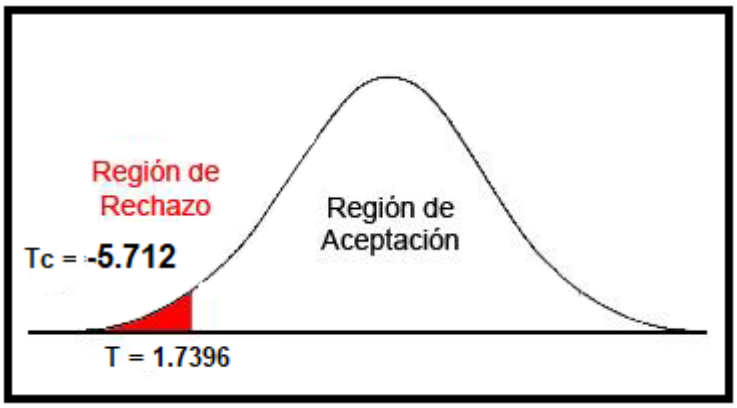
Figura 9:

$$Tc = \frac{-5.64706}{4.07647/\sqrt{17}}$$

$$Tc = \frac{\frac{-5.64706}{1}}{\frac{4.07647}{4.12310563}}$$

$$Tc = \frac{-23.2834}{4.07647}$$

$$Tc = -5.712$$



Estadísticos de tabla T-Student NA

Interpretación

El valor dado en la hipótesis se empleó la prueba para muestra relacionadas siendo paramétrica los datos alcanzados en la investigación se distribuyen normal. El valor es del primer indicador fue de -10.576, el segundo indicador de -5,712 y el tercer indicador 3,474 interpretando que se rechaza la hipótesis nula, reconociendo la hipótesis alterna con un 95% de confianza.

Resultados de Prueba de Wilcoxon del indicador Número de Controles Aplicados

Tabla 8:

Prueba de rangos con signos Wilcoxon del indicador Número de Controles Aplicados

Rangos				
		N	Rango promedio	Suma de rangos
POST - PREST	Rangos negativos	11[a]	6,00	66,00
	Rangos positivos	0[b]	,00	,00
	Empates	103[c]		
	Total	114		

Fuente: Elaboración Propia

En los dados mostrados de la tabla 08 los resultados demuestran que los 114 controles es por la aplicación de ISO 27001 en el indicador mostrando un rango de promedio.

Tabla 9:

Resultados estadísticos de prueba del indicador NCA

Estadísticos de prueba[a]	
	POST - PREST
Z	-3,317[b]
Sig. asintótica(bilateral)	,001

Fuente: Elaboración Propia

Interpretaciones:

Tal como se aprecia en la tabla 08 y tabla 09 se aplicó Wilcoxon siendo no paramétrica no existe una normalidad en vista que el p- valor obtenido (p=0.01 < α= 0.05), entonces existe evidencia para rechazar la hipótesis nula. Este resultado confirma la gestión de riesgos en H1.

V. DISCUSIÓN

En esta presente investigación, se detalló él logró del objetivo en la mejora de la ciberseguridad en la gestión de riesgos por lo cual se dará la exposición de los diversos casos por postura de diferentes autores dando la fidelidad del nivel estadísticos alcanzado en diversas por regla general, las conclusiones recogen los hallazgos más importantes en las organizaciones competitivas. Por lo tanto, en la investigación con una población de 17 activos informáticos con 114 controles mostrando con el ISO 27001 para los controles de seguridad se genera la discusión a continuación.

Por ende, se tiene la hipótesis en general que se aplicó variable 2 en la empresa en el presente año. En la hipótesis se evidencia que se rechazar la hipótesis nula. Se dio la investigación con una prueba de un antes y después con los indicadores nivel de activos en el Pre-test se obtuvo en la prueba de normalidad con Shapiro-Wilk en un nivel sig. de un antes 0,067, cuyo valor es > 0.05 y un después de 0.146, cuyo valor es > 0.05. Dando la prueba estadística con 0,900 a 0,920 y con el resultado de la descriptivo en el indicador nivel de activos que muestra antes de modelo de sistema ciberseguridad fue un valor de 7.88%, mientras que en el Post-test fue de 13,53% así mismo, el nivel de activos mínima fue del 4% y un después de 6% y la en cuanto a la dispersión se tuvo una desviación de 1,83%; sin embargo, se tuvo un valor de 4,17%. se distribuye normal. Con el resultado de la muestra relacionada en el indicador con una media de -5,65%, una desviación de 4,08, con un intervalo de confianza inferior de -7,742 y superior de -3,55 se utilizó una prueba de T-Student con resultado paramétrica distribuye normal.

Se discute por los resultados de los indicadores a través del investigador Aliaga Cristian en el 2021 teniendo una población de 50 usuarios en la organización con un control de informática se da la postura en el indicador nivel de activos se generó una hipótesis no normal estableciendo un nivel de confianza de 95% y un nivel de significancia α = 5% = 0.05 se utilizó la prueba de Kolmogorov-Smirnov. Por lo cual es 0,236 y un valor 0,504 en la fase Post Test teniendo un nivel de significancia p>0.05 por lo que se deriva un nivel de

confianza de 5% y con distribución no normal por lo cual la hipótesis se realizó un a prueba estadística T-Student. Con un resultado descriptivo un promedio de 18,0400 puntos con la desviación +/- de 2,1284 con un valor máximo alcanzado de 23 para su propósito después del sistema de ciberseguridad con un aumento de valor de baja prevalencia de 0-13, media prevalencia de 14-26, alta prevalencia de 27-40 después del Post test se presenta un 14% de media prevalencia y 86% de alta prevalencia que muestra positivamente en el sistema ciberseguridad para mejorar la disminución de ataques. Puesto el resultado brindado que se utilizó se trabajó la misma variable en la presente investigación dando resaltar que el autor Aliaga se obtuvo en la era de la pandemia por COVID 19. Se dio con diversas demostraciones como en la postura de la hipótesis en la tesis del investigador se representó como nula por sus datos estadísticos tiene una similitud.

Por otro lado, se discute el indicador del autor Huerta Carlos en el 2019 con una metodología en ISO 27001:2013 aplico tipo aplicada con un diseño pre experimental y trabajo para su población 24 activos críticos de información siendo una muestra menor se determinó la prueba de normalidad con Shapiro-Wilk aplicando los indicadores su siguientes: En el indicador de nivel de riesgos antes y después de implementar SGSI. Se muestra que 12,32 puntos de promedio, con una desviación +/- de 3,44 puntos, con valor máximo alcanzado de 21,25, se percibe que la disminución de riesgos en el Post Test se reporta un promedio de riesgo de 8,70 puntos, con una variación +/- de 1,69 dando el máximo de 12,00. Con una disminución de riesgos lo cual refleja una influencia significativa de la metodología SGSI aplicada para mejorar el proceso de gestión del riego, se tiene 0,579 posteriormente a 0,714 ambos mayores al nivel de significancia ($p > 0.05$), con una distribución normal, por tanto, la contratación de las hipótesis se realiza mediante la prueba estadística paramétrica de T_Student. El un nivel de significancia p valor= 0,000 y un valor del estadístico de la prueba Wilcoxon de -9,644, en la comparación de medias del Pre y Post Test. Puesto el resultado brindado que se utilizó por el autor Huerta se originó en la pandemia por COVID 19 reflejando los puntos a favor. Sin embargo, se verificó que el resultado demostrado en la postura de la hipótesis en la tesis del investigador se

representó como nula por sus datos estadísticos tiene una similitud y una variación en la prueba en Wilcoxon dando el porcentaje alto. La hipótesis fue rechazada mientras que en la tesis de investigación dio como resultado nulo al indicador.

En el segundo indicador nivel de riesgo se obtuvo en la investigación como una prueba de un antes y después con los indicadores nivel de riesgos se logró en la prueba de normalidad con Shapiro-Wilk en un nivel sig. de un antes 0,712 cuyo valor es > 0.05 y un después de 0.064, cuyo valor es > 0.05. Dando la prueba estadística con 0,964 a 0,898 y con el resultado de la descriptivo en el indicador nivel de riesgos que muestra antes de modelo de sistema ciberseguridad fue un valor de 9.51%, mientras que en el post-test fue de 18,73% así mismo, el nivel de activos mínima fue del 4% y un después de 15% y la en cuanto a la dispersión se tuvo una desviación de 3,27%; sin embargo, se tuvo un valor de 3,11%. se distribuye normal. Con el resultado de la muestra relacionada en el indicador con una media de -9,22%, una desviación de 3,60 con un intervalo de confianza inferior de -11,068 y superior de -7,372 se utilizó una prueba de T-Student con resultado paramétrica distribuye normal en aquel momento se rechaza la hipótesis nula, aceptando la hipótesis alterna con un 95% de confianza.

Se discute los resultados a través del autor Huerta Carlos sobre la hipótesis general sobre el indicador nivel de riesgo con el resultado de descriptivo se tiene el un valor antes del mínimo de 5,67%, con un valor máximo de 21,25%, una media de 12,32% y una desviación estándar de 3,44%. Sin embargo, con un después del mínimo 5,67%, máximo de 12,00%, media de 8,70% y una desviación estándar de 1,69% con una población de 24 se utilizó la metodología de SGSI. Aplicando para el manejo de la gestión de riesgo. Donde se obtuvo en la prueba de normalidad de la hipótesis con la prueba de Shapiro-Wilk con valor estadístico de un antes de ,966% con un nivel de sig. de ,579% y un después en estadístico de ,972% en un nivel de sig. de ,714% con una distribución normal arrojando una hipótesis paramétrica con T_Student. Puesto con una muestra independiente con una varianza de 4,614 con un nivel de sig. (bilateral) de 0,000.

Dando un rechazo a la hipótesis nula(H0) y la aprobación de la hipótesis general. En la prueba de muestras independiente con un intervalo de confianza de inferior de 2,036% y superior de 5,187% con un nivel sig. de 0,000 siendo con un resultado de rechazo a la hipótesis nula (H0) y la afirmación de la primera hipótesis (H1) para la mejora del proceso de riesgo. Puesto lo mostrado se concuerda que los resultados fueron diversos dado que se trabajó con T_Student y puesto se dio con Wilcoxon con no paramétrica.

Se discute los resultados a través del autor Omar Jara en el 2018. Así mismo se considerado 31 activos y 114 puesto a la norma establecida ISO 27001 con un evaluar la confiabilidad de la ficha de observación de los controles, se empleó el método de dos mitades, se encontró un valor de 1.000 para el instrumento mostrando que la escala presentaba una confiabilidad muy elevada. Por lo cual se explica los indicadores que se trabajó. Se tiene el indicador nivel de riesgo con una disminución de nivel de riesgo de (9.96+-2.27) a (5.90+-1.60) en promedio. Donde se generó Shapiro-Wilk los resultados indican que no existe normalidad en ninguna de las distribuciones de la evaluación del riesgo del pre y post test, considerando que el p valor=0.008 <0.05 (pre test), p valor=0.003<0.05 (post test). en la prueba de Wilcoxon respecto a la evaluación del riesgo, tuvo un p valor=0.000 <0.05, de tal manera, que la prueba es significativa, por lo tanto, existen diferencias en la implementación del Sistema de Gestión de Seguridad y el indicador números de controles aplicados no se aplican en el 92.1% en el pre test, sin embargo, el 99.1% (114), se aplican en el post test. Asimismo, sólo se aplican 9 controles (7.9%), al inicio del proceso (pretest) en la prueba de Wilcoxon respecto al tratamiento del riesgo, tuvo un p valor=0.000 <0.05. Puesto el resultado brindado que se utilizó se trabajó la misma variable en la presente investigación se dio el resultado con diversas demostraciones como en la postura de la hipótesis en la tesis del investigador se representó como nula por sus datos estadísticos tiene una similitud.

El tercer en el indicador de número de controles aplicados con la metodología de SGGI. Se aplican en el 89.38% en el Pre_Test, sin embargo, el 99.12% (114), se aplican en el Post_Test. De esta manera, solo se aplican 2 controles (1.77%), al inicio del proceso (pretest) Donde se obtuvo en la prueba

de normalidad con Shapiro-Wilk en un nivel sig. de un antes 0,00 cuyo valor es < 0.05 y un después de 0.00, cuyo valor es > 0.05. Dando la prueba estadística con 0,964 a 0,898 y con el resultado de la descriptivo en el indicador número de controles aplicados que muestra antes de modelo de sistema ciberseguridad fue un valor de 1.13%, mientras que en el Post_Test -test fue de 1,04% así mismo, cuanto a la dispersión se tuvo una desviación de 0,340%; sin embargo, se tuvo un valor 0,185%. se distribuye no normal. Con el resultado de la muestra relacionada en el indicador con una media de 0,096%, una desviación de 0,297%, con un intervalo de confianza inferior de 0,41 y superior de 0,152% se utilizó una prueba de Wilcoxon con resultado no paramétrica distribuye no normal en aquel momento se rechaza la hipótesis nula, aceptando la hipótesis alterna con un 95% de confianza.

Por consiguiente, se discute los resultados de los indicadores a través del autor Huerta Carlos en el 2019. Se tiene otro indicador como números de controles aplicados antes y después de la metodología SGGI se reporta en el Pre Test que del total de los controles aplicables el 90,4% de los No existen, y tan solo el 9,6% Si existen, mientras que después de implementar la metodología SGSI, en el Post Test se reporta que el Sí existen el 91,2% de los controles, y tan solo el 8,8% No existen, resalta que 10 (8,8%) Aplicados, donde podemos apreciar un p valor= 0,000 en la fase Pre Test y un p valor= 0,000 en la fase Post Test, ambos menor al nivel de significancia (p < 0.05), por lo que se concluye con un nivel de significancia de 5%, que los datos Pre y Post Test. no presenta una distribución normal, por tanto, la contratación de las hipótesis se realiza mediante la prueba estadística no paramétrica de Wilcoxon. lo que conlleva al rechazo de la hipótesis nula (H0) y la aceptación de la hipótesis general planteada (Ha). Por lo cual se discrepa que los resultados indicados fueron dados dentro de la pandemia COVID 2019 teniendo un rechazo de la hipótesis nula y la aceptación de la hipótesis general de la propuesta. Dando que la hipótesis fue rechazada mientras que, en la tesis de investigación dio como resultado nulo al indicador.

