UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Implementación de un Sistema de Ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza, 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Aliaga Yupanqui, Christian Adolfo (ORCID: 0000-0002-8724-7721)

ASESOR:

Dr. Acuña Benites, Marlon Frank (ORCID: 0000-0001-5207-9353)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LIMA – PERÚ

2021

Dedicatoria

A Dios por darme la luz, fortaleza y paciencia por perseguir mis sueños y lograrlo

A mi madre Lupe y padre Juan por brindarme su apoyo, amor, ánimos y apoyo incondicional para la consecución de mis objetivos.

Agradecimiento

A la empresa Radiadores Fortaleza por brindarme su apoyo incondicional en la realización de la tesis.

A mi asesor de tesis, por su empeño y dedicación que contribuyeron en la elaboración de mi tesis

Índice de contenido

Índice de tablas

Índice de Figuras

Resumen

La presente investigación tiene por título “Implementación de un Sistema de Ciberseguridad para la prevención de los Ataques Cibernéticos en la Empresa Radiadores Fortaleza, 2021.”, el objetivo general de la presente investigación fue la realización de la implementación de un sistema de ciberseguridad que influye de manera positiva en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.El presente estudio fue de tipo aplicada, con un diseño pre experimental, la población elegida fue de 50 empleados de la empresa Radiadores Fortaleza, se concluye que el valor de la prueba de Student de -46.680, asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación ($p<0,05$) lo que con lleva al rechazo de la hipótesis nula (H_0) y la aceptación de la hipótesis general planteada en la investigación (H_a). El modelo de implementación de ciberseguridad que se adoptó en la empresa fue el idóneo porque hay una mejora notable en la defensa de los ataques informaticos y una disminución de las vulnerabilidades que con lleva a un mejor desempeño de negocio de la empresa Radiadores Fortaleza.

Palabras clave: *ciberseguridad, ataques cibernéticos*

Abstract

The present research is titled "Implementation of a Cybersecurity System for the prevention of cyber-attacks in the company Radiadores Fortaleza, 2021", the general objective of this research was the implementation of a cybersecurity system that positively influences the prevention of cyber-attacks in the company Radiadores Fortaleza, 2021. The present study was of applied type, with a pre-experimental design, the chosen population was 50 employees of the company Radiadores Fortaleza, it is concluded that the value of the Student's test of -46.680, associated to the means of pretest and posttest where there is a significant difference , where it is associated to a significance level p value=0.000 lower than the significance level established in the research ($p<0.05$) which leads to the rejection of the null hypothesis (Ho) and the acceptance of the general hypothesis raised in the research (Ha). The cybersecurity implementation model adopted in the company was the ideal one because there is a notable improvement in the defense against computer attacks and a decrease of vulnerabilities that leads to a better business performance of the company Radiadores Fortaleza.

Keywords: *cybersecurity, cyber-attack*

I. INTRODUCCIÓN

La globalización en el entorno de la tecnificación se incrementó en los últimos 20 años, lo cual nos ha habituado a utilizar los medios digitales, por ello tenemos el riesgo de ciber amenazas, ciberdelitos y ciber riesgo, para lo cual estos mecanismos de salvaguarda de la data renacen en la ciberseguridad. (Arroyo&Hernández, 2020). Actualmente lo preocupante en las empresas es como adaptar este nuevo modelo de teletrabajo. En un estudio realizado por ISIL (2020), ante la pregunta, ¿Cuáles son los riesgos del trabajo remoto?, el 43% de entrevistados), respondieron que el primordial riesgo del trabajo remoto representa la seguridad de la información. Asimismo, obtuvo como resultado que el 89% de empresas trabajan de forma remota. Ante esta circunstancia en el Perú se hace cotidiano percibir que una empresa pública o privada se hayan realizado un ciberdelito que ocasiona un perjuicio a los activos de información, el Diario Gestión (2020) se refiere que, cuando se originó la cuarentena, los amenazas informáticas en dispositivos móviles en el Perú aumentaron, que e-mail enviados con datos fraudulentos crecieron en un 25% a principios del 2020.Cada vez se hace más importante, que la entidad privada y pública y consiguientemente para la existencia habitual que conocemos; parte de este progreso aporta nuevos desafíos como son la defensa ante amenazas de ciberdelitos de complejidad variada, ataques que se despliegan escudriñando vulnerar la data informática del sector público o privado para desenlaces delictivos. (Bohórquez ,2020).

Las brechas de protección en internet han cambiado debido a la globalización. Las organizaciones, los regímenes, las compañías y los cibernautas individuales de Internet están en peligro. Dada la representación de la ciberseguridad que aborda los riesgos actuales como piratas informáticos, virus, malware, ladrones de identificación y otros peligros en internet. (Kamberg&Jiménez, 2018).

En el hoy, realizar conciencia para proteger la información de todo humano o compañía es de fundamental trascendencia en cualquiera tipo de institución al no referir con trabajadores especializados en el área de seguridad de internet. (Rodrigo&Medina, 2021).

La Ciberseguridad protege la estructura informática e internet social en el país de Perú y el planeta, en cualquier parte están expuestos a todo riesgo de ataques cibernéticos realizados por hackers, quienes sustraen data valiosa de estas. Se da como conclusión que la Ciberseguridad como resguardo de medios informáticos potencializa las buenas prácticas en las empresas y protege la información. (Poma&Vargas, 2019)

La consecuente labor del estudio, da a conocer la finalidad primordial establecer la comparación entre la administración de peligros y la defensa de la data del programa fortalece Perú del MTPE, 2019. En que la tesis fue de categoría elemental grado descriptivo correlacional, no experimenta un corte transversal, con la cantidad de habitantes y muestra de 25 asesores del Programa Fortalece Perú. Por ello, se ofreció en práctica los procedimientos de uno y otras variables para que consolide la prevalencia del comercio. (Calderón, 2019)

Actualmente la empresa Nephila Networks se compromete a desplegar y garantizar una elevada categoría de sostén a otras pequeñas y medianas compañías para sus cimientos tecnológicos, disponiendo a Nephila un general de 21 corporaciones a las que apoya esta ayuda. La tesis tiene una orientación cuantitativa, siendo su fin de relacionar las soluciones de modo numérico a través de esquemas estadísticos; asimismo es un estudio elemental lo cual se fundamenta en el discernimiento antepuesto, donde tiene un diagrama descriptivo comparativo luego se utilizan hipótesis adelantadas y se relaciona 2 agrupaciones de encuestados. Prontamente se emplean los métodos estadísticos se gestionó los riesgos de las empresas de modo eficiente y eficaz. (Llontop, 2018)

La coyuntura de la pandemia ha hecho que en la empresa Radiadores Fortaleza, trajera como resultante que el área de sistemas debería revalorar su compañía. Por ello se afianzo en minimizar sus aptitudes en la dirección de la defensa de la data, indicando que las asistencias obtenidas a los clientes como para la dirección interna. La disminución de aptitudes en la defensa de la data se consideró rebelada en decrecimiento de gente y en el excesivo trabajo de responsabilidades a otro equipo.

Sin embargo, la empresa de sistemas ha de conducirse dentro de una visión que direcciona la técnica que contrapone una perspectiva de gestión de asistencias alimentado por las evoluciones. Dado que, en los 5 años ulteriores, no se ha constituido la financiación en la reciente resolución de defensa, se ha sostenido solamente la sustitución de los beneficios de defensas ya acontecidas.

En asunto de la data en la compañía de Radiadores Fortaleza se da una visión centrada en obtener y transformar los entornos de seguridad que resguardan los bienes de la data, en este tipo de dirección se ha puntualizado en la tarea tecnológica de los resultados de defensa.

Así mismo, interpretar la realidad problemática, se presenta la formulación del problema general: ¿Cómo impacta la implementación de un sistema de ciberseguridad para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021?

La presente tesis es justificable dado que en la empresa Radiadores Fortaleza ocurrió un incidente de robo de información por un virus Ranswore que tuvo repercusión en la información sensible, sumada a la globalización de los servicios informaticos y la masificación del internet en el uso de la tecnología informática a consecuencia de la crisis de la pandemia. Se realiza la implementación de un sistema de ciberseguridad para afianzar la defensa de los activos de la información de la empresa que esta expuestas a las amenazas constantes por el uso del internet de los 50 usuarios, cuyas vulnerabilidades serán mitigadas con la concientización y medidas de seguridad para contrarrestar las amenazas de los ataques informáticos.

Con la finalidad de resolver la problemática mencionada anteriormente se realizó como objetivo general:

- Determinar la influencia de la implementación de un sistema de ciberseguridad para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021.

Así cómo también se formula cuatro objetivos específicos siendo ellos:

- Determinar la influencia de la implementación de un sistema de ciberseguridad en el nivel de activos que son adecuados para su propósito para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021.
- Determinar la influencia de la implementación de un sistema de ciberseguridad en el nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa para la prevención de los ataques cibernéticos para la empresa radiadores fortaleza,2021.
- Determinar la influencia de la implementación de un sistema de ciberseguridad en el nivel histórico de tipo de defensas para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021.
- Determinar la influencia de la implementación de un sistema de ciberseguridad en el nivel de protección de amenaza y magnitud de daño para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021.

II. MARCO TEÓRICO

En los antecedentes nacionales respecto al tema, consideramos al investigador Rivera (2019), su investigación usa el sistema de gestión en peligros de ciberseguridad y sus efectos en la prudencia de estafa en la empresa industrial de la jurisdicción de Yanacancha. Cuya tesis manifiesta a las variaciones de categoría social y técnico que ha perjudicado al sistema progresivo de la comunidad de Yanacancha. Conforme al procedimiento de dirección ofrecida en el actual estudio comprende una investigación de orientaciones en los riesgos de ciberseguridad, donde se aumenta otra averiguación referente a las señales de dirección a categoría superior de gerencia, áreas procesales y operantes, que percibe la colocación de la experiencia sobre los 7 procedimientos de verificación para la consecución de los problemas. La interacción sinérgica ofrecida a la compañía de un nivel superior en la utilidad de su dirección de poder enfrentar sus amenazas y replicaciones.

Así mismo según Taipe(2018);el actual estudio tenía como finalidad examinar en ejecutar una auditoria de seguridad Informática cuya incompatibilidad de la ciberseguridad en el sector público; esta investigación pretende plasmar participaciones que ayuden al resultado de la hipótesis que muestra en esta área ; en todo lo que el sistema manejado, que se obtiene de un tipo descriptivo según (Bernal et al.2000), “diseño no experimental descriptiva correlacional”, según Hernández(2014); hacia la recolección de datos se empleó 2 sondeos, uno relativo a la “Auditoria de seguridad informática y el otro relativo a la aplicación en la ciberseguridad en el sector público año 2018”, que fue perfeccionado por el Personal de funcionarios y técnicos del sector público. En lo que se describe a las soluciones, se consigue marcar que los entrevistados al ejecutar una “Auditoria de seguridad informática tiene conocimiento sobre la aplicación de la ciberseguridad en el sector público año 2018”.

De otro lado según; Vilcarromero & Vílchez (2018), la implicancia de la salvaguarda estatal y de la económica de los países sostenida en los peligros de seguridad del internet estallan la progresiva diversidad de dichos métodos, señalando la riqueza,

la seguridad y la salud. También, el peligro económico y el peligro de la ciberseguridad inquieta a los objetivos importantes de la compañía.

Consigue acrecentar los precios y perturbar las entradas, cuya oportunidad obtiene en perjudicar la dimensión de un sistema en mejorar, ofrecer servicios, conquistar y sostener a los clientes. Por lo tanto, esta averiguación se ha transformado en uno de los ingresos más primordiales para alguna institución, y el fortalecimiento de la propia como algo primordial para conseguir méritos profesionales y producir el valor, basándose en la conveniente defensa de la confidencialidad, disponibilidad e integridad de la información. Cuya finalidad de la actual investigación es desplegar y plantear un procedimiento que admita resolver la seguridad de internet de las empresas de la división de telecomunicaciones además el cimiento de una adecuada dirección del peligro y cálculo de las revisiones según su categoría de madurez. Este procedimiento planteado tiene su base en el "Cyber Security Framework (CSF) del National Institute of Standards and Tecnólogo (NIST) divulgada por el presidente Obama mediante la Orden Ejecutiva (EO) 13636".

También según Mendoza (2019), cuya tesis tiene como objetivos determinar la categoría de dimensión de la ciberseguridad en la compañía, en reconocer las distancias para esbozar y plantear las inspecciones principales para fortificar la seguridad del internet y, por consiguiente, preparar y declarar los controles clave en la implementación. Conjuntamente, se limitó la trascendencia a los aspectos conectados en el descubrimiento y la respuesta a los sucesos relacionados en la ciberseguridad. Hay que señalar sobre la investigación ha sido dividido en cinco capítulos. Primeramente, es la introducción, que refiere el argumento presente de la ciberseguridad y los desafíos que este propio muestra. La segunda división demarca con superior determinación del conflicto del elemento en el trabajo como la incompetencia de la compañía para descubrir y replicar a un acontecimiento de seguridad del internet. En la siguiente división, se refiere a la reseña en ciberseguridad del "National Institute of Standards and Technology de Estados Unidos (NIST) (2018)", que se ha utilizado principalmente como reseña. También, se refiere la regla "ISO/IEC 33020-2015 (International Standard Organización 2015)" como concerniente para la valoración de contenido presente de los métodos y la norma COBIT 5 para peligros (ISACA 2013), que es manejada para la dirección

y la inspección de peligros relacionados al conjunto de técnicas de la data. Aquellas documentaciones estarán captadas como agregados a la referencia para este documento en estudio. También, en la cuarta división, se refiere la sistemática utilizada, que alcanza a prevalecer y demarcar los sitios de acción dentro de una condición de importancia, en reconocer los ingresos de data relacionados, realizar los estudios de contenido presente en los métodos, para elaborar una valoración de peligros, y priorizar las brechas encontradas, donde hay una resolución en la ejecución de los adelantos. Prontamente, en el quinto capítulo, se manifiestan las consecuencias del estudio, que pertenecen a la valoración de contenido de los métodos realizados y la observación de peligros dentro del argumento de la ciberseguridad; igualmente, se muestran las inspecciones para destacar la utilización en la capacidad de realizar la hoja de recorrido en la ejecución de las mejoras. A continuación, se manifiestan las soluciones del estudio, que pertenecen a la apreciación de la dimensión de los procedimientos realizados y la designación de los peligros dentro de la demostración de la ciberseguridad; también, se muestran las inspecciones privilegiadas para preponderar las brechas de evaluación determinadas.

Por ello Huayllani (2020), cuyo propósito era calcular la atribución de la utilidad de un sistema manejo de defensa de la data en la gestión del riesgo. El estudio ejecutado tuvo un "método hipotético deductivo, con un enfoque cuantitativo de tipo aplicada, de nivel correlacional y corte longitudinal". La población estaba conformada por 145 colaboradores de la "Unidad de Gestión de Inversiones de Reconstrucción con Cambios del Ministerio de Salud". La información fue recogida durante la utilización de 2 mecanismos para calcular las variables. Para examinar las consecuencias se usó el estadístico de Rho de Spearman se logró validar las conjeturas a partir de la información conseguidos durante la utilización de los artefactos. Los productos demostraron que coexiste una correspondencia afirmativa e indicadora entre las variables "Gestión del Riesgo y Sistemas de Gestión de la Seguridad de la Información".

Resulta que Sánchez (2017), la situación provechosa para operar de los ciberdelincuentes cuyo objetivo malintencionado. Teniendo como objetivo establecer de qué forma la aceptación de habilidades de ciberseguridad atañe la

seguridad de la data en la Oficina de Economía del Ejército. La justificación de la ejecución de las amenazas es en el ciberespacio. La conjetura diseñada fue: El amparo de tácticas de ciberseguridad quebrantaría la defensa de la información en la Oficina de Economía del Ejército. El tipo de estudio es No experimental, de enfoque cuantitativo, siendo una investigación aplicada y sustantiva. De un Nivel Descriptivo y Explicativo; de un diseño transaccional, lo cual se investigó la ocurrencia y los bienes que se indican en las variables que se indagan en un lapso fijo. Lo primordial del estudioso, inmediatamente de un estudio absoluto y efectos estadísticos en la protección de tácticas en ciberseguridad atañe en la salvaguarda de la data en la Oficina de Economía del Ejército,

Sin embargo, Vizcarra Jarez&Zuñiga Figueroa (2017) se formuló principalmente en determinar las barreras que imposibilitan el progreso de la Ciberdefensa que transgreden la protección de la información del Ejército del Perú. "Caso: COPERE 2013 – 2014" cuya finalidad es reconocer los orígenes que la generan y tener cimiento para plantear la utilización de nuevos sapiencias, que ayuden a perfeccionar la defensa de la información; las conjeturas esbozadas formulan que consiguen corregir las carencias de los modelos de capacitación, dificultades en los activos utilizables para la ciberdefensa, inexperiencia o empleo improcedente de las rutinas de seguridad informática e infracciones normativas relacionadas con ciberdefensa, que obstaculizan el progreso de la Ciberdefensa que atañen en la defensa de la data del Ejército del Perú.

Márquez Alayo (2018) examina la relevancia de la ciberseguridad en los activos críticos de información, cuyas tareas se han perfeccionado en esta interpretación de manera global en algunos estados y da sostén a las asociaciones mundiales que ayudan en el sitio de la ciberseguridad. Con respecto a este cimiento, plantea un prototipo para el reconocimiento de las áreas y bienes graves de una economía y una secuencia de inspecciones mínimas para su defensa. En consecuencia, las tecnologías de la información se han diseminado velozmente en todas las secciones de la comunidad y habitualmente no coexisten bienes graves que no se sometan a las aplicaciones, bases de datos, servidores, redes de comunicaciones, centros de datos, etc. La ausencia de inspecciones de ciberseguridad ha originado que algunos servicios se consideren perjudicados a

magnitud global y ocasionado problemas en el orden de la seguridad de la información.

En este sentido Huerta Agurto (2020). Se concluye que la “implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva en el proceso de gestión del riesgo de Coopsol Consultoría, 2019”, expuestos por los hallazgos encontrados en el ensayo estadístico t de Student con valor de 4,614, en contraste de las medias del Pre y Post Test, asociado a un nivel de significancia p valor= 0,000 en el indicador nivel de riesgo. Y los resultados obtenidos mediante la prueba Wilcoxon con valor de -9,644, en contraste a las medias del Pre y Post Test, asociado a un nivel de significancia p valor= 0,000 para el indicador número de controles, lo que sobrellevó a la desaprobación de la hipótesis nula y la aprobación de las hipótesis planteadas en la investigación (p < l0,05).

