FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

TESIS

ANALISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA 2025

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS DE INFORMACIÓN

Autor (es): **ANGELLO GIORDANO RODRIGUEZ SOLSOL**

Asesor (es): Lic. Luis Ronald Rucoba del Castillo. Dr.
https://orcid.org/0000-0002-2842-2761
Lic. Maya Fababa Rodríguez, Mgr.
ORCID 0000-0003-1426-9193

Línea de Investigación: Sistemas de Información

San Juan Bautista - Loreto – Maynas – Perú

Enero – 2026

FACULTAD DE CIENCIAS E INGENIERÍA

UNIVERSIDAD CIENTÍFICA DEL PERÚ

ACTA DE SUSTENTACIÓN

Con Resolución Decanal **N° 004-2025-UCP-FCEI,** del 13 de enero del 2025, se designó jurado.
Con Resolución Decanal **N° 512-2025-UCP-FCEI,** del 05 de mayo del 2025, se cambió al jurado.
Con Resolución Decanal **N° 1085-2025-UCP-FCEI,** del 19 de diciembre del 2025, se autorizó la sustentación.

Siendo las 10:00 a.m. del día 14 de enero del 2026, se constituyó de modo presencial el Jurado para escuchar la presentación y defensa de la Tesis: **"ANÁLISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA 2025".**

Presentado por:

ANGELLO GIORDANO RODRIGUEZ SOLSOL
Para optar el título profesional de Ingeniero de Sistemas de Información

Asesor: Lic. LUIS RONALD RUCOBA DEL CASTILLO, Dr.
CoAsesor: Lic. MAYA FABABA RODRÍGUEZ, Mg

Luego de escuchar la sustentación y defensa ante las preguntas, el Jurado pasó a la deliberación en forma reservada, llegando a la siguiente conclusión:

La sustentación es: Aprobada por mayoría

A las 11:10 horas culminó el acto público.

En fe de los cual los miembros del jurado firman el Acta y comunican en acto público.

Ing. Carmen Patricia Cerdeña del Aguila, Dra.
Presidente del Jurado

Ing. Jimmy Max Ramírez Villacorta, Dr.
Miembro del jurado

Lic. Carlos Enrique Marthans Ruiz, Mtro.
Miembro del jurado

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ – UCP

El presidente del Comité de Ética e Integridad Científica

Hace constar que:

La Tesis titulada:

“ANALISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA 2025”

Del alumno: **ANGELLO GIORDANO RODRIGUEZ SOLSOL,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **16% de similitud**. Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 06 de enero del 2026.

Presidente del Comité de Ética e Integridad Científica
Mgr. Arq. Jorge L. Tapullima Flores

JLTF/C.E.I.C-A
001-2026

UCP_Ingenieria de Sistemas de Informacion_2025_T_Angello_Rodriguez_VI

16% Textos sospechosos

- **6%** Similitudes
  - 0 % similitudes entre comillas
  - 1 % entre las fuentes mencionadas
- **0%** Idiomas no reconocidos
- **10%** Textos potencialmente generados por la IA

Nombre del documento: UCP_Ingenieria de Sistemas de Informacion_2025_T_Angello_Rodriguez_VI.pdf
ID del documento: 4f3ed18871cff540d5ea61d6f626e11ce6af7a31
Tamaño del documento original: 1,74 MB

Depositante: Chris Angela Ramirez Flores
Fecha de depósito: 6/1/2026
Tipo de carga: interface
fecha de fin de análisis: 6/1/2026

Número de palabras: 17.394
Número de caracteres: 103.934

Ubicación de las similitudes en el documento:



Fuentes de similitudes

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**repository.unad.edu.co** | Sustentar los factores que influyen en la ciber-ética de ... http://repository.unad.edu.co/handle/10596/70586	1%		Palabras idénticas: 1% (167 palabras)
2	**repositorio.ucp.edu.pe** http://repositorio.ucp.edu.pe/bitstream/handle/UCP/2767/WONG Y NATALI.pdf?sequence=5 **1 fuente similar**	< 1%		Palabras idénticas: < 1% (148 palabras)
3	**hdl.handle.net** | Clima organizacional y calidad de servicio al público en La Munic... http://hdl.handle.net/20.500.14503/2485 **8 fuentes similares**	< 1%		Palabras idénticas: < 1% (139 palabras)
4	**repository.unad.edu.co** | Sustentar los factores que influyen en la ciber-ética de ... https://repository.unad.edu.co/handle/10596/70586	< 1%		Palabras idénticas: < 1% (126 palabras)
5	**www.transparencia.gob.pe** | Portal del Estado Peruano - Portal de Transparenci... https://www.transparencia.gob.pe/enlaces/pte_transparencia_enlaces.aspx?id_entidad=11067 **8 fuentes similares**	< 1%		Palabras idénticas: < 1% (80 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**repositorio.ucp.edu.pe** http://repositorio.ucp.edu.pe/bitstream/handle/UCP/2770/MARÍA ENIHT DEL CARMEN DÍAZ S...	< 1%		Palabras idénticas: < 1% (40 palabras)
2	**doi.org** https://doi.org/10.5354/0719-2584.2022.66319	< 1%		Palabras idénticas: < 1% (38 palabras)
3	**caib.es** https://caib.es/sacmicrofront/archivopub.do?ctrl=MCRST3405ZI117113&id=117113	< 1%		Palabras idénticas: < 1% (28 palabras)
4	**Documento de otro usuario** #639230 Viene de de otro grupo	< 1%		Palabras idénticas: < 1% (27 palabras)
5	**hdl.handle.net** | Propuesta de un sistema de gestión de seguridad de la informac... http://hdl.handle.net/20.500.12918/8504	< 1%		Palabras idénticas: < 1% (25 palabras)

Fuentes mencionadas (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 http://repositorio.utp.edu.pe/handle/20.500.12867/9636
2 https://www.semanticscholar.org/paper/código-ético
3 https://www.semanticscholar.org/paper/Ciberseguridad-y-vigilancia
4 https://repositorio.unitec.edu//handle/123456789/13660
5 http://repositorio.utp.edu.pe/handle/20.500.12867/8992

HOJA DE APROBACIÓN
PROGRAMA ACADÉMICO DE INGENIERIA DE SISTEMAS DE INFORMACIÓN

BACHILLER: ANGELLO GIORDANO RODRIGUEZ SOLSOL

La Tesis sustentada en acto público el día 14 de enero del 2026, a las 10:00 am, en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ.

ING. CARMEN PATRICIA CERDEÑA DEL AGUILA, DRA.
PRESIDENTE DE JURADO

ING. JIMMY MAX RAMÍREZ VILLACORTA, DR.
MIEMBRO DE JURADO

LIC. CARLOS ENRIQUE MARTHANS RUIZ, MTRO.
MIEMBRO DE JURADO

LIC. LUIS RONALD RUCOBA DEL CASTILLO, DR.
ASESOR

LIC. MAYA FABABA RODRÍGUEZ, MG
COASESOR

DEDICATORIA

“A mi familia, en especial a mi papá el señor Angel Humberto Rodríguez Jacinto y a mi mamá la señora Gabriela Solsol Mera, por su amor, su guía y apoyo incondicional. A mis hermanos y a mis hijos por su paciencia y comprensión.”

“A mí mismo, por la perseverancia y dedicación y a todos aquellos que creyeron en mi”.

.

A la Universidad Científica del Perú
como motivo de formación profesional

ANGELLO GIORDANO

AGRADECIMIENTO

A todas las personas que me apoyaron durante todo este tiempo con sus guías, consejos y motivaciones. Gracias a mi familia por apoyarme en cada decisión que tome durante este periodo de mi vida, el camino no fue sencillo hasta ahora, pero gracias a su apoyo y amor se cumplió con la meta, les agradezco y mi gran afecto por ustedes, mi hermosa familia.

A mis asesores de tesis por su orientación y sabiduría.

Gratitud y agradecimiento a la Universidad Científica del Perú por la oportunidad de haberme permitido ampliar y profundizar mis convicciones personales y profesionales.

El Autor

Contenido

DEDICATORIA ii
AGRADECIMIENTO iii
APROBACIÓN iv
CONSTANCIA DE ORIGINALIDAD v
ACTA DE SUSTENTACIÒN DE TESIS vi
INDICE DE TABLAS ix
ÍNDICE DE FIGURAS ix
RESUMEN x
ABSTRACT xi
INTRODUCCIÓN 1
CAPÍTULO I: Marco Teórico 3
1.1. Antecedentes de Estudio 3
Antecedentes Internacionales 3
1.2. Bases Teóricas 5
1.2.1. ANALISIS DEL IMPACTO DE LA CIBERSEGURIDAD 5
1.2.2. PROTECCIÓN DE DATOS SENSIBLES 8
1.3. Definición de Términos Básicos 12
CAPÍTULO II: Planteamiento del Problema 13
2.1. Descripción del Problema 13
2.2. Formulación del Problema 14
2.2.1. Problema General 14
2.2.2. Problemas Específicos 14
2.3. Objetivos 14
2.3.1. Objetivo General 14
2.3.2. Objetivos Específicos 14
2.4. Justificación e Importancia de la Investigación 15
2.5. Hipótesis 16
2.5.1. Hipótesis General 16
2.5.2. Hipótesis Derivadas 16
2.6. Variables 16
2.6.1. Identificación de las Variables 16
2.6.1. Variables 16
2.6.2. Definiciones Operacionales 16
2.6.3. Operacionalización de las Variables 18
CAPÍTULO IV: Metodología 20
4.1. Nivel y Tipo y Diseño de Investigación 20

4.1.1. Nivel de Investigación 20
4.1.2. Tipo de Investigación 20
4.1.3. Diseño de Investigación 20
4.2. Población y Muestra 21
4.2.1. Población 21
4.2.2. Muestra 21
4.3. Técnica, Instrumentos y Procedimientos de Recolección de Datos 21
4.3.1. Técnica de Recolección de Datos 21
4.3.2. Instrumentos de Recolección de Datos 21
4.3.3. Procedimientos de Recolección de Datos. 21
4.4. Procesamiento y Análisis de la Información 22
4.4.1. Procesamiento de la Información 22
4.4.2. Análisis de la Información 22
CAPÍTULO IV: Resultados 23
4.1. Analisis descriptivo 23
4.2. Analisis Inferencial 27
CAPÍTULO V: Discusión. Conclusiones. Recomendaciones 31
5.1. Discusión 31
5.2. Conclusiones 33
5.2.1. Conclusiones Específicas 33
5.2.2. Conclusión General 33
5.3. Recomendaciones 34
5.3.1. Recomendaciones Específicas 34
5.3.2. Recomendaciones General 34
Referencias Bibliográficas 35
Anexos 38
ANEXO N°01: Matriz de Consistencia 39
ANEXO 02 40
ANEXO 02 43
ANEXO N°3: Validez y Confiabilidad 45
ANEXO N°4: Consentimiento Informado 49
ANEXO N°5: Prueba Piloto de Impacto de la Ciberseguridad en la Protección de Datos Sensibles 50
Anexo 06: Base de Datos de Ciberseguridad en la Protección de Datos Sensibles 51

INDICE DE TABLAS

N°	TITULO	Pág.
01.	Confidencialidad de los datos	21
02.	Integridad de los Datos	22
03.	Disponibilidad de los Datos	23
04.	Protección de datos Sensibles	24
05.	Prueba de Normalidad	25
06.	Estadísticos de prueba	27

ÍNDICE DE FIGURAS

N°	TITULO	Pág.
01.	Confidencialidad de los datos	21
02.	Integridad de los Datos	22
03.	Disponibilidad de los Datos	23
04.	Protección de datos Sensibles	24

RESUMEN

La presente investigación tuvo como objetivo evaluar el impacto de la Ciberseguridad en la protección de datos sensibles en la MDSB 2025. El estudio se desarrolló bajo un enfoque cuantitativo de tipo preexperimental, con un diseño de un solo grupo con mediciones antes y después. La población estuvo conformada por 30 trabajadores municipales vinculados a la gestión de información sensible, por lo que se trabajó con una muestra censal.

En el Análisis descriptivo, previo a la intervención, el 96.7% de los participantes presento un nivel insuficiente en la protección de datos sensibles, mientras que posterior a la implementación de las medidas de ciberseguridad, el 90% alcanzo un nivel adecuado y el 6,7% un nivel óptimo. Se evidencio una mejora significativa en las dimensiones de confidencialidad, integridad y disponibilidad de los datos, reflejan un cambio positivo en la gestión y salvaguarda de la información institucional.

Para el análisis inferencial, se aplicó la prueba de normalidad de Shapiro-Wilk, cuyos resultados indicaron la no normalidad de los datos ($p < 0,005$). En consecuencia, se utilizó la prueba no paramétrica de rangos con signo de Wilcoxon para muestras relacionadas, con nivel de significancia de $\alpha = 0,05$. Los resultados mostraron un valor $p = 0,001$, lo que permitió rechazar la hipótesis nula y aceptar la hipótesis alternativa.

Se concluye, con un nivel de confianza del 95%, que la ciberseguridad tiene un impacto significativo en la protección de datos sensibles en la Municipalidad Distrital de San Juan Bautista, mejorando de manera sustancial la confidencial, integridad y disponibilidad de la información.

Palabras Clave: Ciberseguridad, protección de datos sensibles, confidencialidad, integridad y disponibilidad**.**

ABSTRACT

This research aimed to evaluate the impact of cybersecurity on the protection of sensitive data in the District Municipality of San Juan Bautista during 2025. The study adopted a quantitative approach with a pre-experimental design, using a single group with pre-test and post-test measurements. The population consisted of 30 municipal employees involved in the management of sensitive information; therefore, a census sample was applied.

In the descriptive analysis, prior to the intervention, 96.7% of the participants presented an insufficient level of sensitive data protection. After the implementation of cybersecurity measures, 90,0% reached an adequate level and 6.7% achieved an optimal level. Significant improvements were observed in the dimensions of confidentiality, integrity, and availability, demonstrating a positive effect on institutional information management and data safeguarding.

For the inferential analysis, the Shapiro-Wilk normality test indicated that the data did not follow a normal distribution ($p < 0.05$). Consequently, the non-parametric Wilcoxon signed-rank test for paired samples was applied, using a significance level of $\alpha = 0.05$. The results showed a p-value of 0.001, leading to the rejection of the null hypothesis and acceptance of the alternative hypothesis.

It is concluded, with a 95% confidence level, that cybersecurity has a significant impact on the protection of sensitive data in the District Municipality of San Juan Bautista, substantially improving data confidentiality, integrity, and availability.

Keywords: Cybersecurity, sensitive data protection, confidentiality, integrity, availability.

INTRODUCCIÓN

La protección de los datos sensibles en el ámbito público ha dado paso a ser una cuestión de relevancia mundial debido a la dependencia creciente de los sistemas informáticos en el funcionamiento de la administración pública. En este sentido, la ciberseguridad presenta amenazas constantes para la integridad, la confidencialidad y la disponibilidad de datos, por lo que toda institución necesita implementar medidas eficaces de ciberseguridad que protejan dichos bienes de la información.

Este tema es relevante para el distrito porque ayuda a proteger los datos contra eventuales ataques, y también a tener un acceso seguro a la información, que es clave para prestar servicios y ayudar a los ciudadanos. El tipo de estudio que se realizó para medir hasta qué nivel la implementación de ciberseguridad mejora cada dimensión clave de los datos sensibles fue cuantitativo y preexperimental.

La defensa de la presente investigación enfatiza comprender en profundidad la efectividad y/o deficiencias que las medidas de seguridad implementadas tienen para ayudar a respaldar decisiones fundamentadas en los diagnósticos para evaluar dónde la ciberseguridad en el distrito requiere más infraestructura.

Permite identificar qué dimensiones son más vulnerables y dónde se requieren mejoras de infraestructura, tecnología y capital humano, posibilitando priorización de inversiones y acciones.