Por lo cual manifestando los temas de investigación se da con el discurso que se obtuvo diverso resultado en hipótesis nula con diferentes cantidades de población utilizando diversidad pruebas para el cálculo estadísticos que nos muestra la importancia en la seguridad informática para la mejora de la gestión de riesgos.

VI. CONCLUSIONES

Primera: El impacto alcanzado por el objetivo general de la variable e indicadores se mejoró con el instrumento atreves de ficha de observación en el nivel de crítico con la implementación de la metodología de SGI y con el ISO 27001 con una mejora en el análisis descriptivo se concluye que en el indicador nivel de activos se obtuvo de 7.88% aplicado mediante la implementación se logró 13.53%, el nivel de riesgos se obtuvo de 9.5% aplicado mediante la implementación se logró 18.73% y número de controles aplicados se obtuvo de 89.38% no aplica y si aplica un 99.12%.

Segunda: En la determinación del objetivo específicos principal puesto al porcentaje alcanzado por la prueba de estadística de Shapiro-Wilk por cada indicador en un antes y después. Se Muestra que en la prueba normalidad en el indicador nivel de riesgos se obtuvo de 0.712%. Se conllevo al rechazo de la hipótesis nula en la investigación realizada con un aumento de resultados en la empresa de matizado de pintura

Tercera: Adecuando a lo alcanzado por el objetivo específicos segundario de la implementación del tema de investigación. Satisfactorio al resultado que afirmaron la mejora en la aplicación de la ciberseguridad para la mejora de la gestión de riesgos. Se obtuvo en el nivel de activos se obtuvo de 0.067% se logró 0.146% con la prueba de T-Student obteniendo positiva

Cuarta: Se obtiene por el objetivo específicos tercero en el resultado del indicador número de controles aplicados reportado. Donde el porcentaje del resultado es no paramétrico con la prueba de Wilcoxom por lo cual, se rechaza a la hipótesis nula se obtuvo de 0.00 <0.05 de los 114 controles con la metodología SGSI.

VII. RECOMENDACIONES

Primera: Invertir en materiales para el crecimiento de la empresa para el mejoramiento de la ciberseguridad y su a vez el disminuirá de riesgo en la organización. Como cámara de seguridad en red con un monitoreo de las 24 horas al día.

Segunda: Se recomienda con seguridad en el proceso de activos en la información se establezca con un respaldo en la nube para la protección de información y un área de mesa de ayuda en la gestión de riesgo en ciberseguridad con la finalidad de disminuir riesgos al futuro.

Tercera: Generar un control de productos en el entorno de seguridad se recomienda tener un inventario al año con la finalidad de disminuir robos y una capacitación en la implementación de la metodología de SGGI para el crecimiento de la empresa.

Cuarta: Se considera una capacitación en ISO 27001:2014 Controles de Seguridad para el mejor funcionamiento en el nivel de control en sus empleados y programar estrategia para el crecimiento de la productividad constante en la organización.

REFERENCIAS

Agudelo (2014). Gestión del riesgo en proceso. Repositorio en 29 mayo, 2022 https://docplayer.es/8972612-Cliente-ceoevolucion-com-www-ceoevolucion-com-orientamos-la-mejora-del-desempeno-organizacional.html

Alma (2018). Implementación de un Sistema de Gestión de Riesgos basados en el estándar ISO 31000 en el proceso de Atención de Requerimientos de la empresa Software Enterprise Services en la ciudad de Lima – 2018. Maestro en Ingeniería de sistemas con mención en tecnologías de la información. [Tesis de Maestro inédita]. Universidad Tecnología del Perú

Álvarez y Honorio (2018). Ciberseguridad en la actividad organizacional de la era digital. Maestro en Ingeniería de sistemas con mención en tecnologías de la información. [Tesis de Maestro inédita]. Universidad Nacional Federico Villarreal

Andale (2014). Inferential Statistics: Definition, Uses. Repositorio en 30 junio, 2022. https://acortar.link/wZMk4g

Arias (2022). Guía para elaborar la operacionalización de variables. Espacio I+D, Innovación más Desarrollo, 10(28). https://doi.org/10.31644/IMASD.28.2021.a02 (Original work published 2 de octubre de 2021)

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). Ciberseguridad. CSIC.

Baena G. (2014). Tipos de investigación. *Metodología de la Investigación*. (Primer ed., pág. 11). Editorial Patria

Barbour (2013). Los grupos de discusión en investigación cualitativa. Madrid: Ediciones Morata

Blázquez (2022). La ciberseguridad en gestión de activos: cómo gestionar los riesgos.

Caballero, A. (2014). La investigación científica. *Metodología integral innovadora para planes y tesis*. (Primer ed., pág. 39). Producción y de Plataformas Digitales para Latinoamérica.

Calle (2020). Las 5 etapas del proceso de gestión del riesgo operativo. Repositorio en 30 mayo, 2022 https://www.piranirisk.com/es/blog/las-5-etapas-del-proceso-de-gestion-del-riesgo-operativo

Carrasco E. (2021). Activo: Qué es un activo, clasificación y pérdida de valor. Repositorio en 30 julio, 2022. https://www.stelorder.com/blog/activo/

Casares y Lizarzaburu (2016). Introducción a la Gestión Integral de Riesgos Empresariales. Lima: Platinum Editorial.

Castro (2010). El Nuevo Estándar ISO para la Gestión del Riesgo. Surlatina Consultores.https://capacitacion.gestionderiesgos.gob.ec/courses/40/files/3782/download

Castro M. (2003). Población y Muestra. *El proyecto de investigación y su esquema de elaboración*. (Segunda ed. pág. 69). Editorial Uyapar

Clive (2016), Cybersecurity Threats Challenges Opportunities. Recuperado el 29 de mayo de 2022. https://www.academia.edu/37032090/Cybersecurity_Threats_Challenges_Opportunities

Corletti, A (2017). Ciberseguridad Una estrategia informática/ Militar. ISBN: 978-84-697-7205-8. Recuperado el 18 de mayo de 2022. https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/Libro-Ciberseguridad_A.Corletti_nov2017.pd.pdf

Cybersecurity y Infrastructure Security Agency (CISA). (2019). What is Cybersecurity. [Online] Available at: https://us-cert.cisa.gov/ncas/tips/ST04-001

Defense Onde (2015). The Next Wave of Cyberattacks Won't Steal Data - They'll Change It. https://www.defenseone.com/threats/2015/09/next-wave-cyberattacks-wont-steal-data-theyll-change-it/120701/

Diaz M. (2021). El videoanálisis, evolución a las fichas de observación de clase. Recuperado el 20 de julio de 2022. https://www.codimg.com/education/blog/es/fichas-observacion-clase#:~:text=Las%20fichas%20de%20observaci%C3%B3n%20son,que%20el%20videoan%C3%A1lisis%20puede%20solventar.

Espinoza (2018). Métodos y Técnicas de recolección de la información. http://www.bvs.hn/Honduras/Embarazo/Metodos.e.Instrumentos.de.Recoleccion.pdf

Ferdinando (2016). Cybersecurity: how safe are we as a nation? Maestría en Artes en Estudios Liberales. [Tesis de Master of Arts in Liberal Studies inédita]. Repositorio en University Washington, D.C. https://repository.library.georgetown.edu/bitstream/handle/10822/1040741/Ferdinando_georgetown_0076M_13219.pdf?sequence=1&isAllowed=y

Fred N. Kerlinger (1965) Una buena presentación y discusión de diversos tipos de diseños experimentales. Foundation of behavioral research, Holt Rinehart and Winston.

Hernández-Sampieri, R. & Mendoza, C. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. Ciudad de México: Mc Graw Hill Educación. https://cuadernosdeseguridad.com/2022/02/ciberataques-accenture-informe/

Huerta (2019). Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019. Maestro en Ingeniería de sistemas con mención en tecnologías de la información. [Tesis de Maestro inédita]. Universidad Cesar Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46037/Huerta_ACA-SD.pdf?sequence=1&isAllowed=y

INC. (2020) Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo. Secretaria de comunicación y trasporte. Recuperado el 28 de mayo del 2022. https://www.gob.mx/cms/uploads/attachment/file/555226/Gui_a_de_Ciberseguridad_SCT_VF.pdf

INDC (2006). Cálculo del riesgo. Manual básico para la estimación del riesgo. Recuperado el 28 de julio del 2022. http://bvpad.indeci.gob.pe/doc/pdf/esp/doc319/doc319_contenido.pdf

Internet Users by Country 2016, Internet Life Stats, July 2016 https://www.internetlivestats.com/internet-users-by-country/

Jara (2018). Tecnologías de la información y comunicación. Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018. Maestro en Ingeniería de sistemas con mención en tecnologías de la información. [Tesis de Maestro inédita]. Universidad Cesar Vallejo.

Llontop (2018). Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks. Maestro en Ingeniería de sistemas con mención en tecnologías de la información. [Tesis de Maestro inédita]. Universidad Cesar Vallejo.

Machín, Nieva; Gazapo, Manuel (octubre, 2016) La ciberseguridad como factor crítico en la seguridad de la unión europea. Madrid, España, 48(68). 2386-9453. https://www.redalyc.org/pdf/767/76747805002.pdf

Martínez y Fernández (2020). Ciberdelitos. Ediciones Experiencia. https://ebsco.bibliotecaupn.elogim.com/login.aspx?direct=true&AuthType=ip,uid&db=nlebk&AN=2712945&lang=es&site=ehost-live&ebv=EK&ppid=Page-__-5

Mitxelena, Dal Cin y Bissell (2022) Estado de resiliencia en ciberseguridad 2021. Recuperado del 01 de mayo de 2022. https://www.accenture.com/es-es/insights/security/invest-cyber-resilience

Monroy Mejía, M. D. L. Á. y Nava Sanchezllanes, N. (2018). Metodología de la investigación. México, D.F, Grupo Editorial Éxodo. Recuperado de https://elibro.bibliotecaupn.elogim.com/es/ereader/upnorte/172512?page=106.

Ñaupas (2013). Metodología de la investigación científica y elaboración de tesis. Lima: Universidad Nacional Mayor de San Marcos.

Patricio Tucker (2015). The Next Wave of Cyberattacks Won't Steal Data - They'll Change It. https://www.defenseone.com/voices/patrick-tucker/8219/?oref=d1-post-author

Peltier (2014). Information Security Fundamentals. 2da. Edición. Florida, CRC Press.

Peñaloza (2010). Teoría de las decisiones. Facultad de Administración, Finanzas y Ciencias Económicas, Especialización en Administración de

Empresas virtual. Repositorio en 20 mayo, 2022 de Universidad Católica Boliviana San Pablo https://www.redalyc.org/pdf/4259/425942454012.pdf

Peñaloza (2019). Desafíos del riesgo cibernético en el sector Financiero para Colombia y américa latina. Repositorio en 29 mayo, 2022 https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Ramos A., & Arango, H., & Ticono A. (2018). Riesgos en ciberseguridad y sus efectos sobre la transformación digital en la nueva normalidad, según las empresas operadoras de seguridad. Facultad de Administración, Finanzas y Ciencias Económicas, Especialización en Administración de Empresas virtual. [Tesis de especialización inédita]. Repositorio en Universidad EAN https://repository.ean.edu.co/bitstream/handle/10882/10231/AmadorAntonio2020.pdf?sequence=1&isAllowed=y

Räni (2018). Prediction Model for Tendencies in Cybersecurity. Master's Thesis. [Tesis de Maestro inédita]. Repositorio en University of tartu. https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=62034&year=2018

Reguant (2014) Operacionalización de conceptos/variables. Recuperado el 20 de mayo de 2022. http://diposit.ub.edu/dspace/bitstream/2445/57883/1/Indicadores-Repositorio.pdf

Rendon y Villasis (2016). Estadística descriptiva. Recuperado del 19 de mayo de 2022. https://www.redalyc.org/pdf/4867/486755026009.pdf

Rojas C. (2021). Ficha de Observación. Recuperado el 27 de julio de 2022 https://milformatos.com/escolares/ficha-de-observacion/

Sánchez (2022). El 55% de las empresas no se defiende eficazmente de los ciberataques, según un estudio de Accenture. Recuperado el 30 de mayo del 2022. https://newsroom.accenture.es/es/news/mas-de-la-mitad-de-las-empresas-nose-defiende-eficazmente-de-los-ciberataques.htm

Santiago (2020). Aportes para la adecuación del marco jurídico de la ciberdefensa y la ciberseguridad en Argentina. Maestría en ciberdefensa y ciberseguridad. [Tesis de Maestro inédita]. Repositorio en Universidad de

Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1618_TatoNS.pdf

Saunders, M., Lewis, P., & Thornhill, A. (2015). Research Methods for Business Students (Vol. Seventh edition). New York: Pearson.

