UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“LA IMPLEMENTACIÓN DE UN PROTOCOLO DE PREVENCIÓN CONTRA RANSOMWARE PARA OPTIMIZAR LA SEGURIDAD DEL SERVIDOR EN LA EMPRESA BBTI S.A.C ENTRE EL AÑO 2022"

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTORES:

BRYAM, RODAS DÍAZ
JOHAN ALBERTO, SÁNCHEZ ZORRILLA

ASESOR:

MG. JOSE ANTONIO FARFAN AGUILAR

LÍNEA DE INVESTIGACIÓN: INGENIERÍA Y TECNOLOGÍA

CALLAO, 2024
PERÚ

Ouriginal

Document Information

Analyzed document	TESIS - RODAS, SANCHEZ.docx (D181878390)
Submitted	2023-12-14 23:44:00 UTC+01:00
Submitted by	Unidad FIIS
Submitter email	fiis.investigacion@unac.edu.pe
Similarity	6%
Analysis address	fiis.investigacion.unac@analysis.urkund.com

Sources included in the report

SA	**EXAMEN FINAL- PROYECTO DE TESIS 2 -Depaz Ganoza Carlos Enrique-Rojas Benavides Silvia Deifilia.docx** Document EXAMEN FINAL- PROYECTO DE TESIS 2 -Depaz Ganoza Carlos Enrique-Rojas Benavides Silvia Deifilia.docx (D119178079)	1
SA	**Clara Martí Maynés.pdf** Document Clara Martí Maynés.pdf (D168720218)	1
SA	**submission.pdf** Document submission.pdf (D112061942)	4
SA	**Prueba_3_SPSS_Hoja de respuestas_2021.pdf** Document Prueba_3_SPSS_Hoja de respuestas_2021.pdf (D105358082)	1
SA	**Prueba_2_SPSS_Hoja de respuestas_2019.doc** Document Prueba_2_SPSS_Hoja de respuestas_2019.doc (D51827324)	1
SA	**Ejercicio_5_Palencia_Martínez_Ampar.pdf** Document Ejercicio_5_Palencia_Martínez_Ampar.pdf (D89944446)	3
SA	**Prueba 2_Paula_Iglesias.doc** Document Prueba 2_Paula_Iglesias.doc (D27918786)	2
SA	**1579183398_589__Indicaciones_Practica_Calificada-1_Álvarez.docx** Document 1579183398_589__Indicaciones_Practica_Calificada-1_Álvarez.docx (D62514775)	1
SA	**T3 - PROYECTO DE TESIS 2 -Depaz Ganoza Carlos Enrique-Rojas Benavides Silvia Deifilia.docx** Document T3 - PROYECTO DE TESIS 2 -Depaz Ganoza Carlos Enrique-Rojas Benavides Silvia Deifilia.docx (D117601556)	1

Entire Document

UNIVERSIDAD NACIONAL DEL CALLAO
FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

INFORMACIÓN BÁSICA

FACULTAD: **FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS.**

ESCUELA PROFESIONAL: **ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS.**

TÍTULO: **"LA IMPLEMENTACIÓN DE UN PROTOCOLO DE PREVENCIÓN CONTRA RANSOMWARE PARA OPTIMIZAR LA SEGURIDAD DEL SERVIDOR EN LA EMPRESA BBTI S.A.C ENTRE EL AÑO 2022"**

EJECUTORES: **BRYAM RODAS DIAZ**
CÓDIGO ORCID: 0000-0003-0497-8666
DNI: 77224744

JOHAN ALBERTO SÁNCHEZ ZORRILLA
CÓDIGO ORCID: 0009-0008-3204-0767
DNI: 47378945

ASESOR: **MG. JOSE ANTONIO FARFAN AGUILAR**
CÓDIGO ORCID: 0000-0003-1615-5608
DNI: 08144446

LUGAR DE EJECUCIÓN: **LA EMPRESA BBTI S.A.C. UBICADA EN EL DISTRITO DE CALLAO**

UNIDAD DE ANÁLISIS: **LA EMPRESA BBTI S.A.C ÁREA DE SISTEMAS**

TIPO DE INVESTIGACIÓN: **APLICADA, EXPLICATIVA**

ENFOQUE INVESTIGACIÓN: **CUANTITATIVO**

DISEÑO INVESTIGACIÓN: **EXPERIMENTAL**

TEMA OCDE: **INGENIERÍA Y TECNOLOGÍA**

ACTA DE SUSTENTACIÓN

LIBRO 001 FOLIO Nº 011-2024 ACTA DE SUSTENTACIÓN DE TESIS Nº 011-2024
SUSTENTACIÓN DE TESIS Nº 011-2024 -UIFIIS-UNAC DEL 06.01.2024
ACTA DE SUSTENTACION POR MODALIDAD CON CICLO TALLER DE TESIS
PARA LA OBTENCIÓN DEL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS

Siendo las 14.10 horas del día 06 de Enero del año 2024, encontrándose reunidos en el Auditórium de la FIIS, el **Dr. ENRIQUE GARCÍA TALLEDO**, en representación de la Rectora de la UNAC; el **JURADO DE SUSTENTACIÓN DE TESIS** (designado por resolución **002-2024-CF-FIIS**)de la Facultad Ingeniería Industrial y de Sistemas de la Universidad Nacional del Callao, para la evaluación de las Tesis que conllevan a la obtención del Título Profesional de **INGENIERO DE SISTEMAS**, el que se encuentra conformado por los siguientes docentes ordinarios:

PRESIDENTE	**MG. MANUEL ABELARDO ALCÁNTARA RAMÍREZ**
SECRETARIO	**MG. ANGELINO ABAD RAMOS CHOQUEHUANCA**
VOCAL	**MG. JESÚS JOSÉ BRINGAS ZÚÑIGA**
SUPLENTE	**MG. YESMI KATIA ORTEGA ROJAS**

Con el quórum reglamentario de ley y de conformidad con lo establecido por el Reglamento de Grados y Títulos vigente se dio Inicio al Acto de Sustentación de la Tesis de los Bachilleres: **SÁNCHEZ ZORRILLA JOHAN ALBERTO, RODAS DÍAZ BRYAM** quienes, habiendo cumplido con los requisitos para optar el Título Profesional de **INGENIERO DE SISTEMAS**, sustentan la tesis titulada **"LA IMPLEMENTACIÓN DE UN PROTOCOLO DE PREVENCIÓN CONTRA RANSOMWARE PARA OPTIMIZAR LA SEGURIDAD DEL SERVIDOR EN LA EMPRESA BBTI S.A.C ENTRE EL AÑO 2022"**, cumpliendo con la sustentación en acto público, de manera presencial.

Luego de la exposición, y de la absolución de las preguntas formuladas por el Jurado de Sustentación y efectuadas las deliberaciones pertinentes, **SE ACORDÓ**: Dar por **APROBADO** con la escala de calificación cuantitativa **(17)** y calificación cualitativa **(Muy Bueno)** a la presente tesis, conforme a lo dispuesto en el Art. 24 del Reglamento de Grados y Títulos de la UNAC, aprobado por Resolución de Consejo Universitario Nº 150-2023-CU del 15 de junio del 2023.

Se dio por concluida la Sesión a las 14.40 horas del día 06 de enero del 2024.

MG. MANUEL ABELARDO ALCÁNTARA RAMÍREZ
Presidente

MG. ANGELINO ABAD RAMOS CHOQUEHUANCA
Secretario

MG. JESÚS JOSÉ BRINGAS ZÚÑIGA
Vocal

MG. YESMI KATIA ORTEGA ROJAS
Suplente

INFORME Nº 011-2024 – JS ICTTS

PARA : **DR. PAUL GREGORIO PAUCAR LLANOS**
DECANO FIIS

DE : **JURADO DE SUSTENTACIÓN DEL I CICLO TALLER DE TESIS DE INGENIERÍA DE SISTEMAS**

ASUNTO : **INFORME FAVORABLE DEL JURADO DE SUSTENTACION**

FECHA : **Callao, 06 de enero del 2024**

Los miembros del Jurado de Sustentación designados por **Resolución Nº 002-2024-CF-FIIS** y de acuerdo al Reglamento de Grados y Títulos, aprobado por Resolución 150-2023-CU del 15 de junio de 2023 Art. 71, visto el Acta de Sustentación **Nº 011-2024 – JS ICTTS** de Tesis Titulada: **"LA IMPLEMENTACIÓN DE UN PROTOCOLO DE PREVENCIÓN CONTRA RANSOMWARE PARA OPTIMIZAR LA SEGURIDAD DEL SERVIDOR EN LA EMPRESA BBTI S.A.C ENTRE EL AÑO 2022"**

Presentado por:
SÁNCHEZ ZORRILLA JOHAN ALBERTO
RODAS DÍAZ BRYAM

Para obtener Título de Profesional de **INGENIERO DE SISTEMAS**, por modalidad de Tesis con Ciclo Taller de Tesis, habiendo obtenido nota aprobatoria de (17) diecisiete, Muy Bueno.

En tal sentido, los miembros del Jurado de Sustentación informan que no existe observación alguna a dicha Tesis por lo que se da la **CONFORMIDAD**, lo cual se debe comunicar a los interesados.

Sin otro particular reiteramos los sentimientos y estima personal.

MG. MANUEL ABELARDO ALCANTARA RAMÍREZ
Presidente

MG. ANGELINO ABAD RAMOS CHOQUEHUANCA
Secretario

MG. JESÚS JOSÉ BRINGAS ZÚÑIGA
Vocal

MG. YESMI KATIA ORTEGA ROJAS
Suplente

DEDICATORIA

Los presentes autores dedicamos este trabajo a nuestros seres queridos, que son una fuente inagotable de apoyo y inspiración. A nuestra familia, por su amor incondicional y por ser mi sostén en cada paso de este camino académico. A mis amigos, por sus ánimos constantes y por compartir conmigo este viaje lleno de desafíos y

AGRADECIMIENTO

Los autores del presente trabajo queremos expresar nuestro profundo agradecimiento a la Universidad Nacional del Callao, por brindarnos la oportunidad de formarnos en la Facultad de Ingeniería Industrial y de Sistemas. Este recorrido ha sido una experiencia enriquecedora que ha contribuido significativamente a nuestro crecimiento personal y profesional.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En el cambiante entorno del mundo empresarial actual, la seguridad de la información se erige como uno de los pilares para el funcionamiento óptimo de las organizaciones. ¿Pero qué pasaría en el caso con las empresas pequeñas donde no cuentan con los recursos y conocimientos necesarios para la ciberseguridad? En el presente proyecto de investigación, la empresa BBTI S.A.C., dedicada al desarrollo y fabricación de paneles y tableros eléctricos en la industria eléctrica, ha experimentado desafíos significativos en los últimos años. La necesidad fundamental de salvaguardar su información en los servidores se ha visto comprometida en múltiples ocasiones con amenazas cibernéticas, en específico, los ataques de ransomware.

Este presente trabajo de investigación busca abordar una problemática que aqueja la integridad y continuidad operativa de la empresa BBTI S.A.C. A lo largo de los últimos tres años, ha sufrido ataques de ransomware que han dejado daños críticos en la seguridad de sus servidores. El tipo de investigación de la presente investigación fue aplicada explicativa, además de aplicar un diseño de investigación experimental, se aplicó una encuesta a una muestra de 23 personas de una de sus sedes, mediante pruebas estadísticas se contrasto la hipótesis, se utilizó la prueba de Shapiro-Wilk, Spearman y ANOVA comprobando la relación entre las variables.

Finalmente, los resultados obtenidos fueran satisfactorios ya que se logró comprobar que la implementación de un protocolo de prevención contra ransomware está relacionada directamente con el nivel de seguridad del servidor, concluyendo que la implementación de un protocolo de prevención contra ransomware mejora los resultados que tendremos en la seguridad del servidor.

Palabras clave:

seguridad de la información, ciberseguridad, ransomware, servidores, protocolo de prevención, ataques, pérdida de archivos, continuidad operativa

ABSTRACT

In the changing environment of today's business world, information security stands as one of the pillars for the optimal functioning of organizations. But what would happen in the case of small companies where they do not have the necessary resources and knowledge for cybersecurity? In this research project, the company BBTI S.A.C., dedicated to the development and manufacturing of electrical panels and boards in the electrical industry, has experienced significant challenges in recent years. The fundamental need to safeguard your information on servers has been compromised on multiple occasions with cyber threats, specifically ransomware attacks.

This present research work seeks to address a problem that affects the integrity and operational continuity of the company BBTI S.A.C. Over the past three years, it has suffered ransomware attacks that have left critical damage to the security of its servers. The type of research of this research was applied explanatory, in addition to applying an experimental research design, a survey was applied to a sample of 23 people from one of its headquarters, through statistical tests the hypothesis was contrasted, the test of Shapiro-Wilk, Spearman and ANOVA checking the relationship between the variables.

Finally, the results obtained were satisfactory since it was possible to verify that the implementation of a prevention protocol against ransomware is directly related to the security level of the server, concluding that the implementation of a prevention protocol against ransomware improves the results that we will have in mind. server security.

Keywords:
Information security, cybersecurity, ransomware, servers, prevention protocol, attacks, files loss, operational continuity

INTRODUCCION

La presente tesis titulada “La implementación de un protocolo de prevención contra ransomware para optimizar la seguridad del servidor en la empresa BBTI S.A.C. entre el año 2022". En este contexto, la empresa BBTI S.A.C. que, a lo largo de los últimos años, ha experimentado en primera persona de manera recurrente ataques de ransomware, secuestrando la información del servidor y comprometiendo la integridad y disponibilidad de su información, afectando la continuidad operativa de los trabajadores, sino también generando pérdidas significativas.

El modus operandi de estos ataques implica el cifrado de la información encontrada seguido de la exigencia de un rescate para su “liberación”. La falta de implementación de medidas de seguridad adecuadas y la vulnerabilidad ante prácticas de ingeniería social han situado a BBTI S.A.C. en una posición de riesgo constante dando como ejemplo los incidentes más críticos ocurrieron en los años 2019, 2021 y 2022, donde se experimentó pérdidas significativas de archivos, documentación y bases de datos. En el peor de los casos, en 2021, el ataque de ransomware paralizó las operaciones de BBTI S.A.C. durante dos semanas, afectando el 100% de la base de datos de Recursos Humanos y entre el 40% y 50% de las demás bases de datos y la información encriptada del servidor.

El presente estudio se propone abordar esta realidad problemática a través de la implementación de un protocolo de prevención contra ransomware. La investigación se enfocará en determinar cómo esta medida no solo fortalece la resistencia ante ataques, sino también mejorar el tiempo de recuperación y reduce las brechas de seguridad en la infraestructura informática de BBTI S.A.C. Se busca proteger la información crítica de la empresa, y fortalecer la cultura de ciberseguridad en la organización. El presente estudio busca contribuir a la mitigación de riesgos y al fortalecimiento de la empresa BBTI S.A.C. frente a las crecientes amenazas. La implementación exitosa de un protocolo de prevención contra ransomware no solo protegerá los activos digitales de la empresa, sino que también sentará las bases para un entorno empresarial más seguro y sostenible en el futuro.

I. PLANTEAMIENTO DEL PROBLEMA.

1.1. Descripción de la realidad problemática.

El aumento de los ataques de ransomware a servidores corporativos se ha convertido en un problema creciente en el mundo de la ciberseguridad. Estos ataques de ransomware tienen como objetivo secuestrar los datos de una empresa, cifrarlos y exigir un rescate económico por su liberación, que en muchos casos equivale a cantidades exorbitantes de bitcoins.

Los ataques de ransomware pueden ocurrir por varias causas. Una de las principales causas es la falta de implementación de seguridad en los sistemas informáticos corporativos.

Una empresa puede estar en riesgo si no cuenta con medidas de seguridad actualizadas, como instalar parches de seguridad, usar contraseñas seguras y protegerse contra malware.

Otra causa común de ataques de ransomware es la falta de concienciación sobre la seguridad entre los empleados de la empresa. Si los empleados no prestan atención a las prácticas de ciberseguridad, podrían hacer clic en enlaces maliciosos, descargar archivos infectados o comprometer la seguridad de la empresa de otras maneras.

Además, los ataques de ransomware también pueden ocurrir debido a la falta de copias de seguridad de los datos: si una empresa no tiene un sistema de copia de seguridad de los datos adecuado y controlado, podría perder todos sus datos en caso de un ataque de ransomware.

Hoy en día a nivel global se viene presentando un incremento en los casos de ataques cibernéticos en varios países del mundo empezando desde 2012 y teniendo su boom en el año 2020, esto se da a partir de un gran número de casos que se hacen públicos donde muchos comparten el tema en común de que se llega a afectar a la

disponibilidad, confidencialidad e integridad de la información de las personas u organizaciones. Entre estos casos se puede mencionar el caso de Pipeline Company uno de los principales proveedores de combustible del sureste de EE.UU. que debido al ataque de ransomware provocó no solo pérdidas económicas para la empresa sino también escasez y pánico entre los consumidores de gasolina del sureste de EE.UU. (Harán, 2021)

El reciente informe de un ataque de un ransomware ocurrido en España a un Servicio Público de empleo Estatal (SEPE) que llegó a afectar a sus servidores, Género lo que es una restricción de accesos a la información por parte de los trabajadores y a los usuarios en marzo del 2021, afectando a múltiples empresas y usuarios que dependían de sus servicios para la búsqueda y contratación de empleos, prestaciones y otras áreas relacionadas, para el proceso de recuperación según lo mencionado por el artículo por el rescate de la información y liberación del control se exigió por parte de los hackers un rescate de 3 millones de euros en bitcoins , se tuvo que trabajar semanas para recuperar datos bloqueados, este ataque es considerado uno de los más grande impacto en la sociedad. (Jose Mendiola Zuriarrain, 2021)

Uno de los ataques de ransomware más conocidos en España, se realizó un ataque a nivel masivo de las empresas incluido el Ministerio de Justicia, que llegó a afectar varios archivos y datos importantes, el impacto generado por ello fue muy grande, retrasando los registros civil y registros de información judicial , poniendo en riesgo los datos personales de los ciudadanos y empresas afectadas, En general, este artículo destaca la importancia de la ciberseguridad y la necesidad de tomar medidas preventivas para protegerse contra posibles ataques de ransomware y otras amenazas cibernéticas. (Jose Mendiola Zuriarrain, 2021)

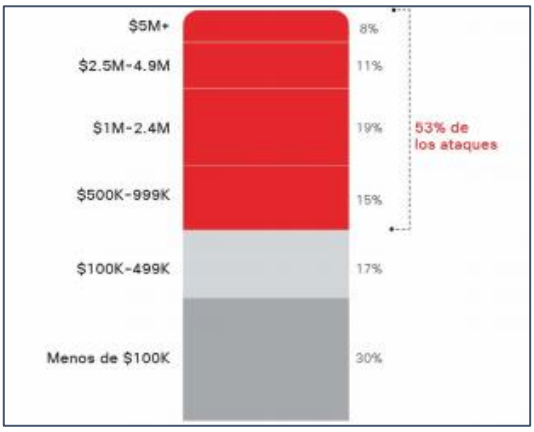
Según Redacción Tecnosfera, (El Tiempo Casa Editorial, 2019) los ataques de malware o código malicioso aumentó en un 13 por ciento en el año 2019 con respecto al año anterior, presentando así 6 de estos

ataques por minuto en los celulares en toda América Latina. Según el informe se indica un reporte de la firma de ciberseguridad de Kaspersky que revela un total de 1300 millones de ataques de malware en toda la región.

Según un reporte hecho por el equipo de ESET-security-report-LATAM (Eset, 2019) en el año 2018, el 61% de las empresas de Latinoamérica, del total de 3000 que fueron recolectados sus datos, sufrió por lo menos un incidente de seguridad, siendo la infección por códigos maliciosos el más recurrentes, 2 de cada 5 empresas sufrieron este tipo de malware. En el mismo reporte, se indica que más de la mitad de estos incidentes está relacionada con el tipo de ataque conocido como ransomware, lo que quiere decir que por lo menos 1 de cada 10 empresas encuestadas del total en toda Latinoamérica sufrió el secuestro de su información. En el área de controles y prevención de riesgos, el 50% del total de empresas encuestadas cumplen con las medidas elementales básicas como una solución de seguridad (antivirus), un backup y una solución de firewall, los que nos indica que la mitad de estas empresas no tienen una cultura de seguridad de la información al no tener una de estas medidas elementales básicas de seguridad.

Según Cisco (Cisco, 2018) , el 53% de los ataques que se dieron en el año 2018, resultaron en daños de $500000 o más de un total de 3600 de organizaciones en 26 países.

Figura 1: Estudio de Referencia de las capacidades de seguridad de cisco 2018



Fuente: (Cisco, 2018)

La realidad del ransomware a nivel de nacional según el diario Gestión (Rojas, 2019) ,la transformación digital ha ayudado a las empresas a impulsar sus negocios exponencialmente, posibilidad que antes no tenían, pero debido a esto, se presentan nuevos escenarios complicados para estas empresas, la ciberseguridad cada vez más aumenta la dependencia de las empresas a los sistemas informáticos. Entre abril y septiembre del 2019, las empresas peruanas sufrieron más de 3000 millones de intentos de ataques informáticos, la mayor parte de estos ataques se dieron en compañías del sector financiero. En dicho portal se indicó que los ataques de ingeniería social a través de correos electrónicos son los más frecuentes con el objetivo de ingresar a los sistemas informáticos de la empresa.

En otro artículo en el mismo diario Gestión (Rojas, 2019) , se hace relevancia a la relación de la ciberseguridad con la inversión que hace una empresa en esta área, en la cuales muchas veces las compañías se enfocan en comprar tecnología dejando de lado las políticas y planes para gestionar la seguridad de la información. En el portal se indica que según un reporte de seguridad en Latinoamérica hecho por Eset, en el Perú solo un 8% de las compañías clasifican su información de la organización y otro 17% tienen un plan de continuidad para el negocio en caso de posibles imprevistos.

Con respecto a la realidad problemática de la empresa en la que se tratara el proyecto, se podría mencionar que actualmente la empresa BBTI S.AC. es una de las empresas dedicada al desarrollo y creación de paneles y tableros eléctricos de la industria eléctrica, es una empresa comprometida con la calidad, innovación y seguridad. Para lograr un adecuado funcionamiento de la empresa BBTI S.A.C. depende principalmente de sus planos, diseños y modelos, es decir de la información almacenada en sus servidores pero de acuerdo a los reportes recientes mostrado por el departamento de sistemas y redes se muestra que en los últimos 3 años la empresa pasó por problemas graves de ataques de malware principalmente los del tipo ransomware dando como los ataques más resaltantes del año 2019 , 2021 y 2022 ,donde en cada año se generó un daño considerable,

teniendo pérdidas de los tanto de la documentación como la de la base de dato, se tuvo en el 2019 una pérdida de un 15% de los archivos almacenados, entre ellos planos, documentación , y base de datos, el año 2021 se registró el peor daño en la empresa, por una lado se sufría el secuestro de la información y se exigía un rescate por dicha, unos 18 unid de bitcoins, por el otro lado se tuvo como perdida un total entre un 40% y 50% de archivos ,como resultado final el daño recibido en pérdidas fue el 100% de la base de datos de RR.HH. y un 30% de las base de datos restantes y dejando a la empresa inoperativa por 2 semanas debido a la necesidad de restauración de las base de datos y archivos, en el año 2022 se sufrió otro ataque de ransomware y se llegó a implementar una beta de protocolo para determinados casos, los resultados finales se obtuvieron en pérdida de archivos de 3% debido a falta de mejoras en la beta y una semana de base de datos y el tiempo total de recuperación fue de 4 días, notándose una reducción considerable de las pérdidas, posterior a ello y lo aprendido se comenzó a replantear y mejorar lo que es un protocolo para dichos incidentes.

1.2. Formulación del problema

1.2.1. Problema general

¿De qué manera la implementación de protocolo de prevención contra ransomware mejora la seguridad de la empresa BBTI S.A.C.?

1.2.2. Problemas específicos

a. ¿De qué manera la implementación de protocolo de prevención contra ransomware mejora la resistencia ante ataques de ransomware en la empresa BBTI S.A.C.?
b. ¿De qué manera la implementación de protocolo de prevención contra ransomware mejoraría el tiempo de recuperación de ataques de ransomware en la empresa BBTI S.A.C.?

c. ¿De qué manera la implementación de protocolo de prevención contra ransomware se mejoraría la reducción la brecha de seguridad en la empresa BBTI S.A.C.?

1.3. Objetivos

1.3.1. Objetivo general

Determinar que la implementación de un protocolo de prevención contra ransomware mejora la seguridad del servidor de la empresa BBTI S.A.C.

1.3.2. Objetivos específicos

a. Determinar que la implementación de protocolo de prevención contra ransomware mejora la resistencia ante ataques de ransomware en la empresa BBTI S.A.C.
b. Determinar que la implementación de protocolo de prevención contra ransomware mejora el tiempo de recuperación de ataques de ransomware en la empresa BBTI S.A.C.
c. Analizar que la implementación de protocolo de prevención contra ransomware mejora la reducción de brechas de seguridad de la empresa BBTI S.A.C.

1.4. Justificación

1.4.1. Legal

La presente investigación se justifica en base a las siguientes normas:

La norma ISO 27001 que se establece respecto a la gestión de la seguridad de la información ya que el presente trabajo busca aplicar medidas de prevención antiransomware y proteger activos de información Normativa de Gestión de la seguridad de la información y ciberseguridad que buscara respetar los pilares de la ciberseguridad de integridad al salvaguardar la data en óptimas condiciones sin alteraciones, confidencialidad de que únicamente personas autorizadas puedan tratar la información y la disponibilidad de garantizarla cuando se

requiera a su vez que buscara mitigar los riesgos y apoyar a la recuperación respecto a los incidentes ocurridos.

1.4.2. Teórica

La presente investigación permitirá ampliar el conocimiento existencial sobre las medidas de seguridad existentes, así mismo concientizar a los usuarios tanto de la carrera de ingeniería de sistemas como personal con conocimientos básicos de los que es la protección o seguridad de la información tanto su data como al momento de elegir el protocolo necesario y efectivo de acuerdo a las necesidades de la empresa. Dicha contribución aplicara tanto para estudiantes, profesionales y empresas que busquen una manera mejorar la protección de los servidores de la empresa

1.4.3. Tecnológica

Con el resiente boom tecnológico tanto de driver como software en el aprovechamiento de avances tecnológicos se podría implementar como la mejora de la infraestructura de seguridad, así como la adopción de mejores prácticas tecnológicas. Dichos procesos y acciones tecnológicas son esenciales para fortalecer la seguridad del servidor y proteger los datos críticos de la empresa contra los ataques de ransomware y a su vez que se mejora el nivel tecnológico y se coloca a la empresa en la vanguardia

1.4.4. Económica

Se sabe que el ataque a un servidor conlleva pérdidas económicas, desde la perdida data, la necesidad de pagar el secuestro y la inactividad de los usuarios a falta de un servidor para procesar y usa la información a trabajar

II. MARCO TEÓRICO

2.1. Antecedentes:

Se presenta a continuación el contexto histórico del trabajo de investigación realizado permitiendo tener una visión más clara y precisa del tema de investigación a realizar. En esta parte se describen y analizan las investigaciones previas relacionadas con el tema de investigación, realizados tanto en el país como en el extranjero.

2.1.1. Internacionales.

El primer antecedente internacional está desarrollado el autor (Fuentes, 2023) que sustento con la tesis “Técnicas de análisis forense para la evaluación de la privacidad e integridad de la información: navegadores web y ataques de ransomware” por el título de doctorado en investigación en tecnología de la investigaciones la Universidad de Santiago de Compostela cuyo objetivo de la tesis es brindar una mejor perspectiva a los usuario y organizaciones de las amenazas y formas de protegerse sobre los navegadores web en su modo privado evaluando su eficacia. La metodología es aplicada experimental, la muestra que llega a tomar son los navegadores web como Google Chrome, Brave, Mozilla Firefox y Tor Browser, entre otros, ejecutando en diversos entornos y evaluando su código, Los instrumentos a usar fueron las encuestas Los resultados demuestran que la aplicación del modo anónimo cuenta con fugas de información y riegos de infección casi similares al estándar que se llega a trabajar, destaca la importancia de comprender las amenazas digitales.

El segundo antecedente internacional está desarrollado por el autor (Trevejo, 2022) que sustento la tesis con el título "Mejora de la Continuidad de Negocio en Cloud Computing: Estrategias para Proteger Datos en Caso de Ataques de Ransomware" en la Universidad Europea cuyo objetivo de la tesis es diseñar una

estrategia con la necesidad de proteger los sistemas operativos de Windows server 2012r2 en adelante de la amenaza de ransomware.

La metodología es practica y experimental, la muestra se compone de organizaciones que servidores SQL 2012r2 en adelante. Los instrumentos a usar son encuestas para realizar la medición de los resultados, Los resultados demuestran que se obtiene mejoras de nivel en comparación del enfoque tradicional y demuestra una protección más eficaz ante otras metodologías siempre y cuando se cumplan las normas de perímetro propuestas.

El tercer antecedente internacional está desarrollado por el autor (chow Zamora, 2018) sustentó la tesis con el título "Prevención de ataques de Ransomware conocidos en redes informáticas, utilizando la tecnología Check Point Sandblast en el perímetro y en usuarios finales comprendido en el periodo de septiembre del 2017 a abril del 2018" en la Universidad Nacional Autónoma de Nicaragua su objetivo es desarrollar una propuesta de seguridad para empresas grandes y medianas que buscan mejorar su seguridad perimetral y mitigar amenazas de Ransomware, incluyendo tanto los casos conocidos como los avanzados. La metodología aplicada es experimental, la muestra a usar para dicho trabajo de investigación fue hipotética debido a que el autor se refiere a los sistemas y elementos de red dentro del entorno virtual utilizado para las demostraciones y pruebas. Los instrumentos utilizados en este trabajo son las encuestas para medir la tecnología Check Point Sandblast, que se implementa en un entorno virtual. Los resultados son la demostración de la eficacia de Check Point Sandblast en la resolución de casos conocidos y avanzados de Ransomware.

2.1.2. Nacionales

El primer antecedente nacional está desarrollado por los autores (Perez Diaz , 2021) sustentaron la tesis con el título “Implementación de Tecnología Sandbox para Proteger de Ataques Ransomware en una Red Informática Local de una Entidad Financiera” en la Universidad Señor de Sipán su objetivo es la implementación de Cuckoo Sandbox, una herramienta de código abierto para el análisis de Ransomware, con el propósito de contribuir a la seguridad perimetral de la red informática. La metodología aplicada es experimental. La muestra a usar consiste en el laboratorio de pruebas virtualizado con 5 equipos Windows 10, que simula una red informática similar a la de la Coopac Norandino Ltda. Los instrumentos utilizados son Cuckoo Sandbox y el Servidor torre Core i5 con 16 gb de RAM con Ubuntu 20.04 LTS como plataforma de implementación de Cuckoo Sandbox. Los resultados demuestran que Cuckoo Sandbox es efectivo en la contribución a la seguridad perimetral de la red informática al detectar y aislar Ransomware de manera eficaz en un entorno de laboratorio.