En el estudio se planteó como problema general: ¿En qué medida el Análisis del Impacto de la Ciberseguridad mejora la Protección de Datos Sensibles de la MDSJB 2025?, para su tratamiento es necesario ver la situación actual de ciberseguridad en la MD SJB, del siguiente modo:

La revisión descriptiva inicial y las evaluaciones de seguridad existentes señalan la necesidad de un diagnóstico claro sobre el estado actual, la identificación de activos críticos y la priorización de intervenciones frente a incidentes reales o potenciales.

La caracterización de riesgos y la planificación de medidas permitirán reducir vulnerabilidades y fortalecer la confianza pública, elementos críticos para la legitimidad y eficacia de la administración local.

Se encuentra ordenado de la siguiente manera:

Capítulo I: Marco Teórico, que abarca los antecedentes, las bases teóricas y la definición de términos clave.

Capítulo II: Planteamiento del Problema, que incluye la descripción y formulación del problema, los objetivos, la justificación e importancia, las hipótesis y las variables.

Capítulo III: Metodología, que abarca el nivel, tipo y diseño de la investigación, la población y muestra, las técnicas, instrumentos y procedimientos para la recolección de datos, así como el procesamiento y análisis de los mismos.

Capítulo IV: Resultados.

Capítulo V: Discusión, conclusiones y recomendaciones.

Finalmente, se presentan las referencias bibliográficas y los Anexos.

El Autor

CAPÍTULO I: Marco Teórico

1.1. Antecedentes de Estudio

Antecedentes Internacionales

En el año 2025, Gonzáles Martínez desarrollarlo un estudio cuantitativo de tipo preexperimental, aplicado a dos grupos conformados por cinco especialistas del área de Tecnología de la información y Seguridad informática (cuatro ingenieros y un gerente TI) y dos usuarios operativos de un sistema ERP, quienes representaban la totalidad de los colaboradores que utilizaban dicha plataforma en la organización. El estudio tuvo como objetivo proponer un plan de ciberseguridad orientado a la gestión de riesgos. Los resultados evidenciaron debilidades relacionados con accesos no autorizados, ataques de phishing, errores humanos y deficiencias en la gestión de incidentes para organizaciones que operan ERP web, fortaleciendo la resiliencia organizacional frente a amenazas digitales.

El 2025, el estudio cuantitativo, preexperimental, en 24 estudiantes. Se determino que establecer relaciones entre las variables independientes (moral) y dependiente (ciber-ética). Concluye que establecen controles de seguridad informática por el mismo especialista, frente a la Confidencialidad, Integridad y Disponibilidad (CIA), para aplicarlo al grupo experimental, conformado por 24 estudiantes y un administrativo. Además, se crean métricas, sustentadas en las Normas ISO/IEC: 27001; 27002 y el Índice de Economía y Sociedad Digitales (DESI), para generar resultados en diagrama nube de puntos, y hacer análisis matemático (Ecuación no lineal de Bernoulli), para cotejar resultados y evidenciar una correlación con la UNAD desde su modelo pedagógico, que concuerda con los objetivos, problema de investigación e hipótesis (Ramírez, Otilia, 2025).

Nacional

El 2024, el estudio cuantitativo, preexperimental, en 15 administrativos y 120 asistenciales de salud, que hacen un total de 135 profesionales. Determino un

avance notable en las acciones de seguridad en salvaguarda de la información personal. Concluyo que la implementación y las sugerencias concretas para la persistencia y mejora constante del SGSI en la clínica acorde a la norma ISO/IEC 27001:2022, resaltando las ventajas concretas en la salvaguarda de la información personal (Cama Jara, Arellano Buleje, 2024).

El 2024, el estudio cuantitativo, preexperimental, en 30 indicadores de compromiso identificados durante el último día operativo. Determino avances notables en varios indicadores. Concluyendo que hubo disminución del 82.61% en el tiempo de elaboración de informes, disminución del 97.53% en el tiempo de divulgación de la información. Además, se consiguió un incremento del 88.12% en el desempeño del proceso de recopilación de datos, se consiguió un aumento del 33% en el grado de satisfacción del usuario y, finalmente, se incrementó un 32.62% en la calidad del formato resultante para la visualización de los informes. Por lo tanto, la puesta en marcha de la plataforma web que incorpora herramientas OSINT, mejoró la administración de incidentes de ciberseguridad, corroborando de esta manera la hipótesis principal de este estudio (León Estofanero, 2024).

El 2024, el estudio cuantitativo, pre experimental, en 18 portales web de los Ministerios peruanos, determinó en base a 3 tipos de dispositivos informáticos, las variaciones en las pruebas de los Grupo 1 y Grupo 2 se realizan de un rendimiento regular 100%; un nivel de bueno 100% en buenas prácticas y concluye que hay diferencias de varianza entre dispositivos informáticos, en la auditoría web (Miranda Zeballos, 2024).

El 2024, el estudio cuantitativo, preexperimental, en 114 controles extraídos de la norma “ISO 27001”, en 20 centrales, puso en marcha el sistema de administración de seguridad informática en una compañía de servicios. Concluyó afirmando que los hallazgos del estudio señalan que la aplicación de la "ISO 27001" optimiza el sistema de administración de la información, reduciendo el número de incidentes que afectan la privacidad en un 99%, el número de incidentes que afectan la integridad en un 99% y el número de

incidentes que afectan la disponibilidad en un 99%. (De La Cruz Santa Cruz, 2024).

El 2024, el estudio cuantitativo, preexperimental, En la oficina central y sus 17 oficinas de la COOPAC Huamanga. Determino la implementación del Sistema de Ciberseguridad para determinar si aumentar el uso del Sistema de Ciberseguridad disminuirá de manera significativa el riesgo operativo. Concluyendo que se confirma por el p-valor (0, 000), que es inferior al nivel de significancia de α=0, 05, que es inferior al nivel de significancia de α=0, 05 (Tolentino Valer, Zorrilla Alva, 2024).

Regional

El 2019, el estudio cuantitativo, preexperimental, en 60 estudiantes, 30 del grupo experimental y 30 del grupo control. Determino comprobar la validez del plan de fortalecimiento en el uso de las TIC; mejora significativamente las habilidades tecnológicas. Concluye la prueba estadística de la t de Student, con α = 0.05 y nivel de confianza de 0.95%. El grupo experimental a quienes se les aplicó dicho plan y los estudiantes del grupo control a quienes no se les aplicó el referido plan, se demuestra que de 30 (100,0% estudiantes del GE, en el 76,7% (23) de ellos el nivel de uso de las Tics encontrado fue Alto, en el 23,3% (7) el nivel de uso fue medio, no hubo estudiante con nivel de uso bajo respectivamente. GC la distribución es distinta, con 23,3% (7) de ellos en nivel de uso alto, el 70,0% (21) el nivel de uso fue medio y en el 6,7% (2) uso fue bajo correspondientemente. (Vásquez Del Águila, 2019).

1.2. Bases Teóricas

1.2.1. ANALISIS DEL IMPACTO DE LA CIBERSEGURIDAD

Proceso crucial que permita medir el impacto el efecto de los diversos métodos de ciberseguridad en la protección de datos de las instituciones. Consta de diversos pasos como el diagnóstico y pronóstico de riesgos, la imposición de medidas de mitigación y la posterior evaluación de su efectividad al proteger la privacidad de los datos y cumplir con regulaciones y normativa tanto nacional como internacional. En los recientes años se han popularizado mucho estos procesos debido al

incremento en la seguridad de ciberataques y la necesidad de proteger las privacidades en línea (Tapia Chica *et al.*, 2024).

El tema de la ciberseguridad se evaluará utilizando los principios de la administración del riesgo. Además, nos centraremos en el concepto de política de seguridad Confianza Cero y ciberseguridad centrada en los datos.

La Evaluación de Impacto en Protección de Datos EIPD es otra base teórica que incluye una identificación de actividades de tratamiento de datos, una evaluación de riesgos específicos y una implementación de medidas para mitigar posibles daños (Dulce Villarreal *et al.*, 2023).

El diagnóstico de ciberseguridad es una evaluación de los niveles de riesgo actuales en una organización, que mide las oportunidades en control de acceso, configuración del sistema de seguridad y resiliencia del libro ante incidentes.

Las evaluaciones de impacto deben estar acompañadas de una gestión que apoye la sostenibilidad de las medidas de protección en el tiempo. Esto contempla la delegación de competencias junto con la elaboración de la rendición de cuentas, el registro de los resultados y la adaptación de políticas al cambio en el contexto de los riesgos que hay. Desde un ángulo crítico, hay que analizar que un enfoque más adecuado sería uno basado en la adaptabilidad. Las amenazas, al menos en la construcción de un sólido marco legal de protección para datos sensibles en la esfera pública, están en constante evolución.

Como se observa en este ensayo, la evaluación de ciberseguridad de una entidad pública tiene relevancia considerando que no solo evalúa los riesgos y las capacidades disponibles, sino que configura un escudo flexible, dinámico y proactivo, lo que a su vez optimiza la confiabilidad y seguridad administrativa. De esta manera, con la adopción de estos modelos se establecen sistemas de gerencia que comienzan desde la planeación de contingencias hasta la gerencia activa de incidentes, a lo

que se puede denominar cultura de ciberseguridad en la administración pública.

Para poder llevar a cabo esta evaluación, se hace desde una perspectiva holística que integra políticas definidas, educación impartida a lo largo del tiempo y reacción a situaciones determinadas. Combinados, estos aspectos logran proteger información altamente confidencial y, por otra parte, vuelven a la organización mucho más adaptable a un entorno en rápida evolución cambiando las realidades en el modo de percibir información y realidad. Por lo tanto, la evaluación sumativa y crítica de estos colaboradores proponen pasos seguros y optimistas frente a la información en un contexto nacional, mientras promueve una cultura de ciberseguridad no solo a nivel organizacional, sino comunal.

1.2.1.1. Eficiencia de las Políticas de Ciberseguridad

La eficiencia en las políticas de ciberseguridad se refiere a la posibilidad de una organización de implementar políticas que puedan reducir ciber amenazas. TICNUS Technology Magazine define una política eficiente según el marco ISO/IEC 27001 y el modelo de NIST como una política con un manejo de riesgos detallado; roles y responsabilidades claramente definidos y protocolos de seguridad sólidos. Estos factores son vitales en el ámbito gubernamental con el fin de obtener un manejo adecuado de recursos, delegar roles en cada nivel de la organización y habilitar métodos como el cifrado y el control de acceso, que son cruciales en la protección de datos (Fonseca, Juárez, 2019).

En conjunto, la perspectiva crítica de la gestión de la política de ciberseguridad sugiere que la prevención es la prioridad principal en el ámbito de la política. Las directrices de ISO y NIST informan expresamente sobre la actividad preventiva: la identificación y contención de las vulnerabilidades a través del monitoreo y la auditoría continuos. Esta recomendación también es evidente en los estudios modernos, que aconsejan la implementación de la política diseñada directamente de

acuerdo con los riesgos específicos en el sector público, dada la continuación de la tendencia en aumento de la cantidad de incidentes reales.

1.2.1.2. Capacitación y Concienciación en Ciberseguridad

Con el fin de crear una cultura general de ciberseguridad, se considera uno de los métodos más eficaces y, al mismo tiempo, más simples. El conocimiento en el campo de la ciberseguridad implica que los empleados se conviertan en la primera línea de defensa contra la suplantación de la identidad, ya que a menudo se convierte en un método de ataque, pescando a las víctimas (Arenas Ramiro, 2021). Este enfoque, que es el pilar de la PNCS de 2023-2028, apoyado por modelos de sensibilización proporcionados por SANS, permite considerar y ser responsable de los elementos de protección más allá de la barrera tecnológica (Álvarez-Carrión, Hernández--Sotomayor, 2024).

1.2.1.3. Respuesta ante Incidentes de Seguridad

La capacidad de respuesta es crucial para la ciberseguridad porque su propiedad permite reducir la amenaza de los ataques en tiempo real (Gonzalez Cárdenas, 2024). Según la capacidad de respuesta según la norma ISO/IEC 27035 u otras similares, TICNUS Technology Magazine hace hincapié en la rápida identificación, contención, erradicación y recuperación, así como la comunicación con un interlocutor sobre el problema relevante. La coordinación con organismos de seguridad y la inversión en medidas de “detección” también pueden resultar beneficiosas. Todo lo anterior incluye un sistema proactivo de respuesta al problema. Esto se basa en la “auditoría” y en la contención temprana de la amenaza, lo que, a su vez, reduce la posibilidad de pérdidas a largo plazo.

1.2.2. PROTECCIÓN DE DATOS SENSIBLES

Se basa en tres principios básicos, a saber, la confidencialidad, la integridad y la disponibilidad, los CIDs, que garantizan que los datos estén disponibles, intactos y a salvo de accesos no autorizados. Comprende

varios aspectos que garantizan la propagación de accesos no autorizados al alterar y destruir datos personales. Para demostrarlo, la confidencialidad implica que solo se autorizará a las personas a las que se les permitirá el acceso. Una vez que un individuo o grupo de personas libera confidencialmente información a través de una persona o dispositivo no autorizado, se produce una filtración. En este caso, es vital que los administradores establezcan las medidas apropiadas. El marco deduce tres pilares, el CID con el acrónimo de confidencialidad, integridad y disponibilidad. La confidencialidad se centra en garantizar que solo las personas indicadas estén permitidas en la información y que los procedimientos sean empleados para que la información no sea alterada. Los afectados y sus contribuciones se componen de la gestión de avances en la municipalidad, puesto que también rescatan la información a nivel personal, lo que eleva el problema (Morillas Fernández, 2023).

Cabe mencionar que existe información personal acerca de los empleados de los ciudadanos. Es importante observar los siguientes principios, aprovechando un enfoque metodológico predeterminado.

La Integridad requiere que los datos permanezcan precisos y completos durante su ciclo de vida, la Disponibilidad asegura que los datos estén a disposición de aquellos con autorización cuando los necesiten, logrado a través de copias de respaldo, redundancia y recuperación de desastres. La Directiva NIS 2 y otros marcos reguladores requieren una evaluación de riesgos, y todas las entidades deben poder identificar y predecir las consecuencias negativas de la falta de protección de datos. Según el pronóstico, si no se toman medidas de protección, todos los niveles de riesgo aumentarán y se producirán pérdidas de datos de escape, pérdidas y daños a la confianza del público. La gestión de la protección de datos incluye una serie de estrategias y prácticas que facilitan la administración de datos sensibles. Los EIPD, que se derivan del GDRP, son tales metodologías y se utilizan para analizar y medir los riesgos asociados con el procesamiento de información personal. Se pueden dividir en varias

etapas: identificación de actividades de procesamiento, evaluación de riesgos, acciones correctivas. Cuando se trata del sector público, se pueden mencionar la implementación de políticas que limitan el acceso, la capacitación en seguridad y una auditoría constante.

Existen varias tendencias que han surgido en el tratamiento de datos sensibles. Por un lado, Ciberseguridad Centrada en los Datos se ha vuelto importante porque más y más datos se comparten entre planteles y con terceros. Se sostiene que los datos deben ser protegidos en el punto de cada, independientemente de la ubicación a través de cifrado y autenticación multifactor. Por el otro, el paradigma de Confianza Cero Zero-Trust sostiene que ningún usuario, sea interno o externo, debe tener acceso a menos que haya logrado verificar su identidad mediante controles de seguridad rígidos. Estos dos enfoques protegen los datos sensibles, al mismo tiempo que reducen el riesgo de incumplimiento de la seguridad, ya que exigen verificaciones continuas y funcionalidades que permiten el acceso con base en roles específicos. Esto se es porque la protección de datos sensibles debe ser continuamente evaluada para compensar el riesgo con medidas preventivas y correctivas. En otras palabras, la Ciberseguridad Centra en los Datos y la Confianza Cero permiten la gestión de políticas que no solamente cumplen con la legislación sobre protección de datos, sino que también consideran la utilidad del público (Fernández Ramírez, 2023).