SGSI. Sistema de Gestión de Seguridad de la Información ISO 27001. El portal de ISO 27001 en español. [en línea] [citado el 12 de mayo 2022]. Disponible en http://www.iso27000.es/iso27000.html

Szymański (2017). Risk management in construction projects. Procedia Engineering, 208,174-182. doi: 10.1016/j.proeng.2017.11.036

Taípe Domínguez & Daniel Iván (2020). La auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018. https://repositorio.unp.edu.pe/bitstream/handle/20.500.12676/2361/INFOR-TAI-DOM-2020.pdf?sequence=1&isAllowed=y

TEC (2022). Valoración de riesgo. Repositorio en 30 mayo, 2022 https://www.tec.ac.cr/valoracion-riesgo

Torres A. (2014) Definiciones de los enfoques cuantitativo y cualitativo sus similitudes y diferencias. Repositorio en 30 mayo, 2022. https://acortar.link/wcJfBN

Turac (2020) Risks with construction project risk management - An insight into how professionals within the construction industry manage risk. Stockholm, Suecia. Recuperado 04 de junio de 2022. https://www.diva-portal.org/smash/get/diva2:1445409/FULLTEXT01.pdf

ANEXOS

Anexo 1: Matriz de Consistencia

<table>
<tr><th colspan="10">Matriz de Consistencia</th></tr>
<tr><td colspan="10">Título: Modelo de Sistema de Ciberseguridad para la Gestión de Riesgo de una Empresa de Matizados de Pintura de Lima, 2022</td></tr>
<tr><td colspan="2">Problema general</td><td colspan="2">Objetivo general</td><td colspan="2">Hipótesis general</td><td colspan="4" rowspan="2">Organización de las variables e indicadores</td></tr>
<tr><td colspan="2" rowspan="2">¿Cómo impacta un modelo de sistema de ciberseguridad para la gestión de riesgo de una empresa de matizados de pintura de Lima, 2022?</td><td colspan="2" rowspan="2">Determinar cómo influye un modelo de sistema de ciberseguridad para la gestión de riesgo de una empresa de matizados de pintura de Lima, 2022.</td><td colspan="2" rowspan="2">La implementación de un modelo de sistema de ciberseguridad para la gestión de riesgo de una empresa de matizados de pintura de Lima, 2022</td></tr>
<tr><td>Variable</td><td>Dimensiones</td><td>Indicadores</td><td>Instrumento</td><td>Escala</td></tr>
<tr><td colspan="2">Problemas específicos</td><td colspan="2">Objetivos específicos</td><td colspan="2">Hipótesis específicas</td><td>Sistema de Ciberseguridad</td><td colspan="4"></td></tr>
<tr><td colspan="2">¿En qué medida el modelo de sistema de ciberseguridad influye en el nivel de activos que son adecuados para su propósito para la gestión del riesgo de una empresa matizado de pinturas, Lima 2022?</td><td colspan="2">Determinar cómo influye un modelo sistema de ciberseguridad en el nivel de activos que son adecuados para su propósito para la gestión del riesgo de una empresa matizado de pinturas, Lima 2022.</td><td colspan="2">La implementación de modelo de sistema de ciberseguridad en el nivel de activos en el proceso de gestión del riesgo en la empresa matizado de pinturas, Lima 2022.</td><td rowspan="3">Gestión de riesgo</td><td rowspan="3">Activos de información

Evaluación del Riesgos

Procedimiento del riesgo</td><td>Nivel de activos</td><td>Ficha de Observación</td><td>Razón</td></tr>
<tr><td colspan="2">¿En qué medida el modelo de sistema de ciberseguridad mejora el l nivel de riesgos para su propósito para la gestión del riesgo de una empresa matizado de pinturas, Lima 2022?</td><td colspan="2">Determinar cómo influye un sistema de ciberseguridad en la mejora del nivel de riesgos para su propósito para la gestión del riesgo de una empresa matizado de pinturas, Lima 2022</td><td colspan="2">La implementación de modelo de sistema de ciberseguridad en el nivel de riesgos en el proceso de gestión del riesgo de una empresa matizado de pinturas, Lima 2022.</td><td>Nivel de riesgo</td><td>Ficha de Observación</td><td>Razón</td></tr>
<tr><td colspan="2">¿En qué medida el modelo de sistema de ciberseguridad mejora el número de controles aplicados en el proceso de gestión del riesgo de una empresa matizado de pinturas, Lima 2022?</td><td colspan="2">Determinar cómo influye un sistema de ciberseguridad en la mejora del número de controles aplicados en el proceso de gestión del riesgo de una empresa matizado de pinturas, Lima 2022</td><td colspan="2">La implementación de modelo de sistema de ciberseguridad en el número de controles aplicados en el proceso de gestión del riesgo de una empresa matizado de pinturas, Lima 2022.</td><td>Números de controles aplicados</td><td>Ficha de Observación</td><td>Nominal</td></tr>
<tr><td colspan="3">Método y Diseño</td><td colspan="3">Población y muestra</td><td colspan="2">Técnicas e instrumentos</td><td colspan="3">Método de análisis de datos</td></tr>
<tr><td colspan="3">Enfoque: Cuantitativo
Tipo de Investigación: Aplicada.
Diseño de investigación: No experimental.</td><td colspan="3">Población: Activos de Información (17 activos)</td><td colspan="2">Técnica: Investigación Aplicada.
Instrumento: Ficha de Observación</td><td colspan="3">Descriptiva: Software SPSS V.25
Inferencial. Probatoria hipótesis.</td></tr>
</table>

Anexo 2: Matriz de Operacionalización de Variables

Variable Independiente	Definición Conceptual	Definición Operacional	Indicadores	Escala de Medición
Gestión de riesgo	Para Peltier (2014), Las estrategias en gestión de riesgos incluyen identificación de riesgos, evaluación que pueden hacer y la adopción de medidas para minimizar todos los riesgos y niveles aceptables. Todos los sistemas de análisis de amenazas utilizan el mismo método. Encuentra los tesoros que quieres explorar. Identificar amenazas, problemas o debilidades.	La variable dependiente gestión de riesgo, será medida con 3 indicadores: (a) nivel de activos, (b) nivel de riesgos y (c) número de controles aplicados.	Nivel de activos	Cuantitativa **razón**
			Nivel de riesgos	Cuantitativa **razón**
			Números de controles aplicados	Cuantitativa **Nominal**

Anexo 3: Lista de activos críticos e información reconocidos

Activos de información

N°	CODIGO	ACTIVOS DE INFORMACIÓN	TIPO	PROPIETARIO
1	RH01	Analista Programador	Recursos humanos	Subgerente de Informática
2	RH02	Subgerente de Administración Tributaria	Recursos humanos	SG. de Administración Tributaria
3	DC01	Requerimiento de fiscalización	Documentos	SG. de Administración Tributaria
4	IF01	WI-FI	Infraestructura	Subgerente de Informática
5	DC02	Estado de cuenta	Documentos	SG. de Administración Tributaria
6	SO01	Servidor de Desarrollo	Software	Área de sistemas
7	SO02	Servidor de Aplicaciones	Software	Área de sistemas
8	SO03	MS Windows Office (2016,2019)	Software	Área de sistemas
9	SO04	Servidor de correo	Software	Área de sistemas
10	RH03	Jefa de RRHH	Recursos humanos	Área de RRHH
11	RH04	Jefa de contabilidad	Recursos humanos	Área de Contabilidad
12	RH05	Página web de la empresa	Recursos humanos	Área de sistemas
13	IF02	Switch de Distribución	Infraestructura	Subgerente de Informática
14	IF03	Firewall	Infraestructura	Subgerente de Informática
15	SO05	Computadora de Escritorio	Software	Área de sistemas
16	DC03	Estado de cuenta	Documentos	SG. de Administración Tributaria
17	SO06	Servidor de Antivirus	Software	Área de sistemas

Anexo 4: Validación de instrumento – Nivel de Riesgos

	**FICHA DE OBSERVACIÓN N° 01: NIVEL DE RIESGOS (SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES)**	
	FASE:	PREST TEST
	CODIGO	FO-001-NR
	FECHA DISEÑO	**CLASIFICACIÓN:**
	Jun-22	**CONFIDENCIAL**
	Proceso:	Gestión de Riesgo
	Puesto:	Jefe de Sistema
	Fecha de Recolección:	18 de mayo de 2022
	Investigador:	Cinthia J. Calderon Aquiño

FICHA DE OBSERVACIÓN: INDICADORE NIVEL DE RIESGO													
	ACTIVOS DE INFORMACIÓN			**AMENAZAS**	**VULNERABILIDADES**	**EVALUACION DEL RIESGO**							**RIESGO PROMEDIO**
N°	**CÓDIGO**	**ACTIVO**	**VALOR**			**DEGRADACIÓN**			**DEGRADACIÓN MÁXIMA**	**IMPACTO**	**PROBABILIDAD**	**RIESGO**	
						C	**I**	**D**					
1	RH01	Analista Programador	3	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
2	RH02	Subgerente de Administración Tributaria	3	Divulgación de La información	Falta de conciencia en								

					confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
3	DC01	Requerimiento de fiscalización	5	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
4	IF01	WI-FI	5	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción								

					a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
5	DC02	Estado de cuenta	4	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
6	SO01	Servidor de Desarrollo	4	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
7	SO02	Servidor de Aplicaciones	5	Divulgación de La información	Falta de conciencia en								

					confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
8	SO03	MS Windows Office (2016,2019)	3	Caída del sistema	Falta de sistemas de contingencia								
				Manipulación de la Configuración	carencia de políticas de protección de sistema de información								
				Error de actualización del sistema	carencia de políticas de protección de sistema de información								
				Error de usuario	Falta de capacitación a usuarios								
9	SO04	Servidor de correo	5	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								

				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
10	RH03	Jefa de RRHH	3	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
11	RH04	Jefa de contabilidad	3	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								

12	RH05	Página web de la empresa		Caída del sistema	Falta de sistemas de contingencia								
				Manipulación de la Configuración	carencia de políticas de protección de sistema de información								
				Error de actualización del sistema	carencia de políticas de protección de sistema de información								
				Error de usuario	Falta de capacitación a usuarios								
13	IF02	Switch de Distribución	5	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
14	IF03	Firewall		Caída del sistema	Falta de sistemas de contingencia								
				Manipulación de la Configuración	carencia de políticas de protección de sistema de								

					información								
				Error de actualización del sistema	carencia de políticas de protección de sistema de información								
				Error de usuario	Falta de capacitación a usuarios								
15	SO05	Computadora de Escritorio	4	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								
				Corrupción de la información	Carencia de respaldo o backup								
16	DC03	Estado de cuenta	4	Divulgación de La información	Falta de conciencia en confidencialidad								
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios								
				Interceptación de Información	Falta de control de acceso y restricción a usuarios								

				Corrupción de la información	Carencia de respaldo o backup								
17	SO06	Servidor de Antivirus	3	Caída del sistema	Falta de sistemas de contingencia								
				Manipulación de la Configuración	carencia de políticas de protección de sistema de información								
				Error de actualización del sistema	carencia de políticas de protección de sistema de información								
				Error de usuario	Falta de capacitación a usuarios								

Firmar Acceso:

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Anexo 5: Validación de instrumento – Nivel de activos

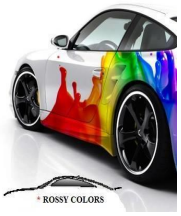
	**FICHA DE OBSERVACIÓN N° 02: NIVEL DE ACTIVOS**	
	FASE:	PREST TEST
	CODIGO	FO-002-NA
	FECHA DISEÑO	**CLASIFICACIÓN:**
	Jun-22	**CONFIDENCIAL**
	Proceso:	Gestión de riesgos
	Puesto:	Jefe de Sistema
	Fecha de Recolección:	02 Junio a 02 julio 2022
	Investigador:	Cinthia J. Calderon Aquiño

FICHA DE OBSERVACIÓN: INDICADORE NIVEL DE ACTIVOS PRE TEST					
N°	**CODIGO**	**ACTIVOS DE INFORMACIÓN**	**TIPO**	**PROPIETARIO**	**PREST_N_A**
1	RH01	Analista Programación			
2	RH02	Subgerente de administración tributaria			
3	DC01	Requerimiento de fiscalización			
4	IF01	WIFI			
5	DC02	Estado de cuenta			
6	SO01	Servidor de Desarrollo			
7	SO02	Servidor de Aplicaciones			
8	SO03	MS Windows Office (2016, 2019)			
9	SO04	Servidor de correo			
10	RH03	Jefa de RRHH			
11	RH04	Jefe de contabilidad			
12	RH05	Página web de la empresa			
13	IF02	Switch de distribución			
14	IF03	Firewall			
15	SO05	Computadora de Escritorio			
16	DC03	Estado de cuenta			
17	SO06	Servidor de Antivirus			

Firmar Acceso:

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Anexo 6: Validación de instrumento – Numero de Control aplicados

	**FICHA DE OBSERVACIÓN N° 03: INDICADOR - NÚMERO DE CONTROLES APLICADOS**	
		(DECLARACIÓN DE APLICABILIDAD DE CONTROLES)
	FASE:	PREST TEST
	CODIGO	FO-003-NCA
	FECHA DISEÑO Jun-22	**CLASIFICACIÓN: CONFIDENCIAL**
	Proceso:	Gestión de riesgos
	Puesto:	Jefe de Sistema
	Fecha de recolocción:	02 Junio a 02 Julio 2022
	Investigador:	Cinthia J. Calderon Aquiño

La elección de controles y objetivos de control se ejecutaron a través de los siguientes criterios:
LR: requerimientos legales
CO: obligaciones contractuales
BR/BP: requerimientos del negocio/mejores prácticas adoptadas
RRA: resultado de la valoración de riesgos

Instrumento de recolección de datos

ISO 27001:2014 Controles de Seguridad			**Aplica o no Aplica**	**Existe SI/NO**	**JUSTIFICACION DE LA APLICACIÓN**			
					LR	**CO**	**BR/BP**	**RRA**
Cláusula	**Sección**	**Objetivo de control / control**						
5 Políticas de Seguridad	**5.1**	**Dirección de la gestión de la seguridad de la información**						
	5.1.1	Políticas de seguridad de la información						
	5.1.2	Revisión de las políticas de seguridad de la información						
6 Organización de la Seguridad de la Información	**6.1**	**Organización interna**						
	6.1.1	Roles y responsabilidades relativas a la seguridad de la información						
	6.1.2	Separación de tareas						
	6.1.3	Contacto con las autoridades						
	6.1.4	Contacto con grupos de especial interés						
	6.1.5	Seguridad de la información en la gestión de proyectos						
	6.2	**Dispositivos móviles y teletrabajo**						
	6.2.1	Política de dispositivos móviles						
	6.2.2	Teletrabajo						