En los antecedentes internacionales respecto al tema, consideramos al investigador Avellán (2019), el objeto de establecer la categoría de la seguridad del internet manejando la norma ISO 27032-2012 con el término de presentar los peligros, ataques y debilidades de los métodos comercializados. Debido a la “Metodología Análisis Modal de Fallos y Efectos (AMFE)”, se comprobó y ajustó la categoría de peligros en toda la influencia de salvaguardia (Data, Redes, Aplicación), lo que admitió diseñar otros controles o procedimientos propuestas en la mejora ya sea a breve o extensa prescripción en las perspectivas de integridad, disponibilidad y confiabilidad de la información. Para su propósito, se emplearon los materiales para las vulnerabilidades Shodan, Nessus y Acunetix en los métodos comercializados de las IES Públicas, exponiendo tal secuela alcances por desiguales niveles de debilidades que poseían aquellos métodos, lo cual ofrecieron sugerencias con el fin de suavizar las incertidumbres en el internet. Cuanto es se tolera a una infinidad de categorías de defensa en los portales, sistemas o productos web, es la manera de ingreso a la data, y que corresponden a ser supervisadas o examinadas permanentemente para su apropiada seguridad de la información. A manera de prevención de respuestas a las investigadoras mejoraron el procedimiento de gestión que admitió a toda la corporación cuya finalidad de la investigación es adquirir medidas para proteger la integridad de la data.

Además, según Heffel (2016), precisar la Ciberseguridad manufacturero, determinar características inseparables al área en el que se desenvuelve la repartición de potencia eléctrica, se establece reciprocidades entre uno y otro universo, analiza la posición presente y la etapa de la habilidad del elemento, examinar vulnerabilidades o insuficiencias, plantear sugerencias, recapacitar y conseguir algunos desenlaces. Concierne en particular la situación de la Argentina, a partir de las fuentes de información público. El argumento que atribuye la materia eléctrica en su lista de asistencia pública fundamental y la distinción en el distingo de las citadas Bases Acusadas soportan a diseñar la representación del contenido. El progreso procede a los 2 argumentos primordiales del actual documento, simbolizados por los cargos y la realización de los sistemas industriales para Supervisión del Control y la Adquisición de Datos -conocidos como SCI/SCADA- y los registradores de agotamiento eléctrico inteligentes -o Smart Meters- en el espacio de la Red Eléctrica Inteligente -o Smart Grid-; eternamente desde de la vida de la Ciberseguridad Industrial. Se presenta de actuar un vistazo amplio, en donde se hace forzoso un ataque integral, multifactorial y multidisciplinario. Sin embargo, la salvaguarda del procesamiento de datos y de la información salen evidentes y escondidas en esta investigación, no es propósito adelantar con mejoras habituales agrupados a la dirección de la seguridad a partir el lugar del juicio funcionario o el característico de la gobernanza relacionada con los métodos informáticos, o a la pura colocación de moderadas inventivas para amparo. Se concluye proporcionar una visión extensa, en donde se hace forzoso un ataque holístico, multifactorial y multidisciplinario.

En tal sentido, según Xiaoyan (2020), la presente investigación tiene como finalidad esbozar un método de dirección de defensa de la data en una compañía de Recursos Humanos, para optimizar la protección de los bienes informáticos de la compañía. Examinando la circunstancia presente de la gestión de protección de la data de la empresa y las dificultades a perfeccionar, se alcanza ultimar que el método de la dirección presente es inconveniente, por la concientización de protección es endeble, el dispositivo de inspección es imperfecto, se desconocen los peligros de protección, etc. Con cimiento en el acatamiento del todo sistema de control determinado por el estudio de aperturas de GAP, y el estudio y valoración de peligros por el procedimiento MAGERIT, oponen la dirección de los

procedimientos para elaborar y optimizar el “Sistema de Gestión de Seguridad de la Información de COC M.T.”, con el término de rebajar los peligros y debilidades que obtienen perturbar las transacciones mercantiles para acreditar de modo efectivo la protección de la data. Esta investigación se cimienta en la norma ISO 27001: 2013 y la maneja como una concepción consejera para sostener a enunciar un método de gestión de protección de la data que sea conveniente para la compañía, de manera que la compañía logre ser más protegida, más ágil y suministre informes para que otras compañías progresen en años venideros

Por otro lado, según Moreno (2020), en el hoy, alguna de las causas que genera problemas en las compañías es la deficientemente administración de la protección de la data; tras los desarrollos tecnológicos, solucionar estos inconvenientes demanda mucho más que terminales y software, posibilitando que sea forzoso la puesta en marcha de modelos que admitan operar la salvaguarda de la infraestructura de la data de forma más eficaz y eficiente. El SGSI admite encauzar a las sociedades en la exploración de circunstancias y áreas de seguridad solicitados hacia un conveniente progreso de métodos y operaciones que colaboran, para asentar su competencia respecto a los sujetos de inspección y sus consumidores, a través de la determinación de posibles peligros, amenazas y debilidades, que al concretarse puedan sobresaltar los activos arrastrando importes monetarios y castigos lícitos. La decisión de bosquejar un sistema de gestión de protección de la data cimentado en la “norma internacional ISO-IEC 270001:2013”, el cual admitirá reconocer los probables peligros agrupados a la protección de la data, en la compañía “Sociedad HOTELERA San PABLO”, los cuales están expuestos en la investigación permanente de renovar y optimizar sus estrategias de asistencia y protección informática para colocarse en la mejor posición del mercado hotelero de la metrópoli.

De igual manera Garbarino (2014), el propósito de esta investigación es el de elaborar un modelo que admita a las Pymes juntar un modelo práctico para dirigir y gerenciar TI convenientemente consiguiendo la valía anhelada de las inversiones ejecutadas. Para lograr el propósito general se ha elaborado una investigación de campo que apruebe saber el entorno de la “gobernanza y la gestión de TI en PyMEs del Uruguay”; debido a la investigación se pudo examinar cuáles son los elementos

más primordiales que no consienten la adecuada utilización de buenas prácticas de gobernanza de TI en estas compañías. Últimamente se aprobaron las consecuencias en un ambiente industrial precisando una investigación de tema. Las consecuencias logradas con un adelanto del 46% en la suma de indicadores determinados conllevan a razonar que el procedimiento del modelo fue triunfador. Para el caso de la investigación es caso único, los efectos no deberían ser comunes y dada la ocasión de labor ulterior es repetir la propia investigación en otras compañías.

De igual forma Marcos (2018) la implicación del trabajo es de ayudar, mejorando un método práctico de valorización de los sistemas de sufragio electrónico remoto, para después aplicarlo a los modelos más selectos. Ulteriormente, se dispone a contestar a los dos primordiales asuntos que facilitan al presente razonamiento: ¿Existe en la coyuntura cierto sistema/tecnología de sufragio electrónico remoto dispuesto hacer implantado en procesos electorales? y de valorarse de esa manera, "¿Bajo qué condiciones y hasta qué punto en términos de nivel de uso, tecnología y tipología de elecciones sería adecuadamente segura su introducción?". Para eso, se intenta favorecer a establecer un cimiento general en modo de procedimiento de examen sobre que cada nación pueda reunir su personalidad particular para examinar las propuestas que se están indicando. El propósito es una preparación del Voto electrónico remoto de un modo progresivo, fundada en razonamientos técnicos y sobre todo seguro.

Ramón Moya (2017), está investigación plantea un procedimiento basado en el juicio experto en elaborar un modelo ingenioso apto para descubrir conductas extrañas y catalogar, en cada caso. Un perito consigue percibir si está en riesgo existente para un activo de TIC a partir de la averiguación comprendida en los registros de log del firewall que vigila su circulación de ingreso/salida. El juicio experto se logra crear, y con el favor de la minería de datos y de procedimientos de adiestramiento automático se logra cimentar un instrumento idóneo de reconocer el tráfico malintencionado. Para escoger el procedimiento de adiestramiento automático más idóneo, la data del tráfico verdadero se ha concluido con datos sintéticos, con la finalidad de representar las variadas actividades infrecuentes en el tráfico real del sistema.

La variable independiente sobre ciberseguridad es

En resumidas cuentas, la correcta implementación de Ciberseguridad la cual debe coordinar de modo equilibrado elementos de seguridad, de privacidad y de usabilidad. La ciberseguridad es una disciplina de nuevo cuño y que todavía está por precisar de manera exacta. (Arroyo & Hernandez,2020)

Asimismo, la estructura tecnológica (servidores, equipos de red, computadores, en unión con sus equipos de dirección), es uno de los cimientos de alguna entidad a categoría internacional; la defensa que se emplea a esta, es un agente importante que conserva el oficio activo, la reputación y la integridad de las instituciones (Chinchilla&Allende,2017).

En su determinación indica que la defensa de las estructuras tecnológicas que afianzan a los productos elementales se ha transformado en una primacía para los variados países y organizaciones, se discurre la sujeción que se tiene de los mismos y que aumente aceleradamente periodo a periodo (Gómez & Parra ,2017). De la misma condición, menciona que la seguridad del internet custodia la protección de la disponibilidad e integridad de las redes e infraestructuras tecnológicas, y por la protección de la confidencialidad de la data sostenida en ésta. (Roy, 2017)

En todo este tiempo se han utilizado algunas tecnologías, progreso de aparatos y elaboración de mecanismos para impedir que acontecimientos peligrosos sucedan, mucho se alude que ninguna red es inviolable en su integridad, jamás consigue acaecer salida de data e aunque también se posee los aparatos más avanzados; en resultado los agresores usan cualquier procedimiento que este a su obtención para realizar la acometida, el rol que desempeña todo el equipo de una institución es fundamental, y por eso se reitera su adiestramiento sostenido en el espacio de protección informática. (Gómez & Parra, 2017)

Con respecto a la dimensión de la variable dependiente de la prevención de los ataques cibernéticos, según (Inoguchi,2017) se despliegan los elementos teóricos de los ataques cibernéticos:

Ataques Cibernéticos de Países; los inconvenientes del orbe en que existimos se amplían en el internet. Pocos tiempos detrás se comienza reconociendo peligros de los internet importantes como, por modelo, el ciberataque a la nación de Estonia en 2007 que causó la prohibición fugaz de infraestructuras bélicas importantes, otro suceso es el ciber amenaza al País de Rusia al País Georgia en 2008 el cual acarreó como consecuencia la incursión por medio vial, otro caso es el ciberataque al País de EEUU, el cual se expresó que el fundamento del ataque se hallaba en el área del País de China.

En los postrimeros tiempos se ha descubierto que varias naciones destinan bastante dinero, infraestructura e individuos para conseguir grandes gestiones de transformación de advertencias cibernéticas muy evolucionadas que alcanzan ejecutar ofensivas de forma violenta y que alcanzan elegir objetivos de infraestructura tecnológica muy concretos consiguiendo estar incrustado en redes cibernéticas exclusivas del perjudicado sin ser atrapados. (Arévalo, Bayona&Rico ,2015) comentan “Las organizaciones deben generar un plan de acción frente a las amenazas. Se hace de manera formal en la norma ISO 27001, donde se recogen los estándares y mejores prácticas de seguridad de la información” . Para (Cram D’Arcyy Proudfoot,2019) “una táctica que las empresas usan para proteger sus sistemas y datos es la creación, implementación y aplicación de políticas de seguridad de la información”

Quedamos alertados que coexisten varios ataques cibernéticos realizados a otras naciones, sino estos mismo son secretas para no ser difundidos ya que con ello las naciones atacadas estarían endebles en protección de la data usufructo de otras probables ofensivas de naciones en disputa o combates.

El estudio de la presenta tesis determina el uso de la implementación de la ciberseguridad donde las compañías actuales han empezado a escanear sus procedimientos y usar modernas tecnologías de internet suscitado por la pandemia, para ello los variados beneficios como así también incalculables obstáculos, ya que las entidades aseguran su data en el ciberespacio resultando su activo más primordial.

La implementación de la ciberseguridad se da en los siguientes marcos de ciberseguridad:

La Norma ISO 27032:2012, admite tomar medidas de forma correctiva y preventiva la disputa contra los ciberdelitos; asimismo trata los peligros ocultos del ciberespacio, las redes y la seguridad de las tecnologías de los datos y de la comunicación. “El complemento a la Norma ISO/IEC 27032:2012” en la reducción de los peligros se requiere la metodología “Análisis Modal de Fallos y Efectos (AMFE)” que se emplea en modelar nuevos bienes, servicios o técnicas. Su objetivo es examinar los probables errores venideros (“modos de fallo”) del logro para clasificarlos según su jerarquía (Jimeno, 2013).

Esta metodología admite examinar los peligros que se resguardan en las sucesivas etapas: “Identificación, Análisis del impacto y de la probabilidad de ocurrir, plan de contingencia o acciones correctivas y Monitorización”. En que se identifica, evalúa y monitoriza o realiza un seguimiento para lograr a cabo el manejo de un modelo de análisis de riesgos, de la cual se forman un “numero de prioridad del riego (NPR)”, teniendo en cuantos estándares como gravedad/seguridad; importantica, probabilidad e impacto, por causa que los materiales en formato Excel saca alto beneficio de la data y admite depurar los peligros por jerarquía y de preferencia en todo momento (García, 2018).

El marco de trabajo para la ciberseguridad NIST CSF desde la perspectiva de cobit 5 está integrado en tres divisiones primordiales del NIST: “El marco básico (Framework Core), los niveles de implementación del marco (Framework Implementation Tiers) y los perfiles del marco (Framework Profiles)”.

El marco básico “(Framework Core)”es un grupo de acciones de ciberseguridad, consecuencias deseables y informes ajustables que son habituales a las divisiones de activos críticos, en términos de estándares de la compañía, directrices y experiencias que admiten la conexión de labores de ciberseguridad y sus efectos a lo largo de la entidad, desde el valor ejecutivo hasta el valor de implementación/ejecución.

Se, utiliza cinco funciones primordiales:

Identificar: Aprueba determinar los sistemas, activos, datos y capacidades de la entidad, su entorno de comercio, los activos que resisten las operaciones importantes y los peligros de ciberseguridad que influyen la situación.

Proteger: Accede a desarrollar e implementar las contra disposiciones y defensas importantes para restringir o reprimir el embate de un suceso primordial de ciberseguridad.

Detectar: Accede a desarrollar e implementar las labores convenientes para reconocer el acontecimiento de un suceso de ciberseguridad a través de la monitorización continua.

Responder: Plantea la situación y despliegue de labores para responder ante un suceso de ciberseguridad reconocido y aminorar su impacto.

Recuperar: Soporta el desdoblamiento de labores para la gestión de fortaleza y la reposición a la actividad habitual inmediatamente de un suceso. (ISO ,2018)

III. METODOLOGÍA

3.1 TIPO Y DISEÑO DE INVESTIGACIÓN

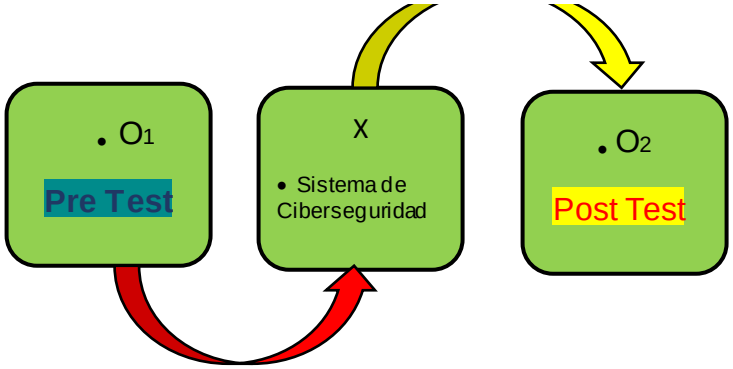
Tipo de investigación: Aplicada.

Diseño de investigación: Experimental del tipo pre – experimental.

Figura 1

Diseño de la Investigación

G=



- **G:** Grupo experimental
- **O_1:** Gestionar la prevención de los ataques cibernéticos antes de la implementación del sistema de ciberseguridad.
- **X:** Sistema de Ciberseguridad
- **O_2:** Gestionar la prevención de los ataques cibernéticos después de la implementación del sistema de ciberseguridad**.**

Tipo de investigación

Esta investigación será aplicada tecnológica ya que muestra múltiples características que vinculan de manera natural con la innovación tecnológica, ya que muestra que se puede utilizar como un instrumento para impulsar el tema de la innovación. (Sampieri, 2019)

Diseño de Investigación

Diseño Experimental del Tipo Pre Experimento, El procedimiento de preprueba – posprueba con una sola agrupación: A esa agrupación se utilizará una evaluación preliminar al método experimental; consecutivamente se tramitará un ensayo y cuyo propósito se efectúa una evaluación posteriormente del ensayo. Ese plan ofrece una oposición supuesta al precedente, donde el apoyo como origen es aprobar qué la categoría estaba en la agrupación de las variables dependientes precedentes del ensayo, por ello, logramos expresar que se posee un estudio del conjunto. (Salas, 2013)

3.2 VARIABLES Y OPERACIONALIZACIÓN

Instaurar la originalidad en el estudio es primordial; colabora a simbolizar lo que es viable y lo que es complicado, si no improbable, de modificar. En este estudio, aplicamos variables de origen como "independientes", así como las variables de resultado como "dependientes". (Losh, 2017)

Variable Independiente

Sistema de Ciberseguridad

La ciberseguridad se caracteriza, sino es una consecuencia de una fusión fortuita de las acciones en el ciberespacio y los representantes en las políticas y leyes concretas. Los mismos representantes añaden también que la variedad de la ciberseguridad, aparece en el aumento de los aparatos que utilizamos y los individuos que utilizamos los aparatos tecnológicos. Se conseguir adjudicarse que el punto más delicado de la ciberseguridad es el sujeto humano. (Friedman, 2015)

Variable Dependiente

Prevención de ataques cibernéticos

La monumental sujeción de la sociedad en relación a los sistemas informáticos y electrónicos están logrando que ésta sea más frágil a las eventuales ofensivas del

ciberespacio. Asimismo, Ciberespacio es un instrumento de simple camino, donde algún humano, consigue ejecutar un ataque que es complejo de relacionar, con la cual, el internet se está transformando en ese recinto excelente para que los malhechores y los terroristas trasladen su fin en operaciones y acciones. De ahí, que el ciberdelito, tenga que ser la más primordial amenaza que sienten seguir a la comunidad. Por tal conocimiento, transcurrido este estudio se revelan estadísticas de cada uno de los componentes que ayudan a impedir las posibles ofensivas del internet y las acciones delictivas en el internet. Además, las prevenciones que se han elaborado para impedir que acrecienten los crímenes informáticos. (López, 2018).