1.2.2.1. Confidencialidad de los Datos

Entre las contramedidas comunes para proteger la confidencialidad se encuentran la autenticación de múltiples factores, el cifrado de datos y las políticas de acceso controlado (Medina Guerrero, 2023). Se debe tener en cuenta que se supone que las políticas basadas en la protección de los datos sensibles deben ser revisadas en una base regular y adaptadas para superar las nuevas amenazas, lo que también promueve un enfoque proactivo de la gestión de seguridad.

1.2.2.2. Integridad de los Datos

La integridad protege los datos de la alteración. Lo hacen más precisos y completos evitando las modificaciones no autorizadas, intencionadas o no, durante el ciclo de vida del dato. Los mecanismos de control de versiones y firmas digitales son formas fáciles de asegurar que los datos permanezcan completamente intactos, y esto es esencial en sectores críticos como la banca o en la administración pública. Sin embargo, sin la protección de la integridad, la información se puede volver incoherente o falsificada, lo que también perjudica la fiabilidad de la toma de decisiones. Críticamente, el principio de integridad implica no solo controles técnicos, sino también auditorías regulares y políticas de separación de funciones. Esto responde a una visión de la seguridad que protege no solo los datos, sino también la confianza del público; es esencial en la administración digital del gobierno (Aznar Sánchez-Parodi, 2023).

1.2.2.3. Disponibilidad de los Datos

La disponibilidad asegura que los datos estén al alcance de usuarios autorizados en el momento que sea necesario. En el gobierno, es esencial, ya que los ciudadanos y empleados utilizan los sistemas y servicios continuamente. Si hay falta de disponibilidad, la organización se puede paralizar, lo que se traduce en servicios públicos deficientes o falta de ellos. Los mejores enfoques para garantizar la disponibilidad pueden incluir la infraestructura redundante, los planes de recuperación de desastres, el monitoreo y la supervisión en tiempo real de los sistemas críticos para visualizar y reducir los efectos de desviación. Hoy en día, el principio de confianza de la ciberseguridad es un ‘must’ y requisito de funcionamiento para poder operar con la confianza pública. En el aspecto cognitivo, dicho principio garantiza la continuidad operativa de la agencia, es decir, es capaz de contener o enfrentar cualquier tipo de incidente y mantener la robustez de la agencia a través del tiempo. (Sánchez Díaz, 2023).

1.3. Definición de Términos Básicos

Capacitación en Ciberseguridad. Refiérase a la capacitación continua y especializada en seguridad de la información para dotar al personal de habilidades que le permiten identificar y responder a las amenazas digitales de manera eficaz.

Concienciación en Ciberseguridad. Proceso de informar a los usuarios de sus responsabilidades de seguridad y seguridad y de motivarlos a adoptar un comportamiento informado y seguro. Pretende minimizar los errores humanos, que están detrás de un número considerable de debilidades de seguridad.

Datos Sensibles. Cualquier recomendación personal que, si se revela o se ve comprometida, pueda presentar un peligro peligroso para la privacidad o la confianza de una única persona. Ejemplos son el flujo monetario consumado y la información sobre la vida real, entre otros.

Disponibilidad de los Datos. Fundamental para la computadora continuar con el uso respaldando y recuperando prácticas para prevenir fallos de acceso.

Incidentes de Seguridad. Cualquier reacción o peligro de cualquier forma a los sistemas de mensajes, incluidos los virus informáticos. Suelen causar daños y perjuicios y deben tratarse de inmediato.

Municipalidad. Administración local en la dirección de reglamentar el bienestar público, servicios, y crecimiento urbano. También tiene la responsabilidad, en este caso, de proteger los detalles privados de los participantes.

Políticas de Ciberseguridad. Reglas y regulaciones estipuladas por una sociedad para recopilar y asegurar sus entradas digitales. Abarca el manejo de riesgos y la criminalidad, entre otros. La prueba se realizó utilizando el CYBONETTE.

CAPÍTULO II: Planteamiento del Problema

2.1. Descripción del Problema

En la Municipalidad Distrital de San Juan Bautista -MDSJB, la salvaguarda de los datos sensibles de los ciudadanos se topa con retos significativos a causa del aumento en la amenaza de ataques cibernéticos. El analisis del impacto de la ciberseguridad, que es la variable independiente de esta investigación, resulta esencial para entender cómo las políticas presentes y futuras en el ámbito de la ciberseguridad pueden disminuir el peligro de exposición y salvaguardar los datos en instituciones municipales vulnerable (Brion Berdote, 2022). Circunscribe cómo los datos se salvan de estas amenazas en ciberespacio, lo que representa una variable vital para la confianza pública en las instituciones estatales. La razón para la vulnerabilidad se determina a través de la falta de infraestructura de seguridad y la dependencia de los sistemas heredados que son vulnerables a la exposición (Bernal-Camargo, Gómez-Córdoba, 2022). Al mismo tiempo, las limitaciones financieras y la inercia son dos de los mayores desafíos para la aplicación de tecnologías modernas de ciberseguridad. A pesar de las amenazas, sigue abierta la ventana para la intrusión en las redes municipales y el compromiso de la privacidad. Sin una exposición adecuada de estos puntos vulnerables, los incidentes de la ciberseguridad probablemente crecerán con impacto en la privacidad del ciudadano y la operabilidad de la municipalidad. Mudar su prioridad ponen la institución en riesgo de una mayor exposición y la consiguiente pérdida de confianza pública. Además de las posibles sanciones legales por incumplir la ley antes mencionada, las intrusiones entrarán en desviación y destruirán la economía. Dado el riesgo potencial para los ciudadanos y las inversiones estatales, esta investigación es vital para la protección de los datos, por lo que se plantea lo siguiente:

2.2. Formulación del Problema

2.2.1. Problema General

¿En qué medida el Analisis del Impacto de la Ciberseguridad mejorara la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025?

2.2.2. Problemas Específicos

¿Cuál es el impacto de la Ciberseguridad en la mejora de la Confidencialidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista-MDSJB 2025?

¿Cuál es el impacto de la Ciberseguridad en la mejora de la Integridad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista-MDSJB 2025?

¿Cuál es el impacto de la Ciberseguridad en la mejora de la Disponibilidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista-MDSJB 2025?

2.3. Objetivos

2.3.1. Objetivo General

Medir el Impacto de la Ciberseguridad en la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.

2.3.2. Objetivos Específicos

Analizar el impacto de la Ciberseguridad en la mejora de la Confidencialidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.

Analizar el impacto de la Ciberseguridad en la mejora de la Integridad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.

Analizar el impacto de la Ciberseguridad en la mejora de la Disponibilidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.

2.4. Justificación e Importancia de la Investigación

Las instituciones públicas enfrentan crecientes riesgos de ciberataques que amenazan la vida de los ciudadanos y la confiabilidad de los servicios vitales, es esencial examinar el impacto de la ciberseguridad en la información sensible dentro de los archivos de Municipalidad Distrital de San Juan Bautista (MDSJB). Por un lado, esta investigación documentará la efectividad de las medidas de ciberseguridad implementadas. Por otro lado, proporcionará medidas técnicas y estratégicas óptimas que evitarán la comprometida de datos críticos mientras protegen, en última instancia, la confianza institucional. Esta investigación es relevante porque la información sensible de los ciudadanos, como datos personales y financieros, a menudo es objetivo de los cibercriminales que explotan vulnerabilidades de seguridad para esquemas fraudulentos y extorsión sin escrúpulos (García Fernández, 2022). La ley de Protección de Datos Personales se inserta en nuestro sistema jurídico el 5.12.2018, como una categoría legal específica, lo que se denomina derechos digitales. En lo social fomentará una buena y sólida administración pública ante amenazas emergentes. A nivel práctico, esta investigación beneficiará directamente a las instituciones municipales, ya que podrán mejorar su capacidad de respuesta y la seguridad de los datos. A la comunidad local al reducir el riesgo de exposición y robo de datos personales. Debido a que esta investigación se centra en un enfoque local de la administración municipal, es innovadora. Este trabajo se enfocará primero en abordar los problemas más básicos de seguridad personal e introducirá los métodos que más ahorran costos, como la autenticación multifactor, para aumentar la eficiencia de los sistemas de información. Sin acciones preventivas para cubrir las deficiencias de seguridad, los problemas existentes solo se intensificarán, resultando en más penalizaciones y una mayor desconfianza hacia los organismos estatales. Los resultados de esta investigación se publicarán en espacios académicos y de administración pública.

*2.*5. Hipótesis

2.5.1. Hipótesis General

La implementación de medidas de ciberseguridad mejora significativamente la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025.

2.5.2. Hipótesis Derivadas

- La implementación de medidas de ciberseguridad mejora significativamente la Confidencialidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025.
- La implementación de medidas de ciberseguridad mejora significativamente la Integridad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025.
- La implementación de medidas de ciberseguridad mejora significativamente la Disponibilidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025.

2.6. Variables

2.6.1. Identificación de las Variables

2.6.1. Variables

V.I. (X): **ANALISIS DEL IMPACTO DE LA CIBERSEGURIDAD**

V.D. (Y): **PROTECCIÓN DE DATOS SENSIBLES**

2.6.2. Definiciones Operacionales

La V.I. (X): **ANALISIS DEL IMPACTO DE LA CIBERSEGURIDAD**, se define conceptualmente como: Proceso de identificar amenazas o vulnerabilidad por lo que sirve para prever incidentes y determinar el nivel de preparación en caso de que ocurran.

Se define operacionalmente en sus dimensiones: **Eficiencia de las Políticas de Ciberseguridad. Capacitación y Concienciación en**

Ciberseguridad. Respuesta ante Incidentes de Seguridad: Categorizados como: **(1) Insuficiente:** Deficiencias significativas o implementación inexistente. **(2) Adecuado:** Cumplimiento moderado con áreas de mejora identificadas. **(3) Óptimo:** Implementación excelente, con pocas o ninguna observación relevante.

La V.D. (Y): **PROTECCIÓN DE DATOS SENSIBLES**, Involucra una serie de acciones que se llevan a cabo para garantizar que el tratamiento de estos datos sea seguro, justo y restringido únicamente a lo necesario: control de acceso e integridad, particularmente en términos de datos personales como la salud, las creencias y los biométricos.

Se define operacionalmente, en sus dimensiones: **Confidencialidad de los Datos. Integridad de los Datos. Disponibilidad de los Datos.** Categorizados como: **(1) Insuficiente:** Deficiencias significativas o implementación inexistente. **(2) Adecuado:** Cumplimiento moderado con áreas de mejora identificadas. **(3) Óptimo:** Implementación excelente, con pocas o ninguna observación relevante.

2.6.3. Operacionalización de las Variables

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Ítem	Instrumento
V.I. (X) **ANALISIS DEL IMPACTO DE LA CIBERSEGURIDAD**	Análisis sistemático de las medidas de ciberseguridad implementadas para identificar su efectividad y el nivel de riesgo residual en una organización	Para medir el impacto de la ciberseguridad en la protección de datos sensibles, se aplicará un cuestionario de evaluación a los responsables de TI y seguridad de la municipalidad en sus dimensiones: **Eficiencia de las Políticas de Ciberseguridad. Capacitación y Concienciación en Ciberseguridad. Respuesta ante Incidentes de Seguridad.**	**Eficiencia de las Políticas de Ciberseguridad**	**Implementación de protocolos de seguridad**	Implementación protocolos de seguridad	**ENCUESTA/CUESTIONARIO** **FICHA DE OBSERVACIÓN.** Guion de entrevista semiestructurada **(1)** **Insuficiente (00-10 puntos)** **(2)** **Adecuado (11-15 puntos):** **(3)** **Óptimo (16-20 puntos):**
					Procedimientos documentados para la gestión	
					Conocimiento de los protocolos de ciberseguridad	
					Revisión y actualización de protocolos	
					Políticas claras sobre el uso seguro de datos	
				Cumplimiento con regulaciones de ciberseguridad	Cumplimiento de la normativa nacional	
					Equipo dedicado al cumplir lo normativo en ciberseguridad	
					Estándares internacionales en ciberseguridad	
					Capacitación sobre leyes de protección de datos	
					Auditorías periódicas para asegurar el cumplimiento normativo	
				Eficacia en la gestión de riesgos	Identifican y evalúan regularmente los riesgos	
					Cuenta con un plan para mitigar riesgos	
					Herramientas de monitoreo para identificar amenazas	
					Analizan y gestionan los incidentes ocurridos	
					Personal capacitado para la evaluación y gestión de riesgos	
			Capacitación y Concienciación en Ciberseguridad	**Capacitación continua del personal**	Formación continua en temas de ciberseguridad	
					Identifican amenazas como phishing o malware	
					Capacitaciones adaptas a las actualizaciones tecnológicas	
					Sesiones de capacitación obligatorias	
					Involucramiento del equipo directivo	
				Conciencia sobre la protección de datos	Comprenden la importancia de proteger datos	
					Campañas de concienciación	
					Aplican prácticas seguras	
					Identifican datos sensibles	
					Fomento de cultura de responsabilidad sobre datos	
				Evaluación de la efectividad de las capacitaciones	Evalúa el conocimiento adquirido	
					Aplican las prácticas de seguridad aprendidas	
					Pruebas de competencia en ciberseguridad	
					Evalúa si la capacitación reduce incidentes	
					Solicitan apoyo adicional	
			Respuesta ante Incidentes de Seguridad	**Tiempo de respuesta ante incidentes**	Respuesta adecuada sobre seguridad	
					Procedimientos de respuesta rápida a incidentes	
					Actúan de manera oportuna	
					Los incidentes menores se manejan sin afectar la operación diaria	
					Evalúa el tiempo de respuesta	
				Contención y mitigación de amenazas	Herramientas para contención rápida	
					Equipo de expertos en mitigación de amenazas	
					Planes de contención frente a daños a datos sensibles	
					Actualizan las estrategias de contención	
					Personal preparado para ejecutar planes de mitigación de amenazas	
				Recuperación y continuidad operativa	Cuentan con plan de recuperación ante incidentes	
					Tras incidentes mantiene la calidad del servicio	
					Simulacros de recuperación para asegurar la continuidad	
					Datos sensibles restaurados	
					Personal responsable	