7 Seguridad en los Recursos Humanos	**7.1**	**Antes del empleo**						
	7.1.1	Investigación de antecedentes						
	7.1.2	Términos y condiciones de contratación						
	7.2	**Durante el empleo**						
	7.2.1	Responsabilidades de la Dirección						
	7.2.2	Concienciación, formación y capacitación en seguridad de la información						
	7.2.3	Proceso disciplinario						
	7.3	**Cese del empleo y cambio de puesto de trabajo**						
	7.3.1	Terminación o cambio de responsabilidades laborales						
8 Gestión de Activos	**8.1**	**Responsabilidad sobre los activos**						
	8.1.1	Inventario de activos						
	8.1.2	Propiedad de los activos						
	8.1.3	Uso aceptable de los activos						
	8.1.4	Devolución de activos						
	8.2	**Clasificación de la información**						
	8.2.1	Clasificación de la información						
	8.2.2	Etiquetado de la información						
	8.2.3	Manejo de activos						
	8.3	**Manipulación de los soportes**						
	8.3.1	Gestión de soportes extraíbles						
	8.3.2	Retirada de soportes						
	8.3.3	Transferencia de soportes físicos						
9 Control de Acceso	**9.1**	**Requisitos de negocio para el control de acceso**						
	9.1.1	Política de control de acceso						
	9.1.2	Acceso a redes y servicios en red						
	9.2	**Gestión del acceso de usuario**						
	9.2.1	Altas y bajas de usuarios						
	9.2.2	Gestión de derechos de acceso de los usuarios						
	9.2.3	Gestión de derechos de acceso especiales						
	9.2.4	Gestión de la información secreta de autenticación de usuarios						
	9.2.5	Revisión de derechos de acceso de usuario						
	9.2.6	Terminación o revisión de los privilegios de acceso						
	9.3	**Responsabilidades de usuario**						
	9.3.1	Uso de la información secreta de autenticación						
	9.4	**Control de acceso al sistema y a las aplicaciones**						
	9.4.1	Restricción del acceso a la información						

	9.4.2	Procedimientos seguros de inicio de sesión						
	9.4.3	Gestión de las contraseñas de usuario						
	9.4.4	Uso de los recursos del sistema con privilegios especiales						
	9.4.5	Control de acceso al código fuente de los programas						
10 Criptografía	**10.1**	**Controles criptográficos**						
	10.1.1	Política de uso de los controles criptográficos						
	10.1.2	Gestión de claves						
11 Seguridad Física y del Entorno	**11.1**	**Áreas seguras**						
	11.1.1	Perímetro de seguridad física						
	11.1.2	Controles físicos de entrada						
	11.1.3	Seguridad de oficinas, despachos e instalaciones						
	11.1.4	Protección contra las amenazas externas y de origen ambiental						
	11.1.5	Trabajo en áreas seguras						
	11.1.6	Áreas de carga y descarga						
	11.2	**Equipos**						
	11.2.1	Emplazamiento y protección de equipos						
	11.2.2	Instalaciones de suministro						
	11.2.3	Seguridad del cableado						
	11.2.4	Mantenimiento de los equipos						
	11.2.5	Retirada de materiales propiedad de la empresa						
	11.2.6	Seguridad de los equipos fuera de las instalaciones						
	11.2.7	Reutilización o retirada segura de equipos						
	11.2.8	Equipo de usuario desatendido						
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia						
12 Seguridad en las Operaciones	**12.1**	**Responsabilidades y procedimientos de operación**						
	12.1.1	Documentación de los procedimientos de operación						
	12.1.2	Gestión de cambios						
	12.1.3	Gestión de capacidades						
	12.1.4	Separación de los entornos de desarrollo, prueba y operación						
	12.2	**Protección contra el código malicioso**						
	12.2.1	Controles contra el código malicioso						
	12.3	**Copias de seguridad**						
	12.3.1	Copias de seguridad de la información						
	12.4	**Registro y monitorización**						
	12.4.1	Registro de eventos						

	12.4.2	Protección de la información de los registros						
	12.4.3	Registros de administración y operación						
	12.4.4	Sincronización del reloj						
	12.5	**Control del software en explotación**						
	12.5.1	Instalación de software en sistemas operacionales						
	12.6	**Gestión de las vulnerabilidades técnicas**						
	12.6.1	Gestión de las vulnerabilidades técnicas						
	12.6.2	Restricciones a la instalación de software						
	12.7	**Consideraciones sobre la auditoría de los sistemas de información**						
	12.7.1	Controles de auditoría de los sistemas de información						
13 Seguridad en las Comunicaciones	**13.1**	**Gestión de la seguridad de las redes**						
	13.1.1	Controles de red						
	13.1.2	Seguridad de los servicios de red						
	13.1.3	Segregación de redes						
	13.2	**Transferencia de información**						
	13.2.1	Políticas y procedimientos de transferencia de información						
	13.2.2	Acuerdos de transferencia de información						
	13.2.3	Mensajería electrónica						
	13.2.4	Acuerdos de confidencialidad o no divulgación						
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	**14.1**	**Requisitos de seguridad de los sistemas de información**						
	14.1.1	Análisis y especificación de los requisitos de seguridad de la información						
	14.1.2	Aseguramiento de los servicios de aplicaciones en las redes públicas						
	14.1.3	Protección de las transacciones de servicios de aplicación						
	14.2	**Seguridad en los procesos de desarrollo y soporte**						
	14.2.1	Política de desarrollo seguro						
	14.2.2	Procedimientos de control de cambios en el sistema						
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma						
	14.2.4	Restricciones a los cambios en los paquetes de software						
	14.2.5	Principios para la ingeniería de sistemas seguros						
	14.2.6	Entorno de desarrollo seguro						
	14.2.7	Externalización del desarrollo de software						
	14.2.8	Pruebas de seguridad del sistema						

	14.2.9	Pruebas de aceptación del sistema						
	14.3	**Datos de prueba**						
	14.3.1	Protección de los datos de prueba						
15 Relaciones con Proveedores	**15.1**	**Seguridad de la información en las relaciones con proveedores**						
	15.1.1	Política de seguridad de la información en las relaciones con proveedores						
	15.1.2	Tratamiento de la seguridad en contratos con proveedores						
	15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones						
	15.2	**Gestión de los servicios prestados por terceros**						
	15.2.1	Supervisión y revisión de los servicios prestados por terceros						
	15.2.2	Gestión del cambio en los servicios prestados por terceros						
16 Gestión de Incidentes de Seguridad de la Información	**16.1**	**Gestión de incidentes de seguridad de la información y mejoras**						
	16.1.1	Responsabilidades y procedimientos						
	16.1.2	Notificación de eventos de seguridad de la información						
	16.1.3	Notificación de puntos débiles de seguridad						
	16.1.4	Evaluación y decisión respecto de los eventos de seguridad de la información						
	16.1.5	Respuesta a incidentes de seguridad de la información						
	16.1.6	Aprendizaje de los incidentes de seguridad de la información						
	16.1.7	Recopilación de evidencias						
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	**17.1**	**Continuidad de la seguridad de la información**						
	17.1.1	Planificación de la continuidad de la seguridad de la información						
	17.1.2	Implementación de la continuidad de la seguridad de la información						
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información						
	17.2	**Redundancia**						
	17.2.1	Disponibilidad de los medios de procesamiento de información						
18 Cumplimiento	**18.1**	**Cumplimiento de los requisitos legales y contractuales**						
	18.1.1	Identificación de la legislación aplicable y requisitos contractuales						
	18.1.2	Derechos de propiedad intelectual (DPI)						
	18.1.3	Protección de los documentos de la organización						
	18.1.4	Protección de datos y privacidad de la información de carácter personal						

	18.1.5	Regulación de los controles criptográficos						
	18.2	**Revisiones de seguridad de la información**						
	18.2.1	Revisión independiente de la seguridad de la información						
	18.2.2	Cumplimiento de las políticas y normas de seguridad						
	18.2.3	Comprobación del cumplimiento técnico						

Firmar Acceso:

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Anexo 7: Ficha de observación – PrestTest - Nivel de Riesgo

	**FICHA DE OBSERVACIÓN N° 01: NIVEL DE RIESGOS (SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES)**	
	FASE:	PREST TEST
	CODIGO	FO-001-NR
	FECHA DISEÑO	**CLASIFICACIÓN:**
	Jun-22	**CONFIDENCIAL**
	Proceso:	Gestión de Riesgo
	Puesto:	Jefe de Sistema
	Fecha de Recolección:	18 de mayo de 2022
	Investigador:	Cinthia J. Calderon Aquiño

FICHA DE OBSERVACIÓN: INDICADORE NIVEL DE RIESGO PRE TEST													
	ACTIVOS DE INFORMACIÓN			**AMENAZAS**	**VULNERABILIDADES**	**EVALUACION DEL RIESGO**							**RIESGO PROMEDIO**
N°	**CÓDIGO**	**ACTIVO**	**VALOR**			**DEGRADACIÓN**			**DEGRADACIÓN MÁXIMA**	**IMPACTO**	**PROBABILIDAD**	**RIESGO**	
						C	**I**	**D**					
1	RH01	Analista Programador	3	Divulgación de La información	Falta de conciencia en confidencialidad	**3**	4	5	4	**2**	4	6	6
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	4	3	4	**2**	3	6	

				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**3**	5	5	5	**2**	5	6	
				Corrupción de la información	Carencia de respaldo o backup	**3**	4	4	4	**2**	4	6	
2	RH02	Subgerente de Administración Tributaria	3	Divulgación de La información	Falta de conciencia en confidencialidad	**4**	2	5	5	**2**	5	8	7
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	2	3	3	**2**	2	6	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**3**	3	4	4	**2**	4	6	
				Corrupción de la información	Carencia de respaldo o backup	**4**	4	4	5	**2**	4	8	
3	DC01	Requerimiento de fiscalización	5	Divulgación de La información	Falta de conciencia en confidencialidad	**4**	4	5	5	**2**	5	8	8
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	4	4	4	**2**	4	6	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**4**	4	4	4	**2**	4	8	

				Corrupción de la información	Carencia de respaldo o backup	**5**	3	4	4	**2**	4	10	
4	IF01	WI-FI	5	Divulgación de La información	Falta de conciencia en confidencialidad	**4**	4	5	4	**1**	4	4	4
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**4**	4	5	5	**1**	5	4	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**4**	4	3	3	**1**	3	4	
				Corrupción de la información	Carencia de respaldo o backup	**4**	4	4	4	**1**	4	4	
5	DC02	Estado de cuenta	4	Divulgación de La información	Falta de conciencia en confidencialidad	**4**	4	4	4	**2**	4	8	7
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	2	4	4	**2**	4	6	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**3**	5	4	5	**2**	5	6	
				Corrupción de la información	Carencia de respaldo o backup	**4**	4	4	4	**2**	4	8	

6	SO01	Servidor de Desarrollo	4	Divulgación de La información	Falta de conciencia en confidencialidad	**3**	5	4	4	**3**	4	9	12
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	4	3	4	**3**	4	9	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**5**	5	5	5	**3**	5	15	
				Corrupción de la información	Carencia de respaldo o backup	**5**	5	5	5	**3**	5	15	
7	SO02	Servidor de Aplicaciones	5	Divulgación de La información	Falta de conciencia en confidencialidad	**3**	5	5	5	**4**	5	12	9
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	5	5	5	**2**	5	6	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**3**	5	5	5	**2**	5	6	
				Corrupción de la información	Carencia de respaldo o backup	**3**	5	5	5	**4**	5	12	
8	SO03		3	Caída del sistema	Falta de sistemas de contingencia	**2**	4	4	4	**2**	4	4	5

		MS Windows Office (2016,2019)		Manipulación de la Configuración	carencia de políticas de protección de sistema de información	**2**	5	5	5	**2**	5	4	
				Error de actualización del sistema	carencia de políticas de protección de sistema de información	**2**	5	3	3	**2**	3	4	
				Error de usuario	Falta de capacitación a usuarios	**2**	5	5	5	**4**	5	8	
9	SO04	Servidor de correo	5	Divulgación de La información	Falta de conciencia en confidencialidad	**4**	5	5	5	**5**	5	20	14.25
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	5	5	5	**5**	5	15	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**3**	5	5	5	**4**	5	12	
				Corrupción de la información	Carencia de respaldo o backup	**2**	5	5	5	**5**	5	10	
10	RH03	Jefa de RRHH	3	Divulgación de La información	Falta de conciencia en confidencialidad	**3**	3	4	4	**4**	4	12	12
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	5	5	5	**4**	5	12	

				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**3**	3	4	4	**4**	4	12	
				Corrupción de la información	Carencia de respaldo o backup	**3**	5	5	5	**4**	5	12	
11	RH04	Jefa de contabilidad	3	Divulgación de La información	Falta de conciencia en confidencialidad	**3**	5	4	4	**3**	4	9	9
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	5	4	4	**3**	4	9	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**3**	5	4	4	**3**	4	9	
				Corrupción de la información	Carencia de respaldo o backup	**3**	4	4	4	**3**	4	9	
12	RH05	Página web de la empresa		Caída del sistema	Falta de sistemas de contingencia	**3**	4	5	4	**4**	4	12	12
				Manipulación de la Configuración	carencia de políticas de protección de sistema de información	**3**	5	4	5	**4**	5	12	
				Error de actualización del sistema	carencia de políticas de protección de sistema de información	**3**	5	4	5	**4**	5	12	

				Error de usuario	Falta de capacitación a usuarios	**3**	5	5	5	**4**	5	12	
13	IF02	Switch de Distribución	5	Divulgación de La información	Falta de conciencia en confidencialidad	**4**	5	3	5	**3**	5	12	15
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**3**	5	4	5	**4**	5	12	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**4**	5	4	5	**4**	5	16	
				Corrupción de la información	Carencia de respaldo o backup	**4**	3	3	5	**5**	5	20	
14	IF03	Firewall		Caída del sistema	Falta de sistemas de contingencia	**3**	3	4	5	**3**	5	9	10.5
				Manipulación de la Configuración	carencia de políticas de protección de sistema de información	**4**	4	4	3	**3**	5	12	
				Error de actualización del sistema	carencia de políticas de protección de sistema de información	**4**	4	3	3	**3**	5	12	
				Error de usuario	Falta de capacitación a usuarios	**3**	5	5	3	**3**	5	9	