3.3 POBLACIÓN, MUESTRA Y MUESTREO

Población

La población es de 50 usuarios de la empresa Radiadores Fortaleza que tiene la disponibilidad de un equipo informático.

La población de investigación es un grupo de temas, determinado, restringido y accesible, que establecerá el referido para el nombramiento del modelo que efectúa con una sucesión de juicios establecidos. Los propósitos de este apartado están encaminados a detallar cada uno de los principios que se solicita obtener en cuenta para la elección de los colaboradores de este estudio, en el instante en que se está confeccionando una formalidad, en que se contienen las nociones de población de investigación, muestra, criterios de selección y técnicas de muestreo. Siguiente a puntualizar la población de investigación, el investigador debe detallar los juicios ha obedecer por los colaboradores. (Arias, 2016)

Muestra:

Para la muestra representativa de la empresa Radiadores Fortaleza se realiza 48 usuarios, pero por la cantidad se utiliza la población total de 50 usuarios. Ver anexo 3

La muestra es el grupo de individuos que podrían clasificarse de la población cuyo procedimiento de muestreo usado en la publicación. Debido que la muestra podría simbolizar solo una porción de la población objetiva, el estudioso tiene que inspeccionar escrupulosamente si lo clasificado se ajusta a los propósitos o

suposición del estudio, y fundamentalmente si concurren metodologías para rebasar los obstáculos. (Martínez, 2016)

Muestreo

La técnica de muestreo, es la muestra designada está más viable a nosotros hacia lograr efectuar dicha investigación

El muestreo se consigue precisar como el procedimiento por medio del cual se escogen sujetos o unidades de muestreo del cuadro de la muestra. La táctica de muestreo podría definirse previamente, puesto que el procedimiento de muestreo consigue sobresaltar a la estimación de la dimensión de la muestra. (Martínez, 2016)

3.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

La información se juntó utilizando el procedimiento nombrada encuesta, la cual tiene como instrumento el cuestionario que constituyen una variable a cuantificar.

“Para las encuestas son ideales para documentar percepciones, actitudes, creencias o conocimientos dentro de una muestra clara y predeterminada de individuos”. (Paradis, 2016),

Las encuestas ayudan a los integrantes disposiciones claras como sea verosímil a partir la iniciación, para efectuar la encuesta en situación sencilla y también sea verosímil el que conteste. (Elyazgi ,2018)

Validación y confiabilidad de los instrumentos.

Validación de los instrumentos.

La validación el instrumento, en cláusulas generales, se describe el valor en que una herramienta verdaderamente calcula la variable que intenta calcular (Hernández, et. al, 2014)

El juicio de expertos se define en cuestionar a las personas peritas también conocidas como jueces acerca de las variables de ciberseguridad, y prevencion de ataques ciberneticos de cada uno de los ítems, en el caso del instrumento.

Confiabilidad de los instrumentos

De concordancia con Parreño (2016), la confiabilidad "se refiere al grado en que su aplicación repetida al mismo sujeto u objeto produce iguales resultados". Las herramientas de recopilación de datos que mostraron ítems fueron analizados a través del coeficiente alfa de Cronbach con el fin de contar con su firmeza linterna, evaluando la correlación media de cada ítem con todas las personas que componen dicha herramienta. Se empleó el ensayo piloto y posteriormente se evaluó mediante el Alfa de Cronbach con el auxilio del software estadístico SPSS.

Por la variable de prevencion de ataques ciberneticos el alfa de Cronbach es de 0.707 es confiable para realizar las pruebas. Ver anexo 4

3.5 PROCEDIMIENTOS

Para el comienzo de la investigación se empleó en la variable dependiente del sistema de ciberseguridad el estado de la infraestructura tecnológica de la empresa radiadores Fortaleza, verificando la operatividad de sus redes, servidores, conexiones y sistemas de protección ante cualquier amenaza informática, por ello se hace un análisis de la situación de la empresa ante la eventualidad cibernética.

Además, se realiza una entrevista a los usuarios sobre los conocimientos informáticos ante una amenaza informática y que mecanismos conoce para evitar esta vulnerabilidad.

Todo ello se representa en el modelo marco de trabajo para la ciberseguridad NIST CSF desde la perspectiva de cobit 5 Básico en la Implementación de ciberseguridad en una empresa, donde se utiliza el marco básico donde se desarrolla las 2 primeras partes de identificar y proteger los activos de información para la seguridad de la empresa

En concerniente de la variable dependiente se toma los mecanismos de protección que actualmente presenta la empresa ante la situación de una amenaza cibernética, lo cual planteamos que probabilidad de amenaza recurrente se presenta en la empresa y que daño significaría en la valía económica y prestigio de la compañía.

Ante ello el presente trabajo toma en consideración las amenazas frecuentes que existe por la utilización del internet que ha sido masificado por la pandemia y resulta emplear un sistema de ciberseguridad para prevenir los riesgos cibernéticos y minimizar las vulnerabilidades existentes en la empresa.

3.6 MÉTODOS DE ANÁLISIS DE DATOS

El proceso de la recopilación de información siguió los sucesivos caminos:

Se utilizó el instrumento mediante las encuestas, para medir la variable dependiente de los ataques cibernéticos y contrarrestando la variable independiente en la implementación de un sistema de ciberseguridad para las mediciones de la efectividad del proceso

Para el análisis de la información conseguidos en el estudio, se utilizó la estadística descriptiva le inferencial. Estos productos fueron incorporados empleando figuras estadísticas para lograr representar y alcanzar mejor el estudio. Para comprobar las hipótesis se manejó la estadística inferencial el método de la T de Student para muestras autónomas.

Consecutivamente, con la información conseguidos se confeccionó la matriz de datos, que se convirtió en valores según los niveles determinados y se ejecutó un completo análisis con el software de reporte de datos estadístico SPPS, con la intención de mostrar las conclusiones y recomendaciones

3.7 ASPECTOS ÉTICOS

Según UPEL l2016), define que la peculiaridad más notable de los requerimientos éticos del investigador es el predominio ético a la gratitud de sus trabajos usados para lograr información, así como el merecimiento a cada individuo que haya ayudado en el estudio. El empleo de opiniones de un estudio sin permiso para hacerlo establece una experiencia extraña a la ética e incluso soporta un robo intelectual o plagio científico.

Por ello la información recopilada en este estudio fueron acopiados del grupo de estudio y se elaboraron de manera adecuada sin falsificaciones. Los colaboradores que se han sumado en este sondeo para la investigación, se han tomado las debidas cautelas del caso para impedir dañar la integridad de la empresa en su confidencialidad, integridad y disponibilidad. De acuerdo al marco teórico se recogió del acuerdo a las medidas concretas y oportunos para efectuar este tipo de investigación, impidiendo la similitud de otros estudios.

Posteriormente, las consecuencias del estudio no han existido plagio o falsedad de otros estudios a través de la buena utilización de la investigación en favor de todos los interesados.

IV. RESULTADOS

En el estudio se aplicó un sistema de ciberseguridad para la prevencion de los ataques ciberneticos en la empresa Radiadores Fortaleza donde se evaluó las fortalezas y vulnerabilidades ante un riesgo de ataque cibernético, dando como resultado la disminución de estos ataques ciberneticos con el sistema de ciberseguridad implantado. De esta metodología se obtiene los resultados de los indicadores Nivel de activos que son adecuados para su propósito, Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa, Histórico de tipo de defensas, Probabilidad de amenaza y magnitud de daño graficados en estadística descriptiva, inferencial y contraste de hipótesis.

4.1 Estadística Inferencial

Hipótesis de normalidad

La prueba de hipótesis de normalidad se efectúa mediante el siguiente enunciado:

H0: Los datos de las dimensiones Pre y Post Test presenta una distribución normal.

Ho: $\mu 2 = \mu 1$

Ha: Los datos de las dimensiones Pre y Post Test no presenta una distribución normal.

Ha: $\mu 2 > \mu 1$

Nivel de significancia de la prueba

Para el análisis de la prueba se establece un nivel de confianza del 95% y un nivel de significancia $\alpha = 5\% = 0.05$.

Selección del estadístico de prueba

• Si la muestra es menor de 50 elementos se hace luso de la prueba Shapiro Wilks.

• Si la muestra es mayor lo igual de 50 elementos se hace luso de la prueba Kolmogorov-Smirnov.

Regla de decisión

La decisión de la prueba se establece si:

p valor < α = 0.05; rechazar la hipótesis nula.

p valor ≥ α = 0.05; aceptar la hipótesis nula.

4.2.1 Pruebas de Normalidad de dimensiones

Prueba de Normalidad del indicador nivel de activos que son adecuados para su propósito antes pretest y después (posttest) después de implementar el sistema de ciberseguridad.

Tabla 1

Prueba de Normalidad del indicador nivel de activos adecuados para su propósito en pretest y posttest

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pretest	,094	50	,200*	,970	50	,236
Posttest	,104	50	,200	,979	50	,504

Interpretación: En la tabla representa un informe de la prueba de normalidad Shapiro-Wilk del indicador nivel de activos que son adecuados para su propósito, donde podemos apreciar un p valor =0,236 en la fase Pres test y un p= valor =0,504 en la fase Post Test , ambos tienen un nivel de significancia (p>0.05), por lo que se infiere con un nivel de significancia de 5% que los datos Pre y Post test del indicador nivel de activos que son adecuados para su propósito se representa una distribución normal, por tanto, la contrastación de las hipótesis se realiza mediante la prueba estadística paramétrica de T de Student.

Prueba de Normalidad del indicador nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa antes pretest y después (posttest) después de implementar el sistema de ciberseguridad.

Tabla 2

Prueba de Normalidad del nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pretest	,116	50	,092	,972	50	,281
Posttest	,104	50	,200*	,969	50	,202

Interpretación: En la tabla representa un informe de la prueba de normalidad Shapiro-Wilk del indicador nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa , donde podemos apreciar un p valor =0,281 en la fase Pres test y un p= valor =0,202 en la fase Post Test , ambos tienen un nivel de significancia (p>0.05), por lo que se infiere con un nivel de significancia de 5% que los datos Pre y Post test del nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa se representa una distribución normal, por tanto, la contrastación de las hipótesis se realiza mediante la prueba estadística paramétrica de T de Student.

Prueba de Normalidad del indicador nivel histórico de defensas antes pretest y después (posttest) después de implementar el sistema de ciberseguridad.

Tabla 3

Prueba de Normalidad del nivel histórico de defensas del pretest y posttest

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pretest	,127	50	,042	,959	50	,083
Posttest	,107	50	,0200	,977	50	,433

Interpretación: En la tabla representa un informe de la prueba de normalidad Shapiro-Wilk del indicador nivel histórico de defensas, donde podemos apreciar un p valor =0,083 en la fase Pres test y un p= valor =0,433 en la fase Post Test , ambos tienen un nivel de significancia (p>0.05), por lo que se infiere con un nivel de significancia de 5% que los datos Pre y Post test del nivel histórico de defensas de toda la empresa se representa una distribución normal, por tanto, la contrastación de las hipótesis se realiza mediante la prueba estadística paramétrica de T de Student.

Prueba de Normalidad del indicador nivel de protección ante la amenaza y magnitud de daño antes pretest y después (posttest) después de implementar el sistema de ciberseguridad.

Tabla 4

Prueba de Normalidad del nivel de protección ante la amenaza y magnitud de daños antes pretest y posttest

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pretest	,120	50	,069	,963	50	,114
Posttest	,127	50	,044	,972	50	,284

Interpretación: En la tabla representa un informe de la prueba de normalidad Shapiro-Wilk del indicador nivel de protección ante la amenaza y magnitud de daño, donde podemos apreciar un p valor =0,114 en la fase Pres test y un p= valor =0,284 en la fase Post Test , ambos tienen un nivel de significancia (p>0.05), por lo que se infiere con un nivel de significancia de 5% que los datos Pre y Post test del nivel de protección ante la amenaza y magnitud de daño se representa una distribución normal, por tanto, la contrastación de las hipótesis se realiza mediante la prueba estadística paramétrica de T de Student

4.2 Estadística Descriptiva

Indicador1: Resultados descriptivos del nivel de activos que son adecuados para su propósito antes pretest y después (posttest) después de implementar el sistema de ciberseguridad.

Tabla 5

Resultados descriptivos del nivel de activos que son adecuados para su propósito pretest y posttest

Estadísticos descriptivos					
	N	**Mínimo**	**Máximo**	**Media**	**Desv. Desviación**
Pretest	50	14,00	23,00	18,0400	2,12814
Posttest	50	22,00	36,00	29,5000	3,09212

Tabla 6

Pretest Agrupada

Pretest (Agrupada)				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Media Prevalencia	50	100,0	100,0	100,0

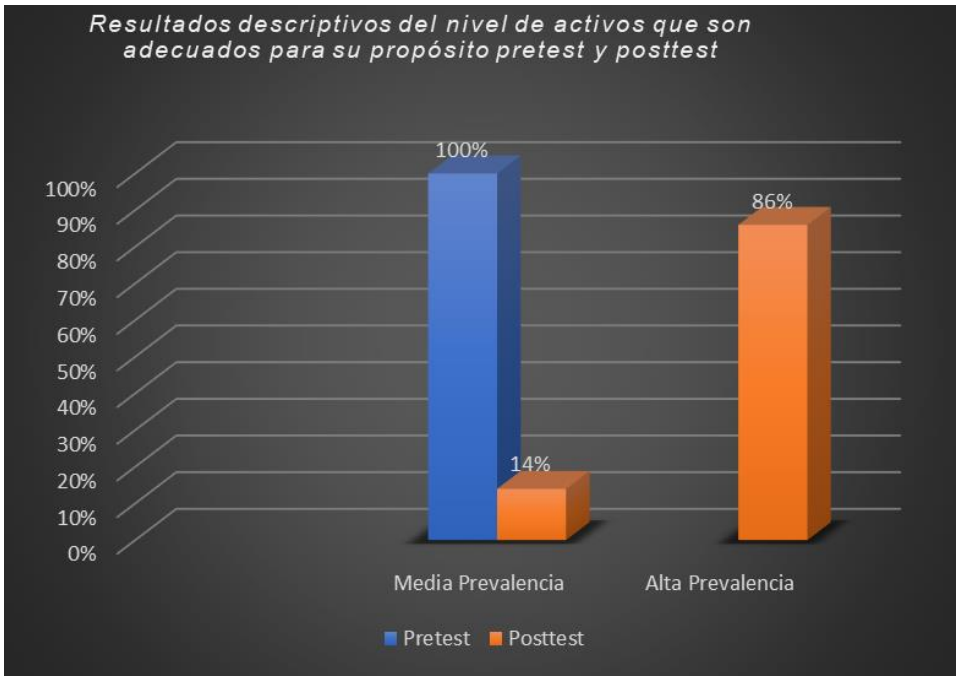
Tabla 7

Posttest Agrupada

Posttest (Agrupada)				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Media Prevalencia	7	14,0	14,0	14,0
Alta Prevalencia	43	86,0	86,0	100,0
Total	50	100,0	100,0	

Figura 2

Resultados descriptivos del nivel de activos que son adecuados para su propósito pretest y posttest



Interpretación : En la tabla se demuestra que el nivel de activos que son adecuados para su propósito antes de aplicar el sistema de ciberseguridad , reporta un Pre test un promedio de 18,0400 puntos con la desviación +/- de 2,1284 con un valor máximo alcanzado de 23 , al relacionar con el nivel de activo que son adecuados para su propósito después de aplicar el sistema de ciberseguridad se observa un aumento de los activos dado que en el Post test indica un promedio de activos de 29,5000 puntos con una variación +/- de 3,09212 siendo un valor máximo de 36.Este aumento del nivel de activos se observa al segmentar los valores en baja prevalencia de 0-13 , media prevalencia de 14-26 , alta prevalencia de 27-40 , donde en el diagrama se presenta en el pretest un 100% de media prevalencia y después del Post test se presenta un 14% de media prevalencia y 86% de alta prevalencia donde se refleja un influencia positiva en la aplicación del sistema de ciberseguridad para mejorar la disminución de los ataques ciberneticos.

Indicador 2: Resultados descriptivos del nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa antes (pretest) y después de (posttest) después de implementar un sistema de ciberseguridad

Tabla 8

Resultados Descriptivos del nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa en pretest y posttest

Estadísticos descriptivos					
	N	**Mínimo**	**Máximo**	**Media**	**Desv. Desviación**
Pretest	50	13,00	24,00	17,7800	2,46850
Postetst	50	24,00	36,00	29,9000	2,47642

Tabla 9

Pretest Agrupada

Pretest (Agrupada)				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Baja Prevalencia	3	6,0	6,0	6,0
Media Prevalencia	47	94,0	94,0	100,0
Total	50	100,0	100,0	

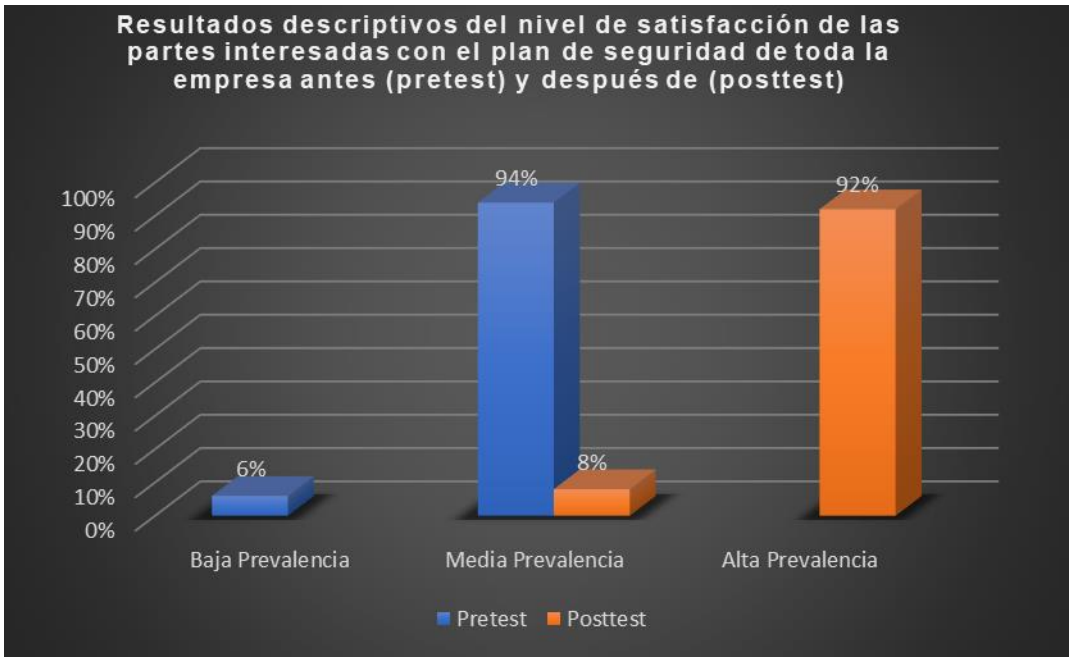
Tabla 10

Posttest Agrupada

Posttest (Agrupada)				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Media Prevalencia	4	8,0	8,0	8,0
Alta Prevalencia	46	92,0	92,0	100,0
Total	50	100,0	100,0	

Figura 3

Resultados descriptivos del nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa antes (pretest) y después de (posttest)



Interpretación : en la tabla se demuestra que el nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa antes de aplicar el sistema de ciberseguridad , reporta un Pre test un promedio de 17,7800 puntos con la desviación +/- de 2,46850 con un valor máximo alcanzado de 24 , al relacionar con el nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa después de aplicar el sistema de ciberseguridad se observa un aumento del nivel de satisfacción dado que en el Post test indica un promedio de activos de 29,9000 puntos con una variación +/- de 2,47642 siendo un valor máximo de 36.Este aumento del nivel de satisfacción se observa al segmentar los valores en baja prevalencia de 0-13 , media prevalencia de 14-26 , alta prevalencia de 27-40 , donde en el diagrama se presenta en el pretest un 6% de baja prevalencia y 94%de media prevalencia y después del Post test se presenta un 8% de media prevalencia y 92% de alta prevalencia donde se refleja un influencia positiva en la aplicación del sistema de ciberseguridad para mejorar la disminución de los ataques ciberneticos.