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Ítem	Instrumento
V.D. (Y) **PROTECCIÓN DE DATOS SENSIBLES**	Medidas y políticas enfocadas en salvaguardar la privacidad y seguridad de los datos que, de ser divulgados sin autorización, podrían tener un impacto negativo significativo en los derechos de los individuos. Esta protección abarca datos de salud, información biométrica y otros elementos personales cuya exposición puede provocar riesgos de discriminación o vulneración de la privacidad	Medición de la Eficiencia de los Protocolos de Protección: Se empleará un análisis de auditoría de incidentes de seguridad para identificar la frecuencia de accesos no autorizados o de violaciones de datos en el último año. Los datos obtenidos permitirán cuantificar la resiliencia de los sistemas de protección de la municipalidad y los procedimientos correctivos aplicados en caso de brechas de seguridad	**Confidencialidad de los Datos**	**Control de acceso a datos sensibles**	Limitan el acceso a datos sensibles	**ENCUESTA/CUESTIONARIO** **FICHA DE OBSERVACIÓN.** Guion de entrevista semiestructurada **(1)** **Insuficiente (00-10 puntos):**. **(2)** **Adecuado (11-15 puntos):** **(3)** **Óptimo (16-20 puntos):**.
					Herramientas de autenticación multifactor para información confidencial	
					Niveles de acceso según su rol en la institución	
					Registros de acceso a datos sensibles	
					Reciben advertencias sobre intentos no autorizados de acceso	
				Políticas de privacidad y manejo de datos	Cuenta con políticas de privacidad	
					Capacitados en el manejo responsable de datos sensibles	
					Revisiones periódicas de las políticas de privacidad	
					Políticas de manejo de datos según normativas	
					Información a usuarios	
				Uso de cifrado en datos sensibles	Datos sensibles cifrados	
					Protocolos cifrados	
					Realizan pruebas de vulnerabilidad	
					Aplican a todos los tipos de datos confidenciales	
					Implementados procedimientos para actualización de claves	
			Integridad de los Datos	**Validación y control de cambios en los datos**	Auditorías regulares	
					Procedimientos de validación para detectar modificaciones no autorizadas	
					Registros de cambios detallados y accesibles	
					Controles para evitar la alteración de datos	
					Reciben notificaciones sobre cambios	
				Protección contra pérdida de datos	Respaldos periódicos de los datos sensibles	
					Respaldos protegidos	
					Plan de recuperación ante desastres	
					Utiliza sistemas de detección de pérdidas de datos	
					Pruebas para recuperación de datos	
				Monitoreo de la integridad de los datos	Cuenta con herramientas de monitoreo en tiempo real	
					Auditorías para identificar incidentes	
					Emiten alertas cuando se detectan modificaciones	
					Revisión de registros de acceso	
					Sistema para rastrear y revertir cambios	
			Disponibilidad de los Datos	**Acceso seguro y continuo a datos sensibles**	Sistemas de datos críticos para evitar interrupciones de acceso	
					Medidas para asegurar el acceso ininterrumpido	
					Acceso a datos sensibles	
					Equipo TI para la rápida resolución de problemas	
					Implementan pruebas periódicas	
				Resiliencia ante ciberataques	Planes de contingencia	
					Sistemas que detectan y mitigan ataques	
					Simulacros de ciberataques	
					Capacitado para mantener la disponibilidad	
					Evalúan periódicamente los sistemas de respaldo de datos	
				Recuperación rápida de datos tras incidentes	Plan de recuperación rápida	
					Pruebas de recuperación de datos	
					Permiten la restauración de datos	
					Entrenamiento en procedimientos de recuperación de datos	
					Equipo dedicado para la gestión de recuperación de datos	

CAPÍTULO IV: Metodología

4.1. Nivel y Tipo y Diseño de Investigación

4.1.1. Nivel de Investigación

Cuantitativa preexperimental con un solo grupo, la cual posibilitó la evaluación del efecto de la CIBERSEGURIDAD en la PROTECCIÓN DE DATOS SENSIBLES al comparar a un conjunto que recibe la intervención y a otro que no, midiendo las competencias antes y después de dicha intervención. (Hernández Sampieri *et al.*, 2014).

4.1.2. Tipo de Investigación

Preexperimental, ya que las características de los empleados y del entorno municipal no permiten la asignación aleatoria de los participantes (Albarracín-Villamizar, 2020).

4.1.3. Diseño de Investigación

Se eligió un conjunto de empleados que fue incluido en el estudio como grupo experimental y de control, con pretest y post test. Esto posibilitó definir una línea de referencia para la comparación. Después se llevó a cabo la intervención, en la que el grupo experimental recibió una intervención temática creada específicamente para fomentar la ciberseguridad en la protección de datos sensibles. Cuando se llevó a cabo un examen final (post test). Esto posibilitó la comparación de los resultados PRE y POST de la intervención con el grupo experimental. El análisis de datos se llevó a cabo con la información mencionada. Asimismo, se examinaron las variaciones entre el periodo anterior y el posterior. El diseño es. (Álvarez, Lópe, 2023)

GE: 01	**X**	**02**

Dónde:

GE: Grupo experimental

X: Experimento

01 observaciones al grupo experimental antes del experimento (Pre-Test)

02 observaciones al grupo experimental después del experimento (Post Test).

4.2. Población y Muestra

4.2.1. Población

Se dispuso de 30 trabajadores municipales que laboran en diferentes oficinas de la municipalidad.

4.2.2. Muestra

Compuesta por un muestreo no aleatorio y por conveniencia. Se trató de un censo, lo cual quiere decir que se utilizó el 100% de la población, o sea los 30. El criterio que dirigió la elección de la muestra fue el requerimiento de incluir solamente a los trabajadores responsables de gestionar datos sensibles en la Municipalidad Distrital de San Juan Bautista (MDSJB), incluyendo tanto el ámbito administrativo como el técnico. Para garantizar una representación funcional, la inclusión dependió de la disponibilidad y el permiso de los participantes e implicó un muestreo por criterios. Se seleccionó un grupo de 30 empleados, pues era la totalidad de la plantilla con competencias vinculadas a la protección de datos. Esto permitió obtener resultados válidos para evaluar el impacto de la ciberseguridad en el entorno institucional.

4.3. Técnica, Instrumentos y Procedimientos de Recolección de Datos

4.3.1. Técnica de Recolección de Datos

Encuesta**.**

4.3.2. Instrumentos de Recolección de Datos

1. Cuestionario para medir el Impacto de la Ciberseguridad en la mejora de La Protección de Datos Sensibles. Dichos instrumentos fueron previamente validados como se puede observar en el anexo 03:
2. Guía de Observación Sistemática.

4.3.3. Procedimientos de Recolección de Datos.

Se describen los pasos a seguir:

1. Elección y preparación de la muestra

   Elección de los participantes: Formada por empleados de la municipalidad

   que trabajan en diferentes departamentos.

   Consentimiento informado: Desde la perspectiva de los trabajadores.

2. Implementación del Cuestionario de CIBERSEGURIDAD para la PROTECCIÓN DE DATOS SENSIBLES
3. Observación de manera sistemática
4. Entrevistas semiestructuradas
5. Examen de datos

Codificación de las respuestas: Se codificarán y procesarán para ser analizadas cuantitativamente con software estadístico.

4.4. Procesamiento y Análisis de la Información

4.4.1. Procesamiento de la Información

Se realizó utilizando el método tabular y fue ejecutada de manera computarizada, con la hoja de cálculo de Excel y el paquete estadístico SPSS V27.

4.4.2. Análisis de la Información

Procesamiento de Datos Recopilados:

Clasificación de Fuentes de Datos. distintas fuentes de datos fueron identificadas y clasificadas en 3 grupos: resultados de encuestas a empleados de la municipalidad, expedientes de incidentes de seguridad cibernética previos y documentación sobre políticas y protocolos de seguridad cibernética existentes en la municipalidad.

Métodos Estadísticos y Descriptivos Aplicación de Datos:

Análisis cuantitativo. Los obtenidos de las encuestas se aplicaron en estadísticas descriptivas, para evaluar cómo los trabajadores perciben problemas importantes relacionados con la protección de datos sensibles y la ciberseguridad.

Análisis inferencial, se empleó la prueba de Wilcoxon para rangos con signo, una prueba estadística no paramétrica. Z estandarizada para contrastar muestras apareadas o relacionadas.

Elaboración de Conclusiones y Recomendaciones, para formular sugerencias fundamentadas en evidencia sobre políticas de seguridad cibernética, capacitación laboral y respuesta ante incidentes de ciberseguridad

CAPÍTULO IV: Resultados

4.1. Analisis descriptivo

4.1.1. Confidencialidad de los datos antes y después de la aplicación de la evaluación del impacto de la ciberseguridad

Tabla 1

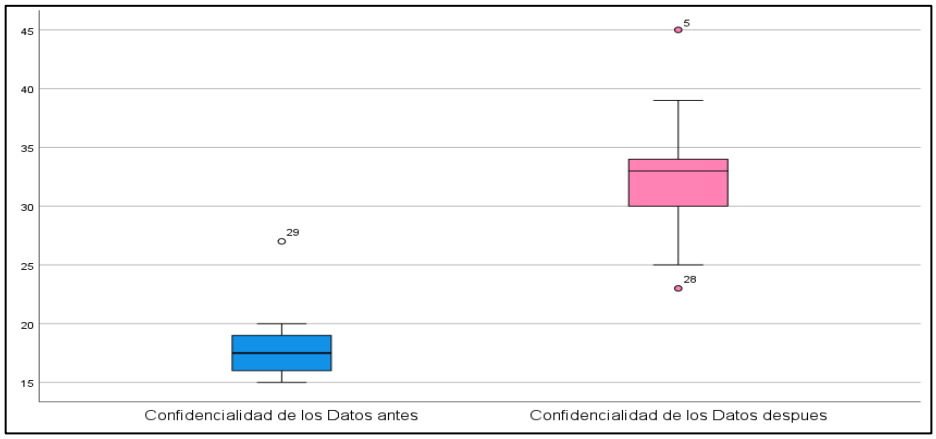
Confidencialidad de los datos

Protección de datos sensibles	Confidencialidad de los datos			
	Antes		Después	
	N°	%	N°	%
Insuficiente	29	96,7	2	6,7
Adecuado	1	3,3	26	86,7
Óptimo	-	-	2	6,7
Total	30	100,0	30	100,0

Fuente: ***Datos del autor***

Gráfico 1

Confidencialidad de los datos



Fuente: Tabla 1

Muestra los niveles de confidencialidad de los datos antes y después de la evaluación de ciberseguridad. Se observa un incremento en la confidencialidad después de la intervención, representado en el gráfico donde la caja rosa (después) está más elevada que la azul (antes), indicando una mejora en la protección de los datos sensibles.

Tabla 2

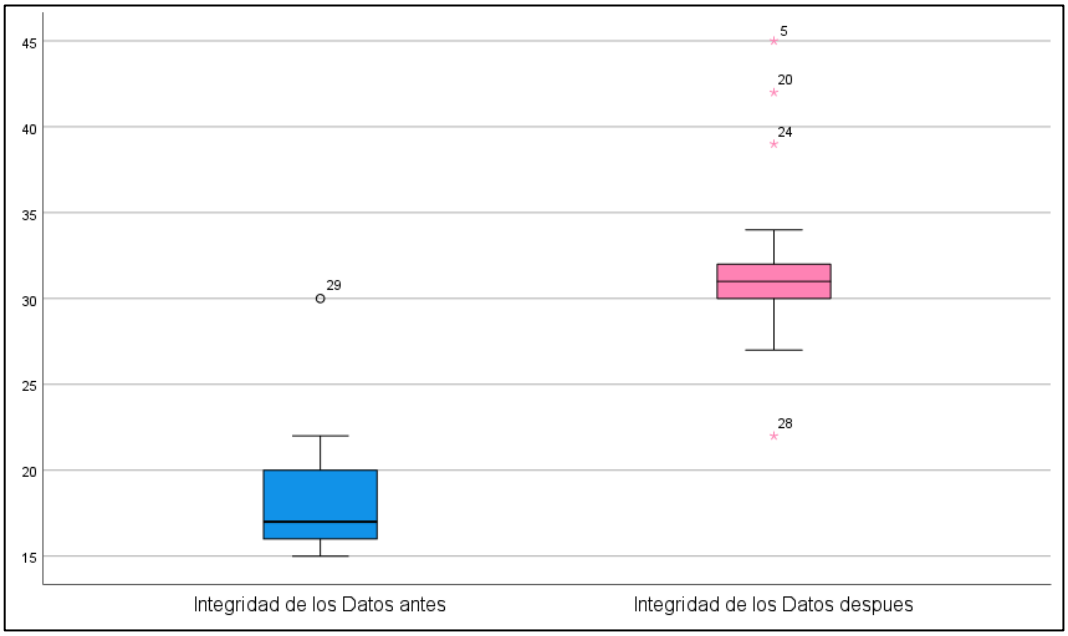
Integridad de los Datos

Protección de datos sensibles	Integridad de los Datos			
	Antes		Después	
	N°	%	N°	%
Insuficiente	29	96,7	1	3,3
Adecuado	1	3,3	26	86,7
Óptimo	-	-	3	10,0
Total	30	100,0	30	100,0

Fuente: ***Datos del autor***

Gráfico 2

Integridad de los Datos



Fuente: Tabla 2

Muestra la integridad de los datos mejora después de la intervención. En el gráfico, la caja rosa muestra una mayor consistencia y valor de integridad en comparación con el estado inicial (caja azul), lo cual sugiere una reducción en el riesgo de alteración de datos.

Tabla 3

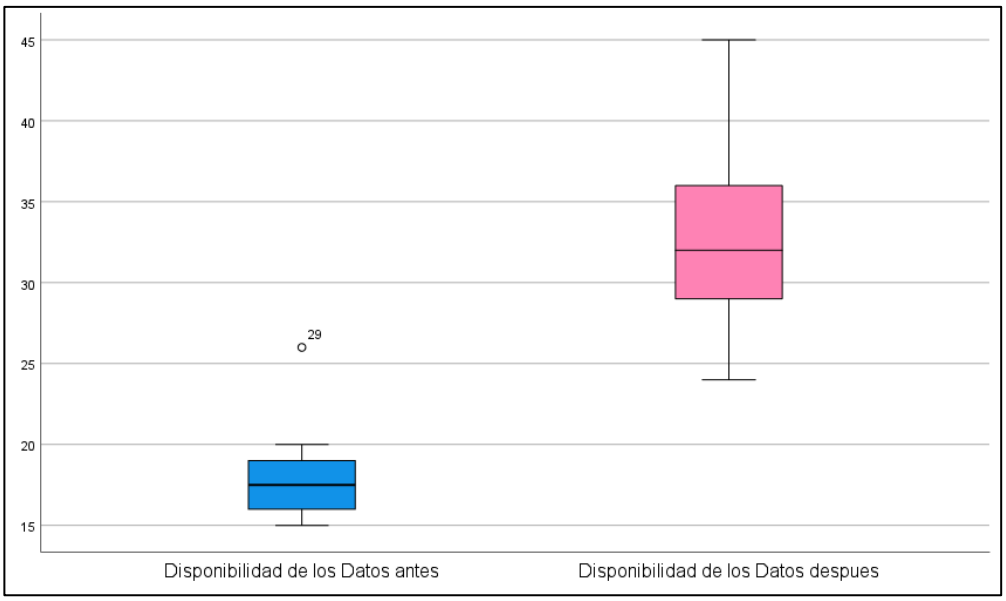
Disponibilidad de los Datos

Protección de datos sensibles	Disponibilidad de los Datos			
	Antes		Después	
	N°	%	N°	%
Insuficiente	29	96,7	2	6,7
Adecuado	1	3,3	26	86,7
Óptimo	-	-	2	6,7
Total	30	100,0	30	100,0

Fuente: ***Datos del Autor***

Gráfico 3

Disponibilidad de los Datos



Fuente: Tabla 3

Muestra la disponibilidad, los datos también muestran una mejora en la post intervención, como indica la caja rosa más alta y amplia en comparación con la azul. Esto sugiere que, tras la evaluación de ciberseguridad, los datos están más accesibles y disponibles.