El segundo antecedente nacional está desarrollado por la autora (Chira Castillo, 2021) sustentó la tesis con el título “Implementación de un plan de control y seguridad de los activos de información en la Estación de Servicios San José” en la Universidad César Vallejo su objetivo general es Implementar un plan de control y seguridad basado en la metodología Cobit para la mejora de los activos de información en la Estación de Servicios San José. La metodología se llevó a cabo mediante una investigación de tipo cuasi experimental con un solo grupo. La muestra que han considerado son 13 personas, que incluía al gerente y al personal de la estación de servicios. Los instrumentos que se utilizaron para recopilar

datos fueron cuestionarios sobre aceptación del plan de control, cuestionarios sobre eficiencia en la toma de decisiones y guías de observación. Los resultados indican una reducción significativa en los errores de facturación, una menor frecuencia de caídas del servidor, un mejor control en la emisión de vales y una aceptación favorable por parte del personal. Además, la gerencia pudo tomar decisiones más eficientes gracias a la implementación del plan. Estos hallazgos respaldan la eficacia del plan de control y seguridad en la mejora de la gestión de activos de información en la estación de servicios.

El tercer antecedente nacional está desarrollado por los autores (Vasquez Gutierrez, 2019) sustentó la tesis con el título "Propuesta de plan de seguridad informática para la sub gerencia de tecnología de la información de la municipalidad provincial de requena, en el año 2019" en la Universidad San Juan bautista su objetivo es establecer un Plan de Seguridad Informática que incluya políticas y medidas de seguridad para proteger los activos informáticos de la Municipalidad Provincial de Requena y minimizar los riesgos de seguridad, tanto internos como externos. La metodología aplicada es experimental. La muestra es el personal que labora en la Municipalidad Provincial de Requena especialmente aquellos que manejan recursos informáticos. Los instrumentos son un diagnóstico situacional, que se utiliza para evaluar la situación actual y detectar problemas y riesgos en el entorno informático de la organización, lo que luego se convierte en la base para la elaboración de un plan de seguridad informática. Los resultados son la identificación de riesgos y problemas de la infraestructura tecnológica y un Plan de Seguridad Informática que incluye propuestas de seguridad, buenas prácticas y recomendaciones para abordar los problemas identificados.

2.2. Bases teóricas.

2.2.1 Seguridad de la información.

Según el autor Godoy en el año 2014 afirmo que La Seguridad de la información tiene como objetivo proteger la información y los sistemas de la información contra el acceso, uso, divulgación, interrupción o destrucción no autorizada; la seguridad es un concepto relacionado con la certeza, falta de riesgo o contingencia; se puede comprender como seguridad, un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Todo lo que pueda tener un impacto directo o consecuencias se considera un peligro o daño. Además, se indica que es el conjunto de medidas preventivas y reactivas implementadas por las organizaciones y los sistemas tecnológicos para resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. (Godoy, 2014) Pag 164

Según la Norma ISO 27001:2013 ISO La seguridad de información, previene a la información de una gama amplia de amenazas, con el fin de garantizar la continuación del negocio, minimizando el daño del mismo y maximizando el retorno de las inversiones y nuevas posibilidades. Asimismo, considera la existencia de la información en varias formas como; impresa o escrita en papel, recolectada electrónicamente, transmitida por un medio electrónico, presentada en imágenes, o expuesta en una conversación. Cuales quiera que sea la forma que tiene la información, o los medios por los cuales se distribuye o centraliza (almacenamiento), debe ser protegida y resguardada siempre de una forma adecuada a fin de preservar la confidencialidad, integridad y disponibilidad términos que constituyen la base sobre la que se cimienta todo el edificio de

seguridad de la información. Además, desde una perspectiva de gestión de riesgos empresariales, es necesario emplear un proceso sistemático que esté bien documentado y comprendido en toda la organización para garantizar que la seguridad de la información se gestione adecuadamente. Un SGSI se compone de este proceso. (27001:ISO, 2013)

Según lo que menciona el autor Pallas en su tesis para optar el titulo Magister en su tesis de la universidad de la República (Uruguay). El pilar primordial de cualquier sistema de seguridad de información o método de gestión de riesgo y de la propia norma ISO/IEC 27001, es la trilogía conformada por confidencialidad, integridad y disponibilidad, debiendo enmarcarse en el entorno del negocio, la estrategia organizacional y del marco legal, asimismo, señala que la
La seguridad de la información es más importante que cualquier otro factor en un negocio de representación estratégica, por lo que debe primar sobre un criterio de mejora costo-beneficio que minimice los riesgos para maximizar el logro de objetivos y alinearse con las prioridades organizacionales. (Mega, 2009)(pag 19-22).

2.2.1.1. Los tres pilares de la seguridad.

Los datos son valores, números, medidas, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento. Los manuales de procedimientos, los datos de los empleados, de los proveedores y clientes de la empresa, la base de datos de facturación son datos estructurados de tal forma que se convierten en información, que aportan valor como compañía. La base de la seguridad de la información está en la necesidad de todos de obtener información, así como su importancia, integridad y disponibilidad,

para maximizar el rendimiento y minimizar el riesgo. (Vergara Quiroz, 2017)

a) **Disponibilidad**

La disponibilidad en la seguridad de la información según Vergara (Vergara Quiroz, 2017) definido como la característica de la información es su capacidad de mantenerse disponible para cualquier persona que debe acceder a ella, ya sea mediante autorizadas personas o sistemas de información, garantizando de este modo el acceso adecuado a la información, cumpliendo así el acceso confiable y oportuno a la información.

La disponibilidad en la seguridad de la información debe cumplir con la capacidad de que, en cualquier sistema de información, solo sea accedido, además de ser utilizable, por personas autorizados cuando estos lo requieran, siendo así una condición que debe cumplir la información para estar a disposición por estos. (Anchatipán, 2015)

b) Integridad

Se define la integridad en la seguridad de la información según Vergara (Vergara Quiroz, 2017) asegurando de este modo la exactitud de la información tal cual fue obtenida, la calidad tiene como objetivo mantener la información fuera de modificaciones no autorizadas de usuarios ajenos en una organización, impidiendo así la manipulación por estos agentes externos. La integridad garantiza que la información sea precisa y confiable.

Según Anchatipán (Anchatipán, 2015), En cuanto a cualquier sistema de información, la integridad es

una carácter necesario para que la información perteneciente an esto no sea modificada, evitando así que se produce alguna manipulación no autorizada y permitiendo así la preservación de la información original.

c) **Confidencialidad**

La confiabilidad en la seguridad de la información según Sánchez (Sánchez, 2017) es uno de los pilares más cruciales para el desarrollo económico de una organización. Como tal, es necesario proporcionar el más alto nivel de privacidad para evitar cualquier tipo de filtración de información confidencial. Una forma de lograrlo es mediante el uso de diversas técnicas de cifrado de datos para evitar fugas o acceso no autorizado a información confidencial dentro de una organización.

La cualidad que evita la fuga de información sensible o no sensible a personas ajenas a la organización se conoce como confidencialidad; evitando así la fuga de estas personas y garantizando que únicamente las personas autorizadas puedan acceder a ella. La pérdida de confidencialidad podría causar serios problemas a la empresa. (Vergara Quiroz, 2017)

Según define Anchatipán (Anchatipán, 2015), la confidencialidad de la información es el atributo que debe tener cualquier sistema de información para que pueda ser obtenido únicamente por personal autorizado de la organización, impidiendo así el acceso a contenidos reservados o sensibles por parte de usuarios ajenos a la organización.

2.2.2. Vulnerabilidades

Según múltiples autores se llega a definir Las vulnerabilidades por lo general como fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso. Cuando se habla de recursos de información, es común decir que una vulnerabilidad es una falla de diseño del sistema, un sistema desactualizado o un sistema mal configurado que le da a un agente externo acceso a recursos o información que el sistema administra sin la autorización necesaria. Dependiendo del tipo de recurso que estemos discutiendo, existen varias fuentes de información donde se pueden encontrar vulnerabilidades relevantes para los sistemas considerados. (Romero Castro, y otros, 2018) Pag 30

2.2.3. Ley del mínimo privilegio

Según múltiples autores se llega a definir como que cualquier sistema organizativo, de reparto de tareas y responsabilidades se debe tener claro que no todo el mundo tiene porque acceder a todos los recursos de la organización, ni tiene que hacerlo de forma permanente. Cada individuo y cada herramienta debe acceder solo a aquello imprescindible para el desempeño de sus funciones, sabiendo a lo que se puede acceder y a lo que no, hay que decidir qué se puede hacer con la información o recursos a los que se tiene acceso, a esto se le denomina privilegios y permisos. Los privilegios son permisos de actuación que un usuario, sea una persona o un sistema tiene para actuar sobre otros recursos. (Romero Castro, y otros, 2018) Pag 32

2.2.4. Implementación de un protocolo de seguridad

Se define por implementación de un protocolo de seguridad el establecer y ejecutar un conjunto de procedimientos destinados a proteger la información y sistemas de una empresa.

En las áreas de informática y telecomunicación, un protocolo de comunicaciones se refiere a un sistema de regulaciones que facilitan la comunicación entre dos o más entidades de un sistema de comunicación para intercambiar información mediante cualquier tipo de variación de una magnitud física. Estándar o reglas que establecen la sintaxis, semántica y sincronización de la comunicación, además de los posibles métodos de recuperación de errores, son lo que se trata de. (Ramos Zapana, 2017)

2.2.5. Actualizaciones y parches

Las actualizaciones suelen ser mejoras en un sistema y corrección de errores mientras que los parches son soluciones a brechas de seguridad para proteger un software y sistemas contra amenazas potenciales.

Uno de los requisitos más importantes para que una organización cumpla con los estándares de seguridad es actualizar sus sistemas operativos y aplicaciones. Las organizaciones son el objetivo principal de los piratas informáticos cuando tienen sistemas operativos y software obsoletos, que a menudo tienen fallas de seguridad o vulnerabilidades que permiten que un atacante se aproveche de ellos. (Meza Montoya, y otros, 2018)

2.2.6. Controles de seguridad

Por controles de seguridad podemos detallar que son medidas que se implementan en una empresa para proteger la información, sistemas y recursos contra amenazas de malware.

Las herramientas de gestión de riesgos incluyen políticas, procedimientos, directrices, prácticas y estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, legal o de gestión. (Martínez Borja, 2014)

2.2.7. Auditorias y pruebas de seguridad

Las auditorias y pruebas de seguridad ayudan a las empresas a identificar, reconocer deficiencias en los protocolos de seguridad de una empresa, y así mediante procesos de control garantizar una mejor protección contra amenazas y riesgos potenciales.

Para obtener evidencia de auditoría y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría, se utiliza un proceso sistemático, independiente y documentado. (De La Rosa Cáceres, 2019)

2.3. Marco conceptual

2.3.1 Seguridad de la Información

Se entiende por seguridad de la información a aquello que consiste en preservar la confidencialidad, integridad y disponibilidad, al igual que los sistemas que los implican a ellos dentro de una organización. Así con ellos podemos concretar que se conocen como la base sobre la que se cimienta toda la seguridad de la información. (27001, 2015)

a. Integridad.

Se entiende que en esta dimensión se busca que un sistema informático no presente errores, al igual que no puedan ser

alteradas por personas no autorizadas, lo que nos da la garantía de que la información original mantendrá su integridad con la que fue ingresada al sistema. (Samaniego, 2018)

Indicadores:

Control de acceso. Se refiere a la regulación y control de accesos permitidos al sistema. (Izquierdo, y otros, 2017)

Precisión de Datos. Se refiere al ingreso de datos entregados de manera correcta sin ningún tipo de alteraciones o errores en el sistema. (Samaniego, 2018)

b. Disponibilidad.

Sostenemos que esta dimensión es la que garantiza que los datos requeridos, estén disponibles en el momento que el usuario los necesite o solicite. (Vergara Quiroz, 2017)

Indicadores:

Acceso a la información. Se refiere que cuando un usuario autorizado solicita el acceso a la información ubicado en el sistema en el intervalo de tiempo. (Samaniego, 2018)

c. Confidencialidad.

Sostenemos que esta dimensión se refiere como la característica de que la información almacenada en un sistema informático pueda garantizar la privacidad, disponibilidad y que solo sea accedida por los usuarios que cuenten con la autorización respectiva para acceder a la misma, lo cual impide que personas ajenas al sistema tengan acceso a la información. (Vergara Quiroz, 2017)

Indicadores:

Identificación de ataques. Se refiere al promedio de ataques por mes en el sistema que llega a reconocer. (Samaniego, 2018)

Efectividad de seguridad. Se refiere al promedio de ataques contrarrestados por el sistema por mes que se llega a registrar. (Samaniego, 2018)

2.4. Definición de términos básicos

a. Amenazas.

Se define como amenaza a cualquier tipo de evento en donde existe un riesgo o la posibilidad de perjudicar directamente a la información o los sistemas que se trabajan en una organización o persona evitando así que permitan realizar sus actividades (Tarazona , 2015).

b. Análisis de riesgos.

Es aquella que evalúa las amenazas y vulnerabilidades de la información y las consecuencias de su impacto en el procesamiento de la información, así como calcular o estimar su probabilidad de ocurrencia. (SÁNCHEZ, 2014).

c. Ataque cibernético bajo perfil.

Son ataque semi discretos que son implementados por personas expertas con conocimiento en el área informática, especializándose en el hacking, permitiéndoles ejecutar ataques informáticos por distintas razones diversas, principalmente motivos económicos (Inoguchi, y otros, 2017).

d. Ataque informático por intercepción.

Es un tipo de ataque que busca interferir con la privacidad y confidencialidad de la información en una empresa o institución, ya que el atacante accede a la información de la misma sin autorización, este tipo de ataque no suele dejar rastro o ser percibido en el instante, ya que su finalizad es plantar un daño y detonarlo en otra ocasión.

e. Ataque informático por interrupción.

Es un ataque directo contra la víctima, interrumpiendo el normal funcionamiento de un sistema de información destruyendo información de una máquina o dañando parte importante del hardware o software causando de esa forma un daño inmediato (Izquierdo, y otros, 2017).

f. Ataque informático por suplantación.

Se presenta como un delito de falsificación de la información, llegando a violar autenticación del mismo suplantando accesos, este ataque puede generar daños de sustitución de datos, inhabitando la integridad y causando problemas al usuario o víctima (Izquierdo, y otros, 2017).

g. Ataque informático por modificación.

Busca modificar la información sin autorización causando una alteración en los datos de la víctima y generando problemas para el mismo y beneficios para del usuario atacante. Es difícil percatarse ya que solo atenta contra la integridad de datos (Izquierdo, y otros, 2017).

h. Backup o Copias de respaldo.

Aquel que busca mantener la integridad y disponibilidad de la información, se requiere un control y seguimiento para el cual se debieran hacer copias de respaldo de la información a través de un software y se debieran probar con regularidad para comprobar la integridad de la información en concordancia con la política de copias de respaldo. (BENDECK, 2017)

i. Código malicioso.

Cualquier software que ingrese a un sistema de información sin autorización e intente romper las reglas se considera malware; ejemplos de esto incluyen troyanos, virus, gusanos, bombas lógicas y otras amenazas creadas intencionalmente.(Delgado, 2017)

j. Confidencialidad.

Este principio se define como el hecho de que la información de una organización sólo es accesible para quienes trabajan en ella, requiriendo un cierto nivel de autorización para acceder a diversos tipos de información. Para ello, es necesario mantener la privacidad de los datos para evitar que sean divulgados a personas no autorizadas (Izquierdo, y otros, 2017) .

k. Copias de respaldo.

Uno de esos términos que parece tener diferentes significados para distintas personas es "gestión de datos copiados". Sin embargo, en términos generales, se refiere a un método de protección de datos que minimiza el consumo de almacenamiento y al mismo tiempo facilita el uso de los datos. (Posey, 2014)

l. Disponibilidad.

Este principio de la seguridad de la información se enfoca en el acceso a la información de todas las personas autorizadas, sin problemas ni restricciones, en el momento necesario. Una de sus principales responsabilidades es identificar posibles fraudes sistémicos, como el robo de datos por parte de personal no autorizado, ya sea interno o externo. (Izquierdo, y otros, 2017) .

m. Integridad.

La finalidad principal de este principio de seguridad de la información es garantizar que los datos del sistema no han sido modificados por distintos usuarios internos o externos, permitiendo así que los datos sean conservados en su estado original, evitando pérdidas o encontrarlos con errores. (Izquierdo, y otros, 2017).

n. Intruso o atacante.

Persona u organización que intenta acceder sin permiso previamente a un sistema informático para extrañar datos relevantes sobre la víctima o el sistema para objetivos delictivos. En términos generales, los intrusos tienen a su disposición diversos mecanismos y tácticas para acceder al sistema en cuestión con intenciones maliciosas. (Florez, y otros, 2018)

o. Malware.

Es un tipo de software que busca acceso a computadoras o sistemas de información sin autorización de los propietarios. (SÁNCHEZ, 2014)

p. Medida de Seguridad

Proceso, procedimiento, técnica o función destinada a disminuir los efectos del riesgo. Rara vez las medidas de seguridad eliminan por completo el riesgo; más bien, sólo lo reducen a un nivel soportable. (Sánchez, 2017)

q. Protocolos de seguridad.

Un protocolo es una regulación o un conjunto de directivas para llevar a cabo lo establecido por acuerdo entre dos o más unidades administrativas internas o con entes externos. Un protocolo es un tipo de documento que define o normaliza la forma en que se deben realizar determinados procedimientos. Por lo tanto, recopila acciones, conductas, guías, formatos, instrucciones, técnicas, estándares y parámetros y apropiados ante determinadas situaciones. En consecuencia, un protocolo es una herramienta cuyo uso trasciende a las propias instituciones; como tal, no debe incluirse como un procedimiento o instrucción para un trabajo exclusivo de un dependiente. (Elecciones, 2017)

En las áreas de informática y telecomunicaciones, un protocolo de comunicaciones se refiere a un sistema de regulaciones que facilitan la comunicación entre dos o más entidades de un sistema de comunicación para intercambiar datos mediante cualquier tipo de variación de una magnitud física. Estándares o reglas que establecen la sintaxis, semántica y sincronización de la comunicación, además de los posibles métodos de recuperación de errores, son de lo que se trata. (Ramos Zapana, 2017)

r. Servicios de seguridad

Es aquel que está dirigido a evitar ataques de seguridad desde un aspecto muy particular buscando la seguridad de un sistema de información y el flujo de la información de una organización. Los principales servicios de seguridad son: control de acceso, confidencialidad, integridad, disponibilidad, y no repudio. (SÁNCHEZ, 2014)

s. Vulnerabilidad.

Es una debilidad o falla en el software o hardware, como también en los procesos relacionados con la información, por lo que se consideran como propia de los mismos o de la infraestructura que lo contiene (Tarazona , 2015).

III. HIPÓTESIS Y VARIABLES

3.1 Hipótesis.

3.1.1. Hipótesis general

La implementación de un protocolo de prevención contra ransomware en el servidor de BBTI S.A.C. tendrá un impacto positivo en la seguridad del servidor de la empresa BBTI S.A.C

3.1.2. Hipótesis especificas

a. La implementación de un protocolo de prevención contra ransomware, la adecuada instalación y configuración del software de prevención y una adecuada concientización del personal tendrán un impacto positivo en la resistencia ante ataques de ransomware en la empresa BBTI S.A.C.

b. La implementación de un protocolo de prevención contra ransomware, combinada con una capacitación y concienciación efectiva del personal, tendrá un impacto positivo en la reducción del tiempo de recuperación de ataques de ransomware en la empresa BBTI S.A.C.

c. La implementación de un protocolo de prevención contra ransomware, combinada con una capacitación y concienciación efectiva del personal, tendrá un impacto positivo en la reducción de la brecha de seguridad en la empresa BBTI S.A.C.

3.2. Variable:

3.2.1. Operacionalización de variable Dependiente

Tabla 1: Operacionalización de la variable dependiente

	VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ÍNDICES	ITEM	MÉTODO	TÉCNICA E INSTRUMENTO
SEGURIDAD DEL SERVIDOR	**Variable Dependiente: SEGURIDAD DEL SERVIDOR DE LA EMPRESA BBTI SAC**	Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información. (ISO 27001, 2016)	Se busca el grado de protección y resistencia del servidor de la empresa BBTI S.A.C. contra amenazas y riesgos que puedan comprometer su integridad, disponibilidad y confidencialidad tiene que ver con los resultados de vulnerabilidades, tiempo de recuperación y al mismo tiempo reducir la brecha de peligro.	**Resistencia ante ataques de ransomware**	El porcentaje de ataques de ransomware bloqueados	$\frac{total\ R.\ bloqueados}{total\ R.\ detectados}$ *x 100*	1 2 3 4 5	Hipotético - Deductivo.	**Técnica:** Encuesta **Instrumento:** cuestionario
				Tiempo de recuperación	El tiempo promedio de recuperación después de un ataque	$\cdot \frac{Total\ tiempo\ real}{Toral\ tiempo\ original}$	6 7 8	Hipotético - Deductivo.	**Técnica:** Encuesta **Instrumento:** cuestionario
				Reducción de brecha de seguridad	La reducción porcentual de la brecha de seguridad	$(1 - \frac{val\ ini\ - val.\ Fin}{Val\ inical})$ *x 100* val ini <> val fin	9 10 11	Hipotético - Deductivo.	**Técnica:** Encuesta **Instrumento:** cuestionario

Fuente: Elaboración propia

3.2.2. Operacionalización de variable Independiente

Tabla 2: Operacionalización de la variable independiente

	VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ÍNDICES	ITEM	MÉTODO	TÉCNICA E INSTRUMENTO
IMPLEMENTACION DE UN PROTOCOLO DE PREVENCION CONTRA RANSOMWARE	**Variable Independiente: IMPLEMENTACION DE UN PROTOCOLO DE PREVENCION CONTRA RANSOMWARE**	Un protocolo es un plan que establece formas de actuar para prevenir y enfrentar amenazas, y tener reglas mínimas de comportamiento que las personas adoptarán para minimizar riesgos. (breve guía para hacer un protocolo de seguridad,2020)	Se utilizó la estrategia de mejora a través de las políticas, procedimientos, herramientas tecnológicas y programas de capacitación implementados por la empresa BBTI S.A.C. para prevenir, detectar y mitigar los riesgos asociados con el ransomware en su infraestructura tecnológica.	**Instalación y configuración del software de prevención**	Nivel de actualización de las configuraciones de seguridad en el servidor	$\frac{Intalacion\ correcta}{Total\ software\ instalado}\ x\ 100$	12 13 14	Hipotético - Deductivo.	**Técnica:** Encuesta **Instrumento:** cuestionario
				Políticas y procedimientos de seguridad	Grado de cumplimiento de las políticas de seguridad	$\frac{politicas\ cumplidas}{Total\ politicas\ implem.}\ x\ 100$	15 16 17 18	Hipotético - Deductivo.	**Técnica:** Encuesta **Instrumento:** cuestionario
				Capacitación y concientización del personal	Satisfacción del personal con la formación recibida	$\frac{conoc.\ adquirido}{Tot.\ cono.\ deseado}\ x\ 100$	19 20 21 22	Hipotético - Deductivo.	**Técnica:** Encuesta **Instrumento:** cuestionario

Fuente: Elaboración propia

Según el autor (Kerlinger, 2002) en el libro llamado "**Investigación del comportamiento: Métodos de investigación en ciencias sociales**" se define como variable independiente al antecedente, es aquella que suele causar cambios en la variable dependiente, aquella que influirá en la predicción o resultado de la variable dependiente pag 43

Según el autor (Kerlinger, 2002) en el libro llamado "**Investigación del comportamiento: Métodos de investigación en ciencias sociales**" define como variable dependiente hacia aquella que se hace la predicción que varía de manera concomitante a los cambios o variaciones en como un resultado supuesto de la variable independiente, en general la variable dependiente es la condición que tratamos de explicar o dar cuenta del aprovechamiento pag 44

IV. METODOLOGÍA DEL PROYECTO

4.1. Diseño metodológico

El presente proyecto de investigación se centra en la implementación de un sistema de prevención contra ransomware en el servidor de la empresa BBTI S.A.C., El presente trabajo es una investigación aplicada, ya que esto implica tomar medidas prácticas para mejorar la seguridad del servidor y prevenir ataques de ransomware, al igual que busca solucionar un problema practico mientras busca tomar acciones concretas y obtener una medición de resultados

4.2. Método de investigación

Se ha usado un método experimental ya que se llevó a cabo manipulaciones y control de variables de manera sistemática para llegar a observar los efectos de la manipulación en relación con el problema que se está investigando

4.3. Población y muestra

4.3.1. Población

La población del presente trabajo de investigación se va a considerar al personal de trabajo de la empresa BBTI S.A.C. y sus sedes en el periodo de 2022 con una población de 200 trabajadores.

4.3.2. Muestra

La muestra de estudio está conformada por los trabajadores de la empresa BBTI S.A.C específicamente en la sede central, se va considerar el total de la población de 23 personas que laboran en la sede central y que dependen del uso del servidor 2022.

Tabla 3: Muestra de población a considerar

	Área	CONFORMAN
1	área de Finanzas	3
2	área de Recursos Humanos	3
3	área de Logística	4
4	área de Contabilidad	5
5	área de Sistemas	1
6	área de Producción	4
7	área de Diseño Grafico	1
8	área de Proyectos	1
9	Gerencia	1
	total, personal	23

Fuente: Elaboración propia.

4.4. Lugar de estudio

La ubicación del estudio es la empresa BBTI S.A.C. identificada con RUC 20565747356 con dirección Cal. 6 Mz. D Lote. 13 · Urbanización Industrial Grimanesa (Alt. de Lima Cargo City) Callao. cual realiza desde 2014, proyectos, fabricaciones, montajes electromecánicos industriales y de electrificación a lo largo y ancho de nuestro país.

4.5. Técnicas e instrumentos para recolección de información

4.5.1. Técnica

La técnica que se usó en la presente investigación fue la encuesta, Esta técnica nos permite obtener información más detallada y contextualizada por parte de las personas involucradas en el tema, tanto de su percepción como experiencias vividas al tema de estudio en el periodo de 2022

a su vez que hoy en día gracias al apoyo de plataformas como Google encuestas nos facilitan el procesamiento y recolección de datos

4.5.2. Instrumentos

El instrumento en el presente trabajo en combinación con la técnica a usar será el cuestionario se utiliza para cuantificar las variables de estudio, utilizando un conjunto sistematizado de preguntas que se dirigen a un grupo predeterminado de personas que poseen la información que interesa a la presente investigación

4.6. Análisis y procesamiento de datos

Para el análisis y procesamiento se datos se utilizó el programa de IBM SPSS STATITICS 29” en donde usando como base la encuesta el modelo de “Likert” y el modelo de “Baremos”, se representó dichos resultados como gráficos de barras y tablas comparativas de los resultados de la encuesta.

Según (Rustom J., 2012) la estadística descriptiva se enfoca en describir, resumir y visualizar la distribución de los datos, utilizando medidas de dispersión central como la media, mediana, moda, rango, desviación estándar y varianza.

Además, se utilizan diversos gráficos y tablas para representar los datos, como histogramas de frecuencia, diagramas de barra y gráficos circulares. En este estudio, se recopilará información utilizando los instrumentos propuestos y se analizarán los datos cuantitativos mediante la desviación estándar, moda, mediana y media, mientras que los datos cualitativos se analizarán a través de gráficos, porcentajes y tablas de frecuencia.

Por otro lado, Aguilar et al. (2022) señalan que la estadística inferencial es un conjunto de métodos y técnicas que permiten realizar deducciones e inferencias a partir de una muestra, con el propósito de interpretar, proyectar y comparar datos. Se utilizan diversas herramientas como pruebas de estimación puntual, pruebas de hipótesis, análisis de correlación y regresión, análisis de varianza, entre otros.

4.7. Aspectos éticos de la investigación

Para el presente trabajo de investigación se consideró los siguientes aspectos éticos:

Se obtuvo el consentimiento de los involucrados en el trabajo de investigación de la empresa BBTI S.A.C. explicando y detallando los procedimientos e incluso hasta posibles riesgos, al igual que la se salvaguardo la integridad de los resultados obtenidos, el cumplimiento del reglamento de seguridad con respecto a la privacidad y protección de data y el impacto positivo que genero dicho protocolo en el servidor de la empresa , se especifica que la información recopilada se utilizara únicamente para fines académicos

V. RESULTADOS

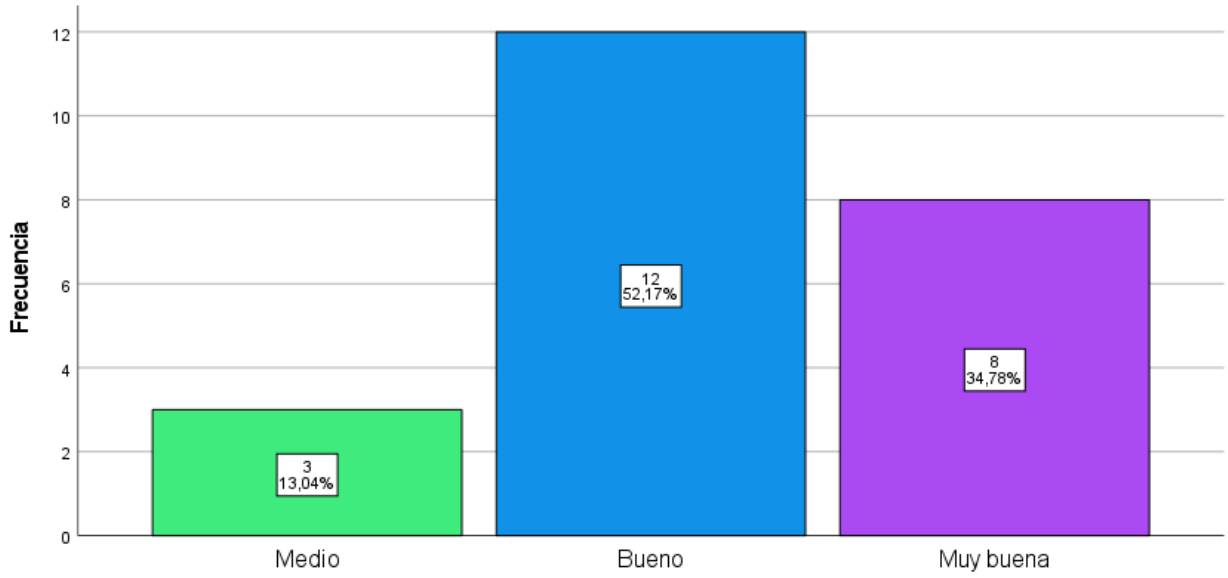
5.1. Resultados descriptivos

Tabla 4: Cómo calificarías a la empresa BBTI S.A.C. en su estrategia para la recuperación de datos en caso de un ataque de ransomware

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	3	13,0	13,0	13,0
	Bueno	12	52,2	52,2	65,2
	Muy buena	8	34,8	34,8	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 2: Gráfica de cómo calificarías a la empresa BBTI S.A.C. en su estrategia para la recuperación de datos en caso de un ataque de ransomware



Fuente: Elaboración propia.