15	SO05	Computadora de Escritorio	4	Divulgación de La información	Falta de conciencia en confidencialidad	**4**	4	3	5	**4**	5	16	13
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**2**	4	3	5	**2**	5	4	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**4**	4	4	5	**4**	4	16	
				Corrupción de la información	Carencia de respaldo o backup	**4**	4	5	5	**4**	5	16	
16	DC03	Estado de cuenta	4	Divulgación de La información	Falta de conciencia en confidencialidad	**3**	3	3	5	**4**	5	12	11
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**2**	2	3	3	**4**	3	8	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**3**	5	3	5	**4**	5	12	
				Corrupción de la información	Carencia de respaldo o backup	**3**	3	4	4	**4**	5	12	
17	SO06	Servidor de Antivirus	3	Caída del sistema	Falta de sistemas de contingencia	**2**	4	3	5	**4**	4	8	7

				Manipulación de la Configuración	carencia de políticas de protección de sistema de información	**2**	2	2	3	**3**	3	6	
				Error de actualización del sistema	carencia de políticas de protección de sistema de información	**2**	2	2	2	**3**	2	6	
				Error de usuario	Falta de capacitación a usuarios	**2**	2	2	2	**4**	2	8	

Anexo 8: Ficha de observación – PostTest - Nivel de Riesgo

	**FICHA DE OBSERVACIÓN N° 01: NIVEL DE RIESGOS (SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES)**	
	FASE:	POST TEST
	CODIGO	FO-001-NR
	FECHA DISEÑO	**CLASIFICACIÓN:**
	Jun-22	**CONFIDENCIAL**
	Proceso:	Gestión de Riesgo
	Puesto:	Jefe de Sistema
	Fecha de Recolección:	25 de Junio de 2022
	Investigador:	Cinthia J. Calderon Aquiño

FICHA DE OBSERVACIÓN: INDICADORE NIVEL DE RIESGO POST TEST													
	ACTIVOS DE INFORMACIÓN			**AMENAZAS**	**VULNERABILIDADES**	**EVALUACION DEL RIESGO**							**RIESGO PROMEDIO**
N°	**CÓDIGO**	**ACTIVO**	**VALOR**			**DEGRADACIÓN**			**DEGRADACIÓN MÁXIMA**	**IMPACTO**	**PROBABILIDAD**	**RIESGO**	
						C	**I**	**D**					
1	RH01	Analista Programador	3	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	4	5	4	**3**	4	15	15
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	4	3	4	**3**	4	15	

				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**5**	5	5	5	**3**	4	15	
				Corrupción de la información	Carencia de respaldo o backup	**5**	4	4	4	**3**	4	15	
2	RH02	Subgerente de Administración Tributaria	3	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	2	5	5	**3**	5	15	15
				Alteración en la configuración	Falta de control de acceoso y restriccion a usuarios	**5**	2	3	3	**3**	3	15	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**5**	3	4	4	**3**	5	15	
				Corrupción de la información	Carencia de respaldo o backup	**5**	4	4	5	**3**	5	15	
3	DC01	Requerimiento de fiscalización	5	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	4	5	5	**3**	5	15	15
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	4	4	4	**3**	5	15	
				Interceptación de Información	Falta de control de acceso y restricción usuarios	**5**	4	4	4	**3**	5	15	

				Corrupción de la información	Carencia de respaldo o backup	**5**	3	4	4	**3**	5	15	
4	IF01	WI-FI	5	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	4	5	4	**4**	5	20	18
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	4	5	5	**4**	5	20	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**4**	4	3	3	**4**	4	16	
				Corrupción de la información	Carencia de respaldo o backup	**4**	4	4	4	**4**	5	16	
5	DC02	Estado de cuenta	4	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	4	4	4	**4**	5	20	19
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	2	4	4	**4**	5	20	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**5**	5	4	5	**4**	5	20	
				Corrupción de la información	Carencia de respaldo o backup	**4**	4	4	4	**4**	4	16	

6	SO01	Servidor de Desarrollo	4	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	5	4	4	**3**	5	15	16
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	4	3	4	**4**	5	20	
				Interceptación de Información	Falta de control de acceoso y restriccion a usuarios	**5**	5	5	5	**4**	5	20	
				Corrupción de la información	Carencia de respaldo o backup	**3**	5	5	5	**3**	5	9	
7	SO02	Servidor de Aplicaciones	5	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	5	5	5	**5**	5	25	25
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	5	5	5	**5**	5	25	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**5**	5	5	5	**5**	5	25	
				Corrupción de la información	Carencia de respaldo o backup	**5**	5	5	5	**5**	5	25	
8	SO03		3	Caída del sistema	Falta de sistemas de contingencia	**4**	4	4	4	**5**	5	20	17

		MS Windows Office (2016,2019)		Manipulación de la Configuración	carencia de políticas de protección de sistema de información	**4**	5	5	5	**4**	5	16	
				Error de actualización del sistema	carencia de políticas de protección de sistema de información	**4**	5	3	3	**4**	3	16	
				Error de usuario	Falta de capacitación a usuarios	**4**	5	5	5	**4**	5	16	
9	SO04	Servidor de correo	5	Divulgación de La información	Falta de conciencia en confidencialidad	**4**	5	5	5	**4**	5	16	17
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**4**	5	5	5	**4**	5	16	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**4**	5	5	5	**4**	5	16	
				Corrupción de la información	Carencia de respaldo o backup	**5**	5	5	5	**4**	5	20	
10	RH03	Jefa de RRHH	3	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	3	4	4	**4**	4	20	20
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	5	5	5	**4**	5	20	

				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**5**	3	4	4	**4**	4	20	
				Corrupción de la información	Carencia de respaldo o backup	**5**	5	5	5	**4**	5	20	
11	RH04	Jefa de contabilidad	3	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	5	4	4	**4**	4	20	18
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	5	4	4	**4**	4	20	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**5**	5	4	4	**4**	4	20	
				Corrupción de la información	Carencia de respaldo o backup	**4**	4	4	4	**3**	4	12	
12	RH05	Página web de la empresa		Caída del sistema	Falta de sistemas de contingencia	**5**	4	5	4	**4**	4	20	20
				Manipulación de la Configuración	carencia de políticas de protección de sistema de información	**5**	5	4	5	**4**	5	20	
				Error de actualización del sistema	carencia de políticas de protección de sistema de información	**5**	5	4	5	**4**	5	20	

				Error de usuario	Falta de capacitación a usuarios	**5**	5	5	5	**4**	5	20	
13	IF02	Switch de Distribución	5	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	5	3	5	**5**	5	25	25
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	5	4	5	**5**	5	25	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**5**	5	4	5	**5**	5	25	
				Corrupción de la información	Carencia de respaldo o backup	**5**	3	3	5	**5**	5	25	
14	IF03	Firewall		Caída del sistema	Falta de sistemas de contingencia	**5**	3	4	5	**5**	5	25	22.5
				Manipulación de la Configuración	carencia de políticas de protección de sistema de información	**3**	4	4	3	**5**	5	15	
				Error de actualización del sistema	carencia de políticas de protección de sistema de información	**5**	4	3	3	**5**	5	25	
				Error de usuario	Falta de capacitación a usuarios	**5**	5	5	3	**5**	5	25	

15	SO05	Computadora de Escritorio	4	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	4	3	5	**4**	5	20	20
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**5**	4	3	5	**4**	5	20	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**5**	4	4	5	**4**	4	20	
				Corrupción de la información	Carencia de respaldo o backup	**5**	4	5	5	**4**	5	20	
16	DC03	Estado de cuenta	4	Divulgación de La información	Falta de conciencia en confidencialidad	**5**	3	3	5	**4**	5	20	18
				Alteración en la configuración	Falta de control de acceso y restricción a usuarios	**4**	2	3	3	**4**	3	16	
				Interceptación de Información	Falta de control de acceso y restricción a usuarios	**4**	5	3	5	**5**	5	20	
				Corrupción de la información	Carencia de respaldo o backup	**4**	3	4	4	**4**	5	16	
17	SO06	Servidor de Antivirus	3	Caída del sistema	Falta de sistemas de contingencia	**4**	4	3	5	**4**	4	16	18

				Manipulación de la Configuración	carencia de políticas de protección de sistema de información	**4**	2	2	3	**5**	3	20	
				Error de actualización del sistema	carencia de políticas de protección de sistema de información	**4**	2	2	2	**4**	2	16	
				Error de usuario	Falta de capacitación a usuarios	**4**	2	2	2	**5**	2	20	

Anexo 9: Ficha de observación – PrestTest – Nivel de Activos

FICHA DE OBSERVACIÓN N° 02: NIVEL DE ACTIVOS	
FASE:	PREST TEST
CODIGO	FO-002-NA
FECHA DISEÑO	**CLASIFICACIÓN:**
Jun-22	**CONFIDENCIAL**
Proceso:	Gestión de riesgos
Puesto:	Jefe de Sistema
Fecha de Recolocción:	02 Junio a 02 julio 2022
Investigador:	Cinthia J. Calderon Aquiño

FICHA DE OBSERVACIÓN: INDICADORE NIVEL DE ACTIVOS PRE TEST					
N°	**CODIGO**	**ACTIVOS DE INFORMACIÓN**	**TIPO**	**PROPIETARIO**	**PREST_N_A**
1	RH01	Analista Programación	3	3	9
2	RH02	Subgerente de administración tributaria	4	2	8
3	DC01	Requerimiento de fiscalización	3	2	6
4	IF01	WIFI	4	1	4
5	DC02	Estado de cuenta	3	2	6
6	SO01	Servidor de Desarrollo	3	3	9
7	SO02	Servidor de Aplicaciones	3	3	9
8	SO03	MS Windows Office (2016, 2019)	2	4	8
9	SO04	Servidor de correo	3	2	6
10	RH03	Jefa de RRHH	3	3	9
11	RH04	Jefe de contabilidad	4	2	8
12	RH05	Página web de la empresa	2	3	6
13	IF02	Switch de distribución	3	4	12
14	IF03	Firewall	4	2	8
15	SO05	Computadora de Escritorio	3	3	9
16	DC03	Estado de cuenta	4	2	8
17	SO06	Servidor de Antivirus	3	3	9

Anexo 10: Ficha de observación – PostTest – Nivel de Activos

FICHA DE OBSERVACIÓN N° 02: NIVEL DE ACTIVOS	
FASE:	POST TEST
CODIGO	FO-002-NA
FECHA DISEÑO	**CLASIFICACIÓN:**
Jun-22	**CONFIDENCIAL**
Proceso:	Gestión de riesgos
Puesto:	Jefe de Sistema
Fecha de recolocción:	02 Junio a 02 julio 2022
Investigador:	Cinthia J. Calderon Aquiño

FICHA DE OBSERVACIÓN: INDICADORE NIVEL DE ACTIVOS POST TEST					
N°	**CODIGO**	**ACTIVOS DE INFORMACIÓN**	**TIPO**	**PROPIETARIO**	**PREST_N_A**
1	RH01	Analista Programación	3	2	6
2	RH02	Subgerente de administración tributaria	5	2	10
3	DC01	Requerimiento de fiscalización	3	3	9
4	IF01	WIFI	3	2	6
5	DC02	Estado de cuenta	4	4	16
6	SO01	Servidor de Desarrollo	4	4	16
7	SO02	Servidor de Aplicaciones	3	4	12
8	SO03	MS Windows Office (2016, 2019)	4	4	12
9	SO04	Servidor de correo	4	3	12
10	RH03	Jefa de RRHH	4	4	16
11	RH04	Jefe de contabilidad	4	5	20
12	RH05	Página web de la empresa	3	5	15
13	IF02	Switch de distribución	4	3	12
14	IF03	Firewall	4	4	16
15	SO05	Computadora de Escritorio	4	4	16
16	DC03	Estado de cuenta	4	4	16
17	SO06	Servidor de Antivirus	4	5	20

Anexo 11: Ficha de observación – PrestTest - Número de controles aplicados

	FICHA DE OBSERVACIÓN N° 03: INDICADOR - NÚMERO DE CONTROLES APLICADOS	
		**(DECLARACIÓN DE APLICABILIDAD DE CONTROLES)**
	FASE:	PREST TEST
	CODIGO	FO-003-NCA
	FECHA DISEÑO Jun-22	**CLASIFICACIÓN: CONFIDENCIAL**
	Proceso:	Gestión de riesgos
	Puesto:	Jefe de Sistema
	Fecha de recolocción:	02 Junio a 02 Julio 2022
	Investigador:	Cinthia J. Calderon Aquiño

La elección de controles y objetivos de control se ejecutaron a través de los siguientes criterios:
LR: requerimientos legales
CO: obligaciones contractuales
BR/BP: requerimientos del negocio/mejores prácticas adoptadas
RRA: resultado de la valoración de riesgos

Instrumento de recolección de datos

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	**Sección**	**Objetivo de control / control**						
5 Políticas de Seguridad	**5.1**	**Dirección de la gestión de la seguridad de la información**						
	5.1.1	Políticas de seguridad de la información	SI	SI			X	
	5.1.2	Revisión de las políticas de seguridad de la información	SI	SI			X	
6 Organización de la Seguridad de la Información	**6.1**	**Organización interna**						
	6.1.1	Roles y responsabilidades relativas a la seguridad de la información	SI	SI			X	
	6.1.2	Separación de tareas	SI	SI			X	
	6.1.3	Contacto con las autoridades	NO	NO				
	6.1.4	Contacto con grupos de especial interés	NO	NO				
	6.1.5	Seguridad de la información en la gestión de proyectos	SI	SI			X	
	6.2	**Dispositivos móviles y teletrabajo**						
	6.2.1	Política de dispositivos móviles	SI	SI			X	