Tabla 4

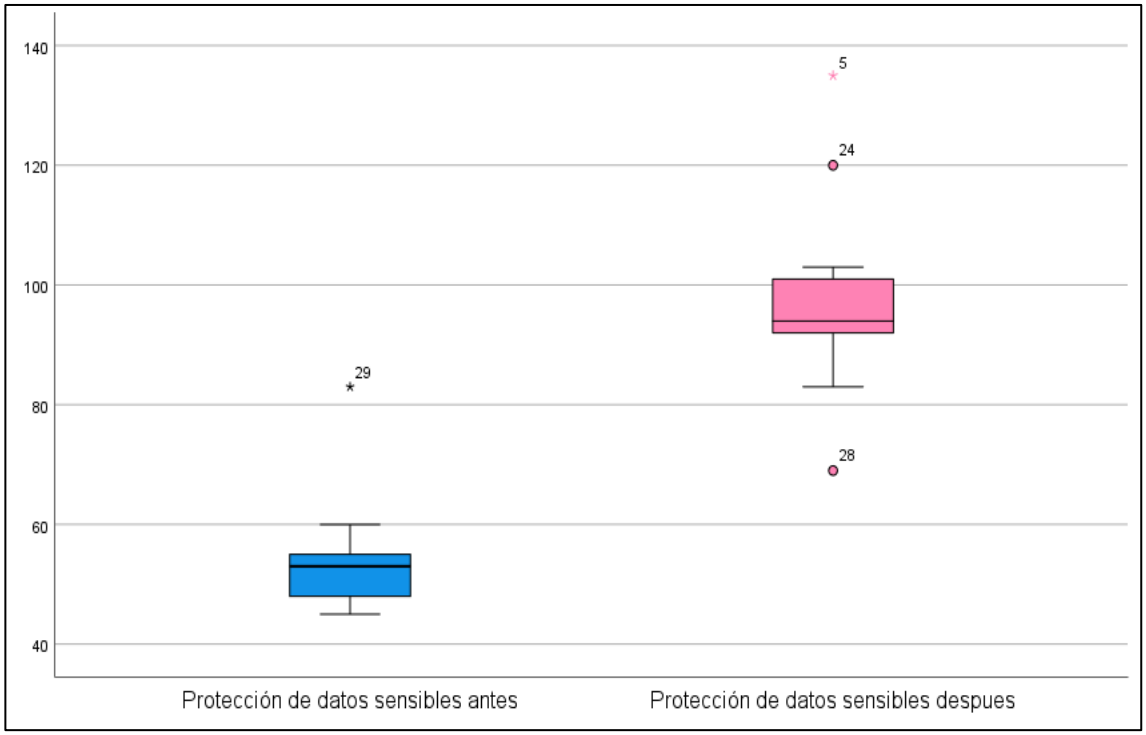
Protección de datos Sensibles

EVALUACIÓN DEL IMPACTO DE LA CIBERSEGURIDAD	Protección de datos Sensibles			
	Antes		Después	
	N°	%	N°	%
Insuficiente	29	96,7	1	3,3
Adecuado	1	3,3	27	90,0
Óptimo	-	-	2	6,7
Total	30	100,0	30	100,0

Fuente: tabla 1, 2 y 3

Gráfico 4

Protección de datos Sensibles



Fuente: Tabla 4

Se aprecia cómo la ciberseguridad impacta en la salvaguarda de los datos delicados. Los datos también revelan un progreso en la disponibilidad, como lo indica el tamaño y la altura de la caja rosa, que son más altos y amplios que los de la azul. Esto indica que los datos se vuelven más accesibles y disponibles después de la evaluación de ciberseguridad.

4.2. Analisis Inferencial

Con el propósito de confirmar las hipótesis propuestas, se empleó el valor de "p" asociado a Shapiro-Wilk, dado que la muestra era menor a 50. Este valor analiza la representatividad del nivel de significancia considerando el tamaño de la muestra analizada. La prueba de Shapiro-Wilk es especialmente adecuada para muestras de tamaño pequeño a moderado (que abarca n=30) y tiene una capacidad relativamente elevada para identificar desviaciones de la normalidad en estos conjuntos, en relación con otros métodos de normalidad. Por lo tanto, tiene sentido utilizarla para comprobar si los datos de las variables de interés (como las encuestas, el cumplimiento de políticas o los índices de seguridad de la información) se distribuyen aproximadamente con normalidad antes de implementar técnicas paramétricas. Si el valor de p es menor o igual a 0.05, se establece que la distribución no sigue una normalidad; si es mayor, no se rechaza la hipótesis nula de normalidad.

Tabla 5

Prueba de Normalidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Protección de datos sensibles antes	,732	30	,000
Protección de datos sensibles después	,850	30	,001

a. Corrección de significación de Lilliefors

Es evidente que los valores de significación bilateral para la protección de datos sensibles, antes y después de evaluar el impacto de la ciberseguridad, fueron menores a 0.05, lo cual significa que estas distribuciones no se adecuan a una distribución normal. Por lo tanto, para la prueba de hipótesis en muestras apareadas o relacionadas, se utilizó una distribución de rangos con signo de Wilcoxon.

Prueba de Hipótesis

Cuando las muestras estén conectadas o apareadas, se empleará la prueba de rangos con signo de Wilcoxon, que es no paramétrica, para analizar la hipótesis del estudio. Esta prueba es útil porque los valores observados no se ajustan a la normalidad. A continuación, se ejecutarán los siguientes pasos para probar la hipótesis.

Hipótesis

El Impacto de la Ciberseguridad mejora la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025.

Hipótesis Estadística

H_o: El Impacto de la Ciberseguridad no mejora la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025

H_1: El Impacto de la Ciberseguridad mejora la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025

Nivel de significancia

α = Alfa = 0.05 = 5%

Estadístico de Prueba

El estadístico de prueba es Z estandarizada para contrastar muestras relacionadas o apareadas en nuestro caso la observación de la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025. La expresión estadística se detalla a continuación:

$$Z = \frac{T - \mu_T}{\sigma_T}$$

Donde:

μ_T = Promedio de las diferencias de los rangos negativos.

σ_T= Desviación típica de las diferencias de los rangos negativos.

T= Menor de los valores absolutos de la suma de los rangos positivos y negativos

Tabla 6

Estadísticos de prueba

	Protección de datos sensibles	Confidencialidad de los Datos	Integridad de los Datos	Disponibilidad de los Datos
Z	-4,784[b]	-4,791[b]	-4,794[b]	-4,787[b]
Sig. asin. (bilateral)	,000	,000	,000	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos negativos.

Valor de Estadístico Z

$$Z_{\,Calculado} = -4.787$$

Estimación del p-valor (mediante el programa SPSS versión 27)

p-valor = 0,001 = 0,0%

Se rechaza la hipótesis nula si: ***p –valor < 0,05*** (p = significación asintótica bilateral).

Toma de decisión

A un nivel de error del 0,000% La protección de datos sensibles mejora en todas sus dimensiones: Confidencialidad de los Datos, Integridad de los Datos y Disponibilidad de los Datos Aceptando las hipótesis derivadas:

- El impacto de la Ciberseguridad mejora de la Confidencialidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025
- El impacto de la Ciberseguridad mejora de la Integridad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025.
- El impacto de la Ciberseguridad mejora de la Disponibilidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025.

Conclusión

Se demuestra a un nivel de confianza del 95% la hipótesis de la investigación: El Impacto de la Ciberseguridad mejora la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.

Es una muestra censal de 30 empleados y se utilizó la prueba de rangos con signo de Wilcoxon para analizar las discrepancias en tres dimensiones de protección de datos: confidencialidad, integridad y disponibilidad. El informe muestra un valor p bilateral de 0.001 y la dirección de la diferencia (rangos negativos), lo cual indica que después de la intervención de ciberseguridad hubo progresos en las tres dimensiones. Para situar la significancia estadística en relación con la magnitud práctica de las alteraciones, es esencial informar sobre tamaños del efecto y medidas de dispersión.

Se incorporó:

Parámetros de dispersión para cada una de las variables analizadas

Para cada dimensión, la mediana y el rango intercuartílico (Q1–Q3) de las discrepancias entre condiciones (por ejemplo, antes de la intervención y después de ella).

Debido a que la mediana y el rango intercuartílico describen con mayor precisión la dispersión central de muestras pequeñas y datos que no son siempre normales (como es habitual en los resultados de cumplimiento o percepción), se puede concluir lo siguiente.

Respecto al:

Tamaño del efecto no paramétrico vinculado al Wilcoxon:

r = Z / raíz cuadrada de N, donde Z es la estadística normalizada reportada (cercana a -4.78 a -4.79 en tu caso) y N es el número de pares que se evaluaron (N = 30). Interpretación general: si r es menor a 0.1, se considera pequeño; si está alrededor de 0.3, es medio; y si es mayor o igual a 0.5, es grande.

Intervalos de confianza (IC) para la mediana de las diferencias (por ejemplo, IC del 95% para la mediana de las diferencias entre antes y después) utilizando técnicas no paramétricas (percentiles Bootstrap si se tiene acceso a software), o

rangos de confianza fundamentados en la distribución de rangos cuando sea pertinente.

CAPÍTULO V: Discusión. Conclusiones. Recomendaciones

5.1. Discusión

En el Análisis descriptivo, en la categoría Insuficiente, se observó un Antes de N = 29 (96,7%) y un Después de N = 1 (3,3%), en la categoría Adecuado, se observó un Antes de N = 1 (3,3%) y un Después de N = 27 (90,0%), en la categoría Óptimo, se observó un Antes de N = 0 (0,0%) y un Después de N = 2 (6,7%). El cambio neto por categoría (valor absoluto) fue: Insuficiente: -28; Adecuado: +26; Óptimo: +2. El cambio relativo (% de cambio respecto al valor anterior) fue: Insuficiente: descenso de 96,7 puntos porcentuales (de 96,7% a 3,3%); Adecuado: aumento de 86,7 puntos porcentuales (de 3,3% a 90,0%); Óptimo: incremento de 6,7 puntos porcentuales (de 0,0% a 6,7%). Las medidas de dispersión mostraron que el rango en cada momento fue igual a 0, ya que las categorías fueron ordinales con tres niveles fijos; no hubo variabilidad dentro de cada celda de conteo. Estos resultados asemejan a lo arribado por Heredia y otros, quienes el 2025 utilizando pruebas t de muestras pareadas encontraron diferencia estadísticamente significativa antes y después de la capacitación, lo que demuestra la efectividad del programa. Puntuación media preprueba: 45%. Puntuación media post prueba: 80%. En esa misma línea León Estofanero el 2024 registraron avances notables en varios indicadores, como: disminución del 82.61% en el tiempo de elaboración de informes, disminución del 97.53% en el tiempo de divulgación de la información. Además, se consiguió un incremento del 88.12% en el desempeño del proceso de recopilación de datos, se consiguió un aumento del 33% en el grado de satisfacción del usuario y, finalmente, se incrementó un 32.62% en la calidad del formato resultante para la visualización de los informes. Así como Montalván Gutiérrez & Wong Pérez el 2022 encontraron que antes de que el nuevo sistema fuera implementado, el tiempo que tardaban era del 75% alto.

Después de la implementación, este porcentaje se redujo al 12.5%. El 62.5% de los encuestados considera que el tiempo requerido para el tratamiento de una historia clínica es bajo, lo cual indica que la interfaz del nuevo sistema es fácil de usar y comprender. Por esta razón, Tapia Chica y otros autores del 2024 subrayan que, en los últimos años, estos procedimientos han ganado popularidad debido al aumento de la seguridad ante ataques cibernéticos y a la necesidad de salvaguardar las privacidades online.

En el análisis inferencial se aprobó que el supuesto de normalidad fuera rechazado para ambas variables mediante Shapiro-Wilk ($p < 0,05$). mediante prueba no paramétrica, con signo de Wilcoxon para muestras apareadas, para verificar la Ho y la Ha: Ho sostenía que el Impacto de la Ciberseguridad no mejoró la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025; Ha sostuvo que sí mejoró. Con $\alpha = 0,05$, Z estandarizada con valores negativos para las tres dimensiones (Confidencialidad, Integridad y Disponibilidad). El p-valor asociado fue $p = 0,001$ (bilateral). La decisión fue rechazar la Ho para todas las dimensiones; se concluyó, a un nivel de confianza del 95%, que la Ciberseguridad mejoró la Protección de Datos Sensibles en Confidencialidad, Integridad y Disponibilidad de la MDSJB 2025. Estos resultados asemejan a lo arribado por Ramírez & Otilia el 2025 crean métricas, sustentadas en las Normas ISO/IEC: 27001; 27002 y el Índice de Economía y Sociedad Digitales (DESI), para generar resultados en diagrama nube de puntos, y hacer análisis matemático (Ecuación no lineal de Bernoulli). Así mismo Calderón Peñafiel el 2025 evidenció una falta de conocimiento sobre regulaciones de protección de datos. Es importante enfatizar en la necesidad de mejorar la transparencia, la comunicación y la educación por parte de las empresas para garantizar un entorno seguro y confiable en el comercio electrónico. Según Morillas Fernández el 2025 resalta que la confidencialidad se centra en garantizar que solo las personas indicadas estén permitidas en la información y que los procedimientos sean

empleados para que la información no sea alterada. Los afectados y sus contribuciones se componen de la gestión de avances en la municipalidad, puesto que también rescatan la información a nivel personal, lo que eleva el problema.

5.2. Conclusiones

5.2.1. Conclusiones Específicas

Confidencialidad de los Datos. La evaluación demuestra que la ciberseguridad ha incrementado significativamente la privacidad de los datos sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB). Se detectó un incremento en los procedimientos de control para protección y una reducción en la divulgación de información. Así, la información personal y otros datos delicados son confidenciales y seguros, pues no se han divulgado, lo cual satisface las expectativas del logro principal.

Integridad de los Datos. Es probable que la implementación permita operar los datos en un contexto de precisión y no desviación, de modo que sean consistentes y confiables. Sin embargo, suele ser crítico para una administración decente.

Disponibilidad de los Datos. Los datos de ciberseguridad corroboran la afirmación de que la disponibilidad de datos también se ha multiplicado más allá de los valores de las medidas y el análisis, lo que garantiza que, cuando sea necesario, no hay interrupciones y, del mismo modo, la información llegue a personas autorizadas. En este sentido, ya que se supone que los datos y la posibilidad de su explotación se utilizarán para maximizar el rendimiento y el conocimiento institucional, los datos están disponibles a los usuarios.

5.2.2. Conclusión General

La ciberseguridad en la Municipalidad Distrital de San Juan Bautista tuvo un impacto muy positivo en la seguridad de datos sensibles.

5.3. Recomendaciones

5.3.1. Recomendaciones Específicas

Confidencialidad de los datos: Para salvaguardar la información frente a accesos no autorizados, se establecerán controles de acceso más rigurosos, que incluirán políticas de control de permisos de usuario y autenticación multifactor. Para detectar y tratar cualquier vulnerabilidad que pueda amenazar la confidencialidad de los datos delicados, se llevarán a cabo auditorías con frecuencia.

Para mejorar la integridad de los datos: mediante un sistema de respaldo y registros de auditoría, se contrastarán y confirmarán incesantemente los datos. Así, se podrá detectar y rectificar cualquier cambio o alteración no autorizada de datos para preservar la integridad y la coherencia de la información. El personal será capacitado en la gestión y protección de datos importantes.

Disponibilidad de los datos: en todos los procedimientos se establecerá un sistema de respaldo automático y una infraestructura para la recuperación de desastres. Igualmente, se diseñarán planes de contingencia para posibilitar el acceso a la información en situaciones de emergencia. Se asegurará que los servidores y el sistema de almacenamiento tengan la aptitud y la compatibilidad necesarias para administrar actualizaciones de manera eficaz y veloz.

5.3.2. Recomendaciones General

Capacitación en Información y Seguridad de la Conciencia: se ofrecerán programas regulares de capacitación e información en seguridad a todos los empleados y funcionarios del municipio.

Referencias Bibliográficas

ALBARRACÍN-VILLAMIZAR, Carmen Zulay, 2020. Objetos de aprendizaje y desarrollo de habilidades del pensamiento numérico: Análisis mediante un diseño cuasiexperimental. 2020. Vol. 3, n° 8.

ÁLVAREZ, M. M. et LÓPE, R. A., 2023. *Metodología de la investigación educativa: Enfoques y diseños.* Editorial Universitaria.

ÁLVAREZ-CARRIÓN, Jenniffer Adriana et HERNÁNDEZ--SOTOMAYOR, Gabriel Paul, 2024. Protección de Datos Personales en Plataformas Educativas Digitales en el Sistema de Educación Superior de Ecuador. *MQRInvestigar*. 16 septembre 2024. Vol. 8, n° 3, pp. 5324-5339. DOI 10.56048/MQR20225.8.3.2024.5324-5339.

ARENAS RAMIRO, Monica, 2021. NUEVAS TECNOLOGÍAS Y RETOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN EUROPA: El rastreo de contactos durante la pandemia por covid-19. *Confluências | Revista Interdisciplinar de Sociologia e Direito*. 4 août 2021. Vol. 23, n° 2, pp. 99-17. DOI 10.22409/conflu.v23i2.50519.