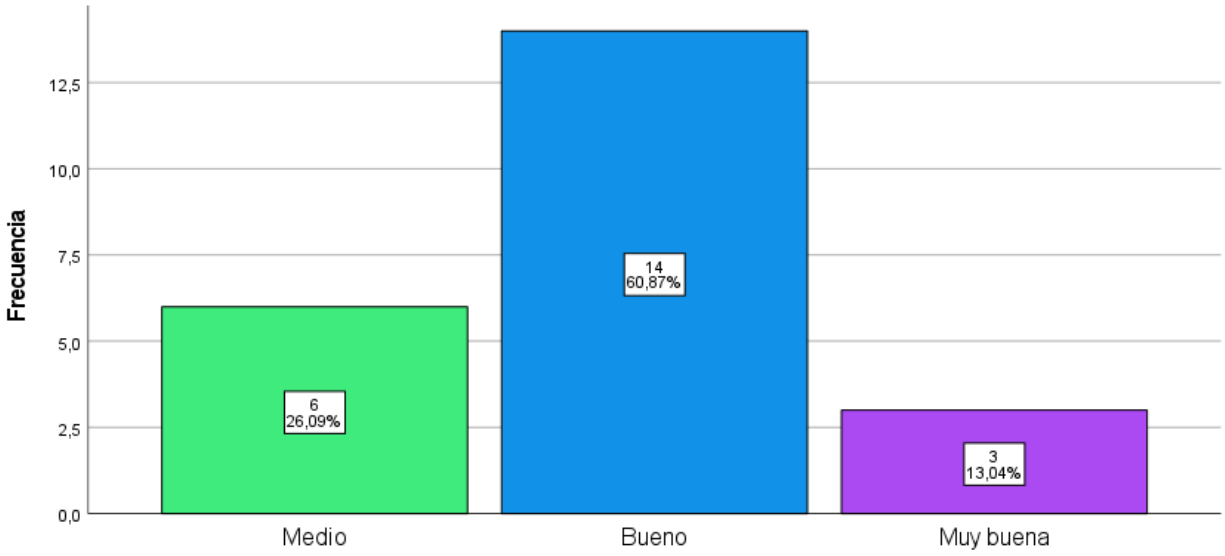
En la gráfica de la figura 2 se puede observar que del 100% (23) de los encuestados respecto a "Cómo calificarías a la empresa BBTI S.A.C. en su estrategia para la recuperación de datos en caso de un ataque de ransomware", el 52.17% (12) es bueno, 34.78% (8) es muy bueno y el 13,04% (3) es Medio.

Tabla 5: Qué tan satisfecho estás con la empresa BBTI S.A.C. con sus políticas y procedimientos establecidos para garantizar que los empleados sigan las prácticas de seguridad ante ransomware

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	6	26,1	26,1	26,1
	Bueno	14	60,9	60,9	87,0
	Muy buena	3	13,0	13,0	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 3: Gráfica de qué tan satisfecho estás con la empresa BBTI S.A.C. con sus políticas y procedimientos establecidos para garantizar que los empleados sigan las prácticas de seguridad ante ransomware



Fuente: Elaboración propia.

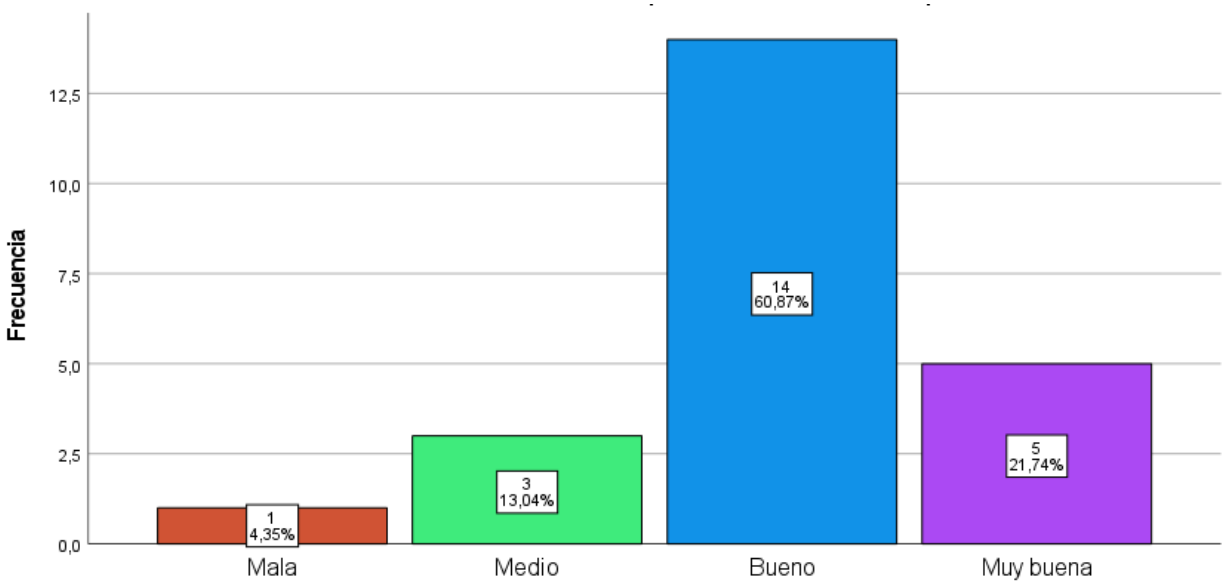
En la gráfica de la figura 3 se puede observar que del 100% (23) de los encuestados respecto a "Qué tan satisfecho estás con la empresa BBTI S.A.C. con sus políticas y procedimientos establecidos para garantizar que los empleados sigan las prácticas de seguridad ante ransomware", el 60.87% (14) es bueno, 26.09% (6) es medio y el 13,04% (3) es Muy Bueno.

Tabla 6: Qué nivel consideras que la empresa BBTI S.A.C. tiene en relación a su resistencia ante ataques de ransomware en función de las lecciones aprendidas de incidentes previos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Mala	1	4,3	4,3	4,3
	Medio	3	13,0	13,0	17,4
	Bueno	14	60,9	60,9	78,3
	Muy buena	5	21,7	21,7	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 4: Gráfica de qué nivel consideras que la empresa BBTI S.A.C. tiene en relación a su resistencia ante ataques de ransomware en función de las lecciones aprendidas de incidentes previos



Fuente: Elaboración propia.

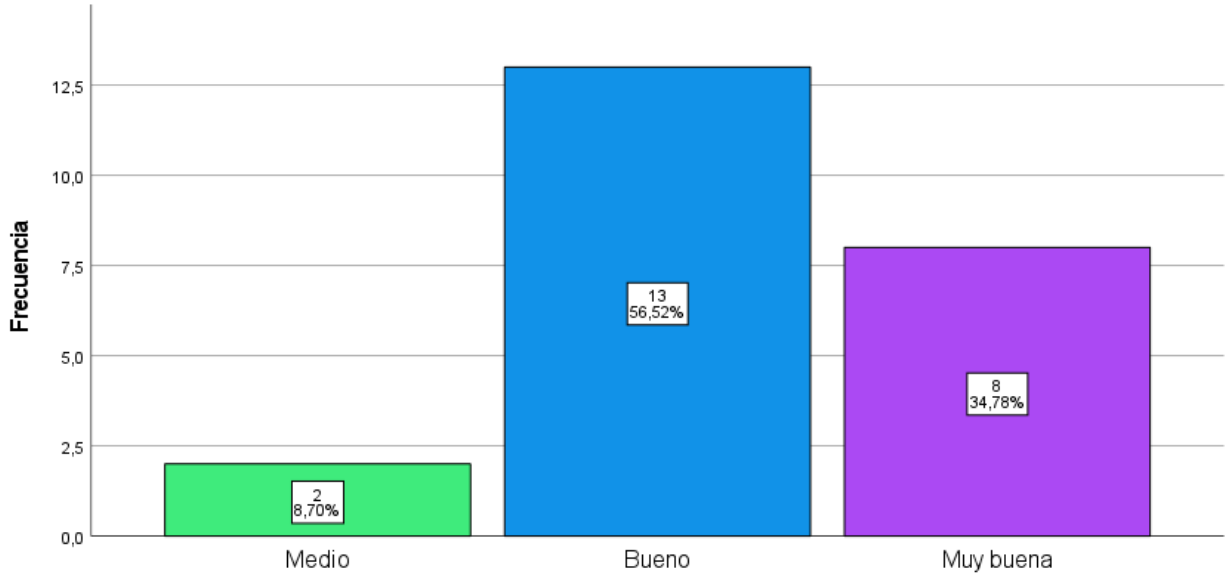
En la gráfica de la figura 4 se puede observar que del 100% (23) de los encuestados respecto a "Qué nivel consideras que la empresa BBTI S.A.C. tiene en relación a su resistencia ante ataques de ransomware en función de las lecciones aprendidas de incidentes previos", el 60.87% (14) es bueno, 21.74% (5) es muy bueno, el 13,04% (3) es Medio y 4.35% (1) es Mala.

Tabla 7: Cómo calificarías la implementación de un protocolo de prevención contra ransomware en la empresa BBTI SAC como parte de la resistencia ante ataques de ransomware

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	2	8,7	8,7	8,7
	Bueno	13	56,5	56,5	65,2
	Muy buena	8	34,8	34,8	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 5: Gráfica de cómo calificarías la implementación de un protocolo de prevención contra ransomware en la empresa BBTI SAC como parte de la resistencia ante ataques de ransomware



Fuente: Elaboración propia.

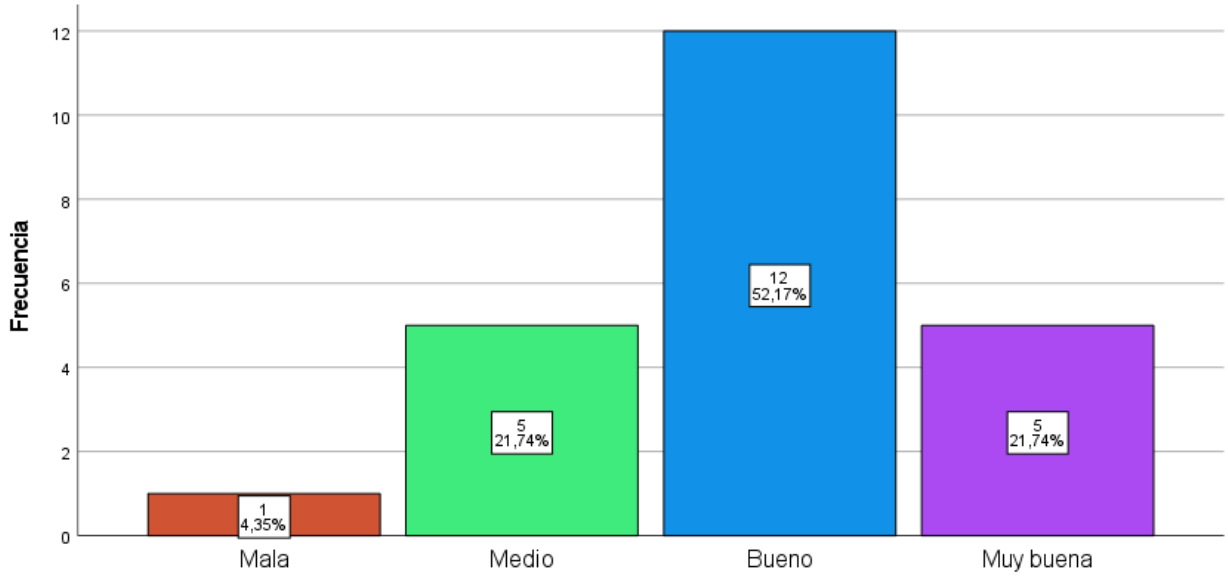
En la gráfica de la figura 5 se puede observar que del 100% (23) de los encuestados respecto a "Cómo calificarías la implementación de un protocolo de prevención contra ransomware en la empresa BBTI SAC como parte de la resistencia ante ataques de ransomware", el 56.52% (13) es bueno, 34.78% (8) es muy bueno y el 8,70% (2) es Medio.

Tabla 8: Con qué frecuencia ha experimentado la empresa BBTI S.A.C. un cambio en su resistencia ante ataques de ransomware desde la implementación de dicho protocolo en comparación al año 2021

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Mala	1	4,3	4,3	4,3
	Medio	5	21,7	21,7	26,1
	Bueno	12	52,2	52,2	78,3
	Muy buena	5	21,7	21,7	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 6: Gráfica de con qué frecuencia ha experimentado la empresa BBTI S.A.C. un cambio en su resistencia ante ataques de ransomware desde la implementación de dicho protocolo en comparación al año 2021



Fuente: Elaboración propia.

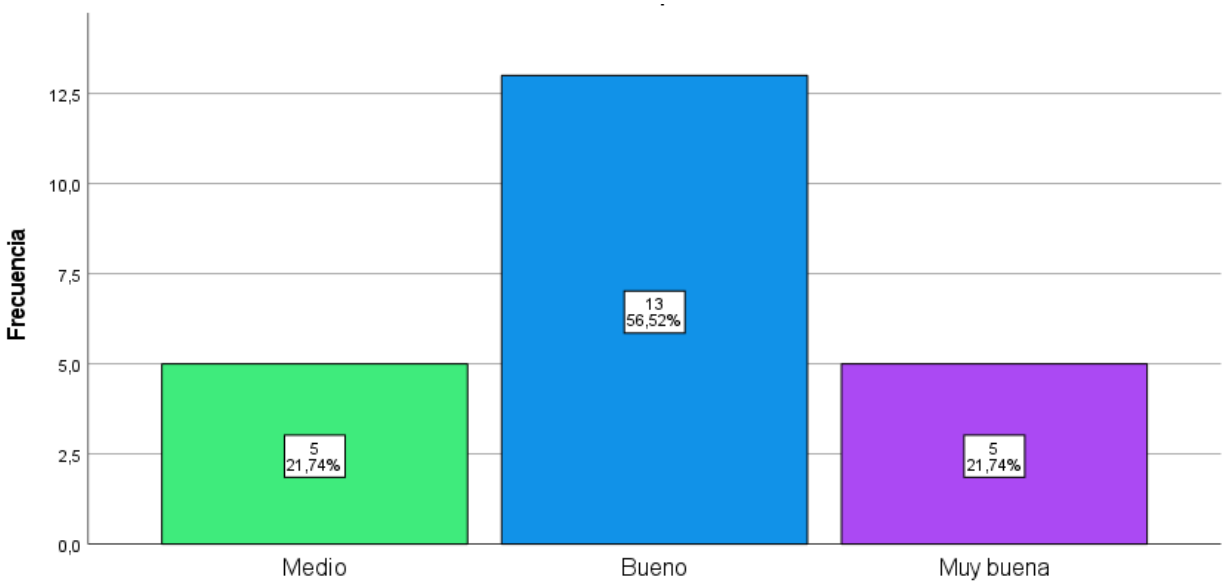
En la gráfica de la figura 6 se puede observar que del 100% (23) de los encuestados respecto a "Con qué frecuencia ha experimentado la empresa BBTI S.A.C. un cambio en su resistencia ante ataques de ransomware desde la implementación de dicho protocolo en comparación al año 2021", el 52.17% (12) es bueno, 21.74% (5) es muy bueno, el 21,74% (5) es Medio y 4.35% (1) es Mala.

Tabla 9: Qué tan efectivo crees que es el plan de acción de la empresa BBTI S.A.C. para minimizar el tiempo de inactividad en caso de un ataque de ransomware

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	5	21,7	21,7	21,7
	Bueno	13	56,5	56,5	78,3
	Muy buena	5	21,7	21,7	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 7: Gráfica de qué tan efectivo crees que es el plan de acción de la empresa BBTI S.A.C. para minimizar el tiempo de inactividad en caso de un ataque de ransomware



Fuente: Elaboración propia.

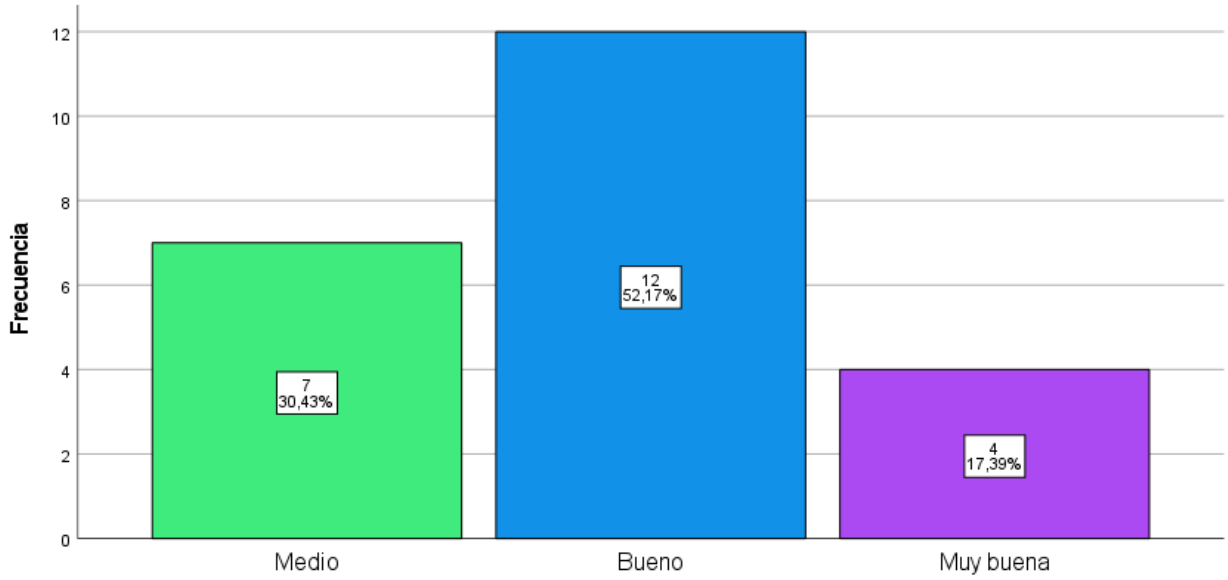
En la gráfica de la figura 7 se puede observar que del 100% (23) de los encuestados respecto a "Qué tan efectivo crees que es el plan de acción de la empresa BBTI S.A.C. para minimizar el tiempo de inactividad en caso de un ataque de ransomware", el 56.52% (13) es bueno, 21.74% (5) es muy bueno y el 21,74% (5) es Medio.

Tabla 10: Como califica la efectividad de los sistemas de respaldo y prioridad S.A.C. en la reducción del tiempo de recuperación después de un ataque de ransomware

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	7	30,4	30,4	30,4
	Bueno	12	52,2	52,2	82,6
	Muy buena	4	17,4	17,4	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 8: Gráfica de cómo califica la efectividad de los sistemas de respaldo y prioridad S.A.C. en la reducción del tiempo de recuperación después de un ataque de ransomware



Fuente: Elaboración propia.

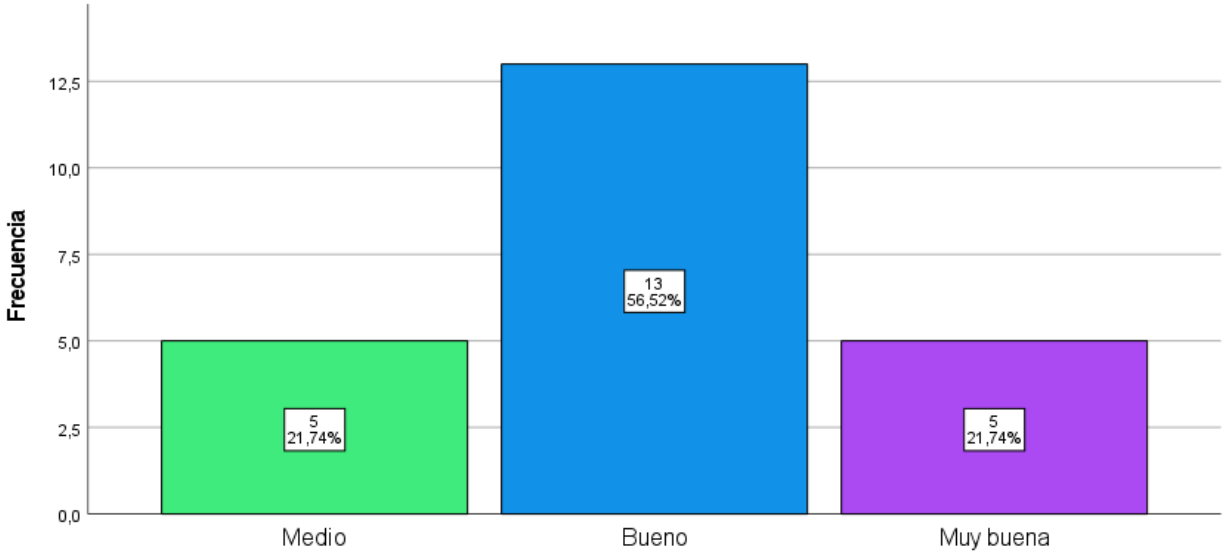
En la gráfica de la figura 8 se puede observar que del 100% (23) de los encuestados respecto a "Como califica la efectividad de los sistemas de respaldo y prioridad S.A.C. en la reducción del tiempo de recuperación después de un ataque de ransomware", el 52.17% (12) es bueno, 30.43% (7) es medio y el 17,39% (4) es Muy bueno.

Tabla 11: Qué tan efectivo crees que es la implementación del protocolo de prevención contra ransomware para reducir el tiempo de recuperación en caso de ataques de ransomware en la empresa BBTI S.A.C.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	5	21,7	21,7	21,7
	Bueno	13	56,5	56,5	78,3
	Muy buena	5	21,7	21,7	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 9: Gráfica de qué tan efectivo crees que es la implementación del protocolo de prevención contra ransomware para reducir el tiempo de recuperación en caso de ataques de ransomware en la empresa BBTI S.A.C.



Fuente: Elaboración propia.

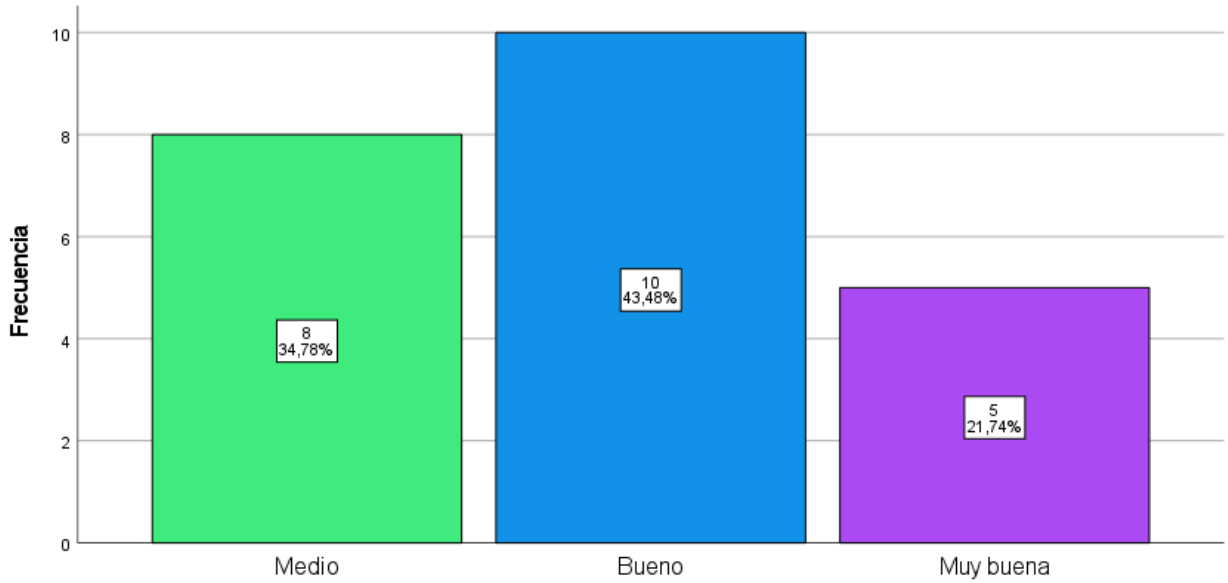
En la gráfica de la figura 9 se puede observar que del 100% (23) de los encuestados respecto a “Qué tan efectivo crees que es la implementación del protocolo de prevención contra ransomware para reducir el tiempo de recuperación en caso de ataques de ransomware en la empresa BBTI S.A.C.”, el 56.52% (13) es bueno, 21.74% (5) es muy bueno y el 21,74% (5) es Medio.

Tabla 12: Qué tan frecuente crees que la empresa BBTI S.A.C. lleva a cabo su proceso de mejora continua en medidas de seguridad con el objetivo de reducir las brechas de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	8	34,8	34,8	34,8
	Bueno	10	43,5	43,5	78,3
	Muy buena	5	21,7	21,7	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 10: Gráfica de qué tan frecuente crees que la empresa BBTI S.A.C. lleva a cabo su proceso de mejora continua en medidas de seguridad con el objetivo de reducir las brechas de seguridad



Fuente: Elaboración propia.

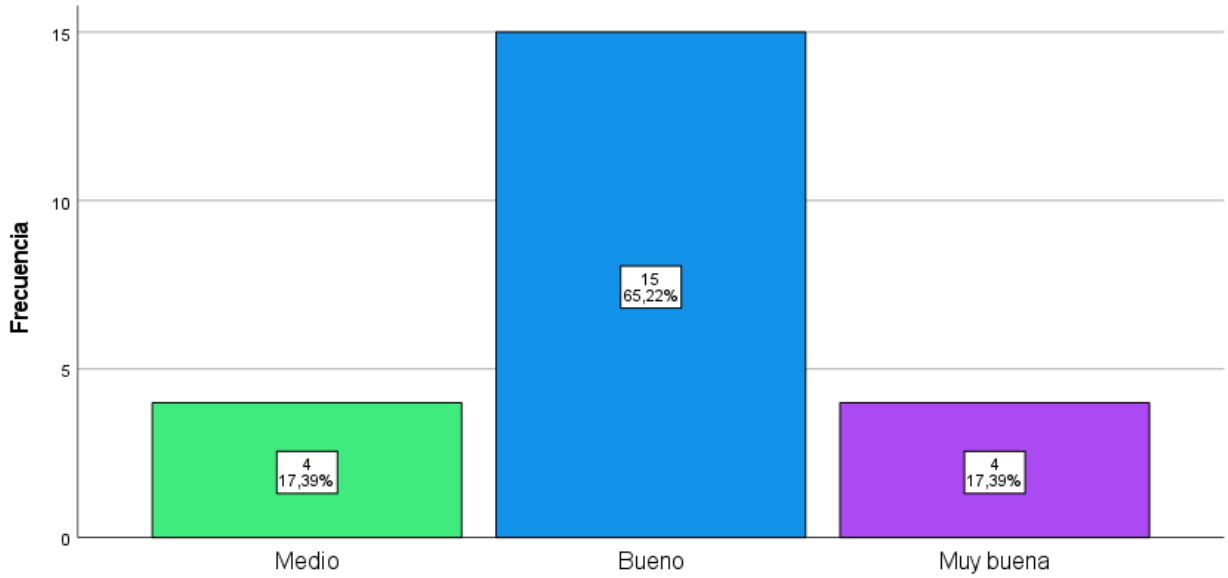
En la gráfica de la figura 10 se puede observar que del 100% (23) de los encuestados respecto a " Qué tan frecuente crees que la empresa BBTI S.A.C. lleva a cabo su proceso de mejora continua en medidas de seguridad con el objetivo de reducir las brechas de seguridad", el 43.48% (10) es bueno, 34.78% (8) es medio y el 21,74% (5) es muy bueno.

Tabla 13: Cuál es el nivel de la empresa BBTI S.A.C. en la implementación de sus controles de seguridad adicionales como parte de su estrategia para reducir brechas de seguridad en el último año

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	4	17,4	17,4	17,4
	Bueno	15	65,2	65,2	82,6
	Muy buena	4	17,4	17,4	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 11: Gráfica de cuál es el nivel de la empresa BBTI S.A.C. en la implementación de sus controles de seguridad adicionales como parte de su estrategia para reducir brechas de seguridad en el último año



Fuente: Elaboración propia.

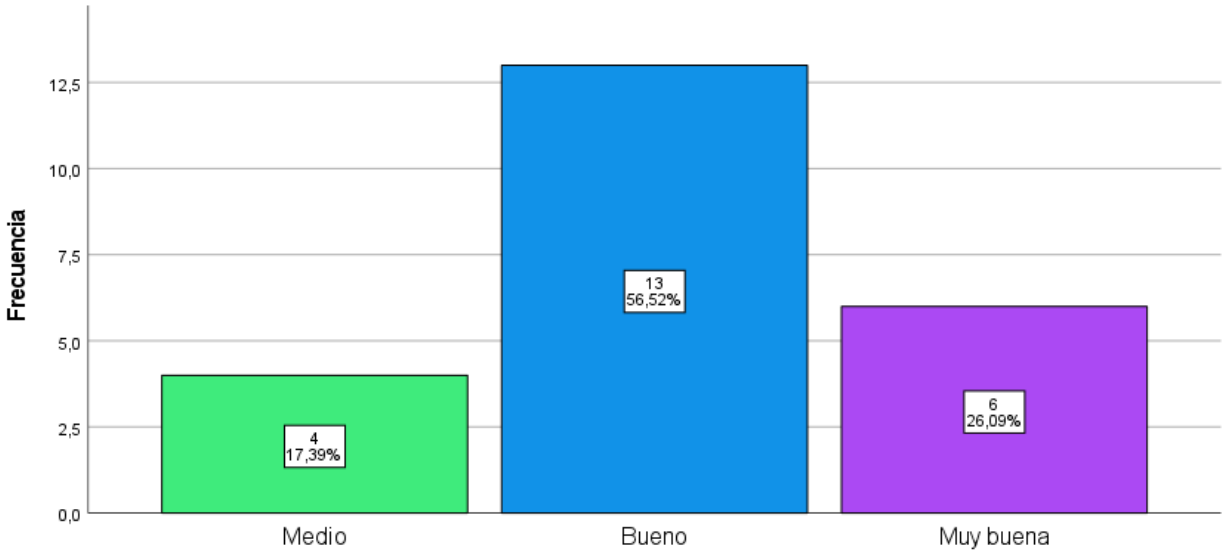
En la gráfica de la figura 11 se puede observar que del 100% (23) de los encuestados respecto a “Cuál es el nivel de la empresa BBTI S.A.C. en la implementación de sus controles de seguridad adicionales como parte de su estrategia para reducir brechas de seguridad en el último año”, el 65.22% (15) es bueno, 17.39% (4) es muy bueno y el 17,39% (4) es Medio.

Tabla 14: Como calificarías la implementación su protocolo de prevención contra ransomware con el objetivo de reducir las brechas de seguridad relacionadas con el ransomware por parte de la empresa BBBTI S.A.C.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	4	17,4	17,4	17,4
	Bueno	13	56,5	56,5	73,9
	Muy buena	6	26,1	26,1	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 12: Gráfica de como calificarías la implementación su protocolo de prevención contra ransomware con el objetivo de reducir las brechas de seguridad relacionadas con el ransomware por parte de la empresa BBBTI S.A.C.



Fuente: Elaboración propia.