	6.2.2	Teletrabajo	NO	NO				
7 Seguridad en los Recursos Humanos	**7.1**	**Antes del empleo**						
	7.1.1	Investigación de antecedentes	NO	NO				X
	7.1.2	Términos y condiciones de contratación	SI	SI				X
	7.2	**Durante el empleo**						
	7.2.1	Responsabilidades de la Dirección	SI	SI				
	7.2.2	Concienciación, formación y capacitación en seguridad de la información	SI	SI			X	
	7.2.3	Proceso disciplinario	SI	SI				
	7.3	**Cese del empleo y cambio de puesto de trabajo**						
	7.3.1	Terminación o cambio de responsabilidades laborales	SI	SI				X
8 Gestión de Activos	**8.1**	**Responsabilidad sobre los activos**						
	8.1.1	Inventario de activos	SI	SI			X	
	8.1.2	Propiedad de los activos	SI	SI				X
	8.1.3	Uso aceptable de los activos	SI	SI			X	
	8.1.4	Devolución de activos	SI	SI				
	8.2	**Clasificación de la información**						
	8.2.1	Clasificación de la información	SI	SI			X	
	8.2.2	Etiquetado de la información	SI	SI			X	
	8.2.3	Manejo de activos	NO	NO				
	8.3	**Manipulación de los soportes**						
	8.3.1	Gestión de soportes extraíbles	SI	SI				
	8.3.2	Retirada de soportes	SI	SI			X	
	8.3.3	Transferencia de soportes físicos	SI	SI			X	
9 Control de Acceso	**9.1**	**Requisitos de negocio para el control de acceso**						
	9.1.1	Política de control de acceso	NO	NO				
	9.1.2	Acceso a redes y servicios en red	SI	SI				X
	9.2	**Gestión del acceso de usuario**						
	9.2.1	Altas y bajas de usuarios	SI	SI				X
	9.2.2	Gestión de derechos de acceso de los usuarios	SI	SI				X
	9.2.3	Gestión de derechos de acceso especiales	SI	SI				X
	9.2.4	Gestión de la información secreta de autenticación de usuarios	SI	SI				X
	9.2.5	Revisión de derechos de acceso de usuario	SI	SI				X
	9.2.6	Terminación o revisión de los privilegios de acceso	SI	SI				X
	9.3	**Responsabilidades de usuario**						
	9.3.1	Uso de la información secreta de autenticación	SI	SI				X
	9.4	**Control de acceso al sistema y a las aplicaciones**						
	9.4.1	Restricción del acceso a la información	SI	SI				X

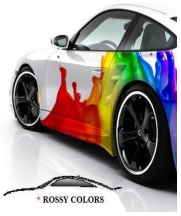
	9.4.2	Procedimientos seguros de inicio de sesión	SI	SI				X
	9.4.3	Gestión de las contraseñas de usuario	SI	SI				X
	9.4.4	Uso de los recursos del sistema con privilegios especiales	SI	SI				X
	9.4.5	Control de acceso al código fuente de los programas	SI	SI				X
10 Criptografía	**10.1**	**Controles criptográficos**						
	10.1.1	Política de uso de los controles criptográficos	SI	SI			X	
	10.1.2	Gestión de claves	SI	SI				X
11 Seguridad Física y del Entorno	**11.1**	**Áreas seguras**						
	11.1.1	Perímetro de seguridad física	SI	SI			X	
	11.1.2	Controles físicos de entrada	SI	SI			X	
	11.1.3	Seguridad de oficinas, despachos e instalaciones	SI	SI			X	
	11.1.4	Protección contra las amenazas externas y de origen ambiental	SI	SI			X	
	11.1.5	Trabajo en áreas seguras	SI	SI			X	
	11.1.6	Áreas de carga y descarga	SI	SI				X
	11.2	**Equipos**						
	11.2.1	Emplazamiento y protección de equipos	SI	SI				X
	11.2.2	Instalaciones de suministro	SI	SI			X	
	11.2.3	Seguridad del cableado	SI	SI			X	
	11.2.4	Mantenimiento de los equipos	SI	SI			X	
	11.2.5	Retirada de materiales propiedad de la empresa	SI	SI				X
	11.2.6	Seguridad de los equipos fuera de las instalaciones	SI	SI				X
	11.2.7	Reutilización o retirada segura de equipos	SI	SI				X
	11.2.8	Equipo de usuario desatendido	SI	SI			X	
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia	NO	NO				
12 Seguridad en las Operaciones	**12.1**	**Responsabilidades y procedimientos de operación**						
	12.1.1	Documentación de los procedimientos de operación	NO	NO				
	12.1.2	Gestión de cambios	NO	NO				
	12.1.3	Gestión de capacidades	SI	SI			X	
	12.1.4	Separación de los entornos de desarrollo, prueba y operación	SI	SI				X
	12.2	**Protección contra el código malicioso**						
	12.2.1	Controles contra el código malicioso	SI	SI			X	
	12.3	**Copias de seguridad**						
	12.3.1	Copias de seguridad de la información	SI	SI			X	
	12.4	**Registro y monitorización**						
	12.4.1	Registro de eventos	SI	SI			X	

	12.4.2	Protección de la información de los registros	SI	SI				X
	12.4.3	Registros de administración y operación	SI	SI			X	
	12.4.4	Sincronización del reloj	NO	NO				
	12.5	**Control del software en explotación**						
	12.5.1	Instalación de software en sistemas operacionales	SI	SI			X	
	12.6	**Gestión de las vulnerabilidades técnicas**						
	12.6.1	Gestión de las vulnerabilidades técnicas	SI	SI			X	
	12.6.2	Restricciones a la instalación de software	SI	SI			X	
	12.7	**Consideraciones sobre la auditoría de los sistemas de información**						
	12.7.1	Controles de auditoría de los sistemas de información	SI	SI			X	
13 Seguridad en las Comunicaciones	**13.1**	**Gestión de la seguridad de las redes**						
	13.1.1	Controles de red	SI	SI			X	
	13.1.2	Seguridad de los servicios de red	SI	SI				X
	13.1.3	Segregación de redes	SI	SI				X
	13.2	**Transferencia de información**						
	13.2.1	Políticas y procedimientos de transferencia de información	NO	NO				
	13.2.2	Acuerdos de transferencia de información	SI	SI				X
	13.2.3	Mensajería electrónica	SI	SI				X
	13.2.4	Acuerdos de confidencialidad o no divulgación	SI	SI				X
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	**14.1**	**Requisitos de seguridad de los sistemas de información**						
	14.1.1	Análisis y especificación de los requisitos de seguridad de la información	SI	SI				X
	14.1.2	Aseguramiento de los servicios de aplicaciones en las redes públicas	SI	SI				X
	14.1.3	Protección de las transacciones de servicios de aplicación	SI	SI				X
	14.2	**Seguridad en los procesos de desarrollo y soporte**						
	14.2.1	Política de desarrollo seguro	SI	SI				X
	14.2.2	Procedimientos de control de cambios en el sistema	SI	SI				X
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma	SI	SI				X
	14.2.4	Restricciones a los cambios en los paquetes de software	SI	SI				X
	14.2.5	Principios para la ingeniería de sistemas seguros	SI	SI				X
	14.2.6	Entorno de desarrollo seguro	SI	SI				X
	14.2.7	Externalización del desarrollo de software	SI	SI				X
	14.2.8	Pruebas de seguridad del sistema	SI	SI				X

	14.2.9	Pruebas de aceptación del sistema	SI	SI				X
	14.3	**Datos de prueba**						
	14.3.1	Protección de los datos de prueba	SI	SI			X	
15 Relaciones con Proveedores	**15.1**	**Seguridad de la información en las relaciones con proveedores**						
	15.1.1	Política de seguridad de la información en las relaciones con proveedores	NO	NO				
	15.1.2	Tratamiento de la seguridad en contratos con proveedores	SI	SI			X	
	15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	SI	SI			X	
	15.2	**Gestión de los servicios prestados por terceros**						
	15.2.1	Supervisión y revisión de los servicios prestados por terceros	SI	SI			X	
	15.2.2	Gestión del cambio en los servicios prestados por terceros	SI	SI			X	
16 Gestión de Incidentes de Seguridad de la Información	**16.1**	**Gestión de incidentes de seguridad de la información y mejoras**						
	16.1.1	Responsabilidades y procedimientos	SI	SI			X	
	16.1.2	Notificación de eventos de seguridad de la información	SI	SI			X	
	16.1.3	Notificación de puntos débiles de seguridad	SI	SI			X	
	16.1.4	Evaluación y decisión respecto de los eventos de seguridad de la información	SI	SI			X	
	16.1.5	Respuesta a incidentes de seguridad de la información	SI	SI			X	
	16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	SI			X	
	16.1.7	Recopilación de evidencias	NO	NO				
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	**17.1**	**Continuidad de la seguridad de la información**						
	17.1.1	Planificación de la continuidad de la seguridad de la información	SI	SI				X
	17.1.2	Implementación de la continuidad de la seguridad de la información	SI	SI			X	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	SI			X	
	17.2	**Redundancia**						
	17.2.1	Disponibilidad de los medios de procesamiento de información	SI	SI				X
18 Cumplimiento	**18.1**	**Cumplimiento de los requisitos legales y contractuales**						
	18.1.1	Identificación de la legislación aplicable y requisitos contractuales	SI	SI				X
	18.1.2	Derechos de propiedad intelectual (DPI)	SI	SI			X	
	18.1.3	Protección de los documentos de la organización	SI	SI				X
	18.1.4	Protección de datos y privacidad de la información de carácter personal	SI	SI				X

	18.1.5	Regulación de los controles criptográficos	NO	NO				X
	18.2	**Revisiones de seguridad de la información**						
	18.2.1	Revisión independiente de la seguridad de la información	SI	SI			X	
	18.2.2	Cumplimiento de las políticas y normas de seguridad	NO	NO			X	
	18.2.3	Comprobación del cumplimiento técnico	SI	SI			X	

Anexo 12: Ficha de observación – PostTest - Número de controles

	**FICHA DE OBSERVACIÓN N° 03: INDICADOR- NÚMERO DE CONTROLES APLICADOS**	
		(DECLARACIÓN DE APLICABILIDAD DE CONTROLES)
	FASE:	POST TEST
	CODIGO	FO-003-NCA
	FECHA DISEÑO Jun-22	**CLASIFICACIÓN: CONFIDENCIAL**
	Proceso:	Gestión de riesgos
	Puesto:	Asistente de sistemas
	Fecha de recolección:	02 Junio 02 julio 2022
	Investigador:	Cinthia J. Calderon Aquiño

La elección de controles y objetivos de control se ejecutaron a través de los siguientes criterios:
LR: requerimientos legales
CO: obligaciones contractuales
BR/BP: requerimientos del negocio/mejores prácticas adoptadas
RRA: resultado de la valoración de riesgos

Instrumento de recolección de datos

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/ BP	RRA
Cláusula	**Sección**	**Objetivo de control / control**						
5 Políticas de Seguridad	**5.1**	**Dirección de la gestión de la seguridad de la información**						
	5.1.1	Políticas de seguridad de la información	SI	SI			X	
	5.1.2	Revisión de las políticas de seguridad de la información	SI	SI			X	
6 Organización de la Seguridad de la Información	**6.1**	**Organización interna**						
	6.1.1	Roles y responsabilidades relativas a la seguridad de la información	SI	SI			X	
	6.1.2	Separación de tareas	SI	SI			X	
	6.1.3	Contacto con las autoridades	SI	SI			X	
	6.1.4	Contacto con grupos de especial interés	NO	NO				
	6.1.5	Seguridad de la información en la gestión de proyectos	SI	SI			X	

	6.2	**Dispositivos móviles y teletrabajo**						
	6.2.1	Política de dispositivos móviles	SI	SI			X	
	6.2.2	Teletrabajo	NO	NO				
7 Seguridad en los Recursos Humanos	**7.1**	**Antes del empleo**						
	7.1.1	Investigación de antecedentes	NO	NO				X
	7.1.2	Términos y condiciones de contratación	SI	SI				X
	7.2	**Durante el empleo**						
	7.2.1	Responsabilidades de la Dirección	SI	SI			X	
	7.2.2	Concienciación, formación y capacitación en seguridad de la información	SI	SI			X	
	7.2.3	Proceso disciplinario	SI	SI			X	
	7.3	**Cese del empleo y cambio de puesto de trabajo**						
	7.3.1	Terminación o cambio de responsabilidades laborales	SI	SI				X
8 Gestión de Activos	**8.1**	**Responsabilidad sobre los activos**						
	8.1.1	Inventario de activos	SI	SI				X
	8.1.2	Propiedad de los activos	SI	SI				X
	8.1.3	Uso aceptable de los activos	SI	SI				X
	8.1.4	Devolución de activos	SI	SI			X	
	8.2	**Clasificación de la información**						
	8.2.1	Clasificación de la información	SI	SI			X	
	8.2.2	Etiquetado de la información	SI	SI			X	
	8.2.3	Manejo de activos	SI	SI			X	
	8.3	**Manipulación de los soportes**						
	8.3.1	Gestión de soportes extraíbles	SI	SI				X
	8.3.2	Retirada de soportes	SI	SI			X	
	8.3.3	Transferencia de soportes físicos	SI	SI			X	
9 Control de Acceso	**9.1**	**Requisitos de negocio para el control de acceso**						
	9.1.1	Política de control de acceso	NO	NO				
	9.1.2	Acceso a redes y servicios en red	SI	SI				X
	9.2	**Gestión del acceso de usuario**						
	9.2.1	Altas y bajas de usuarios	SI	SI				X
	9.2.2	Gestión de derechos de acceso de los usuarios	SI	SI				X
	9.2.3	Gestión de derechos de acceso especiales	SI	SI				X
	9.2.4	Gestión de la información secreta de autenticación de usuarios	SI	SI				X
	9.2.5	Revisión de derechos de acceso de usuario	SI	SI				X
	9.2.6	Terminación o revisión de los privilegios de acceso	SI	SI				X
	9.3	**Responsabilidades de usuario**						
	9.3.1	Uso de la información secreta de autenticación	SI	SI				X
	9.4	**Control de acceso al sistema y a las aplicaciones**						
	9.4.1	Restricción del acceso a la información	SI	SI				X