Indicador 3: Resultados descriptivos del nivel histórico de tipo de defensas antes (pretest) y después de (posttest) después de implementar un sistema de ciberseguridad

Tabla 11

Resultado descriptivos del nivel histórico de defensas pretest y posttest

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
Pretest	50	12,00	23,00	18,0400	2,32080
Posttest	50	24,00	35,00	29,5800	2,61151

Tabla 12

Pretest Agrupada

Pretest (Agrupada)				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Baja Prevalencia	3	6,0	6,0	6,0
Media Prevalencia	47	94,0	94,0	100,0
Total	50	100,0	100,0	

Tabla 13

Posttest Agrupada

Posttest (Agrupada)				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Media Prevalencia	6	12,0	12,0	12,0
Alta Prevalencia	44	88,0	88,0	100,0
Total	50	100,0	100,0	

Figura 4

Resultado descriptivo del nivel histórico de defensas pretest y posttest

Interpretación : en la tabla se demuestra que el nivel histórico de tipo de defensas antes de aplicar el sistema de ciberseguridad , reporta un Pre test un promedio de 18,0400 puntos con la desviación +/- de 2,32080 con un valor máximo alcanzado de 23 , al relacionar con el nivel histórico de defensas de las partes interesadas con el plan de seguridad de toda la empresa después de aplicar el sistema de ciberseguridad se observa un aumento del nivel de satisfacción dado que en el Post test indica un promedio de activos de 29,5800 puntos con una variación +/- de 2,32080 siendo un valor máximo de 34.Este aumento del nivel histórico de defensas se observa al segmentar los valores en baja prevalencia de 0-13 , media prevalencia de 14-26 , alta prevalencia de 27-40 , donde en el diagrama se presenta en el pretest un 6% de baja prevalencia y 94%de media prevalencia y después del Post test se presenta un 12% de media prevalencia y 88% de alta prevalencia donde se refleja un influencia positiva en la aplicación del sistema de ciberseguridad para mejorar la disminución de los ataques ciberneticos.

Indicador 4: Resultados descriptivos del Nivel de protección ante la amenaza y magnitud de daño antes (pretest) y después de (posttest) después de implementar un sistema de ciberseguridad

Tabla 14

Resultados descriptivos de nivel de protección ante la amenaza y magnitud de daño pretest y posttest

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
Pretest	50	14,00	22,00	18,0000	2,06032
Posttest	50	25,00	37,00	30,6000	2,74048

Tabla 15

Pretest Agrupada

Pretest (Agrupada)				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Media Prevalencia	50	100,0	100,0	100,0

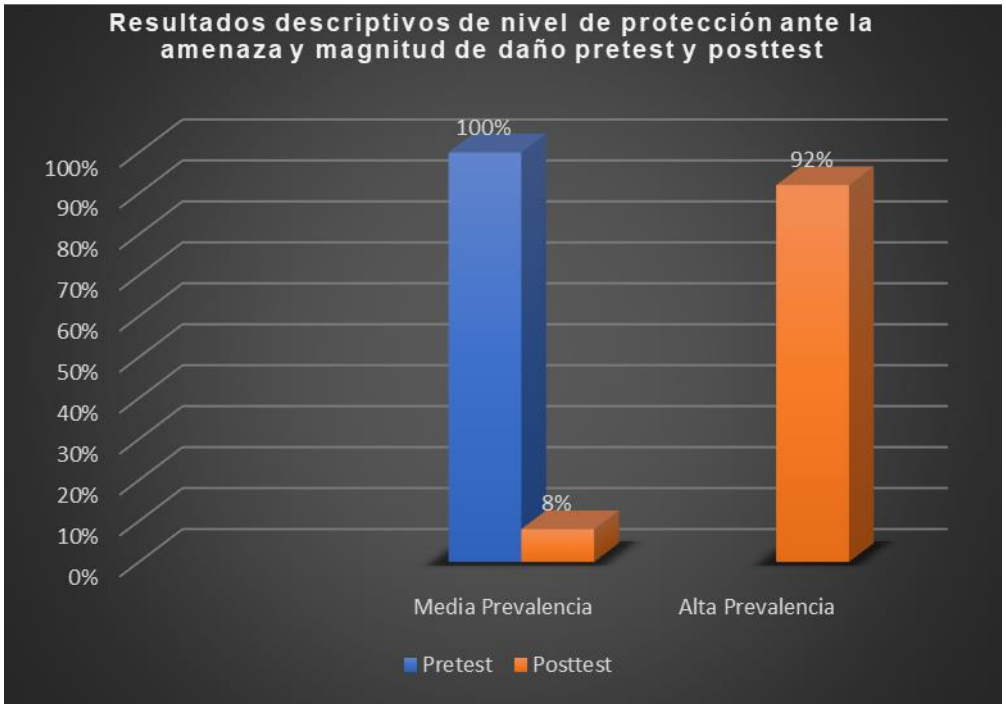
Tabla 16

Posttest Agrupada

Posttest (Agrupada)				
	Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Media Prevalencia	4	8,0	8,0	8,0
Alta Prevalencia	46	92,0	92,0	100,0
Total	50	100,0	100,0	

Figura 5

Resultados descriptivos de nivel de protección ante la amenaza y magnitud de daño pretest y posttest



Interpretación : en la tabla se demuestra que el nivel de protección ante la amenaza y magnitud de daño antes de aplicar el sistema de ciberseguridad , reporta un Pre test un promedio de 18,0000 puntos con la desviación +/- de 2,06032 con un valor máximo alcanzado de 22 , al relacionar con el nivel de protección ante la amenaza y magnitud de daño con el plan de seguridad de toda la empresa después de aplicar el sistema de ciberseguridad se observa un aumento del nivel de satisfacción dado que en el Post test indica un promedio de activos de 30,6000 puntos con una variación +/- de 2,74048 siendo un valor máximo de 37.Este aumento del nivel de protección ante la amenaza y magnitud de daño observa al segmentar los valores en baja prevalencia de 0-13 , media prevalencia de 14-26 , alta prevalencia de 27-40 , donde en el diagrama se presenta en el pretest un 100 %de media prevalencia y después del Post test se presenta un 8% de media prevalencia y 92% de alta prevalencia donde se refleja un influencia

positiva en la aplicación del sistema de ciberseguridad para mejorar la disminución de los ataques ciberneticos.

4.3 Contraste de Hipótesis

Prueba de hipótesis General

$H_{o=}$ La implementación de un sistema de ciberseguridad no influye de manera positiva en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

$H_{a=}$ La implementación de un sistema de ciberseguridad influye de manera positiva en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

Nivel de significancia de la prueba
Para el análisis de la prueba se establece un nivel de confianza del 95% y un nivel de significancia α= 5% = 0.05.

Regla de decisión

La decisión de la prueba se establece si:

p valor < α = 0.05; rechazar la hipótesis nula.

p valor ≥ α = 0.05; aceptar la hipótesis nula.

Tabla 17

Muestras emparejadas

Estadísticas de muestras emparejadas				
	Media	**N**	**Desv. Desviación**	**Desv. Error promedio**
Pretest	71,8600	50	6,39199	,90396
Posttest	119,5800	50	9,15867	1,29523

Tabla 18

Correlaciones de muestras emparejadas

Correlaciones de muestras emparejadas			
	N	Correlación	Sig.
Pretest & Posttest	50	,609	,000

Tabla 19

Diferencias emparejadas

Prueba de muestras emparejadas								
	Diferencias emparejadas							
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
				Inferior	Superior			
Pretest - Posttest	-47,72000	7,30680	1,03334	-49,79657	-45,64343	-46,180	49	,000

Interpretación: En la tabla, se muestra un valor de la prueba de Student de -46,180 asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación (p<0,05) lo que con lleva al rechazo de la hipótesis nula (H_o) y la aceptación de la hipótesis general planteada en la investigación (H_a) concluyendo que : La implementación de un sistema de ciberseguridad influye de manera positiva en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

Prueba de hipótesis específica 1

La prueba de la primera hipótesis especifica mediante el siguiente enunciado:

$H_{o=}$ La implementación de un sistema de ciberseguridad no influye de manera positiva en el aumento del nivel de activos que son adecuados para su propósito en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

Ho: $\mu_2 = \mu_1$

$H_{1=}$ La implementación de un sistema de ciberseguridad influye de manera positiva en el aumento del nivel de activos que son adecuados para su propósito en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

H1: $\mu_2 > \mu_1$

Regla de decisión

La decisión de la prueba se establece si:

p valor < α = 0.05; rechazar la hipótesis nula.

p valor ≥ α = 0.05; aceptar la hipótesis nula.

Tabla 20

Muestras emparejadas

Estadísticas de muestras emparejadas

	Media	N	Desv. Desviación	Desv. Error promedio
Pretest	18,0400	50	2,12814	,30096
Posttest	29,5000	50	3,09212	,43729

Tabla 21

Correlaciones de muestras emparejadas

Correlaciones de muestras emparejadas			
	N	Correlación	Sig.
Pretest & Posttest	50	,270	,058

Tabla 22

Diferencias emparejadas

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			
Pretest - Postest	-11,46000	3,24641	,45911	-12,38262	-10,53738	-24,961	49	,000

Interpretación: En la tabla, se muestra un valor de la prueba de Student de -24,961, asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación (p<0,05) lo que con lleva al rechazo de la hipótesis nula (H_0) y la aceptación de la hipótesis general planteada en la investigación (H_1) concluyendo que : La implementación de un sistema de ciberseguridad influye de manera positiva en el aumento del nivel de activos que son adecuados para su propósito en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021

Prueba de hipótesis específica2

La prueba de la segunda hipótesis especifica mediante el siguiente enunciado:

$H_{0=}$ La implementación de un sistema de ciberseguridad no influye de manera positiva en el aumento del nivel de satisfacción de las partes interesadas con el plan de seguridad de la empresa en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

Ho: $\mu_2 = \mu_1$

$H_{2=}$ La implementación de un sistema de ciberseguridad influye de manera positiva en el aumento del nivel de satisfacción de las partes interesadas con el plan de seguridad de la empresa en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

H_2: $\mu_2 > \mu_1$

Regla de decisión

La decisión de la prueba se establece si:

p valor < α = 0.05; rechazar la hipótesis nula.

p valor ≥ α = 0.05; aceptar la hipótesis nula.

Tabla 23

Muestras emparejadas

Estadísticas de muestras emparejadas

		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	**Pretest**	17,7800	50	2,46850	,34910
	Posttest	29,9000	50	2,47642	,35022

Tabla 24

Correlaciones de muestras emparejadas

Correlaciones de muestras emparejadas			
	N	Correlación	Sig.
Pretest & Posttest	50	,504	,000

Tabla 25

Muestras emparejadas

Prueba de muestras emparejadas								
	Diferencias emparejadas							
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
				Inferior	Superior			
Pretest - Postetst	-12,12000	2,46312	,34834	-12,82001	-11,41999	-34,794	49	,000

Interpretación: En la tabla, se muestra un valor de la prueba de Student de -34, 794 asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación ($p<0,05$) lo que con lleva al rechazo de la hipótesis nula (H_0) y la aceptación de la hipótesis general planteada en la investigación (H_2) concluyendo que : La implementación de un sistema de ciberseguridad influye de manera positiva en el aumento del nivel de satisfacción de las partes interesadas con el plan de seguridad de la empresa en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021

Prueba de hipótesis específica 3

La prueba de la tercera hipótesis especifica mediante el siguiente enunciado:

$H_{o=}$ La implementación de un sistema de ciberseguridad no influye de manera positiva en el aumento del nivel histórico de defensas en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

Ho: $\mu_2 = \mu_1$

$H_{3=}$ La implementación de un sistema de ciberseguridad influye de manera positiva en el aumento del nivel histórico de defensas en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

H_3: $\mu_2 > \mu_1$

Regla de decisión

La decisión de la prueba se establece si:

p valor < α = 0.05; rechazar la hipótesis nula.

p valor ≥ α = 0.05; aceptar la hipótesis nula.

Tabla 26

Muestras emparejadas

Estadísticas de muestras emparejadas				
	Media	**N**	**Desv. Desviación**	**Desv. Error promedio**
Prestest	18,0400	50	2,32080	,32821
Posttest	29,5800	50	2,61151	,36932

Tabla 27

Muestras emparejadas

Correlaciones de muestras emparejadas			
	N	Correlación	Sig.
Prestest & Posttest	50	,464	,001

Tabla 28

Diferencias de muestras emparejadas

Prueba de muestras emparejadas								
	Diferencias emparejadas							
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior	t	gl	Sig. (bilateral)
Pretest - Posttest	-11,54000	2,56515	,36277	-12,26901	-10,81099	-31,811	49	,000

Interpretación: En la tabla, se muestra un valor de la prueba de Student de -31, 811 asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación (p<0,05) lo que con lleva al rechazo de la hipótesis nula (H_0) y la aceptación de la hipótesis general planteada en la investigación (H_3) concluyendo que : La implementación de un sistema de ciberseguridad influye de manera positiva en el aumento del nivel histórico de defensas en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

Prueba de hipótesis específica 4

La prueba de la tercera hipótesis especifica mediante el siguiente enunciado:

H_0= La implementación de un sistema de ciberseguridad no influye de manera positiva en el aumento del nivel de protección ante la amenaza y magnitud de daño en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

Ho: $\mu_2 = \mu_1$

H_3= La implementación de un sistema de ciberseguridad influye de manera positiva en el aumento del nivel de protección ante la amenaza y magnitud de daño en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

$H_4: \mu_2 > \mu_1$

Regla de decisión

La decisión de la prueba se establece si:

p valor < α = 0.05; rechazar la hipótesis nula.

p valor ≥ α = 0.05; aceptar la hipótesis nula.

Tabla 29

Muestras Emparejadas

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Pretest	18,0000	50	2,06032	,29137
	Posttest	30,6000	50	2,74048	,38756

Tabla 30

Correlaciones de muestra emparejadas

Correlaciones de muestras emparejadas			
	N	Correlación	Sig.
Pretest & Posttest	50	,510	,000

Tabla 31

Diferencias emparejadas

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			
Pretest - Posttest	-12,60000	2,44949	,34641	-13,29614	-11,90386	-36,373	49	,000

Interpretación: En la tabla, se muestra un valor de la prueba de Student de -36, 373 asociado a las medias de pres test y postest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación ($p<0,05$) lo que con lleva al rechazo de la hipótesis nula (H_0) y la aceptación de la hipótesis general planteada en la investigación (H_4) concluyendo que : La implementación de un sistema de ciberseguridad influye de manera positiva en el aumento del nivel de protección ante la amenaza y magnitud de daño en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.

V. DISCUSIÓN

De acuerdo al resultado general planteado en la investigación, acerca de su influencia en la implementación de un sistema de ciberseguridad para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza durante el periodo del 2021, se constituye en realizar los descubrimientos obtenidos en la investigación en cuanto a las pruebas realizadas antes (pretest) y después (posttest) en cuanto el valor de la prueba de Student de -46,180, asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación ($p<0,05$) lo que con lleva al rechazo de la hipótesis nula (H_o) y la aceptación de la hipótesis general planteada en la investigación (H_a). Debido a esta investigación se logra identificar las amenazas de los ataques ciberneticos y proteger los sistemas informaticos de la empresa para mitigar los riesgos que acontece debido a los delincuentes informaticos. El investigador Rivera (2019), ofrece una investigación con cierta similitud al afirmar la usabilidad del sistema de gestión en riesgos de ciberseguridad y sus consecuencias en la prudencia en la empresa industrial de la jurisdicción de Yanacancha; dado a la coyuntura económica del fraude por servicios de internet en la institución, se logra consolidar ciertos procedimientos para mitigar los riesgos de delitos ciberneticos. Por su parte Taipe (2018);el actual estudio tiene como finalidad ejecutar una auditoria de seguridad Informática que contenga la pauta necesarias para poder identificar las amenazas poder controlar los riesgos y recurrir a un mecanismo de protección para la fuga de los sistemas de información. Vilcarromero & Vílchez (2018), en la investigación en la Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones ,dada la importancia de la seguridad en el ámbito empresarial al resguardar la información se da la implicancia de la salvaguarda de los datos en consecución a su protección en cuanto a su confidencialidad, integridad y disponibilidad para lograr una ventaja competitiva en el desarrollo del negocio.