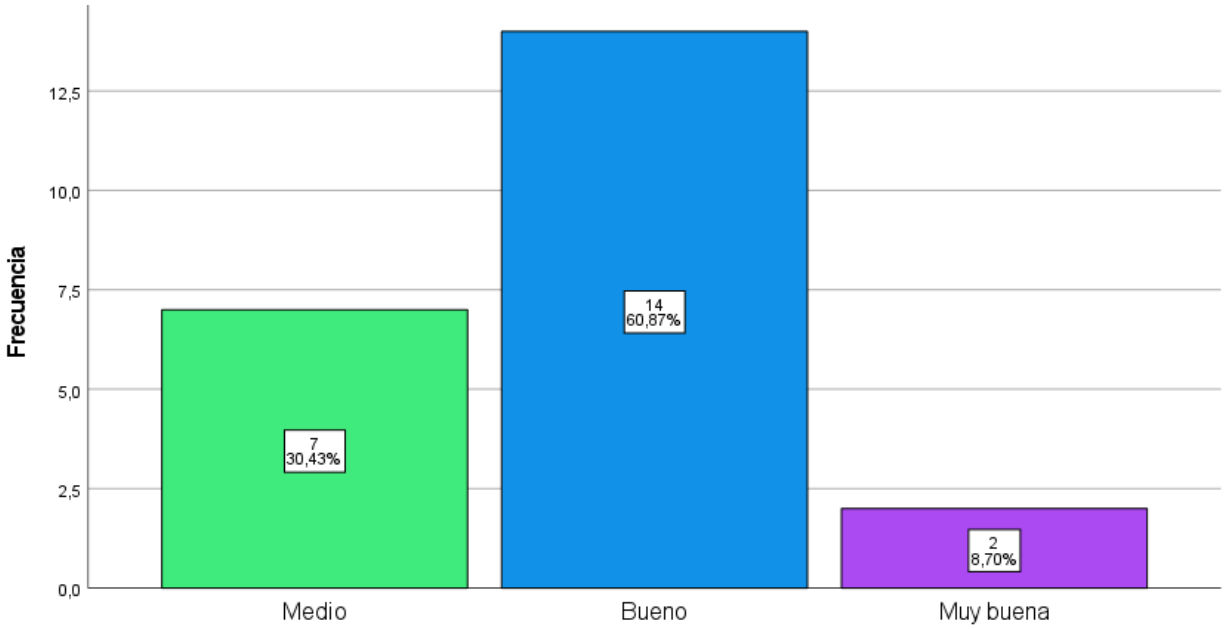
En la gráfica de la figura 12 se puede observar que del 100% (23) de los encuestados respecto a "Como calificarías la implementación su protocolo de prevención contra ransomware con el objetivo de reducir las brechas de seguridad relacionadas con el ransomware por parte de la empresa BBBTI S.A.C.", el 56.52% (13) es bueno, 26.09% (6) es muy bueno y el 17,39% (4) es Medio.

Tabla 15: Cómo calificarías la seguridad del servidor de la empresa BBTI S.A.C.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	7	30,4	30,4	30,4
	Bueno	14	60,9	60,9	91,3
	Muy buena	2	8,7	8,7	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 13: Gráfica de cómo calificarías la seguridad del servidor de la empresa BBTI S.A.C.



Fuente: Elaboración propia.

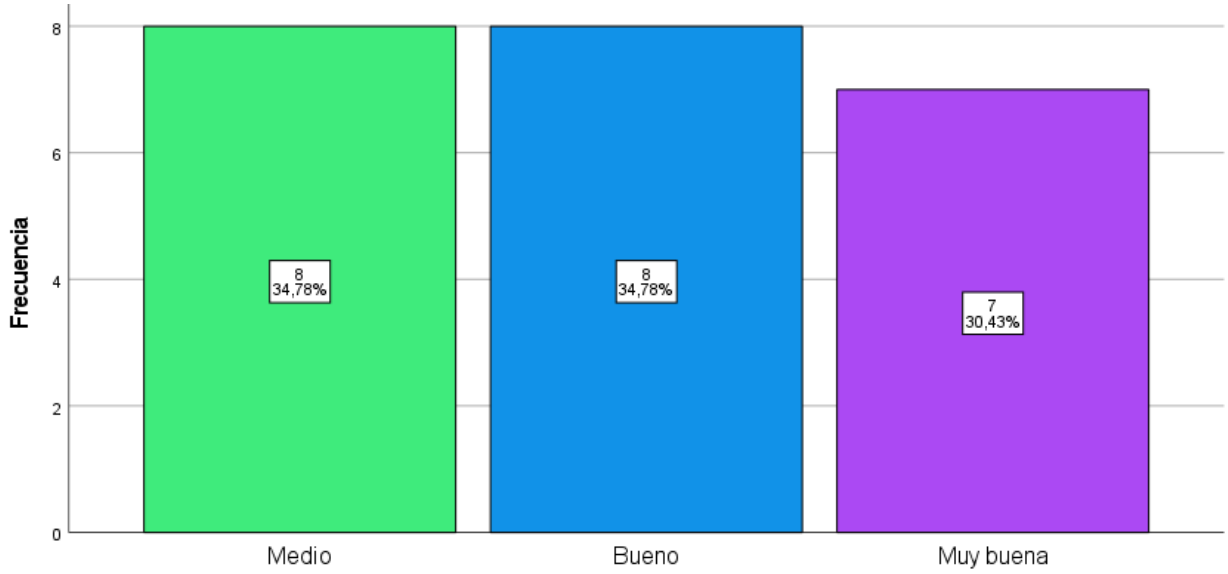
En la gráfica de la figura 13 se puede observar que del 100% (23) de los encuestados respecto a “Cómo calificarías la seguridad del servidor de la empresa BBTI S.A.C.”, el 60.87% (14) es bueno, 30.43% (7) es medio y el 8,70% (2) es muy bueno.

Tabla 16: Cómo calificarías la efectividad de la instalación y configuración del software de prevención en el servidor de BBTI S.A.C.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	8	34,8	34,8	34,8
	Bueno	8	34,8	34,8	69,6
	Muy buena	7	30,4	30,4	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 14: Gráfica de cómo calificarías la efectividad de la instalación y configuración del software de prevención en el servidor de BBTI S.A.C.



Fuente: Elaboración propia.

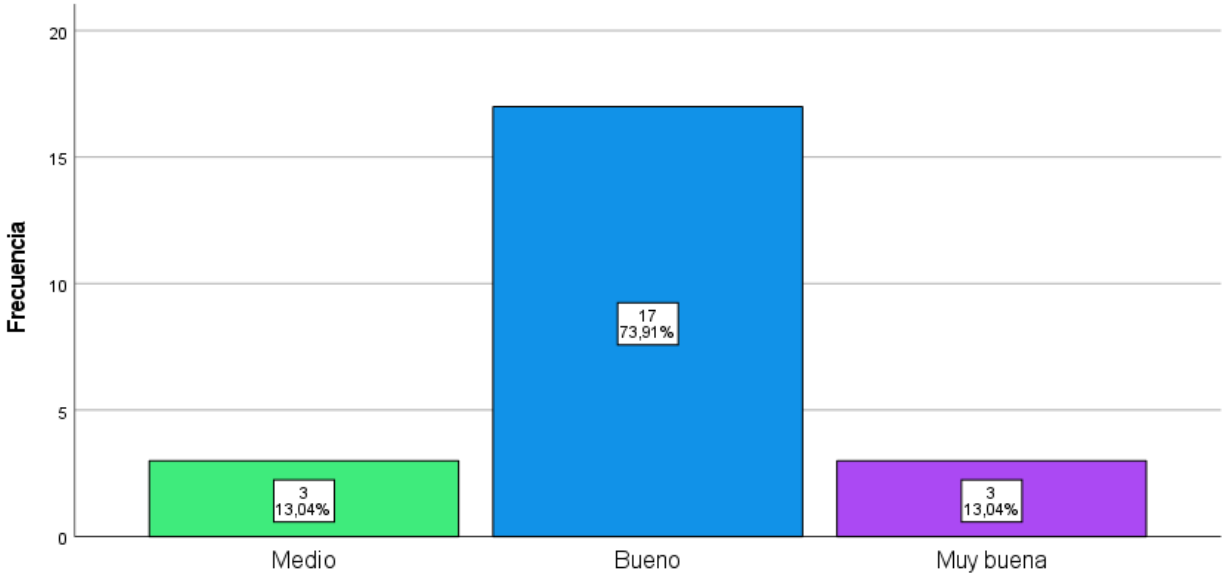
En la gráfica de la figura 14 se puede observar que del 100% (23) de los encuestados respecto a " Cómo calificarías la efectividad de la instalación y configuración del software de prevención en el servidor de BBTI S.A.C.", el 34.78% (8) es bueno, 34.78% (8) es muy bueno y el 30.43% (7) es Medio.

Tabla 17: La instalación y configuración del software de prevención en el servidor de BBTI S.A.C. ha mejorado la seguridad desde su implementación en el año 2021

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	3	13,0	13,0	13,0
	Bueno	17	73,9	73,9	87,0
	Muy buena	3	13,0	13,0	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 15: Gráfica de la instalación y configuración del software de prevención en el servidor de BBTI S.A.C. ha mejorado la seguridad desde su implementación en el año 2021



Fuente: Elaboración propia.

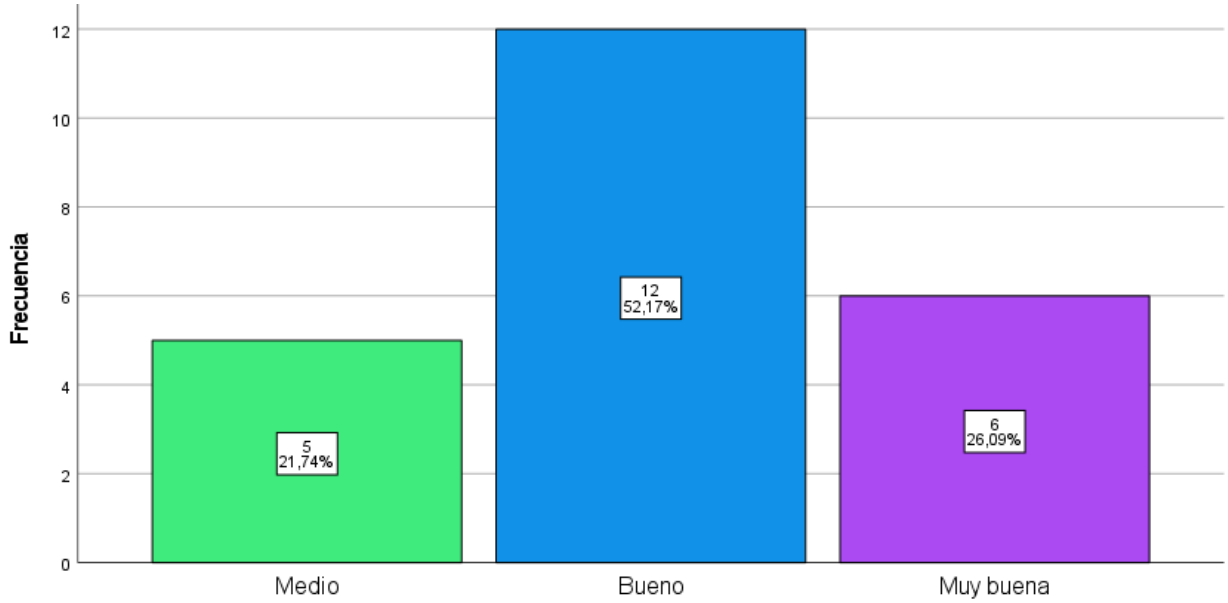
En la gráfica de la figura 15 se puede observar que del 100% (23) de los encuestados respecto a “La instalación y configuración del software de prevención en el servidor de BBTI S.A.C. ha mejorado la seguridad desde su implementación en el año 2021”, el 73.91% (17) es bueno, 13.04% (3) es muy bueno y el 13,04% (3) es Medio.

Tabla 18: Qué opinas sobre la efectividad de las políticas y procedimientos de seguridad de la empresa BBTI S.A.C.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	5	21,7	21,7	21,7
	Bueno	12	52,2	52,2	73,9
	Muy buena	6	26,1	26,1	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 16: Gráfica de qué opinas sobre la efectividad de las políticas y procedimientos de seguridad de la empresa BBTI S.A.C.



Fuente: Elaboración propia.

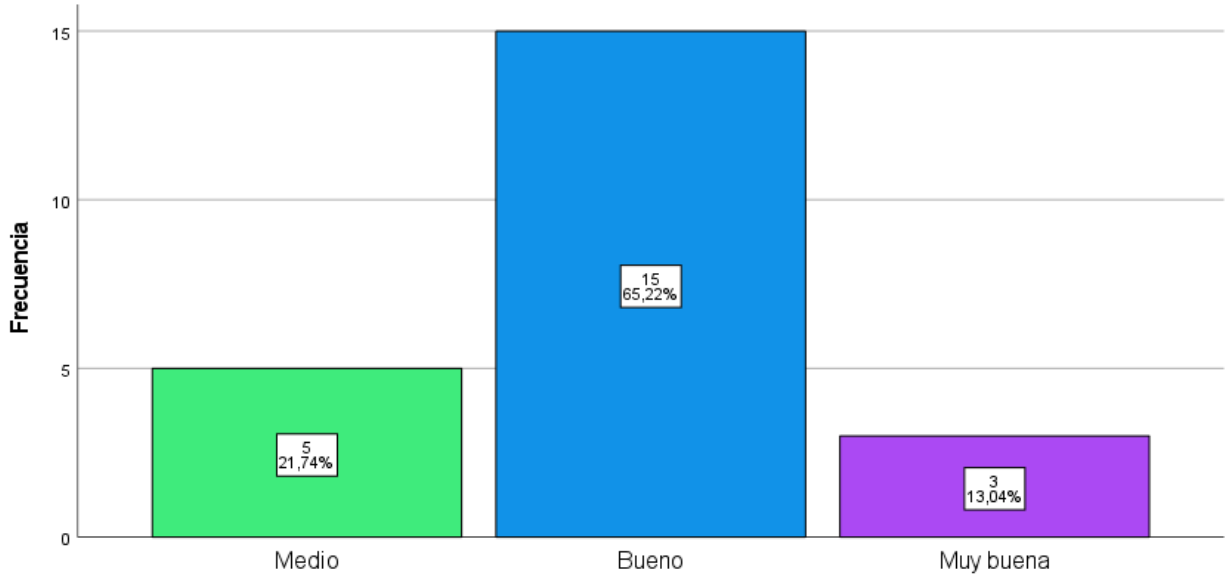
En la gráfica de la figura 16 se puede observar que del 100% (23) de los encuestados respecto a "Qué opinas sobre la efectividad de las políticas y procedimientos de seguridad de la empresa BBTI S.A.C.", el 52.17% (12) es bueno, 26.09% (6) es muy bueno y el 21,74% (5) es Medio.

Tabla 19: Cuál es el nivel de cumplimiento de las políticas y procedimientos de seguridad en la empresa BBTI S.A.C.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	5	21,7	21,7	21,7
	Bueno	15	65,2	65,2	87,0
	Muy buena	3	13,0	13,0	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 17: Gráfica de cuál es el nivel de cumplimiento de las políticas y procedimientos de seguridad en la empresa BBTI S.A.C.



Fuente: Elaboración propia.

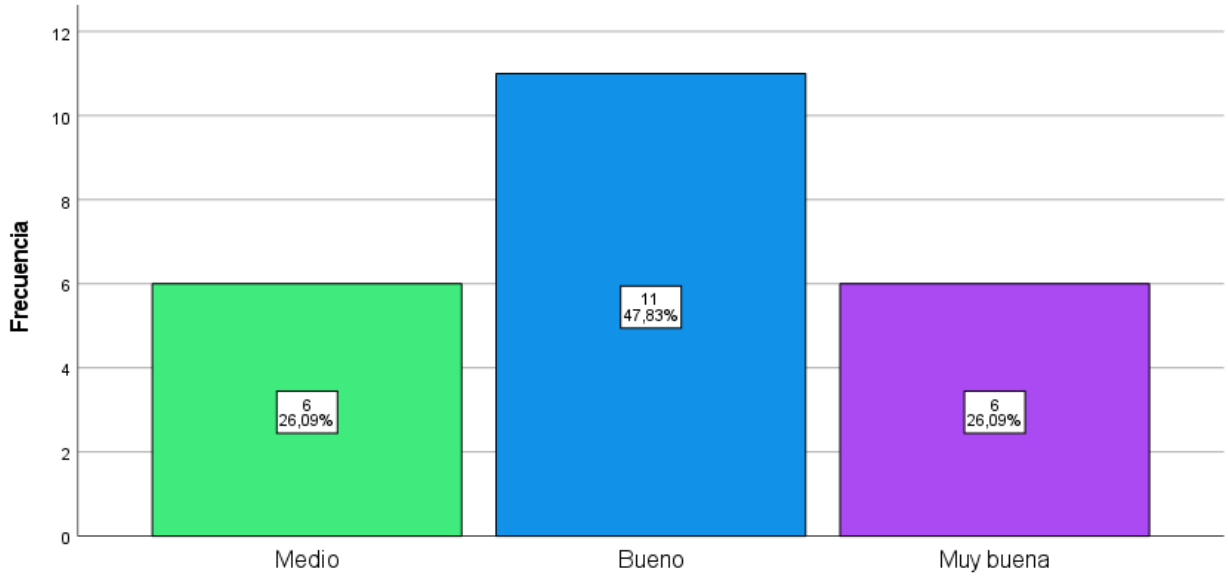
En la gráfica de la figura 17 se puede observar que del 100% (23) de los encuestados respecto a “Cuál es el nivel de cumplimiento de las políticas y procedimientos de seguridad en la empresa BBTI S.A.C.”, el 65.22% (15) es bueno, 21.74% (5) es medio y el 13,04% (3) es Muy bueno.

Tabla 20: Qué tan rigurosamente consideras que la seguridad del servidor de BBTI S.A.C. aplica las políticas y procedimientos de seguridad establecidos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	6	26,1	26,1	26,1
	Bueno	11	47,8	47,8	73,9
	Muy buena	6	26,1	26,1	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 18: Gráfica de qué tan rigurosamente consideras que la seguridad del servidor de BBTI S.A.C. aplica las políticas y procedimientos de seguridad establecidos



Fuente: Elaboración propia.

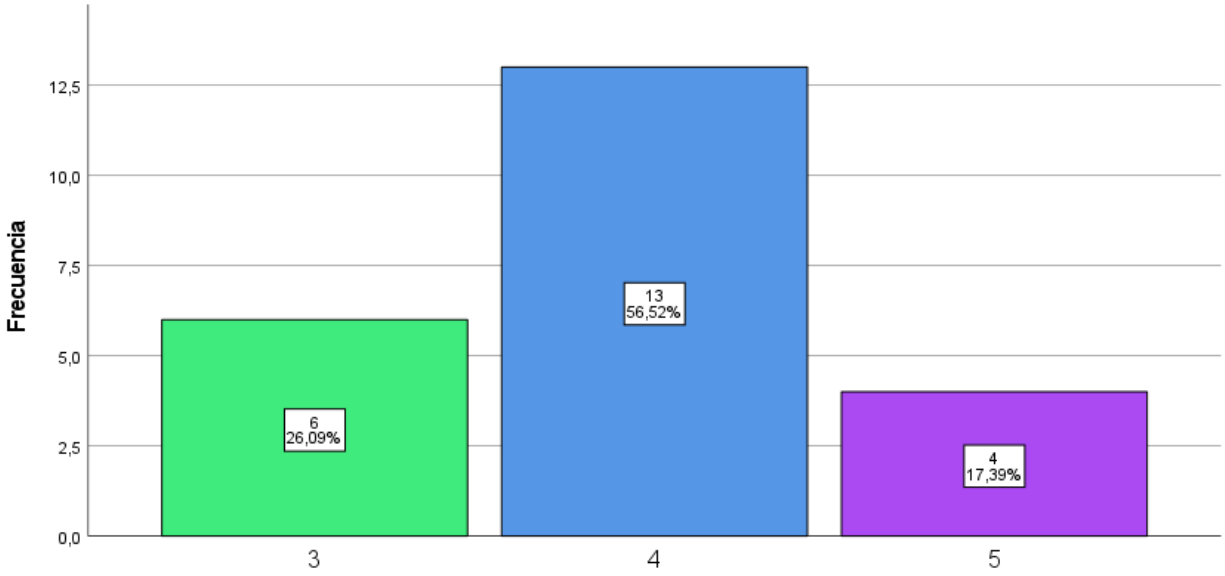
En la gráfica de la figura 18 se puede observar que del 100% (23) de los encuestados respecto a "Qué tan rigurosamente consideras que la seguridad del servidor de BBTI S.A.C. aplica las políticas y procedimientos de seguridad establecidos", el 47.83% (11) es bueno, 26.09% (6) es muy bueno y el 26,09% (6) es Medio.

Tabla 21: Cómo evaluarías la seguridad del servidor de BBTI S.A.C. en relación con las políticas y procedimientos de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	6	26,1	26,1	26,1
	Bueno	13	56,5	56,5	82,6
	Muy buena	4	17,4	17,4	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 19: Gráfica de cómo evaluarías la seguridad del servidor de BBTI S.A.C. en relación con las políticas y procedimientos de seguridad



Fuente: Elaboración propia.

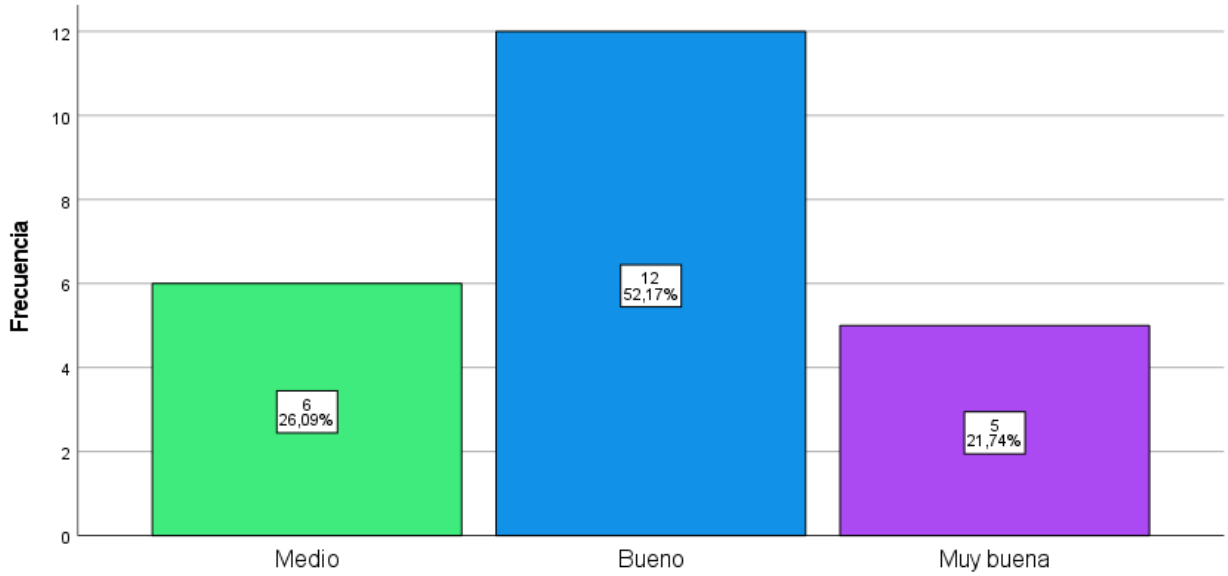
En la gráfica de la figura 19 se puede observar que del 100% (23) de los encuestados respecto a “Cómo evaluarías la seguridad del servidor de BBTI S.A.C. en relación con las políticas y procedimientos de seguridad”, el 56.52% (13) es bueno, 26.09% (6) es medio y el 17,39% (4) es Medio.

Tabla 22: Cómo calificarías la efectividad de la capacitación y concientización del personal en relación con la seguridad del servidor de BBTI S.A.C.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	6	26,1	26,1	26,1
	Bueno	12	52,2	52,2	78,3
	Muy buena	5	21,7	21,7	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 20: Gráfica de cómo calificarías la efectividad de la capacitación y concientización del personal en relación con la seguridad del servidor de BBTI S.A.C.



Fuente: Elaboración propia.

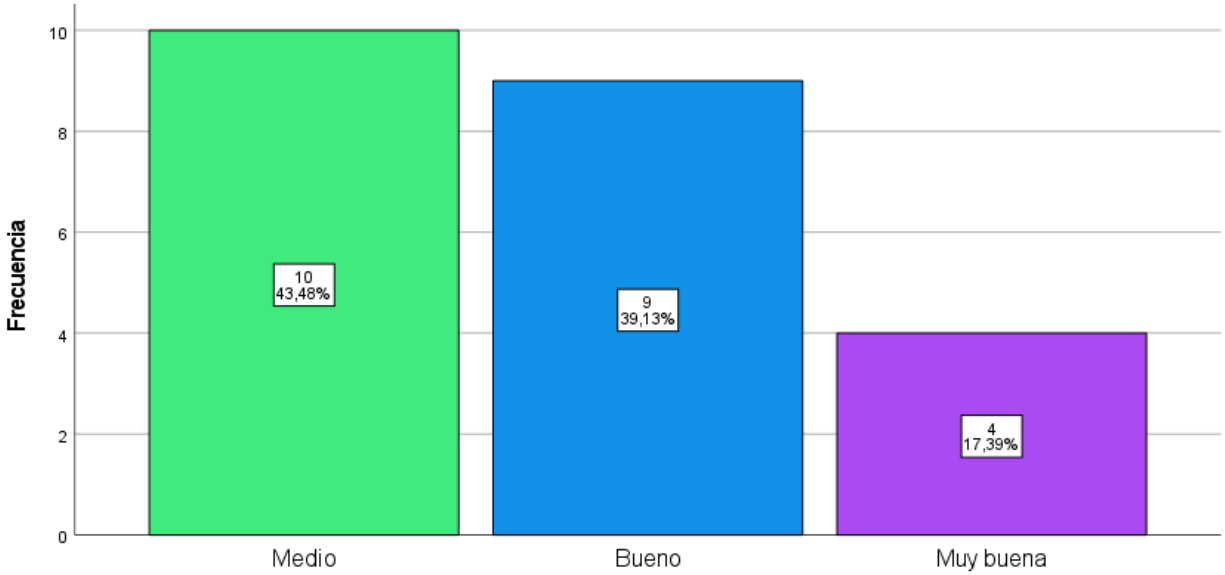
En la gráfica de la figura 20 se puede observar que del 100% (23) de los encuestados respecto a "Cómo calificarías la efectividad de la capacitación y concientización del personal en relación con la seguridad del servidor de BBTI S.A.C.", el 52.17% (12) es bueno, 26.09% (6) es medio y el 21,74% (5) es muy bueno.

Tabla 23: Cuán informados están los empleados de BBTI S.A.C. sobre las políticas de seguridad del servidor

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	10	43,5	43,5	43,5
	Bueno	9	39,1	39,1	82,6
	Muy buena	4	17,4	17,4	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 21: Gráfica de cuán informados están los empleados de BBTI S.A.C. sobre las políticas de seguridad del servidor



Fuente: Elaboración propia.

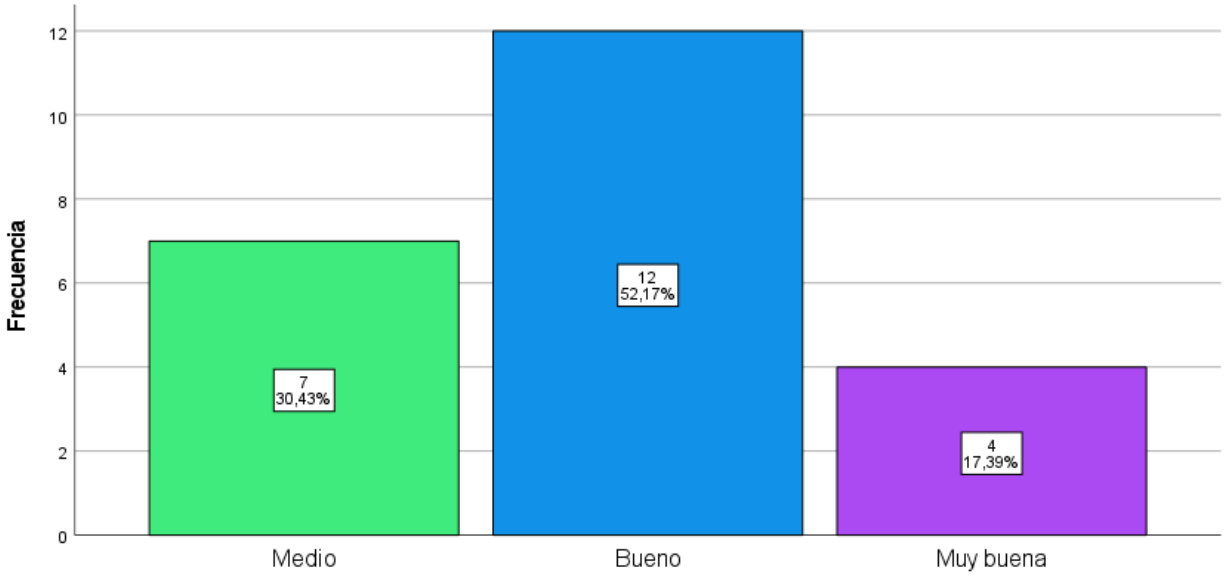
En la gráfica de la figura 21 se puede observar que del 100% (23) de los encuestados respecto a “Cuán informados están los empleados de BBTI S.A.C. sobre las políticas de seguridad del servidor”, el 43.48% (10) es medio, 39.13% (9) es bueno y el 17,39% (4) es muy bueno.

Tabla 24: Cómo mejora la seguridad del servidor después de la implementación de programas de capacitación y concientización para el personal

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	7	30,4	30,4	30,4
	Bueno	12	52,2	52,2	82,6
	Muy buena	4	17,4	17,4	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 22: Gráfica de cómo mejora la seguridad del servidor después de la implementación de programas de capacitación y concientización para el personal



Fuente: Elaboración propia.

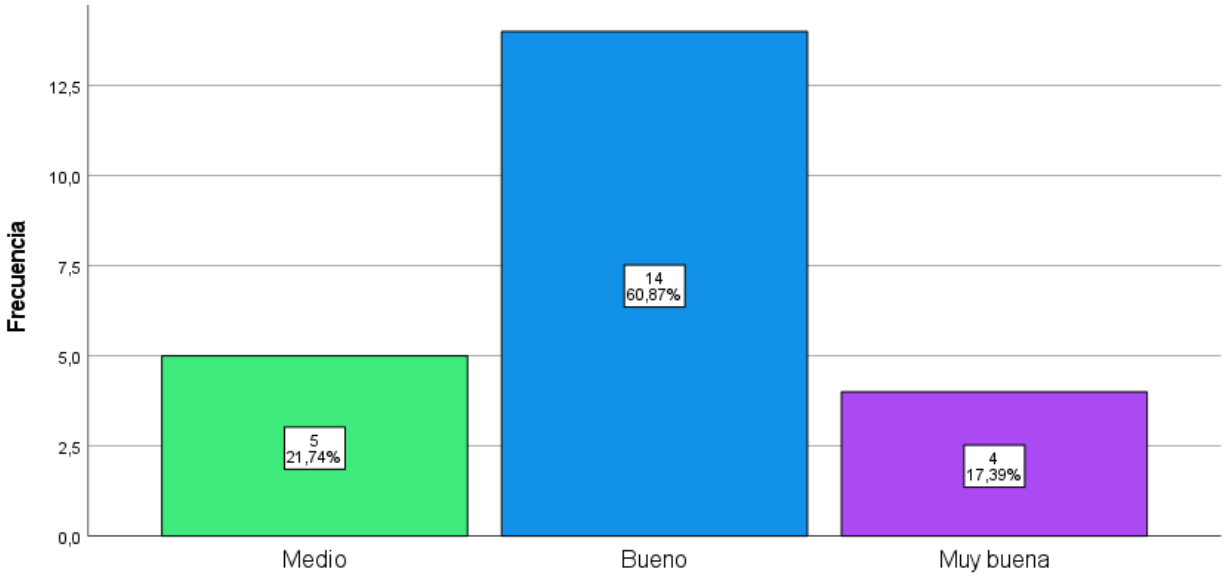
En la gráfica de la figura 22 se puede observar que del 100% (23) de los encuestados respecto a “Cómo mejora la seguridad del servidor después de la implementación de programas de capacitación y concientización para el personal”, el 52.17% (12) es bueno, 30.43% (7) es medio y el 17,39% (4) es muy bueno.