	9.4.2	Procedimientos seguros de inicio de sesión	SI	SI				X
	9.4.3	Gestión de las contraseñas de usuario	SI	SI				X
	9.4.4	Uso de los recursos del sistema con privilegios especiales	SI	SI				X
	9.4.5	Control de acceso al código fuente de los programas	SI	SI				X
10 Criptografía	**10.1**	**Controles criptográficos**						
	10.1.1	Política de uso de los controles criptográficos	SI	SI				X
	10.1.2	Gestión de claves	SI	SI				X
11 Seguridad Física y del Entorno	**11.1**	**Áreas seguras**						
	11.1.1	Perímetro de seguridad física	SI	SI			X	
	11.1.2	Controles físicos de entrada	SI	SI			X	
	11.1.3	Seguridad de oficinas, despachos e instalaciones	SI	SI			X	
	11.1.4	Protección contra las amenazas externas y de origen ambiental	SI	SI			X	
	11.1.5	Trabajo en áreas seguras	SI	SI			X	
	11.1.6	Áreas de carga y descarga	SI	SI				X
	11.2	**Equipos**						
	11.2.1	Emplazamiento y protección de equipos	SI	SI				X
	11.2.2	Instalaciones de suministro	SI	SI			X	
	11.2.3	Seguridad del cableado	SI	SI				X
	11.2.4	Mantenimiento de los equipos	SI	SI			X	
	11.2.5	Retirada de materiales propiedad de la empresa	SI	SI				X
	11.2.6	Seguridad de los equipos fuera de las instalaciones	SI	SI				X
	11.2.7	Reutilización o retirada segura de equipos	SI	SI				X
	11.2.8	Equipo de usuario desatendido	SI	SI			X	
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI	SI			X	
12 Seguridad en las Operaciones	**12.1**	**Responsabilidades y procedimientos de operación**						
	12.1.1	Documentación de los procedimientos de operación	SI	SI			X	
	12.1.2	Gestión de cambios	SI	SI				X
	12.1.3	Gestión de capacidades	SI	SI			X	
	12.1.4	Separación de los entornos de desarrollo, prueba y operación	SI	SI				X
	12.2	**Protección contra el código malicioso**						
	12.2.1	Controles contra el código malicioso	SI	SI			X	
	12.3	**Copias de seguridad**						
	12.3.1	Copias de seguridad de la información	SI	SI			X	
	12.4	**Registro y monitorización**						
	12.4.1	Registro de eventos	SI	SI			X	

	12.4.2	Protección de la información de los registros	SI	SI				X
	12.4.3	Registros de administración y operación	SI	SI			X	
	12.4.4	Sincronización del reloj	SI	SI				X
	12.5	**Control del software en explotación**						
	12.5.1	Instalación de software en sistemas operacionales	SI	SI			X	
	12.6	**Gestión de las vulnerabilidades técnicas**						
	12.6.1	Gestión de las vulnerabilidades técnicas	SI	SI			X	
	12.6.2	Restricciones a la instalación de software	SI	SI			X	
	12.7	**Consideraciones sobre la auditoría de los sistemas de información**						
	12.7.1	Controles de auditoría de los sistemas de información	SI	SI			X	
13 Seguridad en las Comunicaciones	**13.1**	**Gestión de la seguridad de las redes**						
	13.1.1	Controles de red	SI	SI			X	
	13.1.2	Seguridad de los servicios de red	SI	SI			X	
	13.1.3	Segregación de redes	SI	SI			X	
	13.2	**Transferencia de información**						
	13.2.1	Políticas y procedimientos de transferencia de información	SI	SI				X
	13.2.2	Acuerdos de transferencia de información	SI	SI			X	
	13.2.3	Mensajería electrónica	SI	SI				X
	13.2.4	Acuerdos de confidencialidad o no divulgación	SI	SI				X
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	**14.1**	**Requisitos de seguridad de los sistemas de información**						
	14.1.1	Análisis y especificación de los requisitos de seguridad de la información	SI	SI				X
	14.1.2	Aseguramiento de los servicios de aplicaciones en las redes públicas	SI	SI				X
	14.1.3	Protección de las transacciones de servicios de aplicación	SI	SI				X
	14.2	**Seguridad en los procesos de desarrollo y soporte**						
	14.2.1	Política de desarrollo seguro	SI	SI				X
	14.2.2	Procedimientos de control de cambios en el sistema	SI	SI				X
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma	SI	SI				X
	14.2.4	Restricciones a los cambios en los paquetes de software	SI	SI				X
	14.2.5	Principios para la ingeniería de sistemas seguros	SI	SI				X
	14.2.6	Entorno de desarrollo seguro	SI	SI				X
	14.2.7	Externalización del desarrollo de software	SI	SI				X
	14.2.8	Pruebas de seguridad del sistema	SI	SI				X
	14.2.9	Pruebas de aceptación del sistema	SI	SI				X
	14.3	**Datos de prueba**						

	14.3.1	Protección de los datos de prueba	SI	SI			X	
15 Relaciones con Proveedores	**15.1**	**Seguridad de la información en las relaciones con proveedores**						
	15.1.1	Política de seguridad de la información en las relaciones con proveedores	SI	SI				
	15.1.2	Tratamiento de la seguridad en contratos con proveedores	SI	SI			X	
	15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	SI	SI			X	
	15.2	**Gestión de los servicios prestados por terceros**						
	15.2.1	Supervisión y revisión de los servicios prestados por terceros	SI	SI			X	
	15.2.2	Gestión del cambio en los servicios prestados por terceros	SI	SI			X	
16 Gestión de Incidentes de Seguridad de la Información	**16.1**	**Gestión de incidentes de seguridad de la información y mejoras**						
	16.1.1	Responsabilidades y procedimientos	SI	SI			X	
	16.1.2	Notificación de eventos de seguridad de la información	SI	SI			X	
	16.1.3	Notificación de puntos débiles de seguridad	SI	SI			X	
	16.1.4	Evaluación y decisión respecto de los eventos de seguridad de la información	SI	SI				X
	16.1.5	Respuesta a incidentes de seguridad de la información	SI	SI			X	
	16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	SI			X	
	16.1.7	Recopilación de evidencias	SI	SI			X	
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	**17.1**	**Continuidad de la seguridad de la información**						
	17.1.1	Planificación de la continuidad de la seguridad de la información	SI	SI				X
	17.1.2	Implementación de la continuidad de la seguridad de la información	SI	SI			X	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	SI			X	
	17.2	**Redundancia**						
	17.2.1	Disponibilidad de los medios de procesamiento de información	SI	SI				X
18 Cumplimiento	**18.1**	**Cumplimiento de los requisitos legales y contractuales**						
	18.1.1	Identificación de la legislación aplicable y requisitos contractuales	SI	SI				X
	18.1.2	Derechos de propiedad intelectual (DPI)	SI	SI			X	
	18.1.3	Protección de los documentos de la organización	SI	SI				X
	18.1.4	Protección de datos y privacidad de la información de carácter personal	SI	SI			X	

	18.1.5	Regulación de los controles criptográficos	SI	SI				X
	18.2	**Revisiones de seguridad de la información**						
	18.2.1	Revisión independiente de la seguridad de la información	SI	SI				X
	18.2.2	Cumplimiento de las políticas y normas de seguridad	SI	SI			X	
	18.2.3	Comprobación del cumplimiento técnico	SI	SI			X	

Anexo 13: Resumen de Número de controles en fases PreTest y PostTest

TABLA RESUMEN					
INDICADOR: NÚMERO DE CONTROLES FASES: PRE TEST Y POS TEST					
		TOTAL PRE TEST		TOTAL POST TEST	
N° CONTROLES QUE APLICAN	TOTAL	NO EXISTENTE	SI EXISTENTE	NO EXISTENTE	SI EXISTENTE
/EXISTEN SI APLICA /EXISTE	114	101	13	2	112
	100%	89.38%	11.50%	1.77%	99.12%
NO APLICA	2				

Fuente: Elaboración Propia

Anexo 14: Carta de presentación de la empresa

Lima, 13 Julio de 2022

Doc. Luis Enrique Ledesma
Director académico de la Universidad César Vallejo – Lima Norte

Presente.

Tengo el agrado de dirigirme a Usted.
Con la finalidad de hacer de su conocimiento que la Srta. **CALDERÓN AQUIÑO CINTHIA JEANETTE** con DNI N° 46151789 y con código de matrícula N° 6700080437, alumna del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN, de la Institución Universitaria que usted representa, ha sido admitida para realizar su tesis en nuestra empresa Matizado de Pintura **ROSSY COLORS** en el área Sistemas.

Aprovecho la oportunidad para expresarle mi consideración y estima personal.

Atentamente,

MATIZADOS ROSSY COLORS
Fortunata R. Aquiño Melgarejo
Gerente

Anexo 15: Aspectos administrativos

RECURSOS Y PRESUPUESTO

Recursos humanos

El compromiso de investigación asume en cuenta los medios utilizados para llevarlo a cabo. Esto tiene en cuenta los costes de mano de obra, incluidas las fuentes bibliográficas, la compilación de antecedentes, el procesamiento, el comentario y la movilidad con algunos ajustes personales.

Tabla 1:
Presupuesto de Recursos Humanos

Recurses	Description	Monto
Referencia	Fuentes Bibliográficas	S/. 45.00
Transporte	Movilidad	S/. 25.00
Data	Recolección y procesamiento	S/. 2.800.00
Total		S/.2, 870.00

Fuente: Elaboración Propia

Recursos Hardware

Además, se utilizó un equipo. Por lo cual, se considera una computadora portátil tal como se aprecia en la Tabla 5.

Tabla 2:
Presupuesto de Recursos Hardware

Recurses	Descripción	Monto
Equipo	Laptop HP (Core I3 5ma Generación)	S/. 3,200.00
	Total	S/.3, 200.00

Fuente: Elaboración Propia

Recursos de Software

Mientras tanto, se aceptó el software hacia la recuperar y procesar datos llamado SPSS. Las especificaciones visualizadas en el prototipo en la Tabla 3.

Tabla 3:
Presupuesto de Recursos de Software

Recurses	Descripción	Monto
Licencia	Statistical Package for the Social Sciences (SPSS) v23.0	S/. 150.00
	Total	S/. 150.00

Fuente: Elaboración Propia

Presupuesto

Posteriormente, la suma de todos los presupuestos anteriores se forma para el objetivo del presupuesto en la investigación.

Tabla 4:
Presupuesto Total

Sumatoria de costos	Monto
Recursos Humanos	S/. 2, 870.00
Recursos de Hardware	S/. 3, 200.00
Recursos de Software	S/. 150.00
Total	S/. 6, 220.00

Fuente: Elaboración Propia

Financiamiento

La investigación que se realiza U.C.V. está orientada a fortalecer el conocimiento dentro del área de estudio, y todo el software, hardware y recursos humanos son autosuficientes, en base a explicaciones presupuestarias, es financiada.

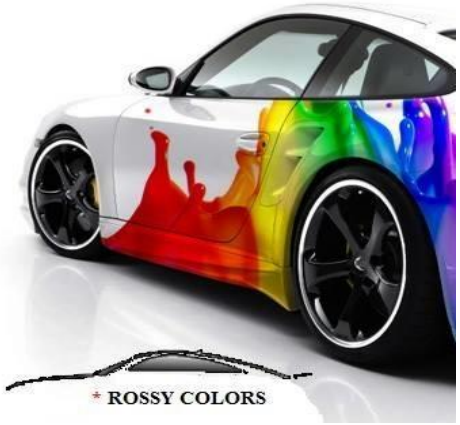
Tabla 5:
Financiamiento

Entidad Financiera	Monto	Porcentaje
Autofinanciado	S/. 6,220.00	100%

Fuente: Elaboración Propia

Anexo 16: Plan de Implementación SGSI

PLAN DE IMPLEMENTACIÓN PARA UN MODELO DE CIBERSEGURIDAD PARA LA GESTIÓN DE RIESGO DE UNA EMPRESA MATIZADOS DE PINTURA DE LIMA, 2022.



1. Objetivo, alcance y usuarios

1.1. Objetivos

Definir la implementación de un modelo de sistema de ciberseguridad para la gestión de riesgo (SGSI), los documentos que se redactaran, los plazos, funciones y responsabilidad del proyecto.

1.2. Alcance

Se aplica en las actividades que están dentro del proyecto de la implantación del SGGI.

1.3. Usuarios

- Gerente General.
- Jefe de sistemas.

2. Documentos de referencia

- ISO/IEC 27001:2014
- ISO/IEC 27002:2014

3. Proyecto de implementación del SGSI

3.1. Objetivo del proyecto

Implementar el modelo de sistema de ciberseguridad para la gestión de riesgo con la norma NTP ISO/IEC 27001:2014 de una empresa de matizados de pintura de Lima, 2022

3.2. Entregables del proyecto

En el proyecto de implantación del SGSI, con los entregables del proyecto establecidos.