Dado que el resultado en su indicador el nivel de activos que son adecuados para su propósito antes de aplicar el sistema de ciberseguridad , reporta un Pre test un promedio de 18,0400 puntos con la desviación +/- de 2,1284 con un valor máximo alcanzado de 23 , al relacionar con el nivel de activo que son adecuados para su propósito después de aplicar el sistema de ciberseguridad se observa un aumento de los activos dado que en el Post test indica un promedio de activos de 29,5000 puntos con una variación +/- de 3,09212 siendo un valor máximo de 36.Este aumento del nivel de activos se observa al segmentar los valores en baja prevalencia de 0-13 , media prevalencia de 14-26 , alta prevalencia de 27-40 , donde en el diagrama se presenta en el pretest un 100% de media prevalencia y después del Post test se presenta un 14% de media prevalencia y 86% de alta prevalencia donde se refleja un influencia positiva en la aplicación del sistema de ciberseguridad para mejorar la disminución de los ataques ciberneticos . Según Mendoza (2019), cuya tesis tiene como similitud en determinar la categoría de dimensión en la gestión de la ciberseguridad de la compañía, en reconocer los nivel de los activos informaticos que gestiona la empresa para poder lograr identificar y poder actuar y tener la respuesta de eventos relacionados a la ciberseguridad para controlar los peligros relacionados a los ataques ciberneticos y mitigar las amenazas de los delincuentes ciberneticos. Márquez Alayo(2018) en la similitud en la investigación de cuyo título es Ciberseguridad y su Relación en la Seguridad de los Sistemas Informáticos del Ejercito del Perú Caso: DITELE 2013-2014, en el orden de la criticidad de los niveles de seguridad toma como referencia los activos a proteger en niveles de prioridades para la consecución del orden interno de la seguridad de la información del Ejecito del Perú, canalizando sus soluciones posteriores en los activos en prioridad, dado de un entorno militar su prioridad demanda mas control y seguridad sobre los activos a salvaguardad. El autor Huerta Agurto (2020) confiere cierta similitud en la preparación de la implementación de un sistema de gestión de la información asegura de forma primordial los activos necesarios para su protección y confiere una mitigación de riesgos de los ataques ciberneticos para la continuidad del negocio, llegando a solicitar activos necesarios, que consoliden el resguardo de la información en forma confidencial, integra y disponible para ello con lleva a varios mecanismos de protección que la empresa deberá de emplear para tener una empresa segura y confiable , deseando a los

clientes la seguridad debida de sus datos y el sistema seguro, confiable de la empresa.

Por lo tanto el indicador del nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa antes de aplicar el sistema de ciberseguridad , reporta un Pre test un promedio de 17,7800 puntos con la desviación +/- de 2,46850 con un valor máximo alcanzado de 24 , al relacionar con el nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa después de aplicar el sistema de ciberseguridad se observa un aumento del nivel de satisfacción dado que en el Post test indica un promedio de activos de 29,9000 puntos con una variación +/- de 2,47642 siendo un valor máximo de 36.Este aumento del nivel de satisfacción se observa al segmentar los valores en baja prevalencia de 0-13 , media prevalencia de 14-26 , alta prevalencia de 27-40 , donde en el diagrama se presenta en el pretest un 6% de baja prevalencia y 94%de media prevalencia y después del Post test se presenta un 8% de media prevalencia y 92% de alta prevalencia donde se refleja un influencia positiva en la aplicación del sistema de ciberseguridad para mejorar la disminución de los ataques ciberneticos. Por otro lado, Moreno (2020), en la similitud de la investigación cuyo título es Diseño de un sistema de gestión de seguridad de la información para la empresa Sociedad Hotelera San Pablo basado en la norma ISO/IEC 270001:2013 ha presentado una deficientemente administración en la seguridad de la información; tras los avances tecnológicos para solucionar estos problemas requiere mucho más que dispositivos y software, propiciando que sea forzoso la implementación de diseños que permitan operar la salvaguardia de los activos de la data de forma más eficaz y eficiente. Para ello toma como factor principal la concientización del personal en la prevencion de los ataques informaticos, llegando a dar al ámbito empresarial del negocio la seguridad debida tanto en confidencialidad, integridad y disponibilidad de la información. De igual manera Garbarino (2014), cuyo parecido en la tesis es el de construir un marco de ciberseguridad integral que gobierne y gestionar las tecnologías de la información, donde esta plan es integral y convierte a cada de uno de los trabajadores participes de la seguridad integral de la empresa ante los ataques ciberneticos logrando un empresa segura y eficaz en sus procesos de negocios.

De igual forma Marcos (2018) en la similitud de la tesis es el objetivo específico se da un entorno de ámbito nacional, cuyos somos integrantes de este plan de seguridad nacional ante la elección de nuestro voto, por ello se llevó a cabo una concientización de los ciudadanos en la seguridad de la información para no infringir ningún tipo anormalidad al momento del voto electrónico, y se recurre a ser transparente y eficaz al momento de elegir nuestro candidato.

Por otro lado, el indicador del nivel histórico de tipo de defensas antes de aplicar el sistema de ciberseguridad , reporta un Pre test un promedio de 18,0400 puntos con la desviación +/- de 2,32080 con un valor máximo alcanzado de 23 , al relacionar con el nivel histórico de defensas de las partes interesadas con el plan de seguridad de toda la empresa después de aplicar el sistema de ciberseguridad se observa un aumento del nivel de satisfacción dado que en el Post test indica un promedio de activos de 29,5800 puntos con una variación +/- de 2,32080 siendo un valor máximo de 34.Este aumento del nivel histórico de defensas se observa al segmentar los valores en baja prevalencia de 0-13 , media prevalencia de 14-26 , alta prevalencia de 27-40 , donde en el diagrama se presenta en el pretest un 6% de baja prevalencia y 94%de media prevalencia y después del Post test se presenta un 12% de media prevalencia y 88% de alta prevalencia donde se refleja un influencia positiva en la aplicación del sistema de ciberseguridad para mejorar la disminución de los ataques ciberneticos. Por ello Huayllani (2020), cuya similitud en el objetivo del nivel histórico de defensas se logra llevar a cabo un plan integral de defensa de todo orden en nivel tecnológico y de concientización del ser humano para lograr en consolidar una sólida barrera para mitigar los riesgos acaecidos por los ataques ciberneticos. Vizcarra Jarez, &Zúñiga Figueroa (2017) en la investigación de Ciberdefensa y su incidencia en la protección de la Información del Ejército del Perú. caso: COPERE 2013 – 2014, donde la información sensible que se maneja en las elites de defensa nacional del Perú (Ejercito) se plantea una restructuración de la ciberdefensa en el entorno de la seguridad de la información, para lograr su máxima defensa antes los ataques ciberneticos. Ramon Moya (2017) toma como importancia la defensa de sus activos informaticos la implementación de un firewall con logs de retroalimentación que en su sistema de aprendizaje controle el tráfico malicioso que genera ataques ciberneticos en el ámbito empresarial.

Sin embargo, el indicador del nivel de protección ante la amenaza y magnitud de daño antes de aplicar el sistema de ciberseguridad , reporta un Pre test un promedio de 18,0000 puntos con la desviación +/- de 2,06032 con un valor máximo alcanzado de 22 , al relacionar con el nivel de protección ante la amenaza y magnitud de daño con el plan de seguridad de toda la empresa después de aplicar el sistema de ciberseguridad se observa un aumento del nivel de satisfacción dado que en el Post test indica un promedio de activos de 30,6000 puntos con una variación +/- de 2,74048 siendo un valor máximo de 37.Este aumento del nivel de protección ante la amenaza y magnitud de daño observa al segmentar los valores en baja prevalencia de 0-13 , media prevalencia de 14-26 , alta prevalencia de 27-40 , donde en el diagrama se presenta en el pretest un 100 %de media prevalencia y después del Post test se presenta un 8% de media prevalencia y 92% de alta prevalencia donde se refleja un influencia positiva en la aplicación del sistema de ciberseguridad para mejorar la disminución de los ataques ciberneticos. Resulta que Sánchez (2017), ante la similitud del objetivo específico de protección y magnitud de daño dada la situación de operar de los ciberdelincuentes cuyo objetivo malintencionado es obtener la información para sus fines de malversación de fondos se instauro un plan de ciberseguridad que atiende las necesidades de mitigar los daños y tener la seguridad de la data de Oficina de la economía del ejercito exceptas de las amenazas del ciberespacio. (Avellán, 2019), en la investigación de ciberseguridad y su aplicación en las instituciones de educación superior públicas de Manabí, dado la circunstancia de establecer la categoría de la seguridad del internet manejando la norma ISO 27032-2012 con el término de presentar los peligros, ataques y debilidades de los métodos comercializados dan como resultado la prevención de respuestas a los ataques ciberneticos y de adquirir medidas para proteger la integridad de la data. Además, según Heffel (2016), la investigación de título de Ciberseguridad industrial en la distribución de energía eléctrica, dada la importancia de la necesidad de la energía electrica ante la seguridad de los ataques informaticos para controlar parte de la soberanía de Argentina; se concluye en proporcionar una visión extensa, en donde se hace forzoso un ataque holístico, multifactorial y multidisciplinario para mitigar los riesgos y se consolide el funcionamiento total de la energía electrica. Consolidando un nivel

integral de la ciberseguridad en todas sus fases para un entorno seguro de la empresa en la seguridad de la información.

VI. CONCLUSIONES

Con los resultados procesados de la presente investigación, se precisan las siguientes conclusiones:

Primera: Se determino en el objetivo general la implementación de un sistema de ciberseguridad que influye de manera positiva en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.Se concluye con el valor de la prueba de Student de -46.680, asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación ($p<0,05$) lo que con lleva al rechazo de la hipótesis nula (H_o) y la aceptación de la hipótesis general planteada en la investigación (H_a). El modelo de implementación de ciberseguridad que se adoptó en la empresa fue el idóneo porque hay una mejora notable en la defensa de los ataques informaticos y una disminución de las vulnerabilidades que con lleva a un mejor desempeño de negocio de la empresa Radiadores Fortaleza

Segundo: Se determino en el objetivo específico primero la implementación de un sistema de ciberseguridad que influye de manera positiva en el aumento del nivel de activos que son adecuados para su propósito en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.Se concluye con el valor de la prueba de Student de -24,961, asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación ($p<0,05$) lo que con lleva al rechazo de la hipótesis nula (H_0) y la aceptación de la hipótesis general planteada en la investigación (H_1).La implementación realizada en la empresa Radiadores Fortaleza aumenta el nivel de activos necesarios para la protección de la seguridad de la información y mitiga las vulnerabilidades existentes para mantener en resguardo la información en forma confidencial, integra y disponible

Tercero: Se determino el objetivo específico segundo en la implementación de un sistema de ciberseguridad influye de manera positiva en el aumento del nivel de satisfacción de las partes interesadas con el plan de seguridad de la empresa en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.Se

concluye con el valor de la prueba de Student de -34,794 asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación (p<0,05) lo que con lleva al rechazo de la hipótesis nula (H_0) y la aceptación de la hipótesis general planteada en la investigación (H_2). El aumento de la satisfacción del personal que concierne el plan de seguridad de la empresa se debe a la concientización en la utilización de los medios de información digitales para la seguridad de la data, teniendo en cuenta que el factor humano es el medio más débil en la protección de información en la empresa.

Cuarto: Se determino el objetivo específico tercero en la implementación de un sistema de ciberseguridad que influye de manera positiva en el aumento del nivel histórico de defensas en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.Se concluye con el valor de la prueba de Student de -31, 811 asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación (p<0,05) lo que con lleva al rechazo de la hipótesis nula (H_0) y la aceptación de la hipótesis general planteada en la investigación (H_3). El aumento de nivel histórico de defensas se debió a una restructuración de políticas de seguridad en los servidores y utilizando firewall para su debida protección de la empresa de los ataques ciberneticos.

Quinto: Se determino el objetivo específico cuarto la implementación de un sistema de ciberseguridad que influye de manera positiva en el aumento del nivel de protección ante la amenaza y magnitud de daño en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.Se concluye con el valor de la prueba de Student de -36, 373 asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación (p<0,05) lo que con lleva al rechazo de la hipótesis nula (H_0) y la aceptación de la hipótesis general planteada en la investigación (H_4). A la instauración en la implementación un sistema de ciberseguridad se obtuvo minimización de los daños ocurridos por los ataques ciberneticos y el aumento de la protección de la seguridad de información de la empresa.

VII. RECOMENDACIONES

Primero: Dado a este tipo de investigación de implementación de ciberseguridad se toma como aplicación de identificar y proteger el sistema de ciberseguridad se recomienda dar un proyecto holístico donde incluya todas las fases como detectar, responder y recuperar en la implementación de la ciberseguridad para dar un entorno seguro en el desarrollo de las actividades de la empresa Radiadores Fortaleza.

Segundo: El nivel de activos de informática que presenta la empresa ante la prevencion de ataques informaticos donde se trata de controlar los parámetros de la seguridad informática como integridad, disponibilidad, confidencialidad se recomienda dar seguimiento y monitoreo continuo de los puntos críticos de la amenaza antes los ataques ciberneticos para verificar que los parámetros que se llevan a cabo sean eficientes y minimizar sus vulnerabilidades.

Tercero: En el nivel de satisfacción de las partes interesadas con el plan de seguridad de la empresa se da un entorno del factor humano donde es el eslabón más débil dentro de la ciberseguridad , para ello se debe dar capacitaciones sobre el uso de los medio digitales y la seguridad de la información, este tipo de aprendizaje debe ser medido por cuestionarios para ver el porcentaje de aprendizaje de esta retroalimentación debido a ello hay que tomar medidas de corrección y sanciones aquellos que los incumplan para la protección de la seguridad de la información de la empresa.

Cuarto: Dada la circunstancia de defensa ante los ataques informaticos, se debe tener en cuenta ante el panorama de la pandemia ha suscitado mayor utilización de los medios digitales y el internet; debido a ello se recomienda utilizar firewall con inteligencia artificial con logs para una retroalimentación de los eventos sucedidos para acelerar la prevención de amenazas, su detección y respuesta, dando lugar a un entorno seguro para el negocio de la empresa.

Quinto: Ante el nivel de protección ante la amenaza y magnitud de daño en la prevención ataques cibernéticos , dado la coyuntura actual de la pandemia ha dado como resultado la utilización y masificación de las herramientas tecnológicas a nivel

del internet; por ello se recomienda estar vigilante en su modernidad con las nuevas tecnológicas como (firewall , routers, endpoints, antivirus) de marcas reconocidas en protección de las amenazas de los ataques ciberneticos para mitigar los daños en los sistemas informaticos de la empresa.

VIII. REFERENCIAS

Arias-Gómez, Jesús; Villasís-Keever, Miguel Ángel; Miranda Novales, María Guadalupe El protocolo de investigación III: la población de estudio Revista Alergia México, vol. 63, núm. 2, abril-junio, 2016

https://www.redalyc.org/pdf/4867/486755023011.pdf

Arévalo Ascanio, J. G., Bayona Trillos, R. A., Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. Implantation of a safety management system information under the ISO 27001: risk analysis information. Vol. 19 Issue 46, p123- 134. 12p. DOI: 10.14483/udistrital.jour.tecnura.2015.4.a10

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

Avellán Zambrano, Nerina Victoria & Zambrano Bravo, María Fernanda (2019). Ciberseguridad y su aplicación en las instituciones de educación superior públicas de Manabí. [Tesis de Maestría]

http://repositorio.espam.edu.ec/handle/42000/1032

Bohórquez Salcedo, Alberto Ismael (2021) Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima – 2020https://hdl.handle.net/20.500.12692/63128

Calderón Taboada, Lourdes Harumi (2019) Gestión de riesgos y seguridad de la información del Programa Fortalece Perú del MTPE

Chinchilla, E. J. S., y Allende, J. S. (2017). Riesgos de ciberseguridad en las Empresas. Tecnología y desarrollo, 15(0), Article 0. https://revistas.uax.es/index.php/tec_des/article/view/1174

Cram, W. A., D'Arcy, J. & Proudfoot, J.G. (2019). Seeing the forest and the trees: a metaanalysis of the antecedents to information security policy compliance. Vol. 43 Issue 2, p525-554. 54p. DOI: 10.25300/MISQ/2019/15117

Diario Gestión. (09 de abril de 2020). Ciberataques a dispositivos móviles en Perú se duplicaron en marzo. Gestión Perú. Recuperado el 2 de setiembre de 2020 de https://gestion.pe/peru/ciberataques-a-dispositivos-moviles-en-peru-se-duplicaron-en-marzo-noticia/

Elyazgi, M., 2018. Review of Gathering Data Instruments and Methods in Children Research. International Journal of Engineering & Technology, vol. 7, pp. 311-316.

Fitni, Q. R. S., y Ramli, K. (2020). Implementation of Ensemble Learning and Feature Selection for Performance Improvements in Anomaly-Based Intrusion Detection Systems. En 2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), 118-124. https://doi.org/10.1109/IAICT50021.2020.9172014

Garbarino, H. (2014). Marco de Gobernanza de TI para empresas PyMES - SMEsITGF [Tesis de doctorado, Universidad Politécnica de Madrid]. http://oa.upm.es/31002/

Gallardo, S. (2020). Diez años más tarde: Retos y amenazas a la seguridad y ciberseguridad en 2030. Sistemas, 155, 61-80. https://doi.org/10.29236/sistemas.n155a5

García, C. (2018). Gestión de la Calidad, Riesgos y Evaluación. Tema 3: Herramientas Gestión y Evaluación (II)

Gómez, F. S., y Parra, J. L. (2017). Cooperación público-privada en la protección de infraestructuras críticas. Cuadernos de estrategia, 185, 171-216.

Heffel, Walter Ernesto (2016). Ciberseguridad industrial en la distribución de energía eléctrica. [Tesis de Maestría]

https://rdu.iua.edu.ar/handle/123456789/1832

Hernández-Sampieri, R. & Mendoza, C. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta. Ciudad de México: Mc Graw Hill Education.

Hernández, J., Gallarzo, M., Espinoza, J. (2011). “Desarrollo Organizacional”. Recuperado de http://www.ebooks7-24.com/?il=4330 [Consulta: 6 de septiembre de 2018].

Huayllani, O. (2020). *Sistema de gestión de seguridad de la información y la gestióndel riesgo en el Ministerio de Salud* [Tesis de Maestría, Universidad Cesar Vallejo]. https://hdl.handle.net/20.500.12692/42775

Huerta Agurto (2020). Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019. https://hdl.handle.net/20.500.12692/46037

Instituto San Ignacio de Loyola (2020). Trabajo remoto: Desafíos en un contexto de crisis, primer estudio sobre trabajo remoto ISIL 2020. Recuperado de https://investigacion.isil.pe/estudio-trabajo-remoto-2020/

Inoguchi Rojas, A., & Macha Moreno, E. L. (2017). Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016. Universidad San Ignacio de Loyola; Repositorio Institucional - USIL.

ISO (Organization International for Standarization). (2018). ISO/IEC 27032:2012 Tecnología de la Información-Técnicas de seguridad-Directrices para la ciberseguridad. Disponible en: https://www.iso.org/standard/44375.html

Jimeno, J. (2013). AMFE: Análisis Modal de Fallos y Efectos – Guía y ejemplos de uso. Disponible en: https://www.pdcahome.com/3891/amfe-guia-de-usodel-analisis-modal-de-fallos-y-efectos/

Kamberg, M.-L., & Jiménez, A. (2018). Ciberseguridad: protege to identidad y tus datos. Rosen Central.