Tabla 25: Cómo evaluarías el nivel de compromiso del personal de BBTI S.A.C. en la promoción de la seguridad del servidor

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio	5	21,7	21,7	21,7
	Bueno	14	60,9	60,9	82,6
	Muy buena	4	17,4	17,4	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

Figura 23: Gráfica de cómo evaluarías el nivel de compromiso del personal de BBTI S.A.C. en la promoción de la seguridad del servidor



Fuente: Elaboración propia.

En la gráfica de la figura 23 se puede observar que del 100% (23) de los encuestados respecto a "Cómo evaluarías el nivel de compromiso del personal de BBTI S.A.C. en la promoción de la seguridad del servidor", el 60.87% (14) es bueno, 21.74% (5) es medio y el 17,39% (4) es muy bueno.

5.2. Resultados inferenciales

Prueba de hipótesis general

La implementación de un protocolo de prevención contra ransomware en el servidor de BBTI S.A.C. tendrá un impacto positivo en la seguridad del servidor de la empresa BBTI S.A.C.

Aquí analizaremos la Implementación de un protocolo de prevención contra ransomware para la seguridad del servidor de BBTI S.A.C. en el año 2022, en la seguridad del Servidor.

Para contrastar esta hipótesis general, analizaremos el comportamiento de los datos obtenidos, primero analizaremos la Bondad de ajuste (la normalidad), luego analizaremos la correlación y el comportamiento de la recta de regresión de los datos usando el SPSS v29:

Primero analizaremos la normalidad de los datos de la variable independiente en base a la variable dependiente:

IMPLEMENTACIÓN DE UN PROTOCOLO DE PREVENCIÓN CONTRA RANSOMWARE.

H0: Los datos del Protocolo de prevención contra Ransomware en la empresa BBTI SAC tienen una distribución normal.

H1: Los datos del Protocolo de prevención contra Ransomware en la empresa BBTI SAC tienen una distribución normal.

SEGURIDAD DEL SERVIDOR .

H0: Los datos de Seguridad del Servidor en la empresa BBTI SAC tienen una distribución normal.

H1: Los datos de Seguridad del Servidor en la empresa BBTI SAC no tienen una distribución normal.

Tabla 26: Comparativa de variables dependiente

Seguridad del servidor	Implementación de un protocolo de prevención contra ransomware
43	42
37	36
41	42
46	43
43	42
46	44
42	42
46	44
46	43
44	40
33	33
40	41
40	39
42	42
55	55
55	55
36	40
42	35
48	48
50	49
41	36
49	50
49	51

Fuente: Elaboración propia

Tabla 27: Prueba de normalidad de hipótesis general de variables dependiente e independiente

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Seguridad_del_Servidor	0.102	23	0.200*	0.973	23	0.768
Implementación_de_un_ Protocolo_de_Prevención _contra_Ransomware	0.181	23	0.050	0.944	23	0.222

Fuente: Elaboración propia.

Como los datos son menos de 30, usamos la prueba de Bondad de ajuste (Normalidad) Shapiro-Wilk.

Para los datos de Seguridad del Servidor el p-valor es 0.765 > 0.05 por lo que se acepta la hipótesis nula: “Los datos de Seguridad del Servidor en la empresa BBTI SAC tienen una distribución normal”.
Para la Implementación del Protocolo de prevención contra Ransomware en la empresa BBTI SAC el p-valor es 0.222 > 0.05 por lo que se acepta la hipótesis nula: “Los datos del Protocolo de prevención contra Ransomware en la empresa BBTI SAC tienen una distribución normal”.

Análisis de Correlación

H_0: La Implementación del Protocolo de prevención contra Ransomware no se relacionan significativamente con los datos de Seguridad del Servidor en la empresa BBTI SAC.
H_1: La Implementación del Protocolo de prevención contra Ransomware se relacionan significativamente con los datos de Seguridad del Servidor en la empresa BBTI S.A.C

Tabla 28: Correlacionales no paramétricas de hipótesis general dependiente e independiente

			Seguridad_del_Servidor	Implementación_de_un_Protocolo_de_Prevención_contra_Romsomware
Rho de Spearman	Seguridad_del_Servidor	Coeficiente de correlación	1.000	0.914**
		Sig. (bilateral)	.	<.001
		N	23	23
	Implementación_de_un_Protocolo_de_Prevención_contra_Romsomware	Coeficiente de correlación	0.914**	1.000
		Sig. (bilateral)	<.001	.
		N	23	23

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia

El Rho de Spearman es 0.914 y de acuerdo a los baremos de estimación de la correlación de Spearman hay correlación positiva muy alta entre la Implementación del Protocolo de prevención contra Ransomware y los datos de Seguridad del Servidor en la empresa BBTI SAC.

Además, el nivel de significación que nos arroja el SPSS es 0.001 es menor que 0.05 esto indica que hay evidencias de que existe una relación significativa entre las dos variables, luego podemos concluir que: “La Implementación del Protocolo de prevención contra Ransomware se relacionan significativamente con los datos de Seguridad del Servidor en la empresa BBTI SAC”.

Tabla 29: Estadístico descriptivo de hipótesis general de variables dependiente e independiente

	Media	Desv. estándar	N
Seguridad_del_Servidor	44.09	5.468	23
Implementación_de_un_Protocolo_de_Prevención_contra_Ransomware	43.13	5.911	23

Fuente: Elaboración propia

Lo que se busca es construir un modelo para determinar la dependencia que exista entre entre la Implementación del Protocolo de prevención contra Ransomware con los datos de Seguridad del Servidor en la empresa BBTI SAC.

Cuya la variable dependiente es:

y: Seguridad del Servidor.

La variable independiente es:

x: Implementación del Protocolo de prevención contra Ransomware.

HIPÓTESIS DE REGRESIÓN

H_0: La Implementación del Protocolo de prevención contra Ransomware no interviene en la Seguridad del Servidor en la empresa BBTI SAC.

H_1: La Implementación del Protocolo de prevención contra Ransomware interviene en la Seguridad del Servidor en la empresa BBTI SAC.

Consideramos el Nivel de Significación $\alpha = 0.05$.

Análisis Estadístico usando Regresión

Utilizando las fórmulas de las ecuaciones normales a los datos obtendremos los coeficientes de regresión o utilizando Regresión de Análisis de datos, en el SPSS podemos calcular también los coeficientes de regresión:

Tabla 30: Resumen del modelo de hipótesis general dependiente e independiente

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Estadísticos de cambio					Durbin-Watson
					Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. Cambio en F	
1	0.917[a]	0.840	0.832	2.238	0.840	110.332	1	21	<.001	2.478

a. Predictores: (Constante), Implementación_de_un_Protocolo_de_Prevención_contra_Ransomware

b. Variable dependiente: Seguridad_del_Servidor

Fuente: Elaboración propia

En este cuadro del análisis tomamos el Estadístico F que evalúa el ajuste general de la ecuación de regresión si es significativo.

La tabla recoge el valor de R^2, el cambio experimentado por R^2 en cada paso, y el estadístico F y su significación. El estadístico F permite contrastar la hipótesis de que el cambio en R^2 vale cero en la data.

El valor de R^2 es 0.840. Lógicamente, en el primer paso, $R^2_{cambio} = R^2$.

Al contrastar la hipótesis de que el valor poblacional de R^2_{cambio} es cero se obtiene un estadístico F de 0,001 que con 1 y 21 grados de libertad, tienen un p-valor de 0,001 (como este valor es menor que 0,05), podemos afirmar que: La Implementación del Protocolo de prevención contra Ransomware interviene en la Seguridad del Servidor en la empresa BBTI SAC.

Bondad de Ajuste

R cuadrado = 0.840

El 84% de la variabilidad de la Implementación del Protocolo de prevención contra Ransomware y la Seguridad del Servidor en la empresa BBTI SAC.

El error estándar de la estimación es 2.238.

Por lo que rechazamos la hipótesis nula y aceptamos que la Implementación del Protocolo de prevención contra Ransomware interviene en la Seguridad del Servidor en la empresa BBTI SAC.

Todo esto se corrobora al usar las estimaciones.

Aquí presentamos el Anova del modelo:

Tabla 31: ANOVA de hipótesis general dependiente e independiente

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	552.640	1	552.640	110.332	<.001[b]
	Residuo	105.186	21	5.009		
	Total	657.826	22			

a. Variable dependiente: Seguridad_del_Servidor

b. Predictores: (Constante), Implementación_de_un_Protocolo_de_Prevención_contra_Ransomware

Fuente: Elaboración propia

F= 110.332, P= 0.001 < 0.05

Se rechaza la hipótesis nula y se concluye que: La Implementación del Protocolo de prevención contra Ransomware interviene en la Seguridad del Servidor en la empresa BBTI SAC.

Tabla 32: Coeficientes de hipótesis general dependiente e independiente

Modelo	Coeficientes no estandarizados	Coeficientes estandarizados			95.0% intervalo de confianza para B		Correlaciones		
	Desv. Error	Beta	t	Sig.	Límite inferior	Límite superior	Orden cero	Parcial	Parte
(Constante)	3.513		2.139	.044	0.209	14.820			
Implementación_de_un_Protocolo_de_Prevención_contra_Ransomware	0.081	0.917	10.504	<.001	0.680	1.016	0.917	0.917	0.917

a. Variable dependiente: Seguridad del Servidor

Fuente: Elaboración propia

Y: Seguridad del Servidor,

La variable independiente es:

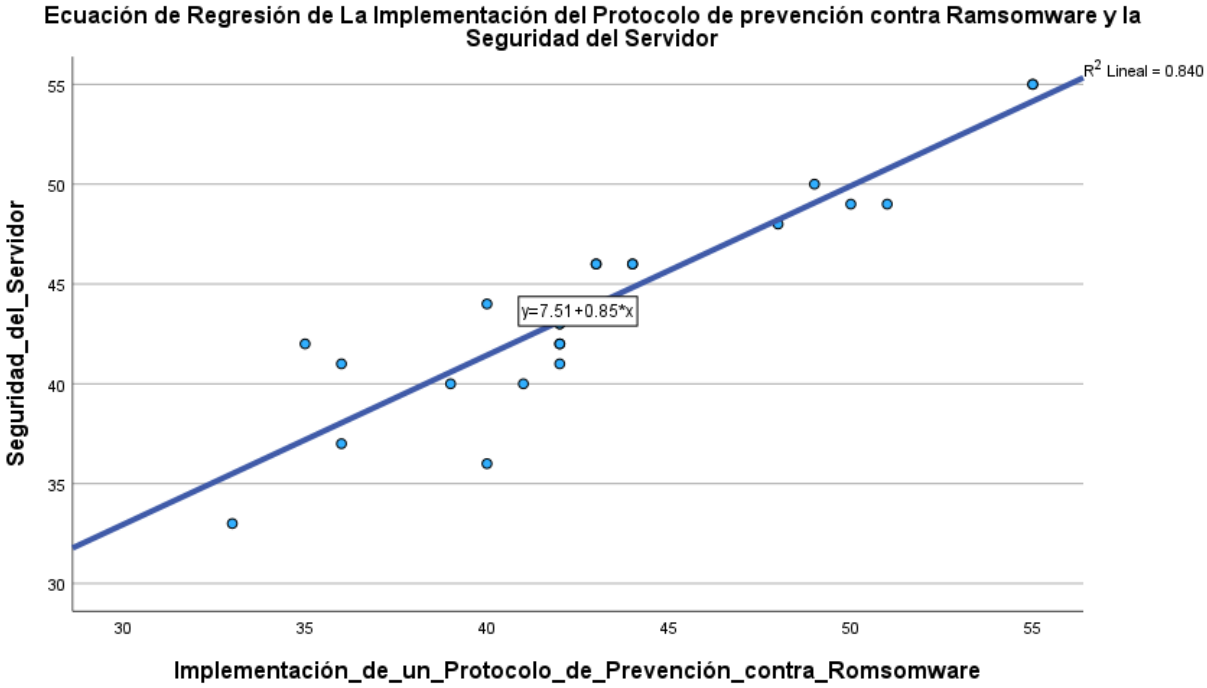
X: La Implementación del Protocolo de prevención contra Ransomware

La siguiente ecuación de regresión es:

Y= 7.15 + 0.848x

Podemos observar que la pendiente es positiva, esto quiere decir que cuando aumenta el puntaje de la Implementación del Protocolo de prevención contra Ransomware aumenta la Seguridad del Servidor.

Figura 24: Gráfica de la ecuación de regresión de hipótesis general dependiente e independiente



Fuente: Elaboración propia

La gráfica de la ecuación de regresión confirma todo nuestro análisis.

Analizaremos los supuestos del modelo de regresión lineal: Independencia, homocedasticidad, normalidad y linealidad.

El estadístico de Durbin-Watson (1951) proporciona información sobre el grado de independencia existente entre ellos:

El estadístico Durbin-Watson oscila entre 0 y 4, cuando toma el valor 2 son independientes, los valores menos de 2 indican autocorrelación positiva y los mayores que 2 autocorrelación negativa. Se puede asumir independencia entre los residuos cuando 1,5 ≤ DW≤2,5.

En nuestro caso DW = 2.478 se tiene autocorrelación negativa y son independientes.

Interpretaciones de los resultados

El 84% de la variabilidad de DW = 2.478 se tiene autocorrelación negativa y son independientes.

El **rs= 0.914** podemos ver que en la correlación de Spearman hay correlación positiva muy alta entre la Implementación del Protocolo de prevención contra Ransomware y los datos de Seguridad del Servidor en la empresa BBTI SAC.

La pendiente de la ecuación de regresión es positiva:

Y = 7.515 +0.848x

VI. DISCUSIÓN DE RESULTADOS

6.1. Contrastación y demostración de la hipótesis con los resultados

6.1.1. Prueba de hipótesis Especifica 1

La implementación de un protocolo de prevención contra ransomware, la adecuada instalación y configuración del software de prevención y una adecuada concientización del personal tendrán un impacto positivo en la resistencia ante ataques de ransomware en la empresa BBTI S.A.C.

Se analizo si la instalación del software de prevención tiene incidencia en la Resistencia al ataque de Ransomware.

Para contrastar esta hipótesis especifica 1, analizaremos el comportamiento de los datos obtenidos, primero analizaremos la Bondad de ajuste (la normalidad), luego analizaremos la correlación y el comportamiento de la recta de regresión de los datos usando el SPSS v29:

Primero analizaremos la normalidad de los datos:

INSTALACIÓN DE SOFTWARE DE PREVENCIÓN.

H0: Los datos de la instalación de software de prevención en la empresa BBTI SAC tienen una distribución normal.

H1: Los datos de la instalación de software de prevención en la empresa BBTI SAC no tienen una distribución normal.

RESISTENCIA AL ATAQUE DE RANSOWARE .

H0: Los datos de Resistencia al ataque de Ransomware en la empresa BBTI SAC tienen una distribución normal.

H1: Los datos de Resistencia al ataque de Ransomware en la empresa BBTI SAC no tienen una distribución normal.

Tabla 33: Hipótesis 1 con dimensiones VD D1 y VI D1

Resistencia al ataque de ransomware	Instalación de software de prevención
20	12
15	10
19	11
20	13
21	12
21	11
19	12
22	12
21	12
20	10
15	9
20	12
19	11
18	12
25	15
25	15
16	10
20	9
22	13
23	13
20	10
22	13
23	13

Fuente: Elaboración propia

Tabla 34: Prueba de normalidad de hipótesis especifica 1 con dimensiones VD D1 y VI D1

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Resistencia_al_Ataque_de_Ransomware	0.156	23	0.150	0.946	23	0.244
Software_de prevención	0.172	23	0.075	0.937	23	0.155

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

Para los datos de la instalación de software el p-valor es 0.155 > 0.05 por lo que se acepta la hipótesis nula: “Los datos de la instalación de software de prevención en la empresa BBTI SAC tienen una distribución normal.”.

Para los datos de Resistencia ante al ataque de Ransomware el p-valor es 0.244 > 0.05 por lo que se acepta la hipótesis nula: “Los datos de Resistencia al ataque de Ransomware en la empresa BBTI SAC tienen una distribución normal.

Análisis de Correlación

H_0: La instalación de software de prevención no se relacionan significativamente con la Resistencia al ataque de Ransomware en la empresa BBTI SAC.

H_1: La instalación de software de prevención se relacionan significativamente con la Resistencia al ataque de Ransomware en la empresa BBTI SAC.

Tabla 35: Correlaciones de hipótesis especifica 1 con dimensiones VD D1 y VI D1

			Resistencia al Ataque de Ransomware	Software_de_prevención
Rho de Spearman	Resistencia al Ataque de Ransomware	Coeficiente de correlación	1.000	0.757**
		Sig. (bilateral)	.	<.001
		N	23	23
	Software de prevención	Coeficiente de correlación	0.757**	1.000
		Sig. (bilateral)	<.001	.
		N	23	23

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia

El Rho de Spearman es 0.757 y de acuerdo a los baremos de estimación de la correlación de Spearman hay correlación positiva alta entre el software de prevención y la Resistencia al ataque de Ransomware.

Además, el nivel de significación que nos arroja el SPSS es 0.001 es menor que 0.05 esto indica que hay evidencias de que existe una relación significativa entre las dos variables, luego podemos concluir que: La instalación de software de prevención se relacionan significativamente con la Resistencia al ataque de Ransomware en la empresa BBTI SAC.

Tabla 36: Estadísticos descriptivos de hipótesis especifica 1 con dimensiones VD D1 y VI D1

	Media	Desv. estándar	N
Resistencia_al_Ataque_de_Ransomware	20.26	2.649	23
Software_de_prevención	11.74	1.630	23

Fuente: Elaboración propia

Lo que buscamos es construir un modelo para determinar la dependencia que exista entre entre el software de prevención y la Resistencia al ataque de Ransomware, cuya la variable dependiente es y: Resistencia al ataque de Ransomware.

la variable independiente es x: el software de prevención

HIPÓTESIS DE REGRESIÓN

H_0: El software de prevención no interviene de manera significativa en la Resistencia al ataque de Ransomware.

H_1: El software de prevención interviene de manera significativa en la Resistencia al ataque de Ransomware.

Consideramos el Nivel de Significación $\alpha = 0.05$.

Análisis Estadístico usando Regresión

Utilizando las fórmulas de las ecuaciones normales a los datos obtendremos los coeficientes de regresión o utilizando Regresión de Análisis de datos, en el SPSS podemos calcular también los coeficientes de regresión:

Tabla 37: Resumen del modelo| de hipótesis especifica 1 con dimensiones VD D1 y VI D1

					Estadísticos de cambio					
Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. Cambio en F	Durbin-Watson
1	0.795[a]	0.633	0.615	1.643	0.633	36.181	1	21	<.001	2.237

a. Predictores: (Constante), Software de prevención

b. Variable dependiente: Resistencia_al_Ataque_de_Ransomware

Fuente: Elaboración propia

En este cuadro del análisis tomamos el Estadístico F que evalúa el ajuste general de la ecuación de regresión si es significativo.

La tabla recoge el valor de R^2, el cambio experimentado por R^2 en cada paso, y el estadístico F y su significación. El estadístico F permite contrastar la hipótesis de que el cambio en R^2 vale cero en la data.

El valor de R^2 es 0.633. Lógicamente, en el primer paso, $R^2_{cambio} = R^2$. Al contrastar la hipótesis de que el valor poblacional de R^2_{cambio} es cero se obtiene un estadístico F de 0,001 que con 1 y 21 grados de libertad, tienen un p-valor de 0,001 (como este valor es menor que 0,05), podemos afirmar que: El software de prevención interviene de manera significativa en la Resistencia al ataque de Ransomware.

Bondad de Ajuste R cuadrado = 0.633

El 63.3% de la variabilidad del software de prevención interviene en la Resistencia al ataque de Ransomware.

El error estándar de la estimación es 1.643.

Por lo que rechazamos la hipótesis nula y aceptamos que: El software de prevención interviene de manera significativa en la Resistencia al ataque de Ransomware.

Todo esto se corrobora al usar las estimaciones

Aquí presentamos el Anova del modelo

Tabla 38: ANOVA de hipótesis especifica 1 con dimensiones VD D1 y VI D1

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	97.718	1	97.718	36.181	<.001[b]
	Residuo	56.717	21	2.701		
	Total	154.435	22			

a. Variable dependiente: Resistencia_al_Ataque_de_Ransomware

b. Predictores: (Constante), Software_de_prevención

Fuente: Elaboración propia

F = 36.181, p´= 0.001<0.05

Se rechaza la hipótesis nula y se concluye que: El software de prevención interviene de manera significativa en la Resistencia al ataque de Ransomware.

Tabla 39: Coeficientes descriptivos de hipótesis especifica 1 con dimensiones VD D1 y VI D1

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados			Correlaciones			Estadísticas de colinealidad	
		B	Desv. Error	Beta	t	Sig.	Orden cero	Parcial	Parte	Tolerancia	VIF
1	(Constante)	5.080	2.547		1.995	0.059					
	Software_de_prevención	1.293	0.215	0.795	6.015	<.001	0.795	**0.795**	**0.795**	1.000	1.000

a. Variable dependiente: Resistencia_al_Ataque_de_Ransomware

Fuente: Elaboración propia

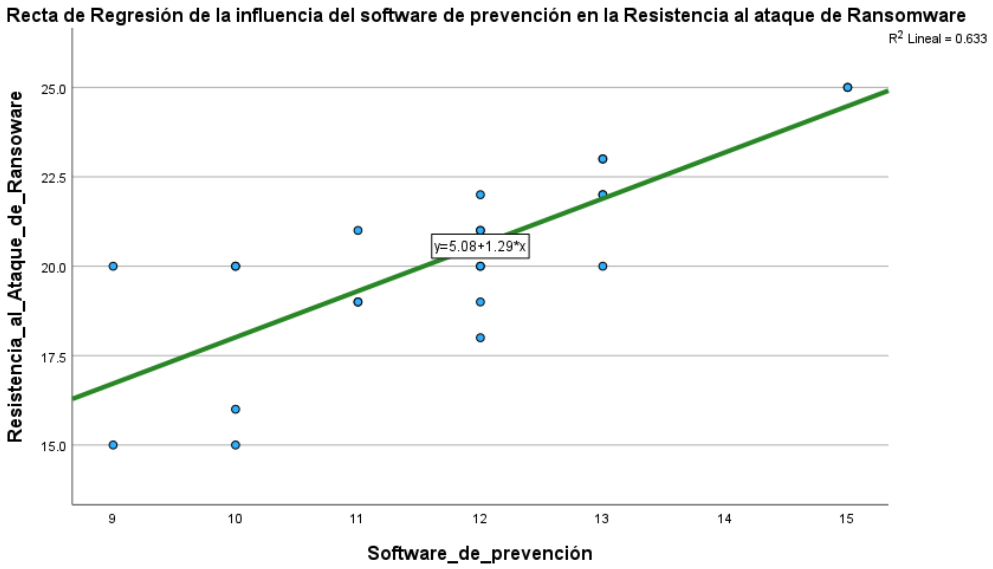
Y: Resistencia al ataque de Ransomware.la variable independiente es:

X: el software de prevención. La siguiente ecuación de regresión es:

y= 5.08 + 1.293x

Podemos observar que la pendiente es positiva, esto quiere decir que cuando aumenta el puntaje de uso del software de prevención aumenta la Resistencia al ataque de Ransomware.

Figura 25: Gráfica de la recta de regresión descriptivos de hipótesis especifica 1 dimensiones VD D1 y VI D1



Fuente: Elaboración propia

La gráfica de la ecuación de regresión confirma todo lo analizado.

Analizaremos los supuestos del modelo de regresión lineal: Independencia, homocedasticidad, normalidad y linealidad.

El estadístico de Durbin-Watson (1951) proporciona información sobre el grado de independencia existente entre ellos:

El estadístico Durbin-Watson oscila entre 0 y 4, cuando toma el valor 2 son independientes, los valores menos de 2 indican autocorrelación positiva y los mayores que 2 autocorrelación negativa. Se puede asumir independencia entre los residuos cuando 1,5 ≤ DW≤2,5.

En nuestro caso DW = 2.237 se tiene autocorrelación negativa y son independientes.

Interpretaciones de los resultados

El 63.3% de la variabilidad de los puntajes de Resistencia al ataque de Ransomware se encuentra explicada por la instalación de software de prevención.

DW = 2.237 se tiene autocorrelación negativa y son independientes.

El rs=0.757 podemos ver que en la correlación de Spearman hay correlación positiva alta entre el software de prevención y la Resistencia al ataque de Ransomware.

La pendiente de la ecuación de regresión es positiva:

y= 5.08 + 1.293x

6.1.2. Prueba de hipótesis especifica 1

Analizaremos si la Instalación de Software de Prevención tiene incidencia en la Reducción de Brecha de Seguridad.

Primero analizaremos la normalidad de los datos:

INSTALACIÓN DE SOFTWARE DE PREVENCIÓN.

H_0: Los datos de la instalación de software de prevención en la empresa BBTI SAC tienen una distribución normal.

H_1: Los datos de la instalación de software de prevención en la empresa BBTI SAC no tienen una distribución normal.

REDUCCIÓN DE BRECHA DE SEGURIDAD.

H_0: Los datos de Reducción de Brecha de Seguridad en la empresa BBTI SAC tienen una distribución normal.

H_1: Los datos de Reducción de Brecha de Seguridad en la empresa BBTI SAC no tienen una distribución normal.

Tabla 40: Hipótesis especifica 1 con dimensiones VD D1 y VI D3

Reducción de brecha de seguridad	Instalación de software de prevención
12	12
12	10
11	11
13	13
11	12
12	11
11	12
12	12
12	12
11	10
9	9
10	12
10	11
12	12
15	15
15	15
11	10
10	9
14	13
14	13
11	10
14	13
13	13

Fuente: Elaboración propia

Tabla 41: Prueba de normalidad de hipótesis especifica 1 con dimensiones VD D1 y VI D3

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Reducción_de_Brecha_de_Seguridad	0.185	23	0.040	0.942	23	0.196
Software_de_prevención	0.172	23	0.075	0.937	23	0.155

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

Para los datos de Reducción de Brecha de Seguridad el p-valor es 0.196 > 0.05 por lo que se acepta la hipótesis nula: “Los datos de Reducción de Brecha de Seguridad en la empresa BBTI SAC tienen una distribución normal.”

Para los datos Instalación de Software de Prevención el p-valor es 0.155 > 0.05 por lo que se acepta la hipótesis nula: “Los datos de la instalación de software de prevención en la empresa BBTI SAC tienen una distribución normal”.

Análisis de Correlación

H_0: La instalación de software de prevención no se relacionan significativamente con la Reducción de Brecha de Seguridad en la empresa BBTI SAC.

H_1: La instalación de software de prevención se relacionan significativamente con la Reducción de Brecha de Seguridad en la empresa BBTI SAC.

Tabla 42: Correlaciones no paramétricas de hipótesis especifica 1 con dimensiones VD D1 y VI D3

			Reducción_de_Brecha_de_Seguridad	Software_de_prevención
Rho de Spearman	Reducción_de_Brecha_de_Seguridad	Coeficiente de correlación	1.000	0.827**
		Sig. (bilateral)	.	<.001
		N	23	23
	Software_de_prevención	Coeficiente de correlación	0.827**	1.000
		Sig. (bilateral)	<.001	.
		N	23	23

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia

El Rho de Spearman es 0.827 y de acuerdo a los baremos de estimación de la correlación de Spearman hay correlación positiva alta entre la instalación del software de prevención y la Reducción de Brecha de Seguridad.

Además, el nivel de significación que nos arroja el SPSS es 0.001 es menor que 0.05 esto indica que hay evidencias de que existe una relación significativa entre las dos variables, luego podemos concluir que: La instalación de software de prevención se relacionan significativamente con la Reducción de Brecha de Seguridad en la empresa BBTI SAC.

Tabla 41: Estadísticos descriptivos de hipótesis especifica 1 con dimensiones VD D1 y VI D3

	Media	Desv. estándar	N
Reducción_de_Brecha_de_Seguridad	11.96	1.637	23
Software_de_prevención	11.74	1.630	23

Fuente: Elaboración propia

Lo que buscamos es construir un modelo para determinar la dependencia que exista entre entre el software de prevención y la Reducción de Brecha de Seguridad cuya la variable dependiente es y: Reducción de Brecha de Seguridad.

la variable independiente es x: Software de prevención.

HIPÓTESIS DE REGRESIÓN

H_0: El software de prevención no interviene de manera significativa en la Reducción de Brecha de Seguridad.

H_1: El software de prevención interviene de manera significativa en la Reducción de Brecha de Seguridad.

Consideramos el Nivel de Significación $\alpha = 0.05$.

Análisis Estadístico usando Regresión

Utilizando las fórmulas de las ecuaciones normales a los datos obtendremos los coeficientes de regresión o utilizando Regresión de Análisis de datos, en el SPSS podemos calcular también los coeficientes de regresión:

Tabla 42: Resumen del modelo de hipótesis especifica 1 con dimensiones VD D1 y VI D3

					Estadísticos de cambio					
Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. Cambio en F	Durbin-Watson
1	0.847[a]	0.718	0.705	0.890	0.718	53.498	1	21	<.001	1.438

a. Predictores: (Constante), Software de prevención

b. Variable dependiente: Reducción_de_Brecha_de_Seguridad

Fuente: Elaboración propia

En este cuadro del análisis tomamos el Estadístico F que evalúa el ajuste general de la ecuación de regresión si es significativo.

La tabla recoge el valor de R^2, el cambio experimentado por R^2 en cada paso, y el estadístico F y su significación. El estadístico F permite contrastar la hipótesis de que el cambio en R^2 vale cero en la data.

El valor de R^2 es 0.718. Lógicamente, en el primer paso, $R^2_{cambio} = R^2$. Al contrastar la hipótesis de que el valor poblacional de

R^2_{cambio} es cero se obtiene un estadístico F de 0,001 que, con 1 y 21 grados de libertad, tienen un p-valor de 0,001 (como este valor es menor que 0,05), podemos afirmar que: El software de prevención interviene de manera significativa en la Reducción de Brecha de Seguridad.

Bondad de Ajuste **R cuadrado = 0.718.**

El 71.8% de la variabilidad del software de prevención interviene en la Reducción de Brecha de Seguridad.

El error estándar de la estimación es 1.643.

Por lo que rechazamos la hipótesis nula y aceptamos que: El software de prevención interviene de manera significativa en la Reducción de Brecha de Seguridad.

Todo esto se corrobora al usar las estimaciones:

Aquí presentamos el Anova del modelo:

Tabla 43: ANOVA de hipótesis especifica 1 con dimensiones VD D1 y VI D3

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	42.337	1	42.337	53.498	<.001[b]
	Residuo	16.619	21	0.791		
	Total	58.957	22			

a. Variable dependiente: Reducción_de_Brecha_de_Seguridad

b. Predictores: (Constante), Software_de_prevención

Fuente: Elaboración propia

F= 53.498, p=0.001 <0.05.