AZNAR SÁNCHEZ-PARODI, Irene, 2023. La protección de datos personales de la víctima de violencia de género en el campo del Registro de la Propiedad. *Anuario de Derecho Civil* [en ligne]. 17 octobre 2023. N° 2. [Consulté le 29 octobre 2024]. DOI 10.53054/adc.v76i2.10063. Disponible à l'adresse : https://revistas.mjusticia.gob.es/index.php/ADC/article/view/10063

BERNAL-CAMARGO, Diana Rocío et GÓMEZ-CÓRDOBA, Ana Isabel, 2022. derecho a la protección de datos personales en la investigación biomédica en Colombia: Una mirada desde el soft law y el hard law. *Revista Chilena de Derecho y Tecnología*. 30 juin 2022. Vol. 11, n° 1, pp. 359-394. DOI 10.5354/0719-2584.2022.66319.

BRION BERDOTE, Estela, 2022. La fragilidad del derecho fundamental a la protección de datos personales del menor ante la exposición de su vida personal y familiar en la red: De la necesidad de nuevos mecanismos y garantías legales. *Estudios de Deusto*. 26 décembre 2022. Vol. 70, n° 2, pp. 49-76. DOI 10.18543/ed.2646.

CAMA JARA, Sigfredo Adolfo et ARELLANO BULEJE, Giampier Marco, 2024. Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para la mejora de protección de datos personales en la Clínica María del Socorro. *Repositorio Institucional - UTP* [en ligne]. 2024. [Consulté le 29 octobre 2024]. Disponible à l'adresse : http://repositorio.utp.edu.pe/handle/20.500.12867/9636

DE LA CRUZ SANTA CRUZ, Claudia, 2024. ISO 27001 para mejorar el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024. [en ligne]. 24 mai 2024. [Consulté le 29 octobre 2024]. Disponible à l'adresse : https://repositorio.uwiener.edu.pe/handle/20.500.13053/11487

DULCE VILLARREAL, Edgar Roberto, BETANCOURT ROMO, James Hernán, SOLARTE SOLARTE, Francisco Nicolás Javier et ROSERO GALÍNDEZ,

Carlos Mauricio, 2023. BLOCKCHAIN: Una mirada desde la protección de datos sensibles en el sector salud. *REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA)*. 19 juillet 2023. Vol. 2, n° 38, pp. 69-78. DOI 10.24054/rcta.v2i38.1279.

FERNÁNDEZ RAMÍREZ, Marina, 2023. código ético como mecanismo de autorregulación empresarial en la protección de datos de sus empleados: singularidades sobre su eficacia | Semantic Scholar. [en ligne]. 2023. [Consulté le 29 octobre 2024]. DOI DOI:10.46661/lexsocial.8758. Disponible à l'adresse : https://www.semanticscholar.org/paper/c%C3%B3digo-%C3%A9tico-como-mecanismo-de-autorregulaci%C3%B3n-en-Ram%C3%ADrez/3b7185337321d7032f01fdc213ccfc15884f66cb

FONSECA, Juan Miguel Castillo et JUÁREZ, B., 2019. Ciberseguridad y vigilancia tecnológica: Un reto para la protección de datos personales en los archivos. *Tlatemoani: Revista Académica de Investigación* [en ligne]. 4 septembre 2019. [Consulté le 29 octobre 2024]. Disponible à l'adresse : https://www.semanticscholar.org/paper/Ciberseguridad-y-vigilancia-tecnol%C3%B3gica%3A-Un-reto-la-Fonseca-Ju%C3%A1rez/7b7a98303236b45bf1496e5715845d050c6e004c

GARCÍA FERNÁNDEZ, María Lydia, 2022. Los derechos digitales en la Ley Orgánica 3/2018, de Protección de Datos Personales y de garantía de los derechos digitales. *Asamblea. Revista parlamentaria de la Asamblea de Madrid*. 30 juin 2022. N° 42, pp. 69-97. DOI 10.59991/rvam/2022/n.42/19.

GONZÁLES, César Francisco Zepeda et MARTÍNEZ, Hermes Joel Vallecillo, 2025. Propuesta de plan de ciberseguridad para la gestión de riesgos en el ERP web empresarial de Tivitrace basado en ISO/IEC 27032 e ITIL V4. [en ligne]. 5 août 2025. [Consulté le 23 octobre 2025]. Disponible à l'adresse : https://repositorio.unitec.edu//handle/123456789/13660

GONZALEZ CÁRDENAS, Luis Fernando, 2024. Violación al Derecho Humano de la Protección de Datos Personales por la Vulnerabilidad de la Ciberseguridad en las Instituciones Públicas del Estado Mexicano. *Ciencia Latina Revista Científica Multidisciplinar*. 3 juin 2024. Vol. 8, n° 3, pp. 892-907. DOI 10.37811/cl_rcm.v8i3.11294.

HERNÁNDEZ SAMPIERI, R., FERNÁNDEZ COLLADO, V et BAPTISTA LUCIO, P., 2014. *Metodología de la investigación*. Sexta. México D. F. : McGraw-Hill.

LEÓN ESTOFANERO, Omar Mauricio, 2024. Implementación de una Plataforma Web basada en la integración de herramientas OSINT para optimizar el Proceso de Gestión de Incidencias en Ciberseguridad en una entidad de Administración Pública. *Repositorio Institucional - UTP* [en ligne]. 2024. [Consulté le 29 octobre 2024]. Disponible à l'adresse : http://repositorio.utp.edu.pe/handle/20.500.12867/8992

MEDINA GUERRERO, Manuel, 2023. El conflicto entre la transparencia y la protección de datos tras la entrada en vigor del Reglamento General de Protección de Datos. *Revista Española de la Transparencia*. 24 juillet 2023. N° 17 Extra, pp. 51-73. DOI 10.51915/ret.306.

MIRANDA ZEBALLOS, Elvis Jhonatan, 2024. Evaluación de tres tipos de dispositivos informáticos en la auditoría web de los Ministerios del Perú, año 2022. *Universidad José Carlos Mariátegui* [en ligne]. 2024. [Consulté le 29 octobre 2024]. Disponible à l'adresse : https://repositorio.ujcm.edu.pe/handle/20.500.12819/2611

MORILLAS FERNÁNDEZ, Marta, 2023. LA PROTECCIÓN DE DATOS COMO GARANTÍA EN LA PREVENCIÓN DE LOS RIESGOS DE LA SOCIEDAD DIGITAL. *Revista Internacional de Doctrina y Jurisprudencia*. 7 juillet 2023. N° 29, pp. 67-92. DOI 10.25115/ridj.vi29.9324.

RAMÍREZ, Giraldo et OTILIA, Luz, 2025. Sustentar los factores que influyen en la ciber-ética de la filosofía 4.0, para el proceso de enseñanza-aprendizaje mediante técnicas de hacking ético UNAD (Universidad Nacional Abierta y a Distancia). [en ligne]. 7 juillet 2025. [Consulté le 23 octobre 2025]. Disponible à l'adresse : http://repository.unad.edu.co/handle/10596/70586

SÁNCHEZ DÍAZ, Maria Fernanda, 2023. El derecho a la protección de datos personales en la era digital | Semantic Scholar. [en ligne]. 2023. [Consulté le 29 octobre 2024]. Disponible à l'adresse : https://www.semanticscholar.org/paper/El-derecho-a-la-protecci%C3%B3n-de-datos-personales-en-D%C3%ADaz/3e84a7250615daac7ca32fac0c468d210b841098

TAPIA CHICA, Carlos Santiago, MORALES JADÁN, Diego Xavier et SÁNCHEZ SARMIENTO, Marcela Paz, 2024. Análisis de vulnerabilidades en medidores inteligentes y concentradores AMI: implicaciones de ciberseguridad y estrategias de protección. *Religación*. 14 octobre 2024. Vol. 10, n° 44, pp. e2501311. DOI 10.46652/rgn.v10i44.1311.

TOLENTINO VALER, Diego Fernando et ZORRILLA ALVA, Margareth Geraldine, 2024. Sistema de ciberseguridad en la prevención de riesgo operacional en la cooperativa de ahorro y crédito San Cristóbal de Huamanga. [en ligne]. 28 août 2024. [Consulté le 29 octobre 2024]. Disponible à l'adresse : http://repositorio.uncp.edu.pe/handle/20.500.12894/11413

VÁSQUEZ DEL ÁGUILA, Samuel Eduardo, 2019. Plan de fortalecimiento en el uso de las TIC en estudiantes de comunicación e inicial del Instituto de Educación Superior Pedagógico Público "Loreto" Iquitos. *Repositorio Institucional - UCV* [en ligne]. 2019. [Consulté le 23 octobre 2025]. Disponible à l'adresse : https://repositorio.ucv.edu.pe/handle/20.500.12692/44130

Anexos

Anexo 01: Matriz de Consistencia

Anexo 02: Instrumento de Recolección de Datos

Anexo 03: Validez y Confiabilidad

Anexo 04: Consentimiento informado

Anexo 05: Prueba Piloto de Impacto de la Ciberseguridad en la Protección de Datos Sensibles

Anexo 06: Base de Datos de Ciberseguridad en la Protección de Datos Sensibles

ANEXO N°01: Matriz de Consistencia

TÍTULO: ANALISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTIRLA DE SAN JUAN BAUTISTA 2025

Autor (as): ANGELLO GIORDANO RODRIGUEZ SOLSOL

<table>
<tr><th>Problema</th><th>Objetivo</th><th>Hipótesis</th><th>Variable</th><th>Indicadores</th><th>Metodología</th></tr>
<tr>
<td>Problema General
¿En qué medida el Analisis del Impacto de la Ciberseguridad mejora la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025?
Problemas Específicos
¿Cuál es el impacto de la Ciberseguridad en la mejora de la Confidencialidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025?
¿Cuál es el impacto de la Ciberseguridad en la mejora de la Integridad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista 2025?
¿Cuál es el impacto de la Ciberseguridad en la mejora de la Disponibilidad de los Datos para la Protección de Datos Sensibles de la MDSJB 2025?</td>
<td>Objetivo General
Medir el Impacto de la Ciberseguridad mejora la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.
Problemas Específicos
Analizar el impacto de la Ciberseguridad en la mejora de la Confidencialidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.
Analizar el impacto de la Ciberseguridad en la mejora de la Integridad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.
Analizar el impacto de la Ciberseguridad en la mejora de la Disponibilidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.</td>
<td>Hipótesis General
El Impacto de la Ciberseguridad mejora la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB)2025.
Hipótesis Derivadas
El impacto de la Ciberseguridad mejora de la Confidencialidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.
El impacto de la Ciberseguridad mejora de la Integridad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.
El impacto de la Ciberseguridad mejora de la Disponibilidad de los Datos para la Protección de Datos Sensibles de la Municipalidad Distrital de San Juan Bautista (MDSJB) 2025.</td>
<td>IMPACTO DE LA CIBERSEGURIDAD</td>
<td>
<table>
<tr><td>A</td><td>Eficiencia de las Políticas de Ciberseguridad</td></tr>
<tr><td>1</td><td>Implementación de protocolos de seguridad</td></tr>
<tr><td>2</td><td>Cumplimiento con regulaciones de ciberseguridad</td></tr>
<tr><td>3</td><td>Eficacia en la gestión de riesgos</td></tr>
<tr><td>B</td><td>Capacitación y Concienciación en Ciberseguridad</td></tr>
<tr><td>1</td><td>Capacitación continua del personal</td></tr>
<tr><td>2</td><td>Conciencia sobre la protección de datos</td></tr>
<tr><td>3</td><td>Evaluación de la efectividad de las capacitaciones</td></tr>
<tr><td>C</td><td>Respuesta ante Incidentes de Seguridad</td></tr>
<tr><td>1</td><td>Tiempo de respuesta ante incidentes</td></tr>
<tr><td>2</td><td>Contención y mitigación de amenazas</td></tr>
<tr><td>3</td><td>Recuperación y continuidad operativa</td></tr>
</table>
</td>
<td rowspan="2">Nivel de Investigación
Aplicada
Tipo de Investigación
Pre-Experimental, Con tratamiento y control para comparar los resultados mediante (pre-test y el post-test).
Diseño de Investigación
El esquema del diseño es el siguiente:
GE: 01 X 02
Dónde:
GE: Grupo experimental
X: Experimento
01 observaciones al grupo experimental antes del experimento (Pre-Test)
02 observaciones al grupo experimental después del experimento (Post Test).
Población
30 trabajadores municipales que laboran en ciertas oficinas de la municipalidad.
Muestra
Conformada por un muestreo no aleatoria y por conveniencia. Sera censal, lo que significa que se trabajara con el 100% de la población, es decir los 30.</td>
</tr>
<tr>
<td>PROTECCIÓN DE DATOS SENSIBLES</td>
<td>
<table>
<tr><td>A</td><td>Confidencialidad de los Datos</td></tr>
<tr><td>1</td><td>Control de acceso a datos sensibles</td></tr>
<tr><td>2</td><td>Políticas de privacidad y manejo de datos</td></tr>
<tr><td>3</td><td>Uso de cifrado en datos sensibles</td></tr>
<tr><td>B</td><td>Integridad de los Datos</td></tr>
<tr><td>1</td><td>Validación y control de cambios en los datos</td></tr>
<tr><td>2</td><td>Protección contra perdida de datos</td></tr>
<tr><td>3</td><td>Monitoreo de la integridad de los datos</td></tr>
<tr><td>C</td><td>Disponibilidad de los Datos</td></tr>
<tr><td>1</td><td>Acceso seguro y continuo a datos sensibles</td></tr>
<tr><td>2</td><td>Resiliencia ante ciberataques</td></tr>
<tr><td>3</td><td>Recuperación rápida de datos tras incidentes</td></tr>
</table>
</td>
</tr>
</table>

ANEXO 02

ANALISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTIRLA DE SAN JUAN BAUTISTA 2025

CUESTIONARIO: EDUCACIÓN EMOCIONAL

(DIRIGIDO A TRABAJADORES DE LA Municipalidad Distrital de San Juan Bautista (MDSJB) 2025)

I. PRESENTACIÓN

El presente cuestionario tiene como finalidad recolectar información sobre: **ANALISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTIRLA DE SAN JUAN BAUTISTA 2025.** Este instrumento es uno de los elementos de la tesis para la obtención del **TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS DE INFORMACIÓN**

II. DATOS PERSONALES

Lugar :……
Día :……
Hora :……

III. INSTRUCCIONES

Antes de proceder al llenado del cuestionario debe leer las siguientes instrucciones:

- Leer cada una de las preguntas y responder de acuerdo a lo que considere pertinente.
- Debe responder a todas las preguntas del cuestionario.
- Podrá solicitar aclaración cuando encuentre alguna dificultad en las preguntas.
- La duración aproximada para el llenado del cuestionario será de 45 min.

IV. CONTENIDO: INSTRUCCIONES

- Lee detenidamente las cuestiones y respóndalas
- La información que nos proporciona será confidencial.
- No deje preguntas sin responder.