Alex Lopez & Geronimo Yedra. (2018) Factores Que Contribuyen A La Prevención De Los Delitos Informáticos En El Estado De Tabasco

https://doi.org/10.22478/ufpb.2179-7137.2017v6n3.37410

LOSH, S.C., (2017). Dependent and Independent Variables. The Wiley-Blackwell Encyclopedia of Social Theory. S.l.: American Cancer Society, pp. 1-3. ISBN 978- 1-118-43087-3.

Llontop Díaz, Gianmarco César (2018) Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks

Ma, Xiaoyan (2020). Diseño de un sistema de gestión de la seguridad de la información en una empresa de recursos humanos.

https://ebuah.uah.es/dspace/handle/10017/44660

Marcos, D. (2018). *Ciberseguridad aplicada a la e-democracia: análisis criptográfico y desarrollo de una metodología practica de evaluación para sistemas de voto electrónico remoto y su aplicación a las soluciones más relevantes* [Tesis de doctorado, Universidad de León]. http://hdl.handle.net/10612/7959

Márquez Alayo (2018). Ciberseguridad y su Relación en la Seguridad de los Sistemas Informáticos del Ejercito del Perú Caso: DITELE 2013-2014. [Tesis de Maestría]http://repositorio.icte.ejercito.mil.pe/handle/ICTE/122

Martínez-Mesa, J., González-Chica, D.A., Duquia, R.P., Bonamigo, R.R.Y Bastos, J.L., (2016). Sampling: ¿how to select participants in my research study? Anais Brasileiros de Dermatologia, vol. 91, no. 3, pp. 326-330. ISSN 0365-0596.DOI 10.1590/abd1806-4841.20165254

Mendoza Silva, Luis Fernando&Vega Gallegos, Giancarlo Roberto (2019).

Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SISC.

https://repositorio.up.edu.pe/handle/11354/2250

Moreno Caro, Ricardo&Otalora Neira, Adrian (2020). Diseño de un sistema de gestión de seguridad de la información para la empresa Sociedad Hotelera San Pablo basado en la norma ISO/IEC 270001:2013.[Tesis de Maestría]

http://repository.unipiloto.edu.co/handle/20.500.12277/7436

Paradis, E., O'brien, B., Nimmon, L., Bandiera, G. Y Martimianakis, M.A. (Tina), 2016. Design: Selection of Data Collection Methods. Journal of Graduate Medical Education, vol. 8, no. 2, pp. 263-264. ISSN 1949-8349. DOI 10.4300/JGMED-16-00098.1.

Poma, A., & Vargas, R. (2019). Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. SCIÉNDO; Vol. 22, Núm. 4 (2019): Octubre-Diciembre; 275-282.

Ramón Moya. (2017). Conocimiento experto y minería de datos sobre re-

portes de firewall aplicado a la detección de Amenazas Persistentes Avanzadas. [Tesis de Maestría] https://dialnet.unirioja.es/servlet/tesis?codigo=135065

Rivera Dávila, A. O. (2019). Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016.

http://repositorio.undac.edu.pe/handle/undac/1372

Rodrigo Cando-Segovia, M., & Medina-Chicaiza, P. (2021). Prevención en Ciberseguridad: Enfocada a Los Procesos De Infraestructura Tecnológica. 3C TIC, 10(1), 17–40.

SALAS, E., (2013). Liberabit. Revista de Psicología, diseños preexperimentales en psicología y educación: una revisión conceptual., vol. 19, pp. 133-141. ISSN 1729-4827.

Sampieri (2019) Método y metodología en la investigación https://es.slideshare.net/digraficaimprentaeditorial/mtodo-y-metodologa-en-la-investigacin-bj

Sánchez, J. (2017). Adopción de estrategias de ciberseguridad en la protección de la información en la oficina de economía del ejército [Tesis de Maestría, Instituto científico tecnológico del ejército]. http://repositorio.icte.ejercito.mil.pe/handle/ICTE/26

Secaira, J., Ocampo, R., Mera, E. & Kovalenko, I. (2020) El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). (Original). Roca. Revista científico-educacional de la provincia Granma, 16, 546-559.

Taipe Domínguez &Daniel Iván (2020). La auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018.

http://repositorio.unp.edu.pe/handle/20.500.12676/2361?show=full

Tiban, B. (2018). Plan informático 2018-2022, basado en la norma ISO/IEC 27032:2012 para mejorar la ciberseguridad de los recursos tecnológicos de información y comunicación (TIC`S) en la unidad educativa Alfredo Pareja Diez Canseco de la ciudad de Santo Domingo. Santo Domingo - Ecuador: Universidad Regional Autónoma de los Andes.

UPEL (2016). Aspectos éticos de la investigación científico. https://eticainvestigativa.wordpress.com/2016/03/29/aspectos-eticos-en-la-investigacion-cientifica/

Herr, T., & Friedman, A. A. (2015). Redefining Cybersecurity. The American Foreign Policy Council

Vasquez Pajuelo, Lida Inoguchi Rojas& Antonio Macha Moreno, Erika Liz (2017) Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú http://repositorio.usil.edu.pe/handle/USIL/2810

Vega, G., y Ramos, R. A. (2017). Vulnerabilidades y amenazas a los servicios web de la intranet de la Universidad Técnica de Babahoyo. 3C Tecnología.Glosas de innovación aplicadas a la pyme, 6(1), 53-66. https://doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

Vilcarromero Zubiate&Ladi Lizeth Vilchez Linares, Evit (2018). Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. [Tesis de Maestría]

https://repositorioacademico.upc.edu.pe/handle/10757/624832

Vizcarra Jarez&Zuñiga Figueroa. (2017). Ciberdefensa y su incidencia en la protección de la Información del Ejército del Perú. caso: COPERE 2013 – 2014. [Tesis de Maestría]
http://repositorio.icte.ejercito.mil.pe/handle/ICTE/32

IX. ANEXOS

Anexo 1: Matriz de Consistencia

Matriz de Consistencia								
Título: Implementación de un Sistema de Ciberseguridad para la prevención de los Ataques Cibernéticos en la Empresa Radiadores Fortaleza,2021								
Problema general	**Objetivo general**	**Hipótesis general**	**Variable**	**Dimensiones**	**Indicadores**	**Ítems**	**Intrumento**	**Escala**
¿De que manera la implementación de un sistema de ciberseguridad influye en la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021?	Determinar la influencia de la implementación de un sistema de ciberseguridad para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021	La implementación de un sistema de ciberseguridad influye de manera positiva en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021.	Sistema de Ciberseguridad	Identificar	Nivelde activos que son adecuados para su proposito	Variables tipo cuantitativa, intervalor, independiente *1 - 8*	Encuesta	Escala Ordinal: .
Problemas específicos	**Objetivos específicos**	**Hipótesis específicas**						
¿De que manera la implementación de un sistema de ciberseguridad influye en el nivel de activos que son adecuados para su proposito en la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021?	Determinar la influencia de la implementación de un sistema de ciberseguridad en el nivel de activos que son adecuados para su proposito para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021	H1: .La implementación de un sistema de ciberseguridad influye de manera positiva aumentando el nivel de activos que son adecuados para su proposito en la prevención ataques cibernéticos en la empresa radiadores fortaleza,2021.						
¿De que manera la implementación de un sistema de ciberseguridad influye en el nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa en la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021?	Determinar la influencia de la implementación de un sistema de ciberseguridad en el nivel de satisfaccion de las partes interesadas con el plan de seguridad de toda la empresa para la prevención de los ataques cibernéticos para la empresa radiadores fortaleza,2021	H2: La implementación de un sistema de ciberseguridad influye de manera positiva aumentando el nivel de satisfaccion de las partes intresadas con el plan de seguridad de la empresa en la prevención ataques cibernéticos en la empresa radiadores fortaleza,2021.		Proteger	Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa	Variables tipo cualitativa, nominal, independiente 9-16	Encuesta	Escala Ordinal: Mucho. Poco. Nada

¿De qué manera la implementación de un sistema de ciberseguridad influye en el nivel histórico de tipo de defensas en la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021?	Determinar la influencia de la implementación de un sistema de ciberseguridad en el nivel histórico de tipo de defensas para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021	H3: La implementación de un sistema de ciberseguridad influye de manera positiva aumentando el nivel histórico de defensas en la prevención ataques cibernéticos en la empresa radiadores fortaleza,2021	Prevención de ataques cibernéticos	Mecanismo de prevencion y protección	Nivel histórico de tipo de defensas	Variables tipo cualitativa, nominal, dependiente. 17-24	Encuesta	Escala Nominal: herramientas de protección (Antivirus, firewall. licencia de software, etc.)
¿De qué manera la implementación de un sistema de ciberseguridad influye en el nivel de protección de amenaza y magnitud de daño en la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021?	Determinar la influencia de la implementación de un sistema de ciberseguridad en el nivel de protección de amenaza y magnitud de daño para la prevención de los ataques cibernéticos en la empresa radiadores fortaleza,2021	H4: La implementación de un sistema de ciberseguridad influye de manera positiva aumentando el nivel de protección ante la amenaza y magnitud de daño en la prevención ataques cibernéticos en la empresa radiadores fortaleza,2021		Tipos de ataques informaticos	Nivel de protección de amenaza y magnitud de daño	Variables tipo cualitativa, nominal, dependiente. 25-32	Encuesta	Escala Ordinal: Alta. Media. Baja.
Método y Diseño		**Población y muestra**		**Técnicas e instrumentos**		**Método de análisis de datos**		
Enfoque: Aplicada Método: Cuantitativo Diseño: Experimental		Población: 50		No probabilístico - Conveniencia		Escala tipo Likert		

Anexo 2: Operacionalización de las variables

Variable Independiente	DEF. CON	DEF. OPE	Dimensiones	Indicadores	Escala
Sistema de Ciberseguridad	Según Friedman(2015)La ciberseguridad no es señal particular, que es consecuencia de una unificación incierta de las actividades en internet y los actores en las políticas y leyes existentes	Según Gallardo (2020) mencionan que es imprescindible mantener el mismo ritmo de innovación en ciberseguridad para poder adoptarse a las nuevas tecnologías sin superar un nivel de riesgo aceptable	Identificar	nivel de activos que son adecuados para su propósito en la prevención ataques cibernéticos	Escala Ordinal:
			Proteger	Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa.	Escala Ordinal:
Variable Dependiente	**DEF. CON**	**DEF. OPE**	**Dimensiones**	**Indicadores**	**Escala**
Prevención de ataques cibernéticos	Vega y Ramos (2017) recalcan que para evitar y en el mejor escenario minimizar los ataques e infiltraciones no deseadas, es indispensable implementar medidas de protección y seguridad a la infraestructura tecnológica, adoptar políticas de seguridad informática y diseñar una intranet segura, lo cual solo es posible, a través de un análisis detallado de los distintos protocolos de seguridad, herramientas tecnológicas y aplicaciones informáticas	Según Fitni (2020)defienden la idea de contar con buenas políticas en los equipos perimetrales (firewall), antivirus, sistemas de detección de intrusos (IDS) y juntamente con una buena capacitación al personal son el arma ideal para minimizar el riesgo de un evento malicioso.	Mecanismo de prevención y protección	Histórico de tipo de defensas	Escala Ordinal:
			Tipos de ataques informáticos	Probabilidad de amenaza y magnitud de daño	Escala Ordinal:

ANEXO 3: Instrumento de recolección de datos

Encuesta

Estimado, con la presente encuesta se pretende obtener datos la empresa Radiadores Fortaleza para el fortalecimiento de la ciberseguridad contra la prevención de los ataques cibernéticos para lo cual le solicito su colaboración, respondiendo a todas las preguntas con la mayor sinceridad posible.

Marque con una (x) la alternativa que considera pertinente en cada pregunta.

ESCALA VALORATIVA

Tabla 33
Escala de Encuesta

CODIGO	CATEGORIA	VALOR
S	Siempre	5
CS	Casi Siempre	4
AV	A veces	3
CN	Casi Nunca	2
N	Nunca	1

	VARIABLE: SISTEMA DE CIBERSEGURIDAD					
	Dimensión 1: Identificar	**N**	**CN**	**AV**	**CS**	**S**
1	¿Se cuenta con equipos informáticos con antiguedad menos de 5 años?					
2	¿En su empresa existen herramientas que aseguren su información? digital?					
3	¿Se cuenta con equipos de respaldo de energía electrica cuando se va el fluido electrico?					
4	¿Los cableados eléctricos y de internet tienen las mismas normas técnicas en la disposición del área de trabajo que laboran?					
5	¿El CPU que utiliza en el trabajo tiene antivirus?					
6	¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?					
7	¿Realizan cambio de cpu o laptops cada 4 años?					
8	¿Cree usted que el área de sistemas atiende su problema rápidamente?					
	Dimensión 2: Proteger	**N**	**CN**	**AV**	**CS**	**S**
9	¿El personal está capacitado en temas de ciberseguridad?					
10	¿Se cambian periódicamente las contraseñas del CPU o laptop para el ingreso del sistema operativo?					
11	¿Puede entrar sin dificultad a las diversas páginas de internet?					

12	¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?					
13	¿Puede entrar al wifi de la empresa y poder navegar sin dificultad?					
14	¿Esta restringido usbs en la pc o laptops de la empresa?					
15	¿Los sistemas informaticos utilizados en la empresa se trabaja con rapidez y ninguna contrariedad?					
16	¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?					
	DIMENSIÓN 3: Mecanismo de prevencion y protección	**N**	**CN**	**AV**	**CS**	**S**
17	¿Se cree usted seguro con el antivirus de la empresa?					
18	¿Se restringen correos no deseados a su bandeja?					
19	¿Los correos normalmente llegan a sus destinatarios?					
20	¿Los documentos que recibes se abren sin ningún problema?					
21	¿Cree usted que el área de TI busca soluciones para los ataques informaticos?					
22	¿La oficina de Ti realiza Backus periódicos de su información?					

23	¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ataque cibernético?					
24	¿El área de ti da capacitaciones acerca de los ataques informaticos?					
	DIMENSION 4: Tipos de ataques informaticos	**N**	**CN**	**AV**	**CS**	**S**
25	¿Existe algún mecanismo de alerta, para la detección de virus?					
26	¿Hay un proceso de evaluación / investigación para identificar tipos de ataques ciberneticos recurrentes?					
27	¿Al utilizar su cpu o laptop es rapida en realizar sus trabajos?					
28	¿Alguna vez al ingresar a su carpeta de trabajo ha podido ingresar?					
29	¿Alguna vez al abrir documento nunca ha visto caracteres no descifrables?					
30	¿Tenemos protección ante cualquier tipo de ataque Cibernéticos?					
31	¿No realiza apertura de correos no deseados en su bandeja de entrada?					
32	¿No registra apago o paralizacion de pc, laptop por conectar un usb?					

ANEXO 4 :Calculo de tamaño de muestra

$$\text{Tamaño de la muestra} = \frac{\frac{z^2 \times p\,(1-p)}{e^2}}{1 + \left(\frac{z^2 \times p\,(1-p)}{e^2 N}\right)}$$

N = tamaño de la población (50)

e = margen de error (porcentaje expresado con decimales)(3%)

z = Parámetro estadístico que depende el Nivel de Confianza(NC)(1.96)

p=Probabilidad de que ocurra el evento estudiado(50%)

q=(1-p)=Probabilidad de que no ocurra el evento estudiado(50%)

Tamaño de muestra =48

Como la población es poca se toma como referencia la población total de 50

ANEXO 5: CONFIABILIDAD DEL INSTRUMENTO

Confiabilidad de la variable Prevención de ataques cibernéticos

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,707	16

Por la variable de prevencion de ataques ciberneticos el alfa de Cronbach es de 0.707 es confiable para realizar las pruebas

ANEXO 6 :Documento de Google Formulario para cuestionario de Ciberseguridad

Cuestionario sobre ciberseguridad de la empresa

Nombres y Apellidos

Tu respuesta

En que área de la empresa trabajas

Tu respuesta

¿Se cuenta con equipos informáticos con antigüedad menos de 5 años?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿En su empresa existen herramientas que aseguren su información? digital?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Se cuenta con equipos de respaldo de energía eléctrica cuando se va el fluido eléctrico?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Los cableados eléctricos y de internet tienen las mismas normas técnicas en la disposición del área de trabajo que laboran?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿El CPU que utiliza en el trabajo tiene antivirus?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Realizan cambio de cpu o laptops cada 4 años?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Cree usted que el área de sistemas atiende su problema rápidamente?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿El personal está capacitado en temas de ciberseguridad?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Se cambian periódicamente las contraseñas del CPU o laptop para el ingreso del sistema operativo?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Puede entrar sin dificultad a las diversas páginas de internet?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Puede entrar al wifi de la empresa y poder navegar sin dificultad?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Esta restringido usbs en la pc o laptops de la empresa?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Los sistemas informáticos utilizados en la empresa se trabaja con rapidez y ninguna contrariedad?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Se cree usted seguro con el antivirus de la empresa?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Se restringen correos no deseados a su bandeja?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Los correos normalmente llegan a sus destinatarios?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Los documentos que recibes se abren sin ningún problema?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Cree usted que el área de TI busca soluciones para los ataques informáticos?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿La oficina de Ti realiza Backups periódicos de su información?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ataque cibernético?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿El área de ti da capacitaciones acerca de los ataques informáticos?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Existe algún mecanismo de alerta, para la detección de virus?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Hay un proceso de evaluación / investigación para identificar tipos de ataques cibernéticos recurrentes?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Al utilizar su cpu o laptop es rápida en realizar sus trabajos?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Alguna vez al ingresar a su carpeta de trabajo ha podido ingresar?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Alguna vez al abrir documento nunca ha visto caracteres no descifrables?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿Tenemos protección ante cualquier tipo de ataque Cibernéticos?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿No realiza apertura de correos no deseados en su bandeja de entrada?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

¿No registra apago o paralización de pc, laptop por conectar un usb?