Se rechaza la hipótesis nula y se concluye que: El software de prevención interviene de manera significativa en la Reducción de Brecha de Seguridad.

Ecuación de Regresión

Tabla 44: Coeficientes de hipótesis especifica 1 con dimensiones VD D1 y VI D3

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados			Correlaciones			Estadísticas de colinealidad	
		B	Desv. Error	Beta	t	Sig.	Orden cero	Parcial	Parte	Tolerancia	VIF
1	(Constante)	1.964	1.379		1.425	0.169					
	Software_de_prevención	0.851	0.116	0.847	7.314	<.001	0.847	0.847	0.847	1.000	1.000

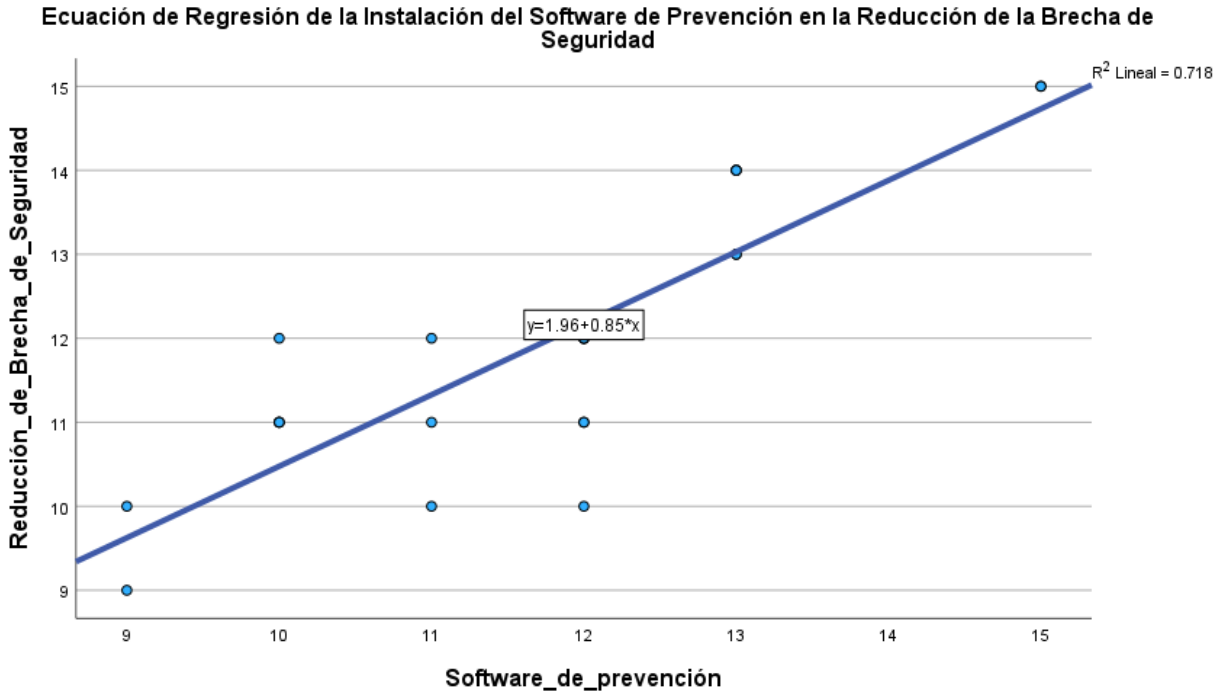
a. Variable dependiente: Reducción_de_Brecha_de_Seguridad

Fuente: Elaboración propia

Y: Reducciónn de Brecha de Seguridad.la variable independiente es: X : el software de prevención.
La siguiente ecuación de regresión es: **Y = 1.964 + 0.851x.**

Podemos observar que la pendiente es positiva, esto quiere decir que cuando aumenta el puntaje de uso del software de prevención aumenta la Reducción de Brecha de Seguridad.

Figura 26: Gráfica de la ecuación de regresión de hipótesis especifica 1 con dimensiones VD D1 y VI D3



Fuente: Elaboración propia

La gráfica de la ecuación de regresión confirma todo lo analizado.

Analizaremos los supuestos del modelo de regresión lineal: Independencia, homocedasticidad, normalidad y linealidad.

El estadístico de Durbin-Watson (1951) proporciona información sobre el grado de independencia existente entre ellos: El estadístico Durbin-Watson oscila entre 0 y 4, cuando toma el valor 2 son independientes, los valores menos de 2 indican autocorrelación positiva y los mayores que 2 autocorrelación negativa. Se puede asumir independencia entre los residuos cuando 1,5 ≤ DW≤2,5.

En nuestro caso DW = 1.438 se tiene autocorrelación positiva y son independientes porque es muy cercano a 1.5.

Interpretación de los resultados

El 71.8% de la variabilidad de los puntajes de Reducción de Brecha de Seguridad se encuentra explicada por la Instalación de software de prevención, DW = 1.438 se tiene autocorrelación positiva y son independientes.

El rs= 0.827 podemos ver que en la correlación de Spearman hay correlación positiva alta entre el software de prevención y la Reducción de Brecha de Seguridad.

La pendiente de la ecuación de regresión es positiva:

Y= 1.964 + 0.851x.

6.1.3. Hipótesis Específica 2

La implementación de un protocolo de prevención contra ransomware, combinada con una capacitación y concienciación efectiva del personal, tendrá un impacto positivo en la reducción del tiempo de recuperación de ataques de ransomware en la empresa BBTI S.A.C.

Se analiza Políticas y Procedimientos de Seguridad en la Reducción de la Brecha de Seguridad. Para contrastar esta hipótesis especifica 2, analizaremos el comportamiento de los datos obtenidos, primero analizaremos la Bondad de ajuste (la normalidad), luego analizaremos la correlación y el comportamiento de la recta de regresión de los datos usando el SPSS v29:

Primero analizaremos la normalidad de los datos:

POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD.

H_0: Los datos de Políticas y Procedimientos de Seguridad en la empresa BBTI SAC tienen una distribución normal.

H_1: Los datos de Políticas y Procedimientos de Seguridad en la empresa BBTI SAC no tienen una distribución normal.

REDUCCIÓN DE BRECHA DE SEGURIDAD.

H_0: Los datos de Reducción de Brecha de Seguridad en la empresa BBTI SAC tienen una distribución normal.

H_1: Los datos de Reducción de Brecha de Seguridad en la empresa BBTI SAC no tienen una distribución normal.

Tabla 45: Hipótesis especifica 2 con dimensiones VD D2 y VI D3

Reducción de brecha de seguridad	Políticas y procedimientos de seguridad
16	12
12	12
17	11
16	13
15	11
17	12
16	11
16	12
15	12
14	11
12	9
16	10
14	10
15	12
20	15
20	15
16	11
12	10
17	10
18	14
13	14
18	11
20	14

Fuente: Elaboración propia

Tabla 46: Prueba de normalidad hipótesis especifica 2 con dimension13es VD D2 y VI D3

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Reducción_de_Brecha_de_Seguridad	0.185	23	0.040	0.942	23	0.196
Políticas_de_Seguridad	0.130	23	0.200*	0.941	23	0.186

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

Para los datos de Reducción de Brecha de Seguridad el p-valor es 0.196 > 0.05 por lo que se acepta la hipótesis nula: “Los datos

de Reducción de Brecha de Seguridad en la empresa BBTI SAC tienen una distribución normal."

Para los datos de Políticas y Procedimientos de Seguridad el p-valor es 0.186 > 0.05 por lo que se acepta la hipótesis nula: "Los datos de Políticas y Procedimientos de Seguridad en la empresa BBTI SAC tienen una distribución normal".

Análisis de Correlación

H_0: Las Políticas y Procedimientos de Seguridad no se relacionan significativamente con la Reducción de Brecha de Seguridad en la empresa BBTI SAC.

H_1: Las Políticas y Procedimientos de Seguridad se relacionan significativamente con la Reducción de Brecha de Seguridad en la empresa BBTI SAC.

Tabla 47: Correlación especifica 2 con dimensiones VD D2 y VI D3

			Reducción_de_Brecha_de_Seguridad	Políticas_de_Seguridad
Rho de Spearman	Reducción_de_Brecha_de_Seguridad	Coeficiente de correlación	1.000	0.736**
		Sig. (bilateral)	.	<.001
		N	23	23
	Políticas_de_Seguridad	Coeficiente de correlación	0.736**	1.000
		Sig. (bilateral)	<.001	.
		N	23	23

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia

El Rho de Spearman es 0.736 y de acuerdo a los baremos de estimación de la correlación de Spearman hay correlación

positiva alta entre las Políticas y Procedimientos de Seguridad y la Reducción de Brecha de Seguridad.

Además, el nivel de significación que nos arroja el SPSS es 0.001 es menor que 0.05 esto indica que hay evidencias de que existe una relación significativa entre las dos variables, luego podemos concluir que: Las Políticas y Procedimientos de Seguridad se relacionan significativamente con la Reducción de Brecha de Seguridad en la empresa BBTI SAC.

Tabla 48: Estadísticos descriptivos especifica 2 con dimensiones VD D2 y VI D3

	Media	Desv. estándar	N
Reducción_de_Brecha_de_Seguridad	11.96	1.637	23
Políticas_de_Seguridad	15.87	2.399	23

Fuente: Elaboración propia

Lo que se busca es construir un modelo para determinar la dependencia que exista entre entre las Políticas y Procedimientos de Seguridad y la Reducción de Brecha de Seguridad. cuya la variable dependiente es y: Reducción de Brecha de Seguridad, la variable independiente es x: Políticas y Procedimientos de Seguridad.

Hipótesis de regresión

H_0: Las Políticas y Procedimientos de Seguridad no interviene de manera significativa en la Reducción de Brecha de Seguridad.

H_1: Las Políticas y Procedimientos de Seguridad interviene de manera significativa en la Reducción de Brecha de Seguridad

Consideramos el Nivel de Significación.

Análisis Estadístico usando Regresión

Utilizando las fórmulas de las ecuaciones normales a los datos obtendremos los coeficientes de regresión o utilizando Regresión de Análisis de datos, en el SPSS podemos calcular también los coeficientes de regresión:

Utilizando las fórmulas de las ecuaciones normales a los datos obtendremos los coeficientes de regresión o utilizando Regresión de Análisis de datos, en el SPSS podemos calcular también los coeficientes de regresión:

Tabla 49: Resumen del modelo descriptivo especifica 2 con dimensiones VD D2 y VI D3

					Estadísticos de cambio					
Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. Cambio en F	Durbin-Watson
1	0.774	0.599	0.580	1.061	0.599	31.375	1	21	<.001	1.902

a. Predictores: (Constante), Políticas_de_Seguridad

b. Variable dependiente: Reducción_de_Brecha_de_Seguridad

Fuente: Elaboración propia

En este cuadro del análisis tomamos el Estadístico F que evalúa el ajuste general de la ecuación de regresión si es significativo.

La tabla recoge el valor de R^2, el cambio experimentado por R^2 en cada paso, y el estadístico F y su significación. El estadístico F permite contrastar la hipótesis de que el cambio en R^2 vale cero en la data.

El valor de R^2 es 0.599. Lógicamente, en el primer paso, $R^2_{cambio} = R^2$. Al contrastar la hipótesis de que el valor poblacional de R^2_{cambio} es cero se obtiene un estadístico F de 0,001 que, con 1 y 21 grados de libertad, tienen un p-valor de 0,001 (como este valor es menor que 0,05), podemos afirmar que: Las Políticas y Procedimientos de Seguridad interviene de manera significativa en la Reducción de Brecha de Seguridad.

Bondad de Ajuste, R al cuadrado = 0.599.

El 59.9% de la variabilidad del las Políticas y Procedimientos de Seguridad interviene en la Reducción de Brecha de Seguridad.

El error estándar de la estimación es 1.061.

Por lo que rechazamos la hipótesis nula y aceptamos que:

Las Políticas y Procedimientos de Seguridad interviene de manera significativa en la Reducción de Brecha de Seguridad. Todo esto se corrobora al usar las estimaciones:

Aquí presentamos el Anova del modelo

Tabla 50: ANOVA de hipótesis especifica 2 con dimensiones VD D2 y VI D3

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	35.318	1	35.318	31.375	<.001[b]
	Residuo	23.639	21	1.126		
	Total	58.957	22			

a. Variable dependiente: Reducción_de_Brecha_de_Seguridad
b. Predictores: (Constante), Políticas_de_Seguridad

Fuente: Elaboración propia

F= 31.375, p=0.001 <0.05

Se rechaza la hipótesis nula y se concluye que: Las Políticas y Procedimientos de Seguridad interviene de manera significativa en la Reducción de Brecha de Seguridad.

Tabla 51: Coeficientes descriptivos especifica 2 con dimensiones VD D2 y VI D3

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados			Correlaciones			Estadísticas de colinealidad	
		B	Desv. Error	Beta	t	Sig.	Orden cero	Parcial	Parte	Tolerancia	VIF
1	(Constante)	3.575	1.513		2.363	0.028					
	Políticas_de_Seguridad	0.528	0.094	0.774	5.601	<.001	0.774	0.774	0.774	1.000	1.000

Fuente: Elaboración propia

Y:

Reducción de Brecha de Seguridad.

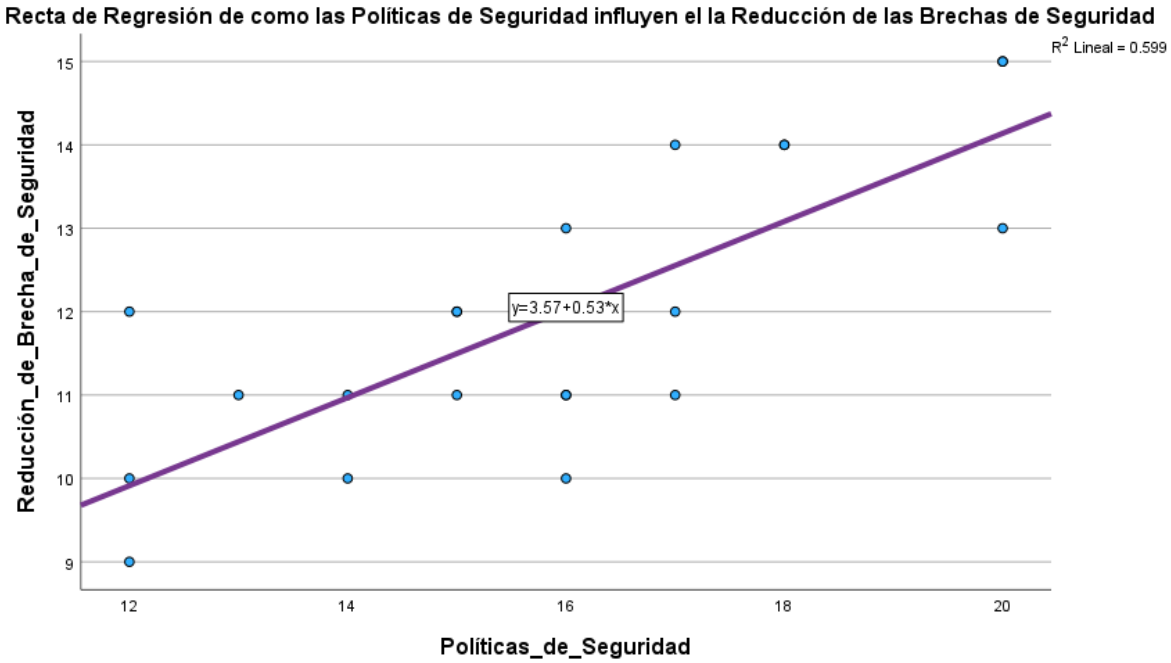
La variable independiente es x: Políticas y Procedimientos de Seguridad.

La siguiente ecuación de regresión es:

Y = 3.575+ 0.528x

Podemos observar que la pendiente es positiva, esto quiere decir que cuando aumenta el puntaje de las Políticas y Procedimientos de Seguridad, aumenta la Reducción de Brecha de Seguridad.

Figura 27: Gráfica de la recta de regresión descriptivos especifica 2 con dimensiones VD D2 y VI D3



Fuente: Elaboración propia

La gráfica de la ecuación de regresión confirma todo lo analizado.

Analizaremos los supuestos del modelo de regresión lineal: Independencia, homocedasticidad, normalidad y linealidad.

El estadístico de Durbin-Watson (1951) proporciona información sobre el grado de independencia existente entre ellos:

El estadístico Durbin-Watson oscila entre 0 y 4, cuando toma el valor 2 son independientes, los valores menos de 2 indican autocorrelación positiva y los mayores que 2 autocorrelación

negativa. Se puede asumir independencia entre los residuos cuando 1,5 ≤ DW≤2,5.

En nuestro caso DW = 1.902 se tiene autocorrelación positiva y son independientes.

Interpretando los resultados

El 59.9% de la variabilidad de los puntajes de Reducción de Brecha de Seguridad se encuentra explicada por las Políticas y Procedimientos de Seguridad.

DW =1.902 se tiene autocorrelación positiva y son independientes.

El rs = 0.736 podemos ver que en la correlación de Spearman hay correlación positiva alta entre el software de prevención y la Reducción de Brecha de Seguridad.

La pendiente de la ecuación de regresión es positiva:

Y = 3.575 + 0.528x

6.1.4. Hipótesis Específica 3

La implementación de un protocolo de prevención contra ransomware, combinada con una capacitación y concienciación efectiva del personal, tendrá un impacto positivo en la reducción de la brecha de seguridad en la empresa BBTI S.A.C.

Se analiza la Capacitación y Concientización del Personal en la Reducción de la Brecha de Seguridad para contrastar nuestra hipótesis específica 3.

Para contrastar esta hipótesis especifica 3, analizaremos el comportamiento de los datos obtenidos, primero analizaremos la Bondad de ajuste (la normalidad), luego analizaremos la correlación y el comportamiento de la recta de regresión de los datos usando el SPSS v29:

Primero analizaremos la normalidad de los datos:

CAPACITACIÓN Y CONCIENTIZACIÓN DE PERSONAL.

H_0: Los datos de Capacitación y Concientización de Personal en la empresa BBTI SAC tienen una distribución normal.

H_1: Los datos de Capacitación y Concientización de Personal en la empresa BBTI SAC no tienen una distribución normal.

REDUCCIÓN DE BRECHA DE SEGURIDAD.

H_0: Los datos de Reducción de Brecha de Seguridad en la empresa BBTI SAC tienen una distribución normal.

H_1: Los datos de Reducción de Brecha de Seguridad en la empresa BBTI SAC no tienen una distribución normal.

Tabla 52: Hipótesis especifica 2 con dimensiones VD D3 y VI D3

Capacitación y concientización del personal	Reducción de la brecha de seguridad
14	12
14	12
14	11
14	13
15	11
16	12
14	11
16	12
16	12
16	11
12	9
13	10
14	10
15	12
20	15
20	15
14	11
14	10
18	14
18	14
13	11
19	14
18	13

Fuente: Elaboración propia

Tabla 53: Prueba de normalidad de Hipótesis especifica 2 con dimensiones VD D3 y VI D3

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Reducción_de_Brecha_de_Seguridad	0.185	23	0.040	0.942	23	0.196
Capacitación_de_Personal	0.225	23	0.004	0.900	23	0.025

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

Para los datos de Reducción de Brecha de Seguridad el p-valor es 0.196 > 0.05 por lo que se acepta la hipótesis nula: “Los datos de Reducción de Brecha de Seguridad en la empresa BBTI SAC tienen una distribución normal.”

Para los datos de Capacitación y Concientización de Personal el p-valor es 0.025 < 0.05 por lo que se rechaza la hipótesis nula y se acepta la hipótesis alterna: “Los datos de Capacitación y Concientización de Personal en la empresa BBTI SAC no tienen una distribución normal”.

Análisis de los residuos

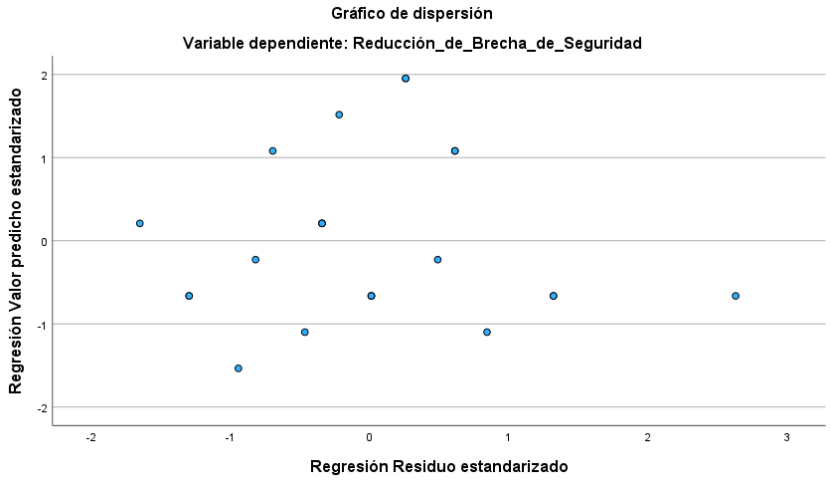
Nuestro trabajo es analizar los residuos y ver si estos valores siguen una distribución normal.

Primero veremos el grafico de probabilidad normal (QQ-Plot)

Un gráfico de probabilidad normal compara los residuos con una distribución normal teórica. Si los puntos del QQ-Plot siguen aproximadamente una línea recta, indica que los residuos se distribuyen normalmente. Las desviaciones significativas de la línea pueden indicar la no normalidad de los residuos.

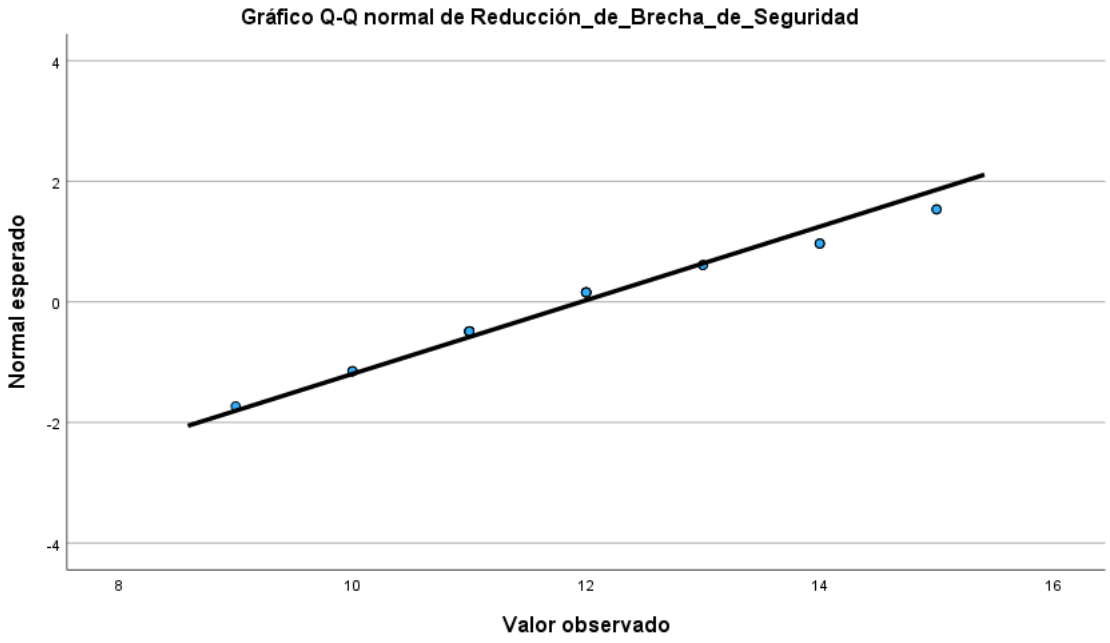
El gráfico de dispersión de los residuos frente a los valores ajustados (predichos) nos ayudan a verificar si hay patrones sistemáticos en los residuos. En un modelo adecuado, los residuos deberían estar distribuidos aleatoriamente alrededor de cero y no mostrar un patrón claro. Si se observa un patrón en el gráfico, como lo es una tendencia lineal o no lineal, podría indicar que el modelo no es adecuado.

Figura 28: Gráfica de la dispersión de variable dependiente de Hipótesis especifica 2 con dimensiones VD D3 y VI D3



Fuente: Elaboración propia

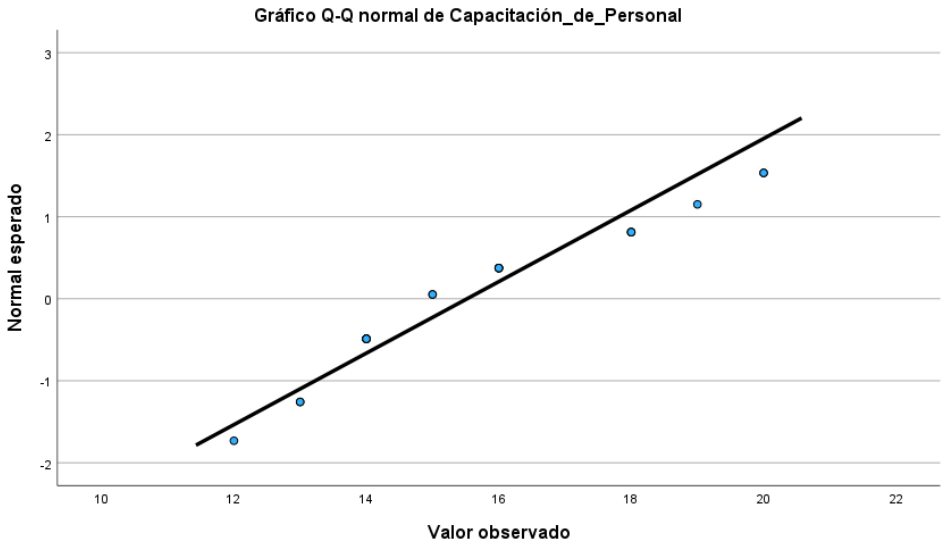
Figura 29: Gráfica de la Q-Q normal reducción de brecha de seguridad



Fuente: Elaboración propia

Observamos que en la variable Brecha de seguridad Q-Q los puntos siguen muy cerca de la recta, pero un poco dispersos esto nos indica que los residuos siguen una distribución normal.

Figura 30: Gráfica de la Q-Q normal capacitación del personal



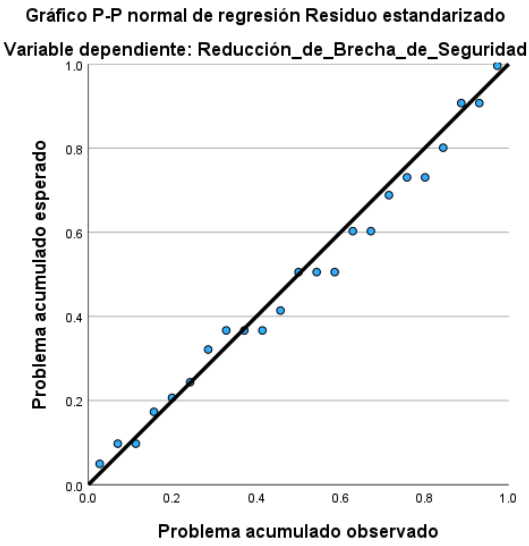
Fuente: Elaboración propia

Observamos que en la variable Capacitación de Personal Q-Q los puntos siguen muy cerca de la recta, pero dispersos esto nos indica que los residuos siguen una distribución normal.

Para obtener los residuos se restan los valores observados de los valores predichos para nuestro modelo de regresión. Los residuos se representan como:

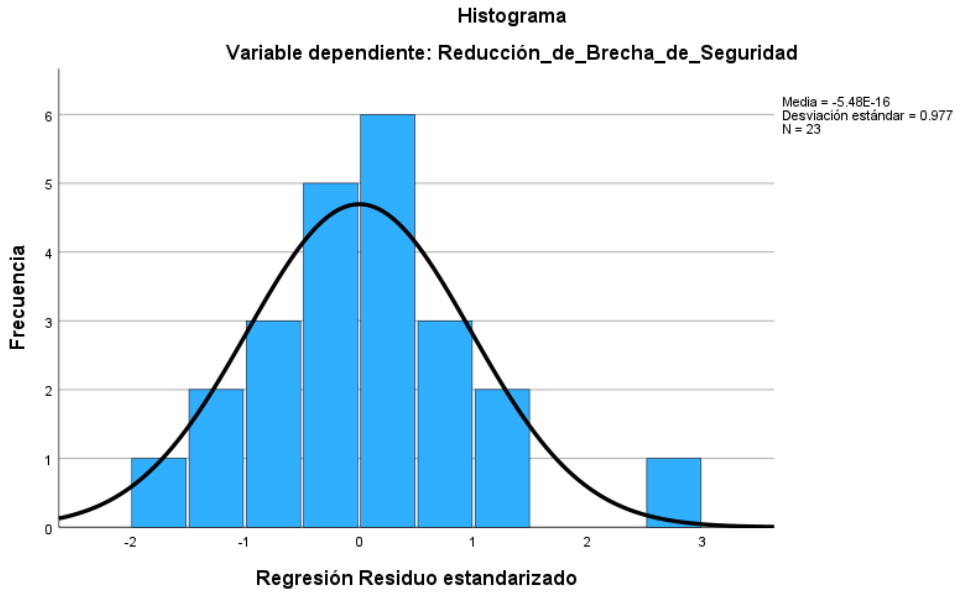
$e_i = y_i - y_i$, donde e_i es el residuo para la observación i, y_i es el valor observado y, y_i es el valor predicho.