	ANALISIS DEL IMPACTO DE LA CIBERSEGURIDAD	(1) Insuficiente (00-10 puntos): Deficiencias significativas o implementación inexistente.	(2) Adecuado (11-15 puntos): Cumplimiento moderado con áreas de mejora identificadas.	(3) Óptimo (16-20 puntos): Implementación excelente, con pocas o ninguna observación relevante
A	**Eficiencia de las Políticas de Ciberseguridad**			
	Implementación de protocolos de seguridad			
A1	Implementación protocolos de seguridad			
A2	Procedimientos documentados para la gestión			
A3	Conocimiento de los protocolos de ciberseguridad			
A4	Revisión y actualización de protocolos			
A5	Políticas claras sobre el uso seguro de datos			
	Cumplimiento con regulaciones de ciberseguridad			
A6	Cumplimiento de la normativa nacional			
A7	Equipo dedicado al cumplir lo normativo en ciberseguridad			
A8	Estándares internacionales en ciberseguridad			
A9	Capacitación sobre leyes de protección de datos			
A10	Auditorías periódicas para asegurar el cumplimiento normativo			
	Eficacia en la gestión de riesgos			
A11	Identifican y evalúan regularmente los riesgos			
A12	Cuenta con un plan para mitigar riesgos			
A13	Herramientas de monitoreo para identificar amenazas			
A14	Analizan y gestionan los incidentes ocurridos			
A15	Personal capacitado para la evaluación y gestión de riesgos			
	T O T A L ($\bar{x}$)			
B	**Capacitación y Concienciación en Ciberseguridad**			
	Capacitación continua del personal			
B1	Formación continua en temas de ciberseguridad			
B2	Identifican amenazas como phishing o malware			
B3	Capacitaciones adaptas a las actualizaciones tecnológicas			
B4	Sesiones de capacitación obligatorias			
B5	Involucramiento del equipo directivo			
	Conciencia sobre la protección de datos			
B6	Comprenden la importancia de proteger datos			
B7	Campañas de concienciación			
B8	Aplican prácticas seguras			
B9	Identifican datos sensibles			
B10	Fomento de cultura de responsabilidad sobre datos			
	Evaluación de la efectividad de las capacitaciones			
B11	Evalúa el conocimiento adquirido			
B12	Aplican las prácticas de seguridad aprendidas			
B13	Pruebas de competencia en ciberseguridad			
B14	Evalúa si la capacitación reduce incidentes			
B15	Solicitan apoyo adicional			
	T O T A L ($\bar{x}$)			
C	**Respuesta ante Incidentes de Seguridad**			
	Tiempo de respuesta ante incidentes			
C1	Respuesta adecuada sobre seguridad			
C2	Procedimientos de respuesta rápida a incidentes			
C3	Actúan de manera oportuna			
C4	Los incidentes menores se manejan sin afectar la operación diaria			
C5	Evalúa el tiempo de respuesta			
	Contención y mitigación de amenazas			
C6	Herramientas para contención rápida			
C7	Equipo de expertos en mitigación de amenazas			
C8	Planes de contención frente a daños a datos sensibles			
C9	Actualizan las estrategias de contención			

C10	Personal preparado para ejecutar planes de mitigación de amenazas			
	Recuperación y continuidad operativa			
C11	Cuentan con plan de recuperación ante incidentes			
C12	Tras incidentes mantiene la calidad del servicio			
C13	Simulacros de recuperación para asegurar la continuidad			
C14	Datos sensibles restaurados			
C15	Personal responsable			
T O T A L ($\bar{x}$)				

¡Muchas gracias por su colaboración!

ANEXO 02

ANALISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTIRLA DE SAN JUAN BAUTISTA 2025

CUESTIONARIO: DESARROLLO DE HABILIDADES SOCIOEMOCIONALES

(DIRIGIDO TRABAJADORES DE LA MUNICIPALIDAD DISTRITAL DE IQUITOS 2025)

I. PRESENTACIÓN

El presente cuestionario tiene como finalidad recolectar información sobre: **ANALISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTIRLA DE SAN JUAN BAUTISTA 2025**. Este instrumento es uno de los elementos de la tesis para la obtención del **TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS DE INFORMACIÓN**

II. DATOS PERSONALES

Lugar :……
Día :……
Hora :……

III. INSTRUCCIONES

Antes de proceder al llenado del cuestionario debe leer las siguientes instrucciones:

- Leer cada una de las preguntas y responder de acuerdo a lo que considere pertinente.
- Debe responder a todas las preguntas del cuestionario.
- Podrá solicitar aclaración cuando encuentre alguna dificultad en las preguntas.
- La duración aproximada para el llenado del cuestionario será de 45 min.

IV. CONTENIDO: INSTRUCCIONES

- Lee detenidamente las cuestiones y respóndalas
- La información que nos proporciona será confidencial.
- No deje preguntas sin responder.

	PROTECCIÓN DE DATOS SENSIBLES	(1) **Insuficiente (00-10 puntos):** Deficiencias significativas o implementación inexistente.	(2) **Adecuado (11-15 puntos):** Cumplimiento moderado con áreas de mejora identificadas.	(3) **Óptimo (16-20 puntos):** Implementación excelente, con pocas o ninguna observación relevante
A	**Confidencialidad de los Datos**			
	Control de acceso a datos sensibles			
A1	Limitan el acceso a datos sensibles			
A2	Herramientas de autenticación multifactor para información confidencial			
A3	Niveles de acceso según su rol en la institución			
A4	Registros de acceso a datos sensibles			
A5	Reciben advertencias sobre intentos no autorizados de acceso			
	Políticas de privacidad y manejo de datos			
A6	Cuenta con políticas de privacidad			
A7	Capacitados en el manejo responsable de datos sensibles			
A8	Revisiones periódicas de las políticas de privacidad			
A9	Políticas de manejo de datos según normativas			
A10	Información a usuarios			
	Uso de cifrado en datos sensibles			
A11	Datos sensibles cifrados			
A12	Protocolos cifrados			
A13	Realizan pruebas de vulnerabilidad			
A14	Aplican a todos los tipos de datos confidenciales			
A15	Implementados procedimientos para actualización de claves			
	T O T A L ($\bar{x}$)			
B	**Integridad de los Datos**			
	Validación y control de cambios en los datos			
B1	Auditorías regulares			
B2	Procedimientos de validación para detectar modificaciones no autorizadas			
B3	Registros de cambios detallados y accesibles			
B4	Controles para evitar la alteración de datos			
B5	Reciben notificaciones sobre cambios			
	Protección contra pérdida de datos			
B6	Respaldos periódicos de los datos sensibles			
B7	Respaldos protegidos			
B8	Plan de recuperación ante desastres			
B9	Utiliza sistemas de detección de pérdidas de datos			
B10	Pruebas para recuperación de datos			
	Monitoreo de la integridad de los datos			
B11	Cuenta con herramientas de monitoreo en tiempo real			
B12	Auditorías para identificar incidentes			
B13	Emiten alertas cuando se detectan modificaciones			
B14	Revisión de registros de acceso			
B15	Sistema para rastrear y revertir cambios			
	T O T A L ($\bar{x}$)			
C	**Disponibilidad de los Datos**			
	Acceso seguro y continuo a datos sensibles			
C1	Sistemas de datos críticos para evitar interrupciones de acceso			
C2	Medidas para asegurar el acceso ininterrumpido			
C3	Acceso a datos sensibles			
C4	Equipo TI para la rápida resolución de problemas			
C5	Implementan pruebas periódicas			
	Resiliencia ante ciberataques			
C6	Planes de contingencia			
C7	Sistemas que detectan y mitigan ataques			
C8	Simulacros de ciberataques			
C9	Capacitado para mantener la disponibilidad			
C10	Evalúan periódicamente los sistemas de respaldo de datos			
	Recuperación rápida de datos tras incidentes			
C11	Plan de recuperación rápida			
C12	Pruebas de recuperación de datos			
C13	Permiten la restauración de datos			
C14	Entrenamiento en procedimientos de recuperación de datos			
C15	Equipo dedicado para la gestión de recuperación de datos			
	T O T A L ($\bar{x}$)			

ANEXO N°3: Validez y Confiabilidad

Estimados Profesionales:

Lic. Cecilia Rios Perez, Dra.

Lic. Silvia del Carmen Arévalo Panduro, Mgr.
Lic. Victor Manuel Zegarra Seminario, Mgr.
Lic. Joseni Tuesta Ruiz, Mgr.
Lic. Jhosiveth Jheninfer Zam,brano Curitima, Mgr.

Con motivo de la investigación que se está realizando sobre: **ANALISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTIRLA DE SAN JUAN BAUTISTA 2025**, es necesario someter a juicio de experto la propuesta de dimensiones, indicadores e índices de las Variables: V.I. (X): **IMPACTO DE LA CIBERSEGURIDAD.** V.D. (Y): **PROTECCIÓN DE DATOS SENSIBLES.**

PARTE 1: Validación del instrumento

Cada vez que necesitamos recopilar información para tomar decisiones, nos enfrentamos al tipo de instrumento que vamos a usar, en ese sentido, un instrumento según **Alvarado, canales y Pineda (1994)**, es el mecanismo que utiliza el investigador para recolectar y registrar información (pp.125).

Con la **validez** se determina la revisión de la presentación del contenido, el contraste de los indicadores con los ítems que miden las variables correspondientes.

Hernández, S. (2006) expresó la validez como el grado de precisión con el que el test utilizado mide realmente lo que está destinado medir. Lo expresado anteriormente define la validación de los instrumentos, como la determinación de la capacidad de los instrumentos para medir las cualidades para lo cual fueron construidos.

Validación por jueces o expertos

Es una de las técnicas utilizadas para calcular el índice de validez de constructo. Se basa en la correspondencia teórica entre los ítems del instrumento y los conceptos del evento. Busca corroborar el consenso entre el investigador y los expertos con respecto a la pertenencia de cada ítem a las respectivas sinergias del evento y, de esta manera, apoyar la definición de la cual se parte. (Hurtado, 2012, p. 792). A, los expertos se les entregó un formato pidiéndosele que evaluaran los instrumentos en su totalidad. Se les pidió que emitieran su opinión sobre diversos aspectos como: Coherencia. Calidad. Escala.

Relevancia.

N° Jueces = 5

Valor Máximo = 20

Tabla 1

		Jueces					Sxi	Vmx	CVC1	Pe	CVC2
		Dra. Cecilia Rios Perez, Dra.	Lic. Silvia del Carmen Arévalo Panduro, Mgr	Lic. Victor Manuel Zegarra Seminario, Mgr.	Lic. Joseni Tuesta Ruiz, Mgr.	Lic. Jhosiveth Jheninfer Zam,brano Curitima, Mgr.					
Item 1	Coherencia	17	18	18	18	17	88	4.4	0.88	0.00032	0.87968
Item 2	Calidad	16	17	17	18	18	86	4.3	0.86	0.00032	0.85968
Item 3	Escala	17	19	17	18	19	90	4.5	0.9	0.00032	0.89968
Item 4	Relevancia	17	18	18	18	17	88	4.4	0.88	0.00032	0.87968
											0.87968

Tabla 2

Interpretación

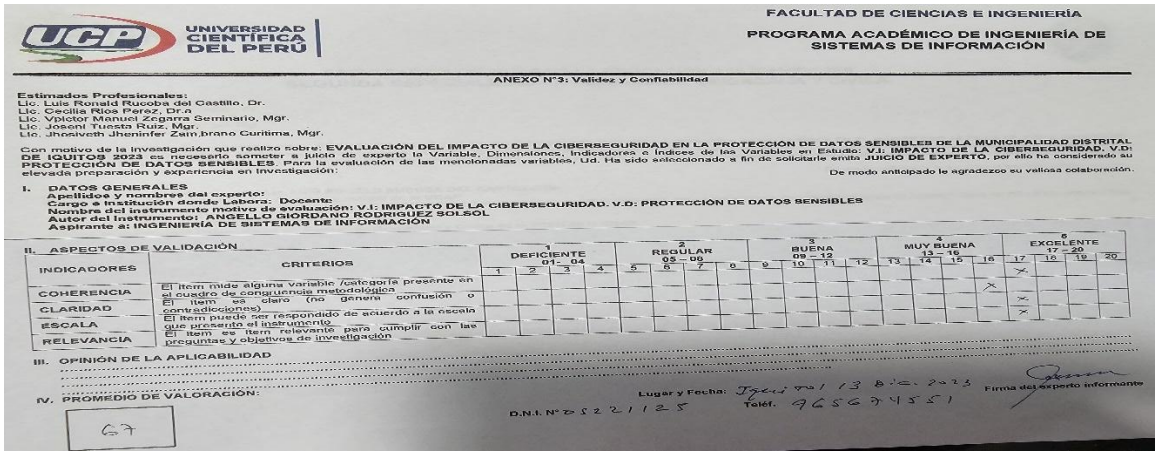
a) Menor que .60, *validez y concordancia inaceptables.*

b) Igual o mayor de .60 y menor o igual que .70, *validez y concordancia deficientes.*

c) Mayor que .71 y menor o igual que .80, *validez y concordancia aceptables.*

d) Mayor que .80 y menor o igual que .90, *validez y concordancia buenas.*

e) Mayor que .90, *validez y concordancia excelentes*



UNIVERSIDAD CIENTÍFICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

ANEXO N°3: Validez y Confiabilidad

Estimados Profesionales:
Lic. Luis Ronald Rucoba del Castillo, Dr.
Lic. Cecilia Rios Perez, Dr.a
Lic. Victor Manuel Zegarra Seminario, Mgr.
Lic. Joseni Tuesta Ruiz, Mgr.
Lic. Jhosiveth Jheninfer Zam,brano Curitima, Mgr.

Con motivo de la investigación que realizo sobre: **EVALUACIÓN DEL IMPACTO DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE DATOS SENSIBLES DE LA MUNICIPALIDAD DISTRITAL DE IQUITOS 2023** es necesario someter a juicio de experto la Variable, Dimensiones, Indicadores o Índices de las Variables en Estudio: **V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES**. Para la evaluación de las mencionadas variables, Ud. Ha sido seleccionado a fin de solicitarle emita **JUICIO DE EXPERTO**, por ello he considerado su elevada preparación y experiencia en investigación.

De modo anticipado le agradezco su valiosa colaboración.

I. **DATOS GENERALES**
Apellidos y nombres del experto:
Cargo e Institución donde Labora: Docente
Nombre del instrumento motivo de evaluación: V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES
Autor del Instrumento: ANGELLO GIORDANO RODRIGUEZ SOLSOL
Aspirante a: INGENIERÍA DE SISTEMAS DE INFORMACIÓN

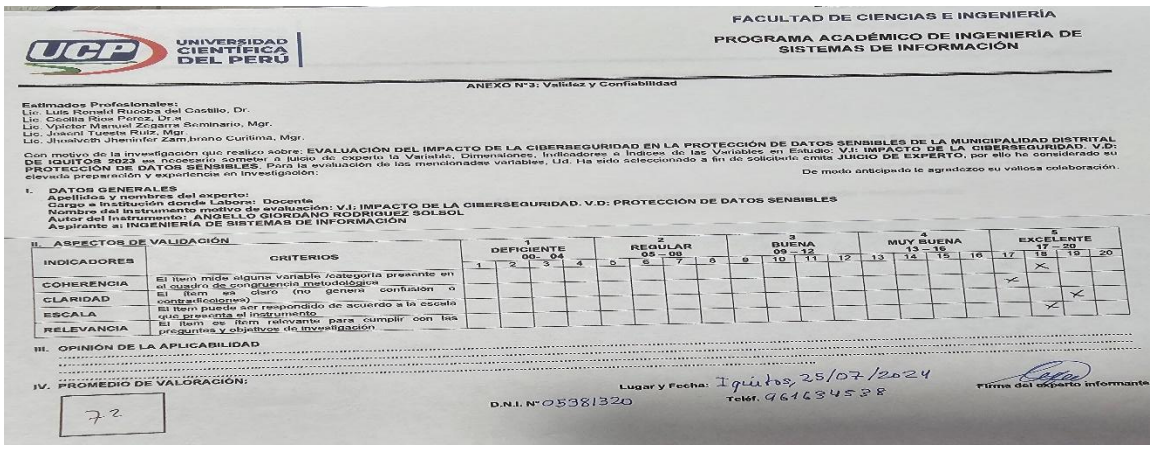
II. **ASPECTOS DE VALIDACIÓN**

INDICADORES	CRITERIOS	1 DEFICIENTE 01 - 04	2 REGULAR 05 - 08	3 BUENA 09 - 12	4 MUY BUENA 13 - 16	5 EXCELENTE 17 - 20
COHERENCIA	El ítem mide alguna Variable /categoría presente en el cuadro de congruencia metodológica					X
CLARIDAD	El ítem es claro (no genera confusión o contradicciones)				X	
ESCALA	El ítem puede ser respondido de acuerdo a la escala que presenta el instrumento					X
RELEVANCIA	El ítem es ítem relevante para cumplir con las preguntas y objetivos de investigación					X

III. **OPINIÓN DE LA APLICABILIDAD**

IV. **PROMEDIO DE VALORACIÓN:** 67

Lugar y Fecha: Iquitos 01/13 Dic. 2023
D.N.I. N° 52211125 Telef. 965674551
Firma del experto informante



UNIVERSIDAD CIENTÍFICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

ANEXO N°3: Validez y Confiabilidad

Estimados Profesionales:
Lic. Luis Ronald Rucoba del Castillo, Dr.
Lic. Cecilia Rios Perez, Dr.a
Lic. Victor Manuel Zegarra Seminario, Mgr.
Lic. Joseni Tuesta Ruiz, Mgr.
Lic. Jhosiveth Jheninfer Zam,brano Curitima, Mgr.