- ◯ Nunca
- ◯ Casi Nunca
- ◯ A veces
- ◯ Casi Siempre
- ◯ Siempre

ANEXO 7 : DATOS DEL CUESTIONARIO ANTES DE LA IMPLEMENTACIÓN DE CIBERSEGURIDAD

	Sistema de Ciberseguridad																Prevencion de ataques ciberneticos															
	Identificar								Proteger								M.Prevención y Proteccion								T.Ataques Ciberneticos							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	2	3	3	2	2	3	1	2	2	2	1	2	2	3	2	2	2	2	2	2	2	2	2	1	3	2	2	2	2	2	2	2
2	1	1	2	2	2	2	2	2	2	2	1	2	1	4	1	2	1	2	1	2	2	2	1	1	2	1	2	1	2	3	2	1
3	2	2	3	1	2	2	1	3	2	1	2	1	1	3	2	2	1	2	2	3	1	2	2	1	2	1	2	2	3	2	2	1
4	2	1	2	2	1	3	2	2	1	2	1	2	1	3	2	1	2	3	2	2	1	3	2	2	2	2	2	2	2	1	1	2
5	1	2	3	1	2	2	2	2	2	3	2	3	2	1	2	2	2	2	3	3	2	2	2	3	2	1	3	2	4	2	1	2
6	2	2	2	2	2	3	2	3	2	2	1	2	1	2	1	2	2	2	2	2	1	2	1	1	2	3	1	3	2	3	2	2
7	3	2	4	2	3	2	3	3	2	1	2	1	2	1	3	1	2	1	3	3	2	1	2	2	3	2	2	2	3	1	1	3
8	1	3	2	1	3	1	2	2	1	2	3	1	2	3	2	1	1	3	2	3	4	3	2	2	1	3	1	2	3	3	2	3
9	3	1	3	3	2	2	3	2	2	2	2	3	2	4	2	1	3	4	3	2	2	2	1	1	2	3	1	2	2	1	2	3
10	3	2	1	2	1	3	2	2	1	1	1	2	3	2	3	3	2	3	2	2	3	1	2	2	3	1	2	2	3	1	1	3
11	3	2	3	3	1	2	2	2	1	3	2	3	2	2	3	2	1	1	2	3	3	3	2	2	2	3	1	3	2	1	3	1
12	2	4	2	2	3	3	2	3	1	3	2	3	2	3	2	1	2	2	3	1	3	1	2	2	1	2	1	2	3	2	2	2
13	3	2	2	2	3	3	2	3	2	2	3	2	2	2	2	1	2	3	1	2	2	3	1	2	3	2	1	3	2	3	1	2
14	1	2	3	3	2	2	2	3	2	2	3	2	3	2	2	2	1	2	1	3	1	2	1	2	3	1	3	1	1	2	2	3
15	2	3	2	2	3	3	2	1	3	2	3	2	1	2	3	3	2	1	2	3	3	2	1	2	3	2	1	2	3	3	2	2
16	1	3	1	3	1	2	1	2	3	3	2	1	2	3	3	1	2	3	3	1	2	2	3	2	2	3	2	2	3	2	1	3
17	2	3	2	4	2	3	2	2	3	2	2	3	2	3	2	3	2	3	2	2	3	2	1	3	2	1	3	1	2	3	2	3
18	2	2	3	2	1	2	3	1	2	3	2	3	2	2	3	3	2	2	2	3	2	2	1	3	3	2	3	1	2	2	3	2
19	3	2	2	3	2	2	2	3	1	2	3	2	1	2	3	2	2	3	2	3	3	2	2	3	2	2	3	3	2	2	3	2
20	2	3	3	2	3	2	3	2	3	2	1	3	2	3	2	1	3	2	3	3	2	3	3	2	1	2	3	2	2	3	2	3
21	3	2	2	3	1	2	1	2	2	1	3	2	3	2	2	2	1	2	2	3	2	3	2	3	2	3	3	2	3	3	2	1
22	2	2	3	2	3	1	1	3	2	1	2	3	2	2	1	3	2	1	2	3	2	1	3	3	3	2	1	2	3	2	3	2
23	2	1	2	3	1	3	2	3	2	3	2	3	3	2	3	2	3	3	2	1	2	3	1	2	2	3	1	3	2	3	2	2
24	3	2	1	2	3	1	2	2	1	3	2	3	2	1	3	2	3	1	3	2	2	2	3	2	3	2	3	4	3	2	3	2

	Sistema de Ciberseguridad																Prevencion de ataques ciberneticos													
	Identificar								Proteger								M.Prevención y Proteccion								T.Ataques Ciberneticos							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
25	2	3	2	3	2	3	2	1	2	3	3	2	1	3	1	3	1	3	2	2	3	3	1	2	3	2	1	2	3	3	2	1
26	3	2	1	3	2	1	1	2	3	3	2	1	3	3	2	1	3	2	1	1	2	3	2	3	3	2	3	2	1	2	3	3
27	2	3	2	3	2	3	2	2	2	3	2	3	2	3	2	3	2	3	2	2	3	2	3	3	2	2	1	1	2	3	2	3
28	2	3	2	3	2	3	2	3	2	3	2	1	3	2	1	3	2	2	3	2	3	2	3	2	3	2	3	3	2	3	2	3
29	2	3	2	2	3	3	1	2	3	3	1	2	3	3	3	3	2	3	2	3	3	2	1	2	3	3	2	2	3	2	3	2
30	2	3	2	3	2	3	2	3	2	2	2	1	2	3	2	2	3	2	3	2	2	3	3	2	1	2	3	2	1	2	3	2
31	2	2	3	2	2	3	2	1	2	2	3	2	3	3	2	3	2	3	4	1	2	2	1	1	3	2	2	1	3	2	3	2
32	3	2	3	3	4	2	3	2	3	2	3	4	3	2	3	2	3	3	2	3	2	3	4	3	2	3	3	2	2	4	3	2
33	1	2	3	1	2	2	3	2	3	3	2	2	3	3	3	2	3	3	2	3	4	3	2	3	2	3	2	3	2	4	2	3
34	2	3	2	3	2	3	2	1	2	1	2	3	2	3	1	3	2	3	2	2	3	3	3	2	4	2	2	3	2	3	1	2
35	3	2	2	3	3	2	1	3	2	2	2	1	2	1	2	2	3	1	2	3	2	3	2	3	2	1	2	3	3	2	3	2
36	2	2	3	2	2	3	2	3	2	2	3	2	4	2	3	2	3	2	1	2	4	3	2	3	3	2	3	4	2	3	2	3
37	3	1	3	2	3	2	1	3	3	2	3	2	3	3	3	2	3	1	3	3	2	1	3	2	3	3	1	2	3	2	3	3
38	2	1	3	3	1	3	2	2	1	3	2	2	1	1	2	3	3	3	1	2	3	1	3	2	2	3	2	1	3	2	3	3
39	2	3	2	3	2	3	3	2	3	2	3	3	2	3	2	2	3	2	3	2	1	2	3	2	1	2	3	2	3	4	2	2
40	3	2	3	3	2	3	4	3	2	1	3	2	3	2	3	2	4	3	2	2	3	1	2	3	3	1	2	1	3	2	2	2
41	2	2	3	2	3	2	1	2	3	3	3	2	1	2	3	2	1	3	2	3	3	4	2	3	2	3	1	2	3	1	2	3
42	2	3	4	2	3	3	2	3	4	3	4	3	2	3	2	3	4	3	2	2	3	1	2	3	2	3	2	3	2	2	4	3
43	1	2	1	2	3	2	3	2	1	2	3	2	1	2	3	2	1	4	3	2	2	3	2	3	2	3	2	3	2	3	2	2
44	2	2	3	2	3	2	3	2	3	3	2	3	2	3	3	2	3	2	2	3	2	3	2	3	3	3	2	3	2	3	2	3
45	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	3	2	3	2	2	3	3	2	3	2	2	1	2	3	1
46	2	3	2	3	2	2	3	2	3	2	3	2	1	3	2	3	2	2	3	2	3	2	3	2	3	2	4	2	2	3	2	3
47	3	3	2	3	2	1	3	2	3	2	2	3	2	3	2	1	2	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
48	1	2	1	4	2	3	2	2	2	3	1	3	2	3	2	3	2	3	2	2	3	2	1	2	3	2	3	2	3	2	2	3
49	2	2	3	2	2	1	3	2	2	4	2	2	3	2	2	3	2	3	2	3	2	2	2	3	2	2	2	2	2	2	3	2
50	2	3	2	2	3	2	2	3	2	2	2	1	2	2	3	2	2	1	3	2	2	3	2	2	1	3	2	2	1	2	2	2

ANEXO 8: DATOS DEL CUESTIONARIO DEL CUESTIONARIO DESPUES DE LA IMPLEMENTACION DE LA CIBERSEGURIDAD

	Sistema de Ciberseguridad																Prevencion de ataques ciberneticos															
	Identificar								Proteger								M.Prevención y Proteccion								T.Ataques Ciberneticos							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	3	3	3	3	3	3	3	3	4	3	3	3	3	4	4	4	3	4	3	3	4	3	4	3	4	3	4	2	2	3	4	3
2	3	3	4	3	4	3	4	3	3	4	3	3	3	5	3	3	3	3	4	3	4	3	4	4	4	3	4	2	3	4	2	3
3	2	2	2	3	3	3	3	4	4	4	4	3	4	3	4	2	3	4	3	4	2	4	2	3	3	4	3	3	4	3	4	4
4	3	3	5	2	3	4	3	3	4	4	4	4	4	4	2	3	3	4	4	3	2	4	5	4	4	4	4	4	3	4	4	3
5	4	4	3	3	2	4	3	4	3	4	3	4	3	4	3	4	2	4	3	3	3	4	3	4	4	3	5	4	4	4	4	4
6	3	3	3	4	3	2	3	4	5	3	4	3	4	3	4	3	4	2	3	4	3	4	3	3	3	4	3	5	3	2	5	3
7	3	3	4	4	3	4	2	3	4	3	3	3	4	2	4	3	3	3	2	4	4	3	3	3	3	3	4	4	4	3	3	4
8	3	4	2	4	3	3	3	2	3	4	3	3	2	3	5	3	4	4	3	2	4	4	3	3	4	4	3	4	3	3	4	4
9	4	3	4	4	3	3	4	3	2	3	4	2	3	4	3	3	3	4	4	3	2	3	3	2	3	4	3	4	3	3	3	4
10	3	4	3	4	3	4	3	4	3	4	4	4	4	4	3	3	4	3	4	3	3	2	3	3	4	3	4	4	3	4	3	4
11	3	3	4	3	4	3	3	3	4	3	4	4	5	3	4	3	4	4	3	3	4	3	4	3	3	3	2	3	4	3	4	3
12	3	3	4	4	3	4	3	4	3	4	2	4	3	4	3	3	4	3	4	3	3	4	3	3	3	4	3	4	3	4	3	4
13	3	3	4	4	3	3	4	3	4	4	3	3	4	4	3	3	3	4	3	4	4	3	3	5	3	2	4	3	4	3	4	3
14	2	4	5	3	4	3	3	4	4	3	4	3	4	5	3	4	3	5	4	3	4	3	4	3	4	3	4	4	3	4	3	4
15	3	4	4	5	4	5	3	3	4	3	3	4	5	3	4	5	3	3	3	4	5	4	3	4	5	4	3	4	5	4	4	3
16	3	4	3	3	4	5	4	3	3	2	5	3	4	5	4	4	3	4	3	3	3	3	4	4	4	3	4	3	4	3	4	4
17	3	4	5	4	3	4	3	4	4	3	5	4	3	3	3	4	5	4	3	3	4	3	2	4	3	3	4	3	3	4	3	5
18	3	4	5	4	3	4	3	4	3	4	5	4	4	4	3	3	4	4	3	3	3	4	3	4	3	4	3	4	4	4	3	4
19	3	4	2	4	4	3	4	5	4	2	2	3	4	5	4	3	4	4	3	4	4	3	4	5	4	4	3	3	4	4	4	4
20	2	4	4	2	4	5	5	2	2	4	3	3	4	5	4	3	4	3	4	3	4	3	3	3	4	4	3	4	4	3	4	4
21	3	4	3	4	3	4	5	4	3	4	4	4	5	4	4	4	3	5	5	4	3	4	3	3	4	3	3	4	4	3	5	4
22	2	4	5	4	4	3	3	4	5	4	2	3	4	2	4	5	4	3	4	5	4	3	4	5	3	3	4	4	4	5	4	4
23	3	5	4	4	3	4	4	3	4	3	4	3	3	3	4	4	4	4	3	4	3	3	4	4	3	3	2	4	3	4	5	4
24	3	4	3	4	5	4	3	4	5	4	3	4	4	5	4	3	4	4	4	3	3	3	4	5	4	4	4	4	2	3	4	5

	Sistema de Ciberseguridad																Prevencion de ataques ciberneticos															
	Identificar								Proteger								M.Prevención y Proteccion								T.Ataques Ciberneticos							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
25	3	4	3	5	4	3	4	3	4	4	4	4	3	4	3	4	3	4	4	4	5	4	3	4	5	4	3	4	3	4	5	4
26	3	4	2	3	4	4	3	4	5	5	4	3	4	4	3	4	3	3	3	3	4	5	4	4	4	5	4	3	4	3	4	5
27	2	4	3	4	4	3	4	4	4	5	4	3	3	4	5	4	3	4	3	3	4	4	5	4	4	4	3	5	3	4	3	4
28	3	3	4	3	4	4	4	4	3	4	4	3	4	3	4	3	4	4	4	3	4	4	4	4	5	4	3	4	3	4	3	4
29	3	4	5	4	4	4	5	3	4	4	3	4	3	3	4	4	4	3	4	5	3	4	3	4	4	4	4	5	4	3	3	5
30	3	4	3	4	3	4	3	4	3	4	3	4	3	4	5	3	4	5	4	3	4	3	4	3	4	3	4	4	5	4	4	4
31	3	4	4	4	5	4	4	3	4	4	4	5	4	3	4	4	4	3	4	5	3	4	5	4	5	4	3	4	4	5	4	3
32	3	4	4	4	4	3	4	5	4	3	4	5	4	4	4	3	4	4	3	4	4	4	4	5	4	4	3	4	4	4	5	4
33	2	4	5	4	3	3	4	5	4	4	5	4	3	3	4	4	4	5	5	3	3	4	4	3	5	5	5	5	5	4	4	4
34	3	5	4	4	4	5	4	3	3	3	3	4	4	4	4	3	4	4	4	4	5	4	5	4	3	5	5	4	5	4	5	4
35	3	4	5	5	5	4	4	4	3	3	3	4	4	3	4	4	3	4	3	4	4	4	4	3	4	4	5	4	4	5	4	4
36	2	3	3	4	5	5	4	3	3	4	4	3	4	4	4	3	4	5	3	4	4	3	4	5	4	3	4	5	4	5	4	5
37	3	4	5	4	4	4	3	4	4	3	4	5	4	5	3	4	5	4	4	4	3	3	5	3	3	5	4	3	4	4	3	4
38	3	4	3	3	4	4	3	4	4	5	3	3	4	4	3	4	4	4	4	3	4	4	4	4	4	4	5	4	3	3	4	4
39	3	4	4	3	3	4	4	3	3	4	4	4	3	4	5	4	3	4	4	3	3	4	4	5	4	3	4	3	4	4	3	5
40	3	3	4	5	4	4	4	4	5	4	4	3	4	3	4	4	5	3	3	4	4	4	4	5	4	4	4	4	3	3	4	4
41	3	3	4	4	4	4	4	3	4	4	4	4	4	4	5	4	4	3	4	3	3	4	3	4	4	4	3	4	3	3	4	5
42	4	4	4	5	5	4	4	5	4	5	4	4	5	5	5	4	5	4	4	4	3	3	5	3	4	4	4	4	4	4	5	4
43	3	4	4	5	5	3	4	5	4	3	4	5	4	3	4	4	4	4	5	4	4	4	5	4	5	5	5	4	4	3	4	4
44	3	4	5	4	5	4	4	3	4	3	4	4	3	4	4	4	5	4	5	4	5	4	4	4	3	4	5	5	4	3	4	4
45	3	5	4	5	5	4	5	5	4	3	4	3	4	4	4	5	4	4	3	4	4	4	5	5	4	3	4	4	5	4	4	5
46	4	4	3	4	5	4	4	4	5	4	4	4	5	3	4	4	3	5	4	4	5	4	5	5	4	5	4	5	4	5	4	4
47	4	4	4	4	4	5	5	5	4	4	4	4	4	4	5	4	4	4	5	5	4	4	3	3	4	4	5	5	4	4	4	5
48	4	4	4	4	4	5	4	4	4	4	3	4	3	3	5	4	4	4	3	3	4	4	3	3	4	4	4	3	4	4	4	5
49	4	5	4	5	4	3	4	5	4	5	4	4	5	5	4	5	4	3	4	4	3	4	4	5	5	5	5	5	4	4	3	3
50	4	5	5	5	4	4	5	4	4	5	5	4	4	5	4	4	5	4	4	3	4	4	3	4	4	5	5	4	5	3	3	4

ANEXO 9 VALIDEZ DEL INSTRUMENTO

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE VARIABLE DE CIBERSEGURIDAD Y PREVENCIÓN DE ATAQUES CIBERNÉTICOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Identificar	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Se cuenta con equipos informáticos con antigüedad menos de 5 años?	X		X		X		
2	¿ En su empresa existen herramientas que aseguren su información digital?	X		X		X		
3	¿Se cuenta con equipos de respaldo de energía electrica cuando se va el fluido electrico?	X		X		X		
4	¿Los cableados eléctricos y de internet tienen las mismas normas técnicas en la disposición del área de trabajo que laboran?	X		X		X		
5	¿El cpu que utiliza en el trabajo tiene antivirus?	X		X		X		
6	¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?	X		X		X		
7	¿Realizan cambio de cpu o laptops cada 4 años?	X		X		X		
8	¿Cree usted que el área de sistemas atiende su problema rápidamente?	X		X		X		
	DIMENSIÓN 2: Proteger	**Si**	**No**	**Si**	**No**	**Si**	**No**	

9	**¿El personal está capacitado en temas de ciberseguridad?**	**X**		**X**		**X**		
10	¿Se cambian periódicamente las contraseñas del CPU o laptop para el ingreso del sistema operativo?	X		X		X		
11	¿Puede entrar sin dificultad a las diversas páginas de internet?	X		X		X		
12	¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?	X		X		X		
13	¿Puede entrar al wifi de la empresa y poder navegar sin dificultad?	X		X		X		
14	¿Esta restringido usbs en la pc o laptops de la empresa?	X		X		X		
15	¿Los sistemas informaticos utilizados en la empresa se trabaja con rapidez y ninguna contrariedad?	X		X		X		
16	¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?	X		X		X		
	DIMENSIÓN 3: Mecanismo de prevencion y protección	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	¿Se cree usted seguro con el antivirus de la empresa?	X		X		X		
18	¿Se restringen correos no deseados a su bandeja?	X		X		X		
19	¿Los correos normalmente llegan a sus destinatarios?	X		X		X		
20	¿Los documentos que recibes se abren sin ningún problema?	X		X		X		
21	¿Cree usted que el área de TI busca soluciones para los ataques informaticos?	X		X		X		
22	¿La oficina de Ti realiza Backus periódicos de su información?	X		X		X		
23	¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ataque cibernético?	X		X		X		
24	¿El área de ti da capacitaciones acerca de los ataques informaticos?	**X**		**X**		**X**		
	DIMENSION 4: Tipos de ataques informaticos	**Si**	**No**	**Si**	**No**	**Si**	**No**	