Figura 31: Gráfico de la Q-Q normal Regresión residuo estandarizado



Fuente: Elaboración propia

Figura 32: Gráfica del Histograma reducción de brecha de seguridad



Fuente: Elaboración propia

Tabla 54: Recuentos de casilla y residuos Hipótesis especifica 2 con dimensiones VD D3 y VI D3

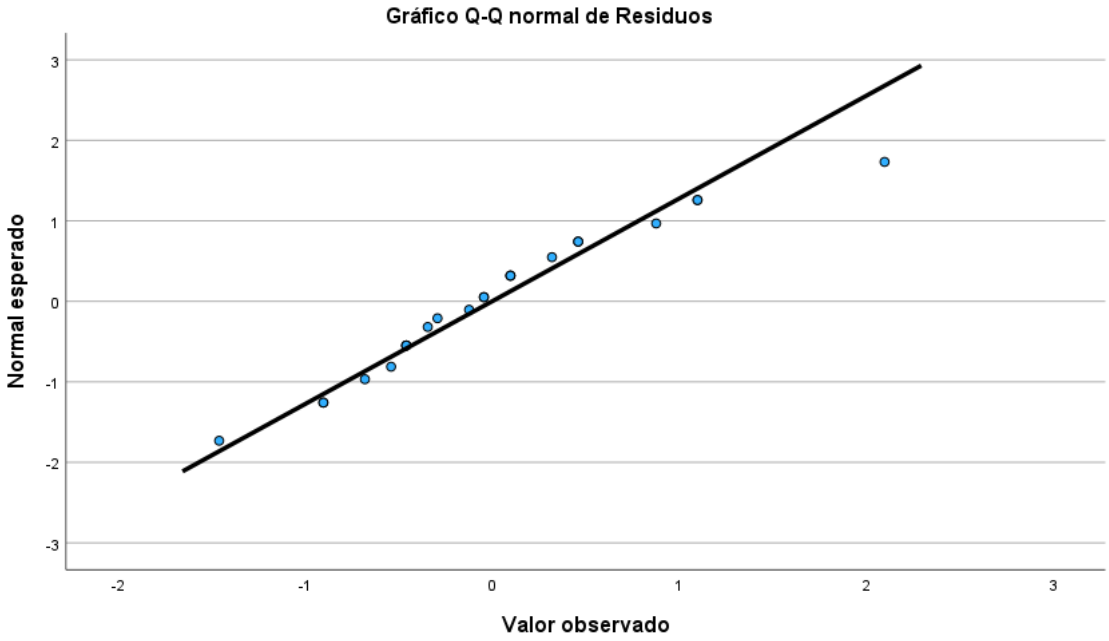
Recuentos de casilla y residuos

	Número	Categoría de respuesta pronosticada	Número de sujetos	Respuestas observadas	Respuestas esperadas	**Residuo**	Probabilidad
LOGIT	1	2.197	14	12	10.902	1.098	.779
	2	2.197	14	12	10.902	1.098	.779
	3	2.197	14	11	10.902	0.098	.779
	4	2.197	14	13	10.902	2.098	.779
	5	2.197	15	11	11.680	-.680	.779
	6	2.197	16	12	12.459	-.459	.779
	7	2.197	14	11	10.902	.098	.779
	8	2.197	16	12	12.459	-.459	.779
	9	2.197	16	12	12.459	-.459	.779
	10	2.197	16	11	12.459	-1.459	.779
	11	2.197	12	9	9.344	-.344	.779
	12	2.197	13	10	10.123	-.123	.779
	13	2.197	14	10	10.902	-.902	.779
	14	2.197	15	12	11.680	.320	.779
	15	2.708	20	15	15.044	-.044	.752
	16	2.708	20	15	15.044	-.044	.752
	17	2.197	14	11	10.902	.098	.779
	18	2.197	14	10	10.902	-.902	.779
	19	2.708	18	14	13.540	.460	.752
	20	2.708	18	14	13.540	.460	.752
	21	2.197	13	11	10.123	.877	.779
	22	2.708	19	14	14.292	-.292	.752
	23	2.708	18	13	13.540	-.540	.752

Fuente: Elaboración propia

El residuo los sometemos a la prueba de normalidad.
Como se puede observar todos los residuos están muy cerca a “0” y no muestran un patrón claro los nos indica que tiene los residuos una distribución normal como los vamos a comprobar.

Figura 33: Gráfica de la Q-Q normal residuos



Fuente: Elaboración propia

H_0: Los datos de los residuos de los datos esperados y observados en la implementación de protocolo de prevención contra ransomware en empresa BBTI SAC tienen una distribución normal.

H_1: Los datos de los residuos de los datos esperados y observados en la implementación de protocolo de prevención contra ransomware en empresa BBTI SAC no tienen una distribución normal.

Tabla 55: Prueba de normalidad tabla x Recuentos de casilla y residuos Hipótesis especifica 2 con dimensiones VD D3 y VI D3

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Residuos	0.146	23	0.200*	0.958	23	0.426

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

El p-valor es 0.426 > 0.05 luego acepta la hipótesis nula: “Los datos de los residuos de los datos esperados y observados en la implementación de protocolo de prevención contra ransomware en empresa BBTI SAC tienen una distribución normal”

OBSERVACIÓN: Ya podemos seguir con el análisis de validación de la hipótesis propuesta, siguiendo el análisis de incidencia.

Análisis de Correlación

H_0: Los datos de Capacitación y Concientización de Personal no se relacionan significativamente con la Reducción de Brecha de Seguridad en la empresa BBTI SAC.

H_1: Los datos de Capacitación y Concientización de Personal se relacionan significativamente con la Reducción de Brecha de Seguridad en la empresa BBTI SAC.

Tabla 56: Correlaciones Hipótesis especifica 2 con dimensiones VD D3 y VI D3

			Reducción_de_Brecha_de_Seguridad	Capacitación_de_Personal
Rho de Spearman	Reducción_de_Brecha_de_Seguridad	Coeficiente de correlación	1.000	0.822**
		Sig. (bilateral)	.	<.001
		N	23	23
	Capacitación_de_Personal	Coeficiente de correlación	0.822**	1.000
		Sig. (bilateral)	<.001	.
		N	23	23

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia

El Rho de Spearman es 0.822 y de acuerdo a los baremos de estimación de la correlación de Spearman hay correlación positiva alta entre las Políticas y Procedimientos de Seguridad y la Reducción de Brecha de Seguridad.

Además, el nivel de significación que nos arroja el SPSS es 0.001 es menor que 0.05 esto indica que hay evidencias de que existe una relación significativa entre las dos variables, luego podemos concluir que: “Los datos de Capacitación y Concientización de Personal se relacionan significativamente con la Reducción de Brecha de Seguridad en la empresa BBTI SAC”.

Tabla 57: Estadísticos descriptivos Hipótesis especifica 2 con dimensiones VD D3 y VI D3

	Media	Desv. estándar	N
Reducción_de_Brecha_de_Seguridad	11.96	1.637	23
Capacitación_de_Personal	15.52	2.294	23

Fuente: Elaboración propia

Lo que se busca es construir un modelo para determinar la dependencia que exista entre entre la Capacitación y Concientización de Personal y la Reducción de Brecha de Seguridad.

Cuya la variable dependiente es y: Reducción de Brecha de Seguridad.

La variable independiente es x: Capacitación y Concientización de Personal.

Hipótesis de regresión

H_0: La Capacitación y Concientización de Personal no interviene de manera significativa en la Reducción de Brecha de Seguridad.

H_1: La Capacitación y Concientización de Personal interviene de manera significativa en la Reducción de Brecha de Seguridad.

Consideramos el Nivel de Significación $\alpha = 0.05$.

Análisis Estadístico usando Regresión

Utilizando las fórmulas de las ecuaciones normales a los datos obtendremos los coeficientes de regresión o utilizando Regresión de Análisis de datos, en el SPSS podemos calcular también los coeficientes de regresión:

Tabla 58: Resumen del modelo Hipótesis especifica 2 con dimensiones VD D3 y VI D3

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Estadísticos de cambio					Durbin-Watson
					Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. Cambio en F	
1	0.890	0.792	0.782	0.764	0.792	80.045	1	21	<.001	1.627

a. Predictores: (Constante), Capacitación de Personal

b. Variable dependiente: Reducción_de_Brecha_de_Seguridad

Fuente: Elaboración propia

En este cuadro del análisis tomamos el Estadístico F que evalúa el ajuste general de la ecuación de regresión si es significativo.

La tabla recoge el valor de R^2, el cambio experimentado por R^2 en cada paso, y el estadístico F y su significación. El estadístico F permite contrastar la hipótesis de que el cambio en R^2 vale cero en la data.

El valor de R^2 es 0.792. Lógicamente, en el primer paso, $R^2_{cambio} = R^2$.

Al contrastar la hipótesis de que el valor poblacional de R^2_{cambio} es cero se obtiene un estadístico F de 0,001 que, con 1 y 21 grados de libertad, tienen un p-valor de 0,001 (como este valor es menor que 0,05), podemos afirmar que: La Capacitación y Concientización de Personal interviene de manera significativa en la Reducción de Brecha de Seguridad.

Bondad de Ajuste R cuadrado = 0.792

El 79.2% de la variabilidad del la Capacitación y Concientización de Personal interviene en la Reducción de Brecha de Seguridad.

El error estándar de la estimación es 0.764. Por lo que rechazamos la hipótesis nula y aceptamos que: La Capacitación y Concientización de Personal interviene de manera significativa en la Reducción de Brecha de Seguridad.

Todo esto se corrobora al usar las estimaciones.

Aquí presentamos el Anova del modelo:

Tabla 59: ANOVA Hipótesis especifica 2 con dimensiones VD D3 y VI D3

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	46.704	1	46.704	80.045	<.001[b]
	Residuo	12.253	21	0.583		
	Total	58.957	22			

a. Variable dependiente: Reducción_de_Brecha_de_Seguridad

b. Predictores: (Constante), Capacitación_de_Personal

Fuente: Elaboración propia

F = 80.045, p=0.001 < 0.05

Se rechaza la hipótesis nula y se concluye que: La Capacitación y Concientización de Personal interviene de manera significativa en la Reducción de Brecha de Seguridad.

Tabla 60: Coeficientes Hipótesis especifica 2 con dimensiones VD D3 y VI D3

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados		95.0% intervalo de confianza para B		Correlaciones			Estadísticas de colinealidad	
		B	Desv. Error	Beta	Sig.	Límite inferior	Límite superior	Orden cero	Parcial	Parte	Tolerancia	VIF
1	(Constante)	2.097	1.114		0.074	-0.219	4.412					
	Capacitación_de_Personal	0.635	0.071	0.890	<.001	0.488	0.783	0.890	0.890	0.890	1.000	1.000

a. Variable dependiente: Reducción_de_Brecha_de_Seguridad

Fuente: Elaboración propia

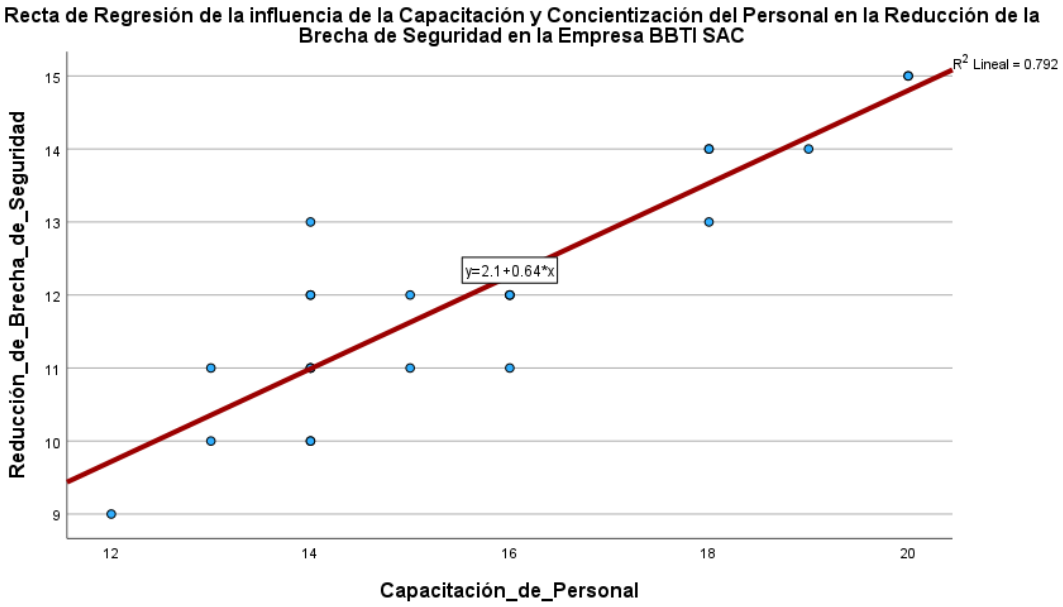
Y: Reducción de Brecha de Seguridad.

La variable independiente es x: La Capacitación y Concientización de Personal.

La siguiente ecuación de regresión es Y = 2.097 + 0.635x

Podemos observar que la pendiente es positiva, esto quiere decir que cuando aumenta el puntaje de la Capacitación y Concientización de Personal Aumenta la Reducción de Brecha de Seguridad.

Figura 34: Gráfica de la recta de regresión Hipótesis especifica 2 con dimensiones VD D3 y VI D3



Fuente: Elaboración propia

La gráfica de la ecuación de regresión confirma todo nuestro análisis.

Analizaremos los supuestos del modelo de regresión lineal: Independencia, homocedasticidad, normalidad y linealidad.

El estadístico de Durbin-Watson (1951) proporciona información sobre el grado de independencia existente entre ellos:

El estadístico Durbin-Watson oscila entre 0 y 4, cuando toma el valor 2 son independientes, los valores menos de 2 indican autocorrelación positiva y los mayores que 2 autocorrelación negativa. Se puede asumir independencia entre los residuos cuando 1,5 ≤ DW≤2,5.

En nuestro caso DW = 1.627 se tiene autocorrelación positiva y son independientes.

Interpretaciones de los resultados

El 79.2% de la variabilidad de los puntajes de Reducción de Brecha de Seguridad se encuentra explicada por la Influencia de la capacitación y

Concientización. DW = 1.627 se tiene autocorrelación positiva y son independientes.

El rs = 0.822 podemos ver que en la correlación de Spearman hay correlación positiva alta entre la Influencia de la capacitación y Concientización.y la Reducción de Brecha de Seguridad.

La pendiente de la ecuación de regresión es positiva: y = 2.097 + 0.635x

Implementación de protocolo de prevención contra ransomware tendrá un impacto positivo en la reducción de la brecha de seguridad *en la empresa BBTI S.A.C.*

6.2. Contrastación de los resultados con otros estudios similares.

Según el autor (Trevejo, 2022) en la tesis titulada " Plan de continuidad de negocio de un file server ante un ataque de malware en Cloud " en su objetivo principal que es la elaboración de un plan o guía ante un ataque de malware en cloud y nuestro objetivo es buscar que nuestro protocolo mejorar la seguridad del servidor contra los ataques de ransomware habiendo utilizado la metodología practica y experimental tomando como muestra a las empresas que utilizan Windows server 2012r2 en adelante en la cual el investigador uso los instrumentos de encuesta y como resultado demuestro que se obtiene mejoras de nivel en comparación del enfoque tradicional y demuestra una protección más eficaz ante otras metodologías siempre y cuando se cumplan y respete las normas de perímetro propuestas con un estricto cumplimiento.

En la presente investigación se tuvo como objetivo general determinar que la implementación de un protocolo de prevención contra ransomware mejora la seguridad del servidor de la empresa BBTI S.A.C. utilizado la metodología experimental tomando como muestra a 23 personas de la sede central del callao de la empresa BBTI SAC uso los instrumentos de encuesta y como resultado se demostró que la implementación de un protocolo de prevención contra ransomware genero una mejora considerable a la seguridad

tanto del servidor como el nivel de concientización del personal y la manera de cómo actuar e interpretar los problemas y se reflejado en las encuestas ya que en gran parte de las encuesta tenemos un alto índice de aprobación y notoriedad de mejora por parte de los trabajadores.

En ambos trabajos se muestra que la implementación exitosa de protocolos contra ransomware en diferentes contextos puede generar un grado positivo de efectividad y eficacia de tales medidas en diversas situaciones que son notorias tanto en las encuestas como por parte del personal y presentes de dichos trabajos de investigación.

Según el autor (chow Zamora, 2018) con su tesis titulada “Prevención de ataques de Ransomware conocidos en redes informáticas, utilizando la tecnología Check Point Sandblast en el perímetro y en usuarios finales comprendido en el periodo de septiembre del 2017 a abril del 2018” cuyo objetivo general es “Evaluar si la tecnología SandBlast de Checkpoint, es la opción más viable para proteger la red informática de una empresa de los ataques de Ransomware Cerber, Goldeneye y Criptolocker” en su objetivo principal que es desarrollar una propuesta de seguridad para empresas grandes y medianas que buscan mejorar su seguridad perimetral y mitigar amenazas de Ransomware, incluyendo tanto los casos conocidos como los avanzados que usa la metodología aplicada experimental tomando como muestra hipotética ya que el autor se refiere sistemas y redes con los instrumentos de encuestas y resultados de eficacia de Check Point Sandblast en la resolución de casos conocidos y avanzados de Ransomware.

En la presente investigación se tuvo como objetivo general determinar que la implementación de un protocolo de prevención contra ransomware mejora la seguridad del servidor de la empresa BBTI S.A.C. utilizado la metodología experimental tomando como muestra a 23 personas de la sede central del callao de la empresa

BBTI SAC uso los instrumentos de encuesta y como resultado se demostró que la implementación de un protocolo de prevención contra ransomware genero una mejora considerable a la seguridad tanto del servidor como el nivel de concientización del personal y la manera de cómo actuar e interpretar los problemas y se reflejado en las encuestas ya que en gran parte de las encuesta tenemos un alto índice de aprobación y notoriedad de mejora por parte de los trabajadores.

En ambos trabajos se muestra que la implementación exitosa de protocolos contra ransomware en empresas grandes y medianas en diferentes contextos puede generar un grado positivo de efectividad y eficacia de la ciberseguridad en diversas situaciones son notorias tanto en las encuestas como en la parte del personal y presentes de dichos trabajos de investigación.

Según los autores (Perez Diaz , 2021) en la tesis titulada “Implementación de Tecnología Sandbox para Proteger de Ataques Ransomware en una Red Informática Local de una Entidad Financiera” en su objetivo principal es la implementación de Cuckoo Sandbox, una herramienta de código abierto para el análisis de Ransomware, con el propósito de contribuir a la seguridad perimetral de la red informática. La metodología aplicada es experimental. La muestra a usar consiste en el laboratorio de pruebas virtualizado con 5 equipos Windows 10, que simula una red informática similar a la de la Coopac Norandino Ltda. Los instrumentos utilizados son Cuckoo Sandbox y el Servidor torre Core i5 con 16 gb de RAM con Ubuntu 20.04 LTS como plataforma de implementación de Cuckoo Sandbox. Los resultados demuestran que Cuckoo Sandbox es efectivo en la contribución a la seguridad perimetral de la red informática al detectar y aislar Ransomware de manera eficaz en un entorno de laboratorio.En la presente investigación se tuvo como objetivo principal determinar que la implementación de un protocolo de prevención contra ransomware mejora la seguridad del servidor de la empresa BBTI S.A.C. utilizado la metodología experimental

tomando como muestra a 23 personas de la sede central del callao de la empresa BBTI SAC uso los instrumentos de encuesta y como resultado se demostró que la implementación de un protocolo de prevención contra ransomware genero una mejora considerable a la seguridad tanto del servidor como el nivel de concientización del personal y la manera de cómo actuar e interpretar los problemas y se reflejado en las encuestas ya que en gran parte de las encuesta tenemos un alto índice de aprobación y notoriedad de mejora por parte de los trabajadores.

En ambos trabajos se muestra que la implementación exitosa de protocolos contra ransomware en diferentes contextos puede generar un grado positivo de efectividad y eficacia de tales medidas en diversas situaciones que son notorias tanto en las encuestas como por parte del personal y presentes de dichos trabajos de investigación.

El segundo antecedente nacional está desarrollado por la autora (Chira Castillo, 2021) sustentó la tesis con el título "Implementación de un plan de control y seguridad de los activos de información en la Estación de Servicios San José" en la Universidad César Vallejo su objetivo general es Implementar un plan de control y seguridad basado en la metodología Cobit para la mejora de los activos de información en la Estación de Servicios San José. La metodología se llevó a cabo mediante una investigación de tipo cuasi experimental con un solo grupo. La muestra que han considerado son 13 personas, que incluía al gerente y al personal de la estación de servicios. Los instrumentos que se utilizaron para recopilar datos fueron cuestionarios sobre aceptación del plan de control, cuestionarios sobre eficiencia en la toma de decisiones y guías de observación. Los resultados indican una reducción significativa en los errores de facturación, una menor frecuencia de caídas del servidor, un mejor control en la emisión de vales y una aceptación favorable por parte del personal. Además, la gerencia pudo tomar decisiones más eficientes gracias a la implementación del plan.

Estos hallazgos respaldan la eficacia del plan de control y seguridad en la mejora de la gestión de activos de información en la estación de servicios.

En ambos trabajos se muestra que la implementación exitosa de protocolos contra ransomware en diferentes contextos puede generar un grado positivo de efectividad y eficacia de tales medidas en diversas situaciones que son notorias tanto en las encuestas como por parte del personal y presentes de dichos trabajos de investigación.

6.3. Responsabilidad ética de acuerdo a los reglamentos vigente

En el presente proyecto de investigación, nos proponemos llevar a cabo un estudio basado en los principios del Código de Ética de Investigación de la Universidad Nacional del Callao (UNAC) aprobado en el año 2019, que busca establecer pautas claras y compromisos éticos con el fin de regir la conducta de docentes, estudiantes, graduados, e investigadores en general en la realización de actividades científicas.

La esencia de mi investigación se alinea especialmente con el Artículo 8 del código, donde se detallan los principios éticos del investigador de la UNAC que se debe seguir y estos son:

En este contexto, mi trabajo se verá regido por los valores de profesionalismo, transparencia, objetividad, igualdad, compromiso, honestidad, confidencialidad, independencia, diligencia y dedicación. Estos principios con el fin de garantizarán la integridad de mi investigación, al igual que asegurarán el respeto a la dignidad de las personas, la confidencialidad y privacidad de la empresa.

Con el respaldo legal de la Constitución Política del Perú, la Ley Universitaria, y otras normativas aplicables, mi investigación se compromete a seguir estándares éticos elevados. Este enfoque ético no solo fortalecerá la calidad de los resultados obtenidos, sino que también contribuirá al desarrollo de la ciencia y tecnología para el

beneficio de la sociedad, en consonancia con la misión y visión de la UNAC.

Así mismo los presentes autores de este trabajo de investigación con nombres:
Bryam Rodas Díaz y Johan Alberto Sanchez Zorrilla declaramos bajo juramento que:

- El presente trabajo de investigación es de nuestra autoría.
- Se ha respetado la normativa ISO 690.
- La presente tesis no ha sido publicada ni presentada anteriormente.
- La información presentados en los resultados son reales adquiridos personalmente por los usuarios del presente trabajo de investigación.
- Los autores del presente trabajo de investigación asumimos las consecuencias y sanciones de nuestras respectivas acciones que se deriven, sometiéndonos a la normatividad vigente de la Universidad Nacional del Callao.

VII. CONCLUSIONES

Concluida la tesis se puede opinar sobre la empresa BBTI S.A.C. lo siguiente:

1. En la Tabla 4 se puede observar que del 100% (23) de los encuestados respecto a "Cómo calificarías a la empresa BBTI S.A.C. en su estrategia para la recuperación de datos en caso de un ataque de ransomware", el 52.17% (12) es bueno, 34.78% (8) es muy bueno y el 13,04% (3) es Medio.
2. En la Tabla 13 se puede observar que del 100% (23) de los encuestados respecto a " Cuál es el nivel de la empresa BBTI S.A.C. en la implementación de sus controles de seguridad adicionales como parte de su estrategia para reducir brechas de seguridad en el último año", el 65.22% (15) es bueno, 17.39% (4) es muy bueno y el 17,39% (4) es Medio.
3. La implementación de un protocolo de prevención contra ransomware en el servidor de BBTI S.A.C. tendrá un impacto positivo en la seguridad del servidor de la empresa BBTI S.A.C.
4. La implementación de protocolo de prevención contra ransomware tendrá un impacto positivo en la resistencia ante ataques de ransomware en la empresa BBTI SAC.
5. La implementación de protocolo de prevención contra ransomware tendrá un impacto positivo en el tiempo de recuperación de ataques de ransomware en la empresa BBTI S.A.C.
6. Implementación de protocolo de prevención contra ransomware tendrá un impacto positivo en la reducción de la brecha de seguridad en la empresa BBTI S.A.C.

VIII. RECOMENDACIONES

Finalizada la tesis se puede recomendar a la empresa BBTI S.A.C. lo siguiente:

1. La empresa BBTI S.A.C. debe seguir implementando estrategias para la recuperación de datos en casos de ataques de ransomware, para de esta manera evitar pérdida de información.
2. La empresa BBTI S.A.C. debe continuar con la implementación de controles de seguridad adicionales como parte de la estrategia para reducir brechas de seguridad en los próximos años.
3. Dado el impacto positivo previsto de la implementación del protocolo de prevención contra ransomware en el servidor de BBTI S.A.C., se recomienda un enfoque proactivo para optimizar y fortalecer continuamente estos protocolos.
4. Dado el reconocimiento del impacto positivo de la implementación del protocolo de prevención contra ransomware en la resistencia ante ataques, se recomienda centrarse en el desarrollo de una cultura de ciberseguridad sólida.
5. Dado el reconocimiento de que la implementación de un protocolo de prevención contra ransomware tiene un impacto positivo en el tiempo de recuperación de ataques, se recomienda enfocarse en la optimización continua de estos procesos.
6. Dado que la implementación del protocolo de prevención contra ransomware se espera que tenga un impacto positivo en la reducción de la brecha de seguridad, se recomienda una estrategia integral para fortalecer la postura de seguridad de la empresa.

IX. REFERENCIAS BIBLIOGRAFICAS

1. **27001, ISO. 2015.** SEGURIDAD DE LA INFORMACION ISO. 2015.

2. **27001:ISO. 2013.** *GUIA DE IMPLANTACION PARA LA SEGURIDAD DE LA INFORMACON.* 2013.

3. **Alva, Marco. 2019.** Gestión. [En línea] Diario Gestión, 5 de Diciembre de 2019. [Citado el: 27 de Junio de 2020.] https://gestion.pe/economia/empresas-sufrieron-3000-millones-de-intentos-de-ciberataques-noticia/?ref=gesr.

4. **Anchatipán, Danilo. 2015.** Implementación de seguridades mediante criptografía para servidores basados en software libre para el laboratorio de redes de la carrera de ingeniería en informática y sistemas computacionales durante el periodo 2013. Latacunga : s.n., 2015.

5. **Barker, William C. 2021.** *Gestión de riesgo de ransomware: un perfil de marco de ciberseguridad.* 2021.

6. **BENDECK, WILLIAM JOSE CLAVIJO. 2017.** *DEFINICIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE ALMACENAMIENTO Y RESPALDO DE DATOS E INFORMACIÓN SEGURO PARA EL SERVICIO GEOLÓGICO COLOMBIANO –SGC- SEDECAN.* 2017.

7. *breve guia para hacer un rprotocolo de seguridad.* **19, ARTICLE. 2020.** 06 de 2020.

8. **Carranza, Martin Facundo Medina. 2017.** *Seguridad Informática: virus ransomware, el Secuestro virtual de datos es Posible.* 2017.

9. **Chira Castillo, Gabriella Lucia. 2021.** *Implementación de un plan de control y seguridad de los activos de información en la Estación de Servicios San José.* Universidad Cesar Vallejo, Piura : 2021.

10. **chow Zamora, Wing Lee. 2018.** *Prevención de ataques de Ransomware conocidos en redes informáticas,utilizando la tecnología Check Point Sandblast en el perímetro y en usuarios finales comprendido en el periodo de septiembre del 2017 a abril del 2018.* UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA UNAN, s.l. : 2018.

11. **Chuco, Marlon. 2013.** Sistema de encriptación RSA para la fiabilidad de transmisión de archivos de textos en la sede campo armiño de Electroperu S.A. Huancayo : s.n., 2013.

12. **Cisco. 2018.** Cisco. [En línea] Febrero de 2018. [Citado el: 28 de Junio de 2020.] https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf.
13. **De La Rosa Cáceres, Richard Kervin. 2019.** *Aplicación de las auditorias de comportamientos seguros para mejorar la cultura de seguridad en la empresa minera cn sac de la cía. minera Volcan saa – unidad Andaychagua.* UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN, Cerro de Pasco : 2019.
14. **Delgado, Carlos Arturo Avenía. 2017.** *Fundamentos de seguridad informática.* Colombia, Bogota : 2017.
15. **El Confidencial. 2021.** *Hackers atacan servidor del SEPE con virus ransomware.* 2021.
16. **El Tiempo Casa Editorial. 2019.** *El cibercrimen no descansa, estas son las proyecciones para el 2020.* [Portal de Noticias] Bogotá : Redaccion Tecnósfera, 2019.
17. **Elecciones, Tribunal Supremo de. 2017.** *INSTRUCCIÓN DE TRABAJO PARA LA CREACIÓN Y ELABORACIÓN DE PROTOCOLOS .* 2017.
18. **Escobar, Mar. 2015.** Criptografía en la clave pública y privada. RSA. Castellón : s.n., 2015.
19. **Eset. 2019.** Welivesecurity. [En línea] Julio de 2019. [Citado el: 27 de 06 de 2020.] https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf.
20. **Florez, Iván y Quintana, Jesús. 2018.** Sistema de detección de ataques informáticos a redes de datos empresariales soportado en honeypots. Cartagena : s.n., 2018.
21. **Fuentes, Xose Fernandez. 2023.** *TECNICAS DE ANALISIS FORENSE PARA LA EVALUACION DE LA PRIVACIDAD E INTEGRIDAD DE LA INFORMACION: NAVEGADORES WEB Y ATAQUES DE RANSOMWARE.* UNIVERSIDAD DE SANTIAGO DE COMPOSTELA, SANTIAGO DE COMPOSTELA : 2023.
22. **Gadalmez. 2015.** [En línea] 20 de 06 de 2015. [Citado el: 29 de 10 de 2020.]
23. **Gil, Martinez. 2003.** *Introdiccion a la Programacion estructurada en C.* 2003.

24. **Godoy. 2014.** *Seguridad de Información. Guatemala: Revista de la Segunda Cohorte.* 2014.

25. **Golwaser. 1982.** *criptografia probabilistica .* 1982.

26. **Great Britain. Government Communications Headquarters; Computer Emergency Response Team UK. 2015.** *Common cyber attacks: reducing the impact.* Londres : The information security arm of GCHQ, 2015.

27. **Guzmán, Goyo. 2015.** *Metodología para la seguridad informática y comunicaciones en la clínica Ortega.* 2015.

28. **Harán, Juan Manuel. 2021.** Ataque de ransomware a compañía de oleoducto afecta el suministro de combustible en Estados Unidos. 6 de 2021.

29. **Herazo. 2011.** *Clonar una base de datos existente con Provisioning and PatchAutomation Pack.* 2011.

30. **Hernandez. 2006.** *Honestidad segun autores.* 2006.

31. **Hernández, Fernández y Baptista. 2012.** *Metodología de la Investigación. Ed. Mc Graw hill.* 2012.

32. **Inoguchi, Antonio y Macha, Erika. 2017.** Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú, 2016. Lima : s.n., 2017.

33. **Izquierdo, Jaime y Tafur, Tania. 2017.** Mecanismos de seguridad para contrarrestar ataques informáticos en servidores web y base de datos. Chiclayo : s.n., 2017.

34. **JIMÉNEZ, HEIDI ALICIA CHAVES. 2008.** *DISEÑO E IMPLEMENTACIÓN DE UN SOFTWARE MULTIMEDIA PARA EL APRENDISAJE DE LA CRIPTOGRAFIA.* 2008.

35. **Jose Mendiola Zuriarrain. 2021.** El ransomware ataca al Ministerio de Justicia y a varias empresas españolas. 05 de 07 de 2021.

36. **Kerckhoffs. 1883.** *La criptografía militar.* 1883.

37. **Kerlinger, Fred N. 2002.** *Investigación del comportamiento: Métodos de investigación en ciencias sociales.* California : McGraw, 2002.

38. *La prevención : Una estrategia global.* **MEXICO, ARTICLE 19. 2005.** 2005.

39. **Lomparde, Katia Leon. 2014.** *ENCRIPTACION RSA DE ARCHIVOS DE TEXTO.* 2014.

40. **Martínez Borja, Jhony Jhoel. 2014.** *CONTROLES DE SEGURIDAD PARA REDUCIR LA CANTIDAD DE INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN DEL AÑO 2012 EN EL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE HUANCAYO.* UNIVERSIDAD NACIONAL DEL CENTRO DEL PERÚ, HUANCAYO : 2014.