- ✓ Alcance del SGSI.
- ✓ Política de seguridad de la información
- ✓ Procedimiento para control de documentos y registros (Documentos Plantilla SGSI-000)
- ✓ Procedimiento para identificación de requisitos
- ✓ Metodología de evaluación y tratamiento de riesgos
- ✓ Matriz de evaluación de riesgos
- ✓ Plan de tratamiento de riesgos (RTP)
- ✓ Declaración de aplicabilidad (SOA)
- ✓ Procedimiento para acciones correctivas

3.3. Plazos

CRONOGRAMA DE TRABAJO - MATIZADO DE PINTURA																		
DESCRIPCIÓN DE FASES/ACTIVIDADES	**ABRIL**				**MAYO**				**JUNIO**				**JULIO**				**AGOSTO**	
Semanas	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
1. PLANIFICAR																		
1.1 Definir alcance																		
1.2 Elaborar política de seguridad de información																		
1.3 Obtener inventario de activos																		
1.4 Establecer línea base mediante evaluación de la situación de seguridad actual																		
1.5 Definir la declaración de aplicabilidad																		
1.6 Evaluar los riesgos																		
1.7 Elaborar plan de tratamiento de riesgos																		
2. HACER																		
2.1 Evaluar controles de seguridad																		
2.2 Identificar métricas e indicadores.																		
2.3 Definir políticas y procedimientos del SGSI																		
2.4 Asignación y distribución de recursos																		
2.5 Propuesta de capacitación																		
2.6 Elaboración de propuestas de proyectos y planes de acción																		
2.7 Definición de responsables																		
3. VERIFICAR																		
3.1 Revisión de métricas e indicadores																		
3.2 Revisión del nivel de riesgo residual																		
4. ACTUAR																		
4.1 Definir e implementar mejoras																		
4.2 Ejecutar acciones correctivas y preventivas.																		
4.3 Comunicar resultados a los StakeHolders																		
4.4 Asegurar el cumplimiento																		

3.4. Gestión de registros

La mejora continua de este documento el cual es consignado en la segunda página del mismo en la tabla Mejora Continua.

- Los informes parciales de la implementación del proyecto
- Las incidencias producto de cambios o mejoras al proyecto

Evaluación de los activos:

Los activos serán puntuados dependiendo de una tabla de ponderaciones en las que se evalúa la importancia para la organización.

Tabla 1

Escala de puntuaciones de los activos

Escala de evaluación	Descripción	Valor
Muy Alta	Es alto de los objetivos que perigee la organización	5
Alta	Crecientemente importante para la empresa	4
Media	Semi Medio de Importante para la empresa	3
Baja	Mínima para el desarrollo de la empresa	2
Muy Baja	Poco útil en la empresa	1

Fuente: Elaboración Propia

Evaluación de la degradación: Los contenidos serán puntuados según un calendario ponderado en el que se evalúa la confidencialidad, integridad y disponibilidad de cada activo.

Confidencialidad: Los derechos de propiedad especifican que la información solo está disponible y se divulga a las personas, entidades u operaciones autorizadas.

Integridad: Activos mantiene la precisión y la integridad de los activos.

Disponibilidad: Indicar que la información puede ser accedida y utilizada según lo requiera la entidad legal autorizada, cuando así lo solicite esa organización.

Tabla 2

Escala de puntuaciones de valores de la degradación

Puntación	Disponibilidad	Integridad	Confidencialidad
5	Persistentemente	Extremo	Uso confidencial
4	Dispensa por horas	Importante	Uso restringido
3	Dispensa por 24 horas	Media	Pre restringido
2	Dispensa por 48 horas	Menos importante	Uso interno
1	Dispensa por varios días	En termino mínimo	Acceso público

Fuente: Elaboración Propia

Degradación máxima- Tomando cada grado de degradación asignado, determinamos el valor máximo de la degradación, que es el dato que nos ayudará a calcular el nivel de riesgo.

Valoración del impacto- El valor de impacto se determina de acuerdo con el programa de evaluación de impacto.

Tabla 3

Estimación del impacto

Valor	Descripción
Muy bajo (1)	Los riesgos pueden tener poco o ningún impacto en la organización.
Bajo (2)	Causa daños a la propiedad o a la imagen que pueden repararse en poco tiempo y no afectan el logro de los objetivos estratégicos.
Medio (3)	Esto podría conducir a una pérdida significativa de capital, incumplimientos regulatorios, problemas operativos, o un deterioro significativo de la imagen.
Alto (4)	Esto podría dar lugar a importantes daños patrimoniales, infracciones normativas, problemas operativos o medioambientales, deterioro de la imagen o los logros corporativos.
Muy Alto (5)	Afecta directamente el cumplimiento de la misión, pérdida de propiedad, problemas operativos, impactos ambientales o degradación de la imagen, también los programas o servicios que brinda la organización se vean afectados.

Fuente: Elaboración Propia

Probabilidad

La probabilidad es la posibilidad de que se lleve a cabo una amenaza. Para la presente investigación, se determina en la siguiente escala:

Tabla 5

Escala de puntuaciones de la probabilidad

Escala de valoración	Descripción	Valor
Muy Alta	La amenaza se llevar a cabo una vez al día como máximo	5
Alta	La amenaza se alcanzar una vez por semana como máximo	4
Media	La amenaza se llevar a cabo a lo sumo una vez cada mes como máximo.	3
Baja	La amenaza se alcanzar a lo sumo una vez cada semestre como máximo.	2
Muy Baja	La amenaza se llevar a cabo a lo sumo una vez cada año como máximo.	1

Fuente: Elaboración Propia

DECLARACIÓN DE APLICABILIDAD.

Según las dimensiones ya definidas para la variable dependiente, serán medibles, según los siguientes criterios:

Valoración del Activos

Se tiene Nivel de activos será instrumento será la ficha de observación. Anexo 9 y 10.

Activos = (Impacto x Probabilidad)

En donde:

NR = Nivel de activo.

I = Nivel de impacto sobre el activo.

P = Probabilidad

Valoración del riesgo

Como indicador tendremos el nivel de riesgo, cuya medida será cuantitativa. Los resultados del análisis descriptivo se detallan en el anexo 7 y anexo 8

El valor del riesgo se determina multiplicando el efecto y la probabilidad:

Riesgo = (Impacto x Probabilidad)

En donde:

NR = Nivel de riesgo.

I = Nivel de impacto sobre el riesgo.

P = Probabilidad

Valoración del control

La técnica utilizada para obtener el número de controles aplicados será el de observación directa, cuyo instrumento será la ficha de observación. Anexo 11 y 12.

Como indicador tendremos el número de controles aplicados, cuya medida será cuantitativa y estará dada por la siguiente fórmula:

CA = Ciso – (CNE + CNA)

En donde:

CA = Número de controles aplicados.

Ciso = Número de controles ISO 31000

CNE = Número de controles no existentes.

CNA = Número de controles no aplicables.

4. Política de seguridad

Según el **ISO 27002** nos manifiesta; **5.1.2** “La política de seguridad de la información debiera ser revisada a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.” (pag.21, 2005).

El principal objetivo de **la ISO 27002** es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa.

Según el **ISO 27002** nos manifieste; **5.1.1** “El documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.” (pag.20, 2005).

La empresa, se encuentra comprometido en cumplir con los objetivos planteados en la ciberseguridad por lo cual se implementará, monitoreará y mejorará, de manera continua, el Sistema de Gestión de Seguridad de la Información (SGSI) según la ISO 27002.

5. Organización de la seguridad de la información

Según el **ISO 27002** nos manifieste; **6.1.8** “Se debiera revisar el enfoque de la organización para manejar la seguridad de la información y su implementación […] de manera independiente a intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.” (pag.28, 2005).

Por lo cual la empresa, al implementar SGSI podrá contar con los controles y mecanismos de seguridad para proteger el hardware y los almacenamientos de la organización.

Copias de seguridad y recuperación de datos

Las copias de seguridad tienen dos objetivos que son muy importantes:

- Permiten la restauración de archivos individuales, se da este caso cuando un usuario borra un archivo accidentalmente o se corrompe y pide restaurarlo desde su último respaldo.

En la actualidad los datos cambian y para el diseño de un procedimiento de respaldo se realizan por dos razones;

- Una copia de seguridad es un reflejo de los datos.
- Los datos que cambian con poca frecuencia se respaldan a menudo, pero los datos que cambian regularmente deben ser copiados frecuentemente.

6. Gestión de activos

Según el **ISO 27002** hace mención en él; **7.1.1** "Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. […], pero el propietario sigue siendo responsable por la protección apropiada de los activos." (pag.36, 2005)

Según la norma, es cualquier la organización requiere ser protegido. Por lo tanto, se recomendó que pueda identificar y clasificar sus activos importantes de modo que un inventario pueda ser organizado y posteriormente mantenido.

7. Seguridad de recursos humanos

Según el **ISO 27002** nos indica en él; **8.1.1** "Se debieran definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización." (pag.42, 2005)

Uno de los objetivos mencionados es que al implementar el ISO 27002, es asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son

considerados; y reducir el riesgo de robo, fraude y mal uso de los medios en la empresa.

Los roles y responsabilidades de la seguridad debieran ser definidos y claramente comunicados a los candidatos para el puesto durante el proceso de pre-empleo.

De acuerdo a la **ley N° 30096 artículo 2**, hace mención: “el que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa” (2014, pág. 3).

8. Gestión de la continuidad del negocio

Según el **ISO 27001** nos indica en él; **A.12.5.2.** “Revisión técnica de las aplicaciones después de cambios en el sistema operativo: Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.” (pag.34, 2005)

Se puede gestionar de forma espontánea o individual para cada tipo de riesgo, se requiere un método completo y sistemático para adquirir la capacidad de anticipar eventos desfavorables (riesgos) para obtener un uso óptimo de los eventos favorables (oportunidades). Este método es Enterprise Risk Management (ERM) el cual se puede desarrollar en línea con los requisitos de la ISO 31000 (Risk Management) para un tratamiento completo del mismo.

MATRIZ DE RIESGOS

A continuación, se hace una lista de los riesgos de este servicio.

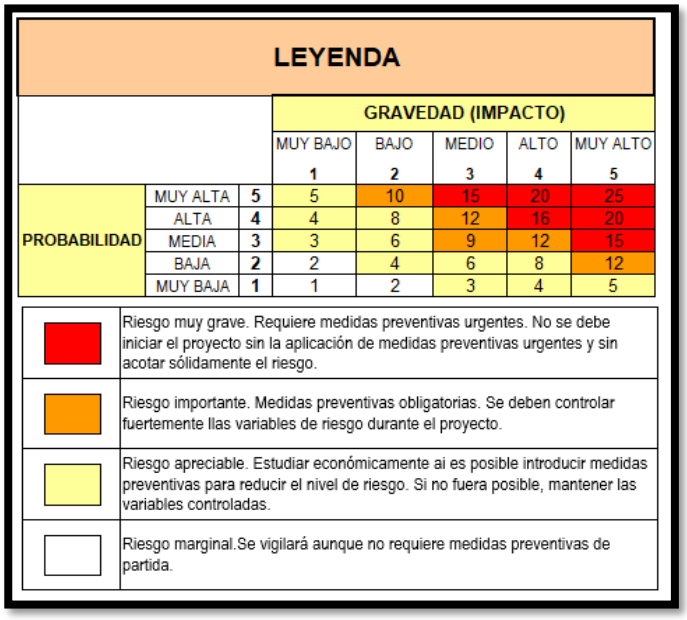
Tabla 6

Matriz de riesgos

MATRIZ DE RIESGOS					
RIESGO	**Probabilidad (Ocurrencia)**	**Gravedad (Impacto)**	**Valor de Riesgo**	**Nivel de riesgo**	**Medidas de mitigación**
Corte de la luz	1	5	**5**	**Apreciable**	Respaldo de energía
Indisponibilidad medica del RRHH	3	3	**9**	**Importante**	Gestión del talento y personal
Ataques de seguridad	5	5	**25**	**Importante**	Backup, blacklist de direcciones IP, FW, etc.
Corte de internet	3	5	**15**	**Muy grabe**	Otro operador de internet
Indisponibilidad de Hardware Cloud	1	5	**5**	**Apreciable**	Tener un Cloud alternativo en una red separada
Indisponibilidad de la BD	1	5	**5**	**Apreciable**	Contar con un servidor alterno de base de datos

Fuente: Elaboración Propia

Figura 01:



Leyenda de Porbabilidad

Tabla 7

Análisis de riesgos

Peligro Muy Alto	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto	Riesgo Muy Alto
Peligro Alto	Riesgo Medio	Riesgo Medio	Riesgo Alto	Riesgo Muy Alto
Peligro Medio	Riesgo Bajo	Riesgo Medio	Riesgo Medio	Riesgo Alto
Peligro Bajo	Riesgo Bajo	Riesgo Bajo	Riesgo Medio	Riesgo Alto
	Vulnerabilidad Baja	**Vulnerabilidad Media**	**Vulnerabilidad Alta**	**Vulnerabilidad Muy Alta**

LEYENDA:

- Riesgo Bajo (< de 25%)
- Riesgo Medio (26% al 50%)
- Riesgo Alto (51% al 75%)
- Riesgo Muy Alto (76% al 100%)

Fuente: instituto nacional de defensa civil

9. Gestión de comunicaciones y operaciones

Según la ISO 27002, menciona que “Se debieran establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados” (2005, pág. 62).

La empresa para cumplir lo mencionado en el párrafo anterior, se compromete tener un mejor control de sus procedimientos de operación de la información y comunicación; realizando la documentación de que cada uno de sus procesos, tales como procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de cómputo, manejo del correo y seguridad.

Diseño de modelo de ciberseguridad en la empresa de matizado de pintura


ROSSY
Matizado RossyColors
SOMOS PARTE DE TI
Seguimiento de su tracking
Numero de su tracking
Escriba el numero de tracking
Año de Emision
2021
INGRESAR


ROSSY
Matizado RossyColors
SOMOS PARTE DE TI
INFORMACION DEL ENVIO:
Ingrese la foto de entrega
Pagos
GUARDAR
INICIO


ROSSY
Matizado RossyColors
SOMOS PARTE DE TI
Cámara de Seguridad
GUARDAR
INICIO

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Modelo de Sistema de Ciberseguridad para la Gestión de Riesgo de una Empresa de Matizados de Pintura de Lima, 2022", cuyo autor es CALDERON AQUIÑO CINTHIA JEANETTE, constato que la investigación cumple con el índice de similitud establecido, y verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 06 de Agosto del 2022

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID** 0001-5207-9353	Firmado digitalmente por: MACUNABE el 06-08-2022 13:05:39

Código documento Trilce: TRI - 0396207

INVESTIGA UCV