25	¿Existe algún mecanismo de alerta, para la detección de virus?	X		X		X		
26	¿Hay un proceso de evaluación / investigación para identificar tipos de ataques cibernéticos recurrentes?	X		X		X		
27	¿Al utilizar su cpu o laptop es rápida en realizar sus trabajos?	X		X		X		
28	¿Alguna vez al ingresar a su carpeta de trabajo ha podido ingresar?	X		X		X		
29	¿Alguna vez al abrir documento nunca ha visto caracteres no descifrables?	X		X		X		
30	¿Tenemos protección ante cualquier tipo de ataque Cibernéticos?	X		X		X		
31	¿No realiza apertura de correos no deseados en su bandeja de entrada?	X		X		X		
32	¿No registra apago o paralización de pc, laptop por conectar un usb?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg**: Mg. Acuña Benites Marlon DNI: 42097456**

Especialidad del validador: Investigador

23 de junio del 2021

[1]**Pertinencia:**El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

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

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE VARIABLE DE CIBERSEGURIDAD Y PREVENCIÓN DE ATAQUES CIBERNÉTICOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Identificar	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Se cuenta con equipos informáticos con antigüedad menos de 5 años?	X		X		X		
2	¿ En su empresa existen herramientas que aseguren su información digital?	X		X		X		
3	¿Se cuenta con equipos de respaldo de energía electrica cuando se va el fluido electrico?	X		X		X		
4	¿Los cableados eléctricos y de internet tienen las mismas normas técnicas en la disposición del área de trabajo que laboran?	X		X		X		
5	¿El cpu que utiliza en el trabajo tiene antivirus?	X		X		X		
6	¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?	X		X		X		
7	¿Realizan cambio de cpu o laptops cada 4 años?	X		X		X		
8	¿Cree usted que el área de sistemas atiende su problema rápidamente?	X		X		X		
	DIMENSIÓN 2: Proteger	**Si**	**No**	**Si**	**No**	**Si**	**No**	

9	**¿El personal está capacitado en temas de ciberseguridad?**	**X**		**X**		**X**		
10	¿Se cambian periódicamente las contraseñas del CPU o laptop para el ingreso del sistema operativo?	X		X		X		
11	¿Puede entrar sin dificultad a las diversas páginas de internet?	X		X		X		
12	¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?	X		X		X		
13	¿Puede entrar al wifi de la empresa y poder navegar sin dificultad?	X		X		X		
14	¿Esta restringido usbs en la pc o laptops de la empresa?	X		X		X		
15	¿Los sistemas informaticos utilizados en la empresa se trabaja con rapidez y ninguna contrariedad?	X		X		X		
16	¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?	X		X		X		
	DIMENSIÓN 3: Mecanismo de prevencion y protección	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	¿Se cree usted seguro con el antivirus de la empresa?	X		X		X		
18	¿Se restringen correos no deseados a su bandeja?	X		X		X		
19	¿Los correos normalmente llegan a sus destinatarios?	X		X		X		
20	¿Los documentos que recibes se abren sin ningún problema?	X		X		X		
21	¿Cree usted que el área de TI busca soluciones para los ataques informaticos?	X		X		X		
22	¿La oficina de Ti realiza Backus periódicos de su información?	X		X		X		
23	¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ataque cibernético?	X		X		X		
24	¿El área de ti da capacitaciones acerca de los ataques informaticos?	**X**		**X**		**X**		
	DIMENSION 4: Tipos de ataques informaticos	**Si**	**No**	**Si**	**No**	**Si**	**No**	

25	¿Existe algún mecanismo de alerta, para la detección de virus?	X		X		X		
26	¿Hay un proceso de evaluación / investigación para identificar tipos de ataques cibernéticos recurrentes?	X		X		X		
27	¿Al utilizar su cpu o laptop es rápida en realizar sus trabajos?	X		X		X		
28	¿Alguna vez al ingresar a su carpeta de trabajo ha podido ingresar?	X		X		X		
29	¿Alguna vez al abrir documento nunca ha visto caracteres no descifrables?	X		X		X		
30	¿Tenemos protección ante cualquier tipo de ataque Cibernéticos?	X		X		X		
31	¿No realiza apertura de correos no deseados en su bandeja de entrada?	X		X		X		
32	¿No registra apago o paralización de pc, laptop por conectar un usb?	X		X		X		

Observaciones (precisar si hay suficiencia):EXISTE SUFICIENCIA

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg**: Mg. Ramos Choquehuanca Angelino DNI: 10101015**

Especialidad del validador: Investigador

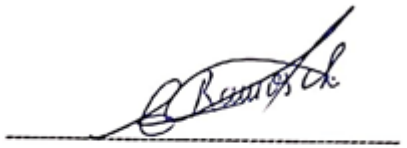
29 de junio del 2021

[1]**Pertinencia:**El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



Mg. Ramos Choquehuanca Angelino

Código Docente 5011

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE VARIABLE DE CIBERSEGURIDAD Y PREVENCIÓN DE ATAQUES CIBERNÉTICOS

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1: Identificar	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Se cuenta con equipos informáticos con antigüedad menos de 5 años?	X		X		X		
2	¿ En su empresa existen herramientas que aseguren su información digital?	X		X		X		
3	¿Se cuenta con equipos de respaldo de energía electrica cuando se va el fluido electrico?	X		X		X		
4	¿Los cableados eléctricos y de internet tienen las mismas normas técnicas en la disposición del área de trabajo que laboran?	X		X		X		
5	¿El cpu que utiliza en el trabajo tiene antivirus?	X		X		X		
6	¿Cree usted que oficina de tecnología de información resguarda los backups de la información de la empresa adecuadamente?	X		X		X		
7	¿Realizan cambio de cpu o laptops cada 4 años?	X		X		X		
8	¿Cree usted que el área de sistemas atiende su problema rápidamente?	X		X		X		
	DIMENSIÓN 2: Proteger	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	**¿El personal está capacitado en temas de ciberseguridad?**	**X**		**X**		**X**		
10	¿Se cambian periódicamente las contraseñas del CPU o laptop para el ingreso del sistema operativo?	X		X		X		
11	¿Puede entrar sin dificultad a las diversas páginas de internet?	X		X		X		

12	¿Se está aprendiendo de forma proactiva de incidentes, mejorando los conocimientos de riesgo y los controles de seguridad?	X		X		X		
13	¿Puede entrar al wifi de la empresa y poder navegar sin dificultad?	X		X		X		
14	¿Esta restringido usbs en la pc o laptops de la empresa?	X		X		X		
15	¿Los sistemas informaticos utilizados en la empresa se trabaja con rapidez y ninguna contrariedad?	X		X		X		
16	¿Cree usted que la oficina de tecnología de información cuenta con programas para concientizar las amenazas en la ciberseguridad?	X		X		X		
	DIMENSIÓN 3: Mecanismo de prevencion y protección	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	¿Se cree usted seguro con el antivirus de la empresa?	X		X		X		
18	¿Se restringen correos no deseados a su bandeja?	X		X		X		
19	¿Los correos normalmente llegan a sus destinatarios?	X		X		X		
20	¿Los documentos que recibes se abren sin ningún problema?	X		X		X		
21	¿Cree usted que el área de TI busca soluciones para los ataques informaticos?	X		X		X		
22	¿La oficina de Ti realiza Backus periódicos de su información?	X		X		X		
23	¿Cree usted que la oficina de tecnología de información tiene planes de contingencia en caso de un ataque cibernético?	X		X		X		
24	¿El área de ti da capacitaciones acerca de los ataques informaticos?	X		X		X		
	DIMENSION 4: Tipos de ataques informaticos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Existe algún mecanismo de alerta, para la detección de virus?	X		X		X		
26	¿Hay un proceso de evaluación / investigación para identificar tipos de ataques ciberneticos recurrentes?	X		X		X		
27	¿Al utilizar su cpu o laptop es rápida en realizar sus trabajos?	X		X		X		

28	¿Alguna vez al ingresar a su carpeta de trabajo ha podido ingresar?	X		X		X		
29	¿Alguna vez al abrir documento nunca ha visto caracteres no descifrables?	X		X		X		
30	¿Tenemos protección ante cualquier tipo de ataque Cibernéticos?	X		X		X		
31	¿No realiza apertura de correos no deseados en su bandeja de entrada?	X		X		X		
32	¿No registra apago o paralizacion de pc, laptop por conectar un usb?	X		X		X		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [

]Apellidos y nombres del juez validador. Dr/ Mg: Wilson Ricardo Marín Verástegui dni: 45801046

Especialidad del validador: Investigador

13 de Julio del 2021

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.

[2]**Relevancia:** El ítem es apropiado para representar al componente odimensión específica del constructo

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, esconciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteadosson suficientes para medir la dimensión

Mg.Wilson Ricardo Marín Verastegui

DNI:45801046

ANEXO 10 :CARTA DE PRESENTACION DE LA EMPRESA

UNIVERSIDAD CÉSAR VALLEJO

POSGRADO

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

Lima, 5 de julio de 2021
Carta P. 0547-2021-UCV-VA-EPG-F01/J

Lic.
Leonel Sánchez Aliaga
Gerente General
Empresa Radiadores Fortaleza S.A

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a ALIAGA YUPANQUI, CHRISTIAN ADOLFO; identificado con DNI N° 09913194 y con código de matrícula N° 6500014622; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

Implementación de un Sistema de Ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza, 2021

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador ALIAGA YUPANQUI, CHRISTIAN ADOLFO asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dr. Carlos Venturo Orbegoso
Jefe
ESCUELA DE POSGRADO
UCV FILIAL LIMA
CAMPUS LIMA NORTE

RADIADORES FORTALEZA S.A.

LEONEL SÁNCHEZ ALIAGA
Gerente General

ANEXO 11 :IMPLEMENTACION DE CIBERSEGURIDAD EN EL MARCO BASICO DE LA NIST

N°	Función	Categoría	Subcategoría
1	IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar objetivos de negocio se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de negocio y la estrategia de riesgo de la organización.	**ID.AM-1:** Los dispositivos físicos y los sistemas dentro de la organización son inventariados
2			**ID.AM-2:** Las plataformas de software y las aplicaciones dentro de la organización son inventariadas
3			**ID.AM-3:** La comunicación organizacional y los flujos de datos están mapeados
4			**ID.AM-4:** Se catalogan los sistemas de información externos

N°	Función	Categoría	Subcategoría
5			**ID.AM-5:** Los recursos (por ejemplo, hardware, dispositivos, datos y software) se priorizan en función de su clasificación, criticidad y valor comercial
6			**ID.AM-6:** Se establecen las funciones y responsabilidades de la ciberseguridad para toda la fuerza de trabajo y las partes interesadas de terceros (por ejemplo, proveedores, clientes, socios)
7		**Entorno Empresarial (ID.BE):** Se entiende y prioriza la misión, los objetivos, las partes interesadas y las actividades de la organización; Esta información se utiliza para informar las funciones de ciberseguridad, las responsabilidades y las decisiones de gestión de riesgos.	**ID.BE-1:** El rol de la organización en la cadena de suministro es identificado y comunicado
8			**ID.BE-2:** El lugar de la organización en la infraestructura crítica y su sector industrial se identifica y se comunica
9			**ID.BE-3:** Se establecen y se comunican las prioridades de la

N°	Función	Categoría	Subcategoría
			misión, los objetivos y las actividades de la organización
10			**ID.BE-4:** Se establecen dependencias y funciones críticas para la prestación de servicios críticos
11			**ID.BE-5:** Los requisitos de resistencia para apoyar la prestación de servicios críticos se establecen
12		**Gobernabilidad (ID. GV):** Las políticas, procedimientos y procesos para administrar y monitorear los requerimientos regulatorios, legales, de riesgo, ambientales y operativos de la organización son entendidos e informar a la gerencia del riesgo de ciberseguridad.	**ID. GV-1:** Se establece la política de seguridad de la información organizacional
13			**ID. GV-2:** Las funciones y responsabilidades de seguridad de la información están coordinadas y alineadas con las funciones internas y los socios externos

N°	Función	Categoría	Subcategoría
14			**ID. GV-3:** Los requisitos legales y reglamentarios relativos a la ciberseguridad, incluidas las obligaciones en materia de privacidad y libertades civiles, se entienden y se gestionan
15			**ID. GV-4:** Los procesos de gobernanza y gestión de riesgos abordan los riesgos de la ciberseguridad
16		**Evaluación de riesgos (ID.RA):** La organización entiende el riesgo de ciberseguridad para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y los individuos.	**ID.RA-1:** Se identifican y documentan las vulnerabilidades de activos
17			**ID.RA-2:** La información sobre amenazas y vulnerabilidades se recibe de los foros y fuentes de intercambio de información
18			**ID.RA-3:** Las amenazas, tanto internas como externas, son identificadas y documentadas

N°	Función	Categoría	Subcategoría
19			**ID.RA-4:** Se identifican los posibles impactos y probabilidades de los negocios
20			**ID.RA-5:** Se usan amenazas, vulnerabilidades, probabilidades e impactos para determinar el riesgo
21			**ID.RA-6:** Las respuestas al riesgo son identificadas y priorizadas
22		**Estrategia de Gestión de Riesgos (ID.RM):** Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y utilizan para apoyar las decisiones de riesgo operacional.	**ID.RM-1:** Los procesos de gestión de riesgos son establecidos, gestionados y acordados por las partes interesadas de la organización
23			**ID.RM-2:** La tolerancia al riesgo organizacional se determina y se expresa claramente
24			**ID.RM-3:** La determinación de la organización de la tolerancia al riesgo se basa en su papel en la infraestructura crítica y en el

N°	Función	Categoría	Subcategoría
			análisis de riesgos específicos de cada sector
25	PROTEGER (PR)	**Control de acceso (PR.AC):** El acceso a los activos e instalaciones asociadas está limitado a usuarios, procesos o dispositivos autorizados, ya las actividades y transacciones autorizadas.	**PR.AC-1:** Las identidades y credenciales se administran para dispositivos y usuarios autorizados
26			**PR.AC-2:** El acceso físico a los activos se gestiona y protege
27			**PR.AC-3:** El acceso remoto se gestiona
28			**PR.AC-4:** Los permisos de acceso se gestionan, incorporando los principios del privilegio mínimo y la separación de funciones

N°	Función	Categoría	Subcategoría
29			**PR.AC-5:** La integridad de la red está protegida, incorporando la segregación de red cuando sea apropiado
30		**Sensibilización y Capacitación (PR.AT):** El personal y los socios de la organización reciben educación para la concienciación en ciberseguridad y están adecuadamente capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad de la información, de acuerdo con las políticas, procedimientos y acuerdos relacionados.	**PR.AT-1:** Todos los usuarios están informados y capacitados
31			**PR.AT-2:** Los usuarios privilegiados entienden las funciones y responsabilidades
32			**PR.AT-3:** Terceros interesados (por ejemplo, proveedores, clientes, socios) entienden las funciones y responsabilidades

N°	Función	Categoría	Subcategoría
33			**PR.AT-4:** Los altos ejecutivos entienden roles y responsabilidades
34			**PR.AT-5:** El personal de seguridad física y de la información entiende las funciones y responsabilidades.
35		**Seguridad de datos (PR.DS):** La información y los registros (datos) se manejan de acuerdo con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-1:** Los datos en reposo están protegidos
36			**PR.DS-2:** Los datos en tránsito están protegidos
37			**PR.DS-3:** Los activos se administran formalmente durante la remoción, las transferencias y la disposición
38			**PR.DS-4:** Se mantiene la capacidad adecuada para garantizar la disponibilidad

N°	Función	Categoría	Subcategoría
39			**PR.DS-5:** Las protecciones contra fugas de datos se implementan
40			**PR.DS-6:** Los mecanismos de verificación de integridad se utilizan para verificar el software, el firmware y la integridad de la información
41			**PR.DS-7:** Los entornos de desarrollo y prueba están separados del entorno de producción
42		**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y utilizan las políticas de seguridad (que abordan el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la administración y la coordinación entre las entidades organizacionales), procesos y procedimientos	**PR.IP-1:** Se crea y mantiene una configuración de línea de base de los sistemas de tecnología de la información / control industrial
43			**PR.IP-2:** Se implementa un ciclo de vida de desarrollo de sistemas para gestionar sistemas

N°	Función	Categoría	Subcategoría
44		para administrar la protección de los sistemas y activos de información.	**PR.IP-3:** Los procesos de control de cambio de configuración están en su lugar
45			**PR.IP-4:** Las copias de seguridad de la información se realizan, se mantienen y se prueban periódicamente
46			**PR.IP-5:** Se cumplen las políticas y reglamentos relativos al entorno físico de funcionamiento de los activos de la organización
47			**PR.IP-6:** Los datos se destruyen según la política
48			**PR.IP-7:** Mejora continua de los procesos de protección
49			**PR.IP-8:** La eficacia de las tecnologías de protección se comparte con las partes apropiadas
50			**PR.IP-9:** Planes de respuesta (Respuesta a Incidentes y Continuidad de Negocio) y planes de recuperación (Recuperación de

N°	Función	Categoría	Subcategoría
			Incidentes y Recuperación de Desastres)
51			**PR.IP-10:** Se analizan los planes de respuesta y recuperación
52			**PR.IP-11:** La ciberseguridad se incluye en las prácticas de recursos humanos (por ejemplo, desprovisionamiento, selección de personal)
53			**PR.IP-12:** Se desarrolla e implementar un plan de gestión de la vulnerabilidad
54		**Mantenimiento (PR.MA):** El mantenimiento y las reparaciones de los componentes del control industrial y del sistema de información se realizan de acuerdo con las políticas y procedimientos.	**PR.MA-1:** El mantenimiento y la reparación de los activos de la organización se realizan y registran de manera oportuna, con herramientas aprobadas y controladas.
55			**PR.MA-2:** El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de una manera que evita el acceso no autorizado

N°	Función	Categoría	Subcategoría
56		**Tecnología de Protección (PR.PT):** Las soluciones de seguridad técnica se gestionan para garantizar la seguridad y la resiliencia de los sistemas y activos, de acuerdo con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-1:** Los registros de auditoría / registro son determinados, documentados, implementados y revisados de acuerdo con la política
57			**PR.PT-2:** Los medios extraíbles están protegidos y su uso está restringido según la política
58			**PR.PT-3:** Se controla el acceso a sistemas y activos, incorporando el principio de menor funcionalidad
59			**PR.PT-4:** Las redes de comunicaciones y control están protegidas