41. **Mega, Pallas. 2009.** *Metodologia de implantacion de un SGSI en un grupo empresarial jerarquico.* 2009.

42. **Meza Montoya, Stalin Miguel y Zambrano Pinto, José Luis. 2018.** *IMPLEMENTACIÓN DE UN PROCESO Y POLÍTICAS PARA LA GESTIÓN DE ACTUALIZACIONES DE SOFTWARE Y PARCHES DE SEGURIDAD DE PRODUCTOS MICROSOFT EN UNA INSTITUCIÓN SIN FINES DE LUCRO.* ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL, GUAYAQUIL : 2018.

43. **Morocho, Raul armando Ramos. 2019.** *Infección con ransomware en el servidor de base de datos del sistema ONSYSTEC ERP.* 2019.

44. *New Directions in Cryptography.* **Diffie, Whitfield. 1975.** California : Standford, 1975.

45. **Palacios, Rafael. 2006.** *Introducción a la Criptografía: tipos de algoritmos.* 2006.

46. **Pastor, Danilo. 2017.** *PROPUESTA DE UN METODO ALTERNATIVO DE ENCRIPTACIÓN DINAMICA PARA UN ADMINISTRADOR DE CORREO ELECTRONICO.* 2017.

47. **—. 2015.** *PROPUESTA DE UN METODO ALTERNATIVO DE ENCRIPTACIÓN DINAMICA PARA UN ADMINISTRADOR DE CORREO ELECTRONICO.* 2015.

48. **Peña Godos, Sandy Yajahira (. 2021.** *Protocolo de seguridad y salud para el trabajo remoto de los servidores públicos de la Municipalidad Distrital La Brea – Negritos 2021.* 2021.

49. **Perez Diaz , Neiler Wilter. 2021.** *Implementación de tecnología sandbox para proteger de ataques ransomware en una red informática local de una entidad financiera.* Universidad Señor de Sipan, Pimentel : 2021.

50. **Posey. 2014.** *Cuál es la diferencia entre gestión de datos copiados y el respaldo tradicional Search Data Center.* 2014.

51. **Quinto, Angelica Mosquera. 2011.** *Los antivirus y sus tendencias futuras.* 2011.

52. **Ramos Zapana, John Williams. 2017.** *IMPLEMENTACIÓN DEL PROTOCOLO GETVPN PARA OPTIMIZAR EL PROCESO DE SEGURIDAD MEDIANTE LA ENCRIPTACIÓN DE TRÁFICO EN UNA ENTIDAD FINANCIERA.* UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR, Lima : 2017.

53. **Ríos, Josue. 2017.** Sistema de encriptación para optimizar el proceso de desarrollo de software de una empresa de lima. Lima : s.n., 2017.

54. **Rojas, Paolo. 2019.** Gestión. [En línea] Diario Gestión, 14 de Noviembre de 2019. [Citado el: 29 de Junio de 2020.] https://gestion.pe/economia/empresas/ciberseguridad-situacion-de-las-empresas-peruanas-frente-a-sus-pares-de-la-region-noticia/?ref=gesr.

55. **Romero Castro, Martha Irene , y otros. 2018.** *INTRODUCCIÓN A LA SEGURIDAD INFORMATICA Y EL ANALISIS DE VULNERABILIDADES.* s.l. : Área de Innovación y Desarrollo,S.L., 2018.

56. **Rustom J., Antonio . 2012.** *ESTADÍSTICA DESCRIPTIVA, PROBABILIDAD E INFERENCIA. Una visión conceptual y aplicada.* Santiago de Chile ed : Facultad de ciencias agronomas - Unoversidad de Chile, 2012.

57. **Sáenz, Andrés. 2015.** Técnicas de transparencia y encriptación de información. Bogotá : s.n., 2015.

58. **Samaniego, Ana. 2018.** Evaluación de algoritmos criptográficos para mejorar la seguridad en la comunicación y almacenamiento de la información. Lima : s.n., 2018.

59. **Sampieri. 2003.** *Diseño de investigacion.* 2003.

60. **Sanchez, Hector Corrales. 2012.** *Criptografía y Métodos de Cifrado.* 2012.

61. **Sánchez, Jhonny. 2017.** Técnicas de encriptación para mejorar la seguridad en la transferencia de archivos en un entorno fiable. Chiclayo : s.n., 2017.

62. **SÁNCHEZ, LETICIA HERNÁNDEZ.** *Buenas practicas para la implementacion de la seguridad de un centro de computo.*

63. **Sánchez, Willian. 2017.** Utilización de un algoritmo de encriptación aplicado a la comunicación humano-robot. Riobamba : s.n., 2017.

64. **Tarazona , Cesar. 2015.** *Amenazas informáticas y seguridad de la información.* s.l. : Derecho Penal y Criminología, 2015.

65. **Trevejo, Luis Alonso Talavera. 2022.** *Plan de continuidad de negocio de un file server ante un ataque de malware en Cloud.* UNIVERSIDAD EUROPEA, s.l. : 2022.

66. **Vancells. 2002.** *Prototipo de control para un cultivo de tomate cherry en un invernadero.* 2002.

67. **Vasquez Gutierrez, Dennis Alberto. 2019.** *PROPUESTA DE PLAN DE SEGURIDAD INFORMÁTICA PARA LA SUB GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE REQUENA, EN EL AÑO 2019.* Universidad Cientifica del Peru, Loreto : 2019.

68. **Vergara Quiroz, Gladis. 2017.** *Seguridad de informacion y calidad de servicio en la Universidad Nacional Federico Villareal , 2016.* Universidad Cesar Vallejo, Peru : 2017.

69. **—. 2017.** *Seguridad de información y calidad de servicio en la universidad nacional federico villareal, 2016.* Universidad Cesar Vallejo, Peru : 2017.

70. **Vernam, Gilbert. 1917.** *El cifrado de Vernam .* 1917.

X. ANEXOS

10.1. Matriz de consistencia

TITULO:	"IMPLEMENTACION DE UN PROTOCOLO DE PREVENCION CONTRA RAMSOMWARE PARA LA SEGURIDAD DEL SERVIDOR DE BBTI S.A.C. EN EL AÑO 2022"								
AUTOR 1:	SANCHEZ ZORRILLA , JOHAN ALBERTO	AUTOR 2:	RODAS DIAZ , BRYAN						
"IMPLEMENTACION DE UN PROTOCOLO DE PREVENCION CONTRA RAMSOMWARE PARA LA SEGURIDAD DEL SERVIDOR DE BBTI S.A.C. EN EL AÑO 2022"									
LINEA INVESTIGACIÓN	**INSTITUCIÓN**	**PROBLEMA**	**OBJETIVO**	**HIPÓTESIS**	**VARIABLES**	**DIMENSION**	**INDICADORES**	**INDICE**	**INSTRUMENTOS**	**METODOLOGÍA**
INGENIERÍA Y TECNOLOGÍA	B B T I S . A . C .	**Problema General** ¿De qué manera la implementación de protocolo de prevención contra ramsomware mejora la seguridad de la empresa BBTI S.A.C?	**Objetivo General** Determinar que Implementación un protocolo de prevención contra ransomware para mejorar la seguridad del servidor de la empresa BBTI S.A.C.	**Hipótesis General** La implementación de un protocolo de prevención contra ransomware en el servidor de BBTI S.A.C. tendrá un impacto positivo en la seguridad del servidor de la empresa BBTI S.A.C	**Variable 1 / Variable independiente:** IMPLEMENTACION DE UN PROTOCOLO DE PREVENCIÓN CONTRA RANSOMWARE	**Instalación y configuración del software de prevención**	nivel de actualización de las configuraciones de seguridad en el servidor	$\%\ ramsomware\ Bloq. = \frac{total\ R.bloqueados}{total\ R.detectados} x\,100$	Entrevista	**Tipo de Investigación:** APLICADA Y EXPLICATIVA **Método:** Hipotético - Deductivo. **Diseño de Investigación:** Experimental **Población y Muestra** **Población:** Informacion data de BBTI S.A.C. en el periodo de 2022 **Muestra:** empresa BBTI S.A.C **Técnicas:** Encuesta **Instrumentos:** Cuestionarios **Técnica de procedimiento de Datos:** Calculo de promedios
						Políticas y procedimientos de seguridad	Grado de cumplimiento de las políticas de seguridad	$tiempo. = \frac{Total\ tiempo\ real}{Toral\ tiempo\ original}$	Entrevista	
						Capacitación y concientiación del personal	satisfacción del personal con la formación recibida	$red.\ brecha = (1 - \frac{val\ ini\ - val.Fin}{Val\ inical}) x\,100$	Entrevista	
		Problema Específico 1 ¿De que manera la implementación de protocolo de prevención contra ramsomware mejorala resitencia ante ataques de ramsomware en la empresa BBTI S.A.C.?	**Objetivo Específico 1** Determinar que la implementación de protocolo de prevención contra ramsomware mejora la resitencia ante ataques de ramsomware en la empresa BBTI S.A.C	**Hipótesis Específica 1** La implementación de un protocolo de prevención contra ransomware , la adecuada instalación y configuración del software de prevención y una adecuada concientizacion del personal tendrán un impacto positivo en la resistencia ante ataques de ransomware en la empresa BBTI S.A.C.	**Variable 2 / Variable Dependiente:** SEGURIDAD DEL SERVIDOR DE LA EMPRESA BBTI S.A.C.	Resistencia ante ataques de ramsomware	% de ataques de ramsomware bloqueados	$\%\ ramsomware\ res. = \frac{total\ R.bloqueados}{total\ R.detectados} x\,100$	Entrevista	
		Problema Específico 2 ¿De que manera la implementación de protocolo de prevención contra ramsomware mejora el tiempo de recuperacion de ataques de ramsomware en la empresa BBTI S.A.C.?	**Objetivo Específico 2** Determinar que la implementación de protocolo de prevención contra ramsomware mejora el tiempo de recuperacion de ataques deramsowmare en la empresa BBTI S.A.C.	**Hipótesis Específica 2** La implementación de un protocolo de prevención contra ransomware, combinada con una capacitación y concienciación efectiva del personal, tendrá un impacto positivo en la reducción del tiempo de recuperación de ataques de ransomware en la empresa BBTI S.A.C.		Tiempo de recuperacion	tiempo promedio de recuperación después de un ataque	$tiempo. = \frac{Total\ tiempo\ real}{Toral\ tiempo\ original}$	Entrevista	
		Problema Específico 3 ¿De que manera la implementación de protocolo de prevención contra ramsomware mejora la reduccion la brecha de seguridad en la empresa BBTI S.A.C.?	**Objetivo Específico 3** Analizar que la implementación de protocolo de prevención contra ramsomware mejora la reduccion de brechas de seguridad de la emrpesa BBTI S.A.C	**Hipótesis Específica 3** La implementación de un protocolo de prevención contra ransomware,combinada con una capacitación y concienciación efectiva del personal,tendrá un impacto positivo en la reducción de la brecha de seguridad en la empresa BBTI S.A.C.		Reducción de brecha de seguridad	reducción porcentual del brecha de seguridad	$red.\ brecha = (\frac{val\ final - valinicla}{Val\ inical}) x\,100$	Entrevista	

10.2. Instrumentos validados

	DIMENCIONES	PREGUNTAS	VALORACION				
			5	4	3	2	1
SEGURIDAD DEL SERVIDOR	RESISTENCIA ANTE ATAQUES DE RANSOMWARE	1.¿Cómo calificarías a la empresa BBTI S.A.C en su estrategia para la recuperación de datos en caso de un ataque de ransomware?					
		2. ¿Qué tan satisfecho estás con la empresa BBTI S.A.C. con sus políticas y procedimientos establecidos para garantizar que los empleados					
		3.¿qué nivel consideras que la empresa BBTI S.A.C tiene en relacion a su resistencia ante ataques de ransomware en función de las					
		4. ¿Cómo calificarías la implementación de un protocolo de prevención contra ransomware en la empresa BBTI SAC como parte de la resistencia ante ataques de ransomware?					
		5. ¿Con qué frecuencia ha experimentado la empresa BBTI SAC uncambio en su resistencia ante ataques de ransomware desde la implementación de dicho protocolo en comparacion al año 2021?					
	TIEMPO DE RECUPERACION	6. ¿ Qué tan efectivo crees que es el plan de acción de la empresa BBTI S.A.C para minimizar el tiempo de inactividad en caso de un ataque de ransomware?					
		7. ¿Como califica la efectividad de los sistemas de respaldo y prioridad S.A.C en la reducción del tiempo de recuperación después de un ataque de ransomware?					
		8. ¿Qué tan efectivo crees que es la implementación del protocolo de prevención contra ransomware para reducir el tiempo de recuperación en caso de ataques de ransomware en la empresa BBTI S.A.C?					
	REDUCCION DE LA BRECHA DE SEGURIDAD	9.¿Qué tan frecuente crees que la empresa BBTI S.A.C. lleva a cabo su proceso de mejora continua en medidas de seguridad con el objetivo de reducir las brechas de seguridad?					
		10.¿Cuál es el nivel de la empresa BBTI S.A.C en la implementacion de sus controles de seguridad adicionales como parte de su estrategia para reducir brechas de seguridad en el último año?					
		11.¿Como calificarias la implementacion su protocolo de prevención contra ransomware con el objetivo de reducir las brechas de seguridad relacionadas con el ransomware por parte de la empresa BBBTI SAC?					

IMPLEEMNTACION DE UN PROTOOLO ANTIRAMSOMWARE	INSTALACION Y CONFIGURACION DEL SOFTWARE DE PREVENCION	12.¿Cómo calificarías la seguridad del servidor de la empresa BBTI SAC?					
		13. ¿Cómo calificarías la efectividad de la instalación y configuración del software de prevención en el servidor de BBTI S.A.C.?					
		14.¿La instalación y configuración del software de prevención en el servidor de BBTI SAC ha mejorado la seguridad desde su implementación en el año 2021?					
	POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD	15.¿Qué opinas sobre la efectividad de las políticas y procedimientos de seguridad de la empresa BBTI SAC?					
		16.¿Cuál es el nivel de cumplimiento de las políticas y procedimientos de seguridad en la empresa BBTI SAC?					
		17.¿Qué tan rigurosamente consideras que la seguridad del servidor de BBTI SAC aplica las políticas y procedimientos de seguridad establecidos?					
		18.¿cómo evaluarías la seguridad del servidor de BBTI SAC en relación con las políticas y procedimientos de seguridad?					
	CAPACITACION Y CONCIENTIZACION DEL PERSONAL	19.¿Cómo calificarías la efectividad de la capacitación y concientización del personal en relación con la seguridad del servidor de BBTI SAC?					
		20.¿cuán informados están los empleados de BBTI SAC sobre las políticas de seguridad del servidor?					
		21.¿En tu opinion como mejora la seguridad del servidor después de la implementación de programas de capacitación y concientización para el personal?					
		22.¿Cómo evaluarías el nivel de compromiso del personal de BBTI SAC en la promoción de la seguridad del servidor?					

10.3. Ficha de validación de expertos

FICHA DE VALIDEZ POR JUECES EXPERTOS (II)

ESCALA DE CALIFICACIÓN

Estimado (a): Ramos Choquehuanca Angelino Abad

Estimado (a): Dra. Erika Jueva Zavallos Vera

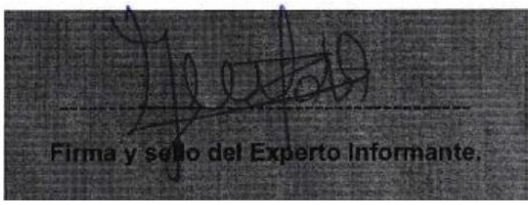
Teniendo como base los criterios que a continuación se presenta, se le solicita dar su opinión sobre el instrumento de recolección de datos que se adjunta:

Estimado (a): Dr. GUILLERMO ANTONIO MAS AZAHUANCHE

Teniendo como base los criterios que a continuación se presenta, se le solicita dar su opinión sobre el instrumento de recolección de datos que se adjunta:

Estimado (a): Mg. José Antonio Farfan Aguilar

Teniendo como base los criterios que a continuación se presenta, se le solicita dar su opinión sobre el instrumento de recolección de datos que se adjunta:



FICHA DE VALIDEZ POR JUECES EXPERTOS (II)

ESCALA DE CALIFICACIÓN

Estimado (a): Casazola Cruz Osmildo Daniel

Teniendo como base los criterios que a continuación se presenta, se le solicita dar su opinión sobre el instrumento de recolección de datos que se adjunta:

Firma y sello del Experto Informante.

Estimado (a): Dra. Bertila García Díaz

Teniendo como base los criterios que a continuación se presenta, se le solicita dar su opinión sobre el instrumento de recolección de datos que se adjunta:

Firma y sello del Experto Informante.

10.4. Consentimiento Informado

bbti s.a.c.

DOCUMENTO DE CONFIDENCIALIDAD

Con fecha de 06/09/2023, se reúnen el representante Legal de la empresa ***BBTI S.A.C.*** con RUC 20565747356, Sr. Kenji Alberto Chung Sanchez con DNI 46920214 y los Sres Johan Alberto Sanchez Zorrilla con DNI 76472788 y Rodas Días Bryan con DNI 77224744

Los señores solicitan al representante legal de la empresa BBTI S.A.C, poder utilizar información del área de sistemas y redes de los periodos 2019 al 2023.

Esta información se solicita con fines académicos al informar que desarrollaran la tesis titulada ***"LA IMPLEMENTACION DE UN PROTOCOLO DE PREVENCION CONTRA RAMSOMWARE PARA OPTIMIZAR LA SEGURIDAD DEL SERVIDOR EN LA EMPRESA BBTI S.A.C ENTRE EL AÑO 2022"*** con fines de obtener el título profesional de Ingeniero de Sistemas en la facultad Ingeniería Industrial y sistemas (FIIS) de la escuela profesional de Ingeniería de sistemas (EPIS) en la universidad nacional del callao.

De caso cumplir con los fines, los señores se comprometen a entregar una copia de la Tesis aprobada.

BBTI S.A.C.
Kenji Chung Sanchez
GERENTE GENERAL

10.5. Base de datos Variable Dependiente

VARIABLE DEPENDIENTE: SEGURIDAD DEL SERVIDOR														
RESISTENCIA ANTE ATAQUES DE RANSOMWARE					SUMA	TIEMPO DE RECUPERACION			SUMA	REDUCCION DE LA BRECHA DE SEGURIDAD			SUMA	SUMA TOTAL
1.¿Cómo calificarías a la empresa BBTI S.A.C en su estrategia para la	2. ¿Qué tan satisfecho estás con la empresa BBTI S.A.C. con sus	3. ¿Qué nivel consideras que la empresa BBTI S.A.C tiene en relacion a su	4. ¿Cómo calificarías la implementación de un protocolo de prevención contra	5. ¿Con qué frecuencia ha experimentado la empresa BBTI SAC		6. ¿ Qué tan efectivo crees que es el plan de acción de la empresa BBTI S.A.C	7. ¿Cómo califica la efectividad de los sistemas de respaldo y prioridad S.A.C en	8. ¿Qué tan efectivo crees que es la implementación del protocolo de		9.¿Qué tan frecuente crees que la empresa BBTI S.A.C. lleva a cabo su proceso de	10.¿Cuál es el nivel de la empresa BBTI S.A.C en la implementación de	11.¿Cómo calificarías la implementación su protocolo de prevención con el		
4	4	4	4	4	**20**	4	3	4	**11**	4	4	4	**12**	43
3	3	2	5	2	**15**	3	3	4	**10**	4	4	4	**12**	37
4	4	4	4	3	**19**	4	4	3	**11**	3	4	4	**11**	41
4	3	4	5	4	**20**	4	4	5	**13**	4	5	4	**13**	46
5	4	4	4	4	**21**	3	4	4	**11**	3	4	4	**11**	43
5	4	4	4	4	**21**	4	4	5	**13**	4	4	4	**12**	46
4	3	4	4	4	**19**	4	4	4	**12**	3	4	4	**11**	42
5	4	3	5	5	**22**	4	4	4	**12**	4	4	4	**12**	46
5	4	4	4	4	**21**	5	4	4	**13**	4	4	4	**12**	46
4	4	4	4	4	**20**	4	4	5	**13**	4	4	3	**11**	44
3	3	3	3	3	**15**	3	3	3	**9**	3	3	3	**9**	33
4	3	4	5	4	**20**	3	3	4	**10**	3	3	4	**10**	40
4	4	4	4	3	**19**	4	3	4	**11**	3	4	3	**10**	40
4	3	4	4	3	**18**	4	4	4	**12**	4	4	4	**12**	42
5	5	5	5	5	**25**	5	5	5	**15**	5	5	5	**15**	55
5	5	5	5	5	**25**	5	5	5	**15**	5	5	5	**15**	55
3	4	3	3	3	**16**	3	3	3	**9**	3	3	5	**11**	36
4	4	4	4	4	**20**	4	4	4	**12**	4	3	3	**10**	42
4	4	5	5	4	**22**	4	5	3	**12**	5	4	5	**14**	48
5	4	5	4	5	**23**	4	5	4	**13**	5	4	5	**14**	50
4	4	4	4	4	**20**	4	3	3	**10**	3	4	4	**11**	41
5	4	5	4	4	**22**	5	4	4	**13**	5	4	5	**14**	49
4	5	4	5	5	**23**	5	4	4	**13**	4	5	4	**13**	49

10.6. Base de datos Variable Independiente

VARIABLE INDEPENDIENTE: IMPLEMENTACION DE UN PROTOCOLO PREVENCION CONTRA RANSOMWARE														
INSTALACION Y CONFIGURACION DE SOFTWARE DE PREVENCION				POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD					CAPACITACION Y CONCIENTIZACION DEL PERSONAL					
12.¿Cómo calificarías la seguridad del servidor de la empresa BBTI SAC?	13. ¿Cómo calificarías la efectividad de la instalación y	14.En tu opinión, ¿la instalación y configuración del software de	SUMA	15.¿Qué opinas sobre la efectividad de las políticas y procedimientos de	16.En tu experiencia, ¿Cuál es el nivel de cumplimiento de las políticas y	17.¿Qué tan rigurosamente consideras que la seguridad del servidor	18.En general, ¿Cómo evaluarías la seguridad del servidor de BBTI SAC en	SUMA	19.¿Cómo calificarías la efectividad de la capacitación y concientización del	20.En tu opinión, ¿cuán informados están los empleados de BBTI SAC sobre	21.¿En tu opinion como mejora la seguridad del servidor después de la	22.¿Cómo evaluarías el nivel de compromiso del personal de BBTI	SUMA	SUMA TOTAL
4	4	4	12	4	4	4	4	16	4	3	3	4	14	42
3	3	4	10	3	3	3	3	12	3	3	4	4	14	36
3	4	4	11	5	4	4	4	17	3	3	4	4	14	42
4	5	4	13	4	4	4	4	16	4	3	4	3	14	43
4	4	4	12	4	4	4	3	15	4	3	4	4	15	42
4	4	3	11	4	4	5	4	17	4	4	4	4	16	44
4	4	4	12	4	4	4	4	16	4	3	3	4	14	42
4	3	5	12	4	4	4	4	16	4	4	4	4	16	44
4	4	4	12	4	3	4	4	15	4	4	4	4	16	43
3	3	4	10	4	4	3	3	14	4	4	4	4	16	40
3	3	3	9	3	3	3	3	12	3	3	3	3	12	33
4	4	4	12	4	4	4	4	16	3	3	3	4	13	41
4	3	4	11	3	4	3	4	14	4	3	4	3	14	39
4	4	4	12	4	4	4	3	15	4	4	3	4	15	42
5	5	5	15	5	5	5	5	20	5	5	5	5	20	55
5	5	5	15	5	5	5	5	20	5	5	5	5	20	55
3	3	4	10	4	4	4	4	16	4	4	3	3	14	40
3	3	3	9	3	3	3	3	12	3	4	4	3	14	35
4	5	4	13	4	4	4	5	17	4	5	4	5	18	48
4	5	4	13	5	4	5	4	18	5	4	5	4	18	49
3	3	4	10	3	3	3	4	13	3	3	3	4	13	36
4	5	4	13	5	4	5	4	18	5	4	5	5	19	50
4	5	4	13	5	5	5	5	20	5	5	4	4	18	51

10.7. Comparativa de la implementación del protocolo en la empresa BBTI S.A.C. previa y post implementación

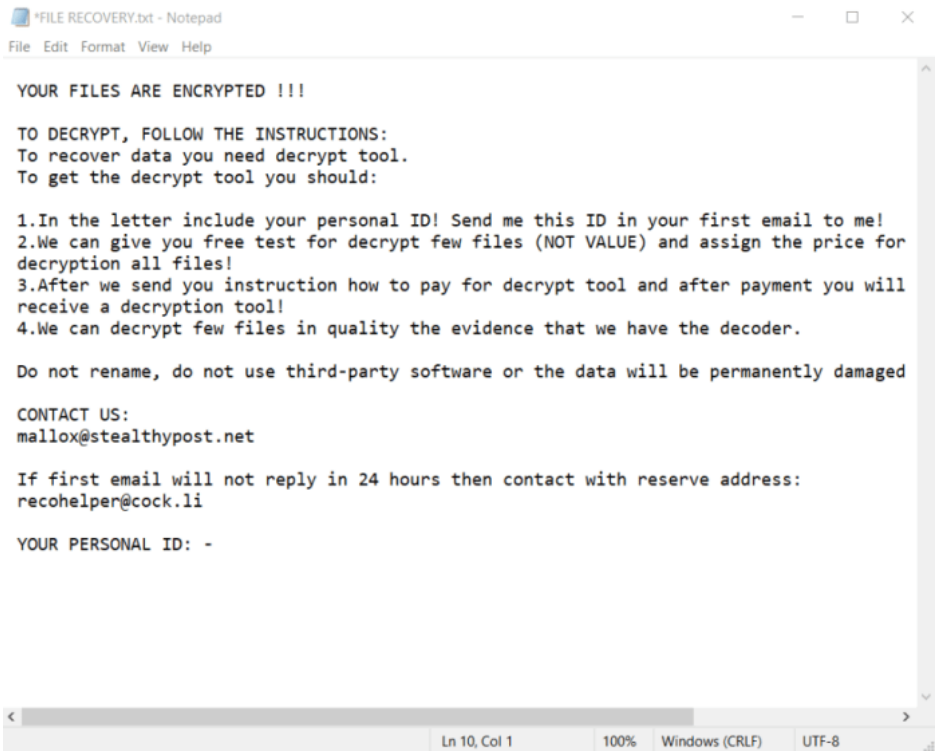
	PREVIO A LA IMPLEMENTACION DEL PROTOCOLO	DESPUES DEL PROTOCOLO
FIREWALLS	*La empresa no contaba con monitoreo en la data que se almacenaba en el servidor, por lo general se usaba como almacenamiento de archivos personales (fotos, videos ,etc) *Cualquier usuario podia acceder a cualquier carpeta sin limitaciones *Los accesos a USB en los equipos estaban completamente libres *Libertad de navegacion en las paginas web	*Se inplemento un plan de limpieza semanal con cada area y sus respectivas carpetas que manipulan *Se restringio el acceso de cualquier dispositivo externo a los equipos y servidor *Se genero una "lista negra" como filtro en el router del internet para el acceso a los sitios web
ACTUALIZACIONES Y PARCHES	*Se contaba con versiones antiguos de programas (sql , windows server,etc) y se corria el riesgo de que se pudieran explotar vulnerabilidades de determinadas versiones de programas *No se actualizaba periodicamente las versiones o parches del sistema operativo	*Se actualizo a la version mas reciente tanto los programas como sistema operativo
CONTROL DE ACCESO	*El acceso era libre y era tratado como una pc mas del monton *No existia usuarios con sus limitaciones de carpetas, todos compartian un unico usuario "admin"	Se restringio el acceso a todo el personal no capacitado y no autorizado al servidor y las redes *Se crearon usuarios y limitaron los accesos a las carpetas(principio de privilegio minimo), brindando solo lo necesario para trabajar
AUDITORIA Y MONITOREO	*Los archivos se almacenaban por periodos de tiempo largos sin analizarlos o purgarlos lo cual generaba mucho trafico en el espacio del disco *No se comprobaba la seguridad de los archivos que ingresaban al servidor	* Implemento herramientas de auditoría y monitoreo para rastrear eventos y detectar posibles actividades maliciosas.(SOPHOS) *Se configuro alertas y notificaciones en caso de anomalias en la red
RESPALDOS REGULARES	*No se contaba con copias de seguridad de los archivos de proyectos (documentacion ,fotos y videos) *El backup de las base de datos se realizaba semestral	*Se implemento un programa de backup diferencial de archivos que permite salvaguardar la informacion del servidor en forma semanal a nivel general en un disco cifrado *Se implemento un programa de backup para base de datos (SQL BACKUP) que extrae 2 veces al dia y se guarda en una nube, un dispositivo USB cifrado, un disco duro cifrado
SEGURIDAD FISICA	* La Ubicación del servidor se encontraba en un lugar de facil acceso y sin vigilancia	*Se creo el departamento de sistemas resguardado por videovigilancia y a la vista de los usuarios de sistemas y se mudo el servidor a una zona mas protegida y limitada

PROTECCION CONTRA ATAQUES EXTERNOS	*No contaba con licencias Originales de antivirus *Muchos de los programas con los que contaba eran "crakeados" *Se tenia libertad de descarga en el servidor desde cualquier lugar	*Se adquirio licencias originales de antivirus especializados con los problemas comunes de rasomware (SOPHOS y KASPERSKY) *Se restringio la instalacion limitado solo de programas a usar (Sql Server, antivirus ,STARSOFT) *Se restringio las descargas libres, exclusivas solo de 1 equipo externo a la red
FORMACION Y CONCIENTIZACION	*Trabajadores desconocian el uso correcto de la red *Trabajadores usaban sus equipos apra guardar sus archivos personales *Descargaban archivos sin filtro de virus y dudosas paginas web *Realizaban instalaciones personales de programas sin consulta *No contaban con antivirus *Trabajaban sobres las maquinas incluso si mostraba una clara infeccion *Se perdia constantemente archivos y correos improtantes	*Se asesora a los trabajadores del uso correcta tanto de la red como de sus equipos *Se instala antivirus a todos los equipos *Se asesora como tratar con un archivo sospechoso (filtros web) *Se limita el uso de instalaciones exclusivo para el area de sistemas *Toda maquina infectada se extraia de la red y se formateaba con toda la data *Cada equipo contabacon su generador de bk exclusivo para correos

10.8. Pruebas de ataque del Ransomware, encriptación de la información en la empresa BBTI S.A.C.

Herramientas

```
YOUR FILES ARE ENCRYPTED !!!

TO DECRYPT, FOLLOW THE INSTRUCTIONS:
To recover data you need decrypt tool.
To get the decrypt tool you should:

1.In the letter include your personal ID! Send me this ID in your first email to me!
2.We can give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files!
3.After we send you instruction how to pay for decrypt tool and after payment you will receive a decryption tool!
4.We can decrypt few files in quality the evidence that we have the decoder.

Do not rename, do not use third-party software or the data will be permanently damaged

CONTACT US:
mallox@stealthypost.net

If first email will not reply in 24 hours then contact with reserve address:
recohelper@cock.li

YOUR PERSONAL ID: 44033560F5E8
```



10.9. Encriptación de archivos secuestrados