Con motivo de la investigación que realizo sobre: **EVALUACIÓN DEL IMPACTO DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE DATOS SENSIBLES DE LA MUNICIPALIDAD DISTRITAL DE IQUITOS 2023** es necesario someter a juicio de experto la Variable, Dimensiones, Indicadores o Índices de las Variables en Estudio: **V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES**. Para la evaluación de las mencionadas variables, Ud. Ha sido seleccionado a fin de solicitarle emita **JUICIO DE EXPERTO**, por ello he considerado su elevada preparación y experiencia en investigación.

De modo anticipado le agradezco su valiosa colaboración.

I. **DATOS GENERALES**
Apellidos y nombres del experto:
Cargo e Institución donde Labora: Docente
Nombre del instrumento motivo de evaluación: V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES
Autor del Instrumento: ANGELLO GIORDANO RODRIGUEZ SOLSOL
Aspirante a: INGENIERÍA DE SISTEMAS DE INFORMACIÓN

II. **ASPECTOS DE VALIDACIÓN**

INDICADORES	CRITERIOS	1 DEFICIENTE 00 - 04	2 REGULAR 05 - 08	3 BUENA 09 - 12	4 MUY BUENA 13 - 16	5 EXCELENTE 17 - 20
COHERENCIA	El ítem mide alguna variable /categoría presente en el cuadro de congruencia metodológica					X
CLARIDAD	El ítem es claro (no genera confusión o contradicciones)					X
ESCALA	El ítem puede ser respondido de acuerdo a la escala que presenta el instrumento					X
RELEVANCIA	El ítem es ítem relevante para cumplir con las preguntas y objetivos de investigación					X

III. **OPINIÓN DE LA APLICABILIDAD**

IV. **PROMEDIO DE VALORACIÓN:** 72

Lugar y Fecha: Iquitos, 25/07/2024
D.N.I. N° 05381320 Telef. 961634538
Firma del experto informante

UNIVERSIDAD CIENTÍFICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

ANEXO N°3: Validez y Confiabilidad

Estimados Profesionales:
Lic. Luis Ronald Rucoba del Castillo, Dr.
Lic. Cecilia Rios Perez, Dr.a
Lic. Vpictor Manuel Zegarra Seminario, Mgr.
Lic. Joseni Tuesta Ruiz, Mgr.
Lic. Jhosiveth Jheninfer Zam,brano Curitima, Mgr.

Con motivo de la investigación que realizo sobre: **EVALUACIÓN DEL IMPACTO DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE DATOS SENSIBLES DE LA MUNICIPALIDAD DISTRITAL DE IQUITOS 2023** es necesario someter a juicio de experto la Variable, Dimensiones, Indicadores e Índices de las Variables en Estudio: **V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES**. Para la evaluación de las mencionadas variables, Ud. Ha sido seleccionado a fin de solicitarle emita **JUICIO DE EXPERTO**, por ello he considerado su elevada preparación y experiencia en Investigación:

De modo anticipado le agradezco su valiosa colaboración.

I. DATOS GENERALES
Apellidos y nombres del experto:
Cargo e institución donde Labora: Docente
Nombre del instrumento motivo de evaluación: V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES
Autor del Instrumento: ANGELLO GIORDANO RODRIGUEZ SOLSOL
Aspirante a: INGENIERÍA DE SISTEMAS DE INFORMACIÓN

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	1 DEFICIENTE 00- 04	2 REGULAR 05 – 08	3 BUENA 09 – 12	4 MUY BUENA 13 – 16	5 EXCELENTE 17 – 20
		1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20
COHERENCIA	El ítem mide alguna variable /categoría presente en el cuadro de congruencia metodológica					X
CLARIDAD	El ítem es claro (no genera confusión o contradicciones)					X
ESCALA	El ítem puede ser respondido de acuerdo a la escala que presenta el instrumento					X
RELEVANCIA	El ítem es ítem relevante para cumplir con las preguntas y objetivos de investigación					

III. OPINIÓN DE LA APLICABILIDAD

.....

IV. PROMEDIO DE VALORACIÓN:

70

Lugar y Fecha: Iquitos, 25 de Julio 2024

D.N.I. N° 05371191 Teléf. 910299531

Firma del experto informante

UNIVERSIDAD CIENTÍFICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

ANEXO N°3: Validez y Confiabilidad

Estimados Profesionales:
Lic. Luis Ronald Rucoba del Castillo, Dr.
Lic. Cecilia Rios Perez, Dr.a
Lic. Vpictor Manuel Zegarra Seminario, Mgr.
Lic. Joseni Tuesta Ruiz, Mgr.
Lic. Jhosiveth Jheninfer Zam,brano Curitima, Mgr.

Con motivo de la investigación que realizo sobre: EVALUACIÓN DEL IMPACTO DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE DATOS SENSIBLES DE LA MUNICIPALIDAD DISTRITAL DE IQUITOS 2023 es necesario someter a juicio de experto la Variable, Dimensiones, Indicadores e Índices de las Variables en Estudio: V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES. Para la evaluación de las mencionadas variables, Ud. Ha sido seleccionado a fin de solicitarle emita JUICIO DE EXPERTO, por ello he considerado su elevada preparación y experiencia en Investigación:

De modo anticipado le agradezco su valiosa colaboración.

I. DATOS GENERALES
Apellidos y nombres del experto:
Cargo e institución donde Labora: Docente
Nombre del instrumento motivo de evaluación: V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES
Autor del Instrumento: ANGELLO GIORDANO RODRIGUEZ SOLSOL
Aspirante a: INGENIERÍA DE SISTEMAS DE INFORMACIÓN

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	1 DEFICIENTE 00- 04	2 REGULAR 05 – 08	3 BUENA 09 – 12	4 MUY BUENA 13 – 16	5 EXCELENTE 17 – 20
		1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20
COHERENCIA	El ítem mide alguna variable /categoría presente en el cuadro de congruencia metodológica					X
CLARIDAD	El ítem es claro (no genera confusión o contradicciones)					X
ESCALA	El ítem puede ser respondido de acuerdo a la escala que presenta el instrumento					X
RELEVANCIA	El ítem es ítem relevante para cumplir con las preguntas y objetivos de investigación					

III. OPINIÓN DE LA APLICABILIDAD

.....

IV. PROMEDIO DE VALORACIÓN:

Lugar y Fecha: Iquitos, 25 de julio de 2024

D.N.I. N° 05958034 Teléf. 918889179

Firma del experto informante

UNIVERSIDAD CIENTÍFICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

ANEXO N°3: Validez y Confiabilidad

Estimados Profesionales:
Lic. Luis Ronald Rucoba del Castillo, Dr.
Lic. Cecilia Rios Perez, Dr.a
Lic. Vpictor Manuel Zegarra Seminario, Mgr.
Lic. Joseni Tuesta Ruiz, Mgr.
Lic. Jhosiveth Jheninfer Zam,brano Curitima, Mgr.

Con motivo de la investigación que realizo sobre: EVALUACIÓN DEL IMPACTO DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE DATOS SENSIBLES DE LA MUNICIPALIDAD DISTRITAL DE IQUITOS 2023 es necesario someter a juicio de experto la Variable, Dimensiones, Indicadores e Índices de las Variables en Estudio: V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES. Para la evaluación de las mencionadas variables, Ud. Ha sido seleccionado a fin de solicitarle emita JUICIO DE EXPERTO, por ello he considerado su elevada preparación y experiencia en Investigación:

De modo anticipado le agradezco su valiosa colaboración.

I. DATOS GENERALES
Apellidos y nombres del experto:
Cargo e institución donde Labora: Docente
Nombre del instrumento motivo de evaluación: V.I: IMPACTO DE LA CIBERSEGURIDAD. V.D: PROTECCIÓN DE DATOS SENSIBLES
Autor del Instrumento: ANGELLO GIORDANO RODRIGUEZ SOLSOL
Aspirante a: INGENIERÍA DE SISTEMAS DE INFORMACIÓN

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	1 DEFICIENTE 00- 04	2 REGULAR 05 – 08	3 BUENA 09 – 12	4 MUY BUENA 13 – 16	5 EXCELENTE 17 – 20
		1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20
COHERENCIA	El ítem mide alguna variable /categoría presente en el cuadro de congruencia metodológica					X
CLARIDAD	El ítem es claro (no genera confusión o contradicciones)					X
ESCALA	El ítem puede ser respondido de acuerdo a la escala que presenta el instrumento					X
RELEVANCIA	El ítem es ítem relevante para cumplir con las preguntas y objetivos de investigación					

III. OPINIÓN DE LA APLICABILIDAD

.....

IV. PROMEDIO DE VALORACIÓN:

72

Lugar y Fecha: Iquitos 25 de julio

D.N.I. N° 70814009 Teléf. 936149161

Firma del experto informante

PARTE 2: Confiabilidad del instrumento

Con respecto a la **Confiabilidad** se estima que un instrumento de medición es confiable cuando permite determinar que el mismo, mide lo que el investigador quiere medir, y que, aplicado varias veces, replique el mismo resultado.

Criterio de confiabilidad valores

0,81 a 1,00 Muy Alta confiabilidad

0,61 a 0,80 Alta confiabilidad

0,41 a 0,60 Moderada confiabilidad

0,21 a 0,40 Baja confiabilidad

0,01 a 0,20 Muy Baja

Para la validación de los cuestionarios sobre: **IMPACTO DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE DATOS SENSIBLES,** Confianza sobre los Medios de Comunicación Tradicionales, se utilizó el Alfa de Cronbach el cual arrojó el siguiente resultado:

Tabla 3

Confiabilidad del cuestionario sobre sobre: V.I. (X): **IMPACTO DE LA CIBERSEGURIDAD**

Estadísticos de fiabilidad	
Alfa de Cronbach	N° de elementos
0,819	10

El coeficiente alfa es 0,873 por lo que nos está indicando que existe una alta confiabilidad en el cuestionario.

Para la validación del cuestionario sobre: **IMPACTO DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE DATOS SENSIBLES**, se utilizó el Alfa de Cronbach el cual arrojó el siguiente resultado:

Tabla 4

Confiabilidad del cuestionario sobre sobre: V.D. (Y): **PROTECCIÓN DE DATOS SENSIBLES**

Estadísticos de fiabilidad	
Alfa de Cronbach	N°de elementos
0,897	10

El coeficiente alfa es 0,927 por lo que nos está indicando que existe una muy alta confiabilidad en el cuestionario.

ANEXO N°4: Consentimiento Informado

El Plan de Tesis titulado: **ANALISIS DEL NIVEL DE CIBERSEGURIDAD Y SU IMPLICANCIA EN LA PROTECCIÓN DE DATOS SENSIBLES EN LA MUNICIPALIDAD DISTIRLA DE SAN JUAN BAUTISTA 2025,** tiene como objetivo: Medir el Impacto de la Ciberseguridad mejora la Protección de Datos Sensibles de la MDSJB 2025.

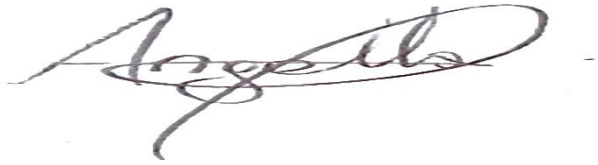
Solicito a Ud. su colaboración y permiso para que sea participe de este proyecto de investigación y tomar los datos necesarios, manteniendo total confidencialidad y anonimidad.

Yo……
He leído la información que se me ha entregado.
He podido hacer preguntas sobre el estudio.
He recibido suficiente información sobre el estudio.
He hablado con el investigador: **ANGELLO GIORDANO RODRIGUEZ SOLSOL**
Comprendo que mi participación, es bajo mi voluntad.
Comprendo que me puedo retirar del estudio en las siguientes situaciones:

1. Cuando quiera
2. Sin tener que dar explicaciones

Presto libremente mi conformidad para ser participe en el estudio
Firma del estudiante ……

Le hemos explicado este proyecto al participante y hemos contestado todas sus preguntas, comprende la información descrita en este documento y accede a participar en forma voluntaria.



ANGELLO GIORDANO RODRIGUEZ SOLSOL

DNI N°72868253

ANEXO N°5: Prueba Piloto de Impacto de la Ciberseguridad en la Protección de Datos Sensibles

Ciberseguridad										
ID	1	2	3	4	5	6	7	8	9	10
1	3	3	3	2	3	3	3	3	3	3
2	3	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	3	3
4	2	2	2	2	2	3	3	3	3	2
5	3	2	2	2	2	2	3	1	1	3
6	3	2	3	3	3	3	3	3	2	3
7	2	2	2	2	2	3	3	3	3	3
8	3	3	3	3	3	3	3	3	3	1
9	3	3	3	3	3	3	3	3	3	3
10	3	3	3	3	3	3	3	3	3	3

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,819	10

Protección de Datos Sensibles										
ID	1	2	3	4	5	6	7	8	9	10
1	3	3	3	3	3	3	3	3	3	3
2	3	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	2	3	3	3	3
4	2	2	2	3	3	3	3	3	3	3
5	3	2	2	3	2	2	3	1	1	3
6	3	2	3	3	3	3	3	3	3	3
7	2	3	3	3	2	3	3	3	3	3
8	2	2	2	2	2	2	2	2	2	1
9	2	3	3	3	3	3	3	3	3	3
10	3	3	3	3	3	3	3	3	3	3

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,897	10

Anexo 06: Base de Datos de Ciberseguridad en la Protección de Datos Sensibles

EVALUACIÓN DEL IMPACTO DE LA CIBERSEGURIDAD (PRE TEST)

	Eficiencia de las Políticas de Ciberseguridad															Capacitación y Concienciación en Ciberseguridad									
	lementación de protocolos de seguri					plimiento con regulaciones de cibersegu					Eficacia en la gestión de riesgos					Capacitación continua del personal					Conciencia sobre la protección de datos				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1
2	1	1	1	2	2	2	1	1	1	1	2	1	1	1	1	1	2	2	1	1	2	1	1	1	2
3	1	1	1	1	1	2	1	1	1	1	1	1	1	1	|	1	1	1	1	2	1	1	2	1	1
4	1	1	2	1	1	1	1	1	2	2	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1
5	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	1	1	2	1	1	2	2	1	1	1	2	2	1	1	1	1	2	1	1	1	1	1	1	1	2
7	2	2	1	1	2	1	1	2	1	1	1	1	2	1	1	1	1	1	2	1	2	2	1	1	1
8	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	2	1	2
9	2	1	1	2	1	1	1	1	2	1	1	1	1	2	1	1	1	1	2	2	1	2	2	1	2
10	1	1	1	1	2	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
11	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1
12	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	2	2	1	1	2	1	1	1	2
13	1	2	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1	2	2	1	1
14	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
16	1	1	1	2	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	3	1	1	1
18	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
19	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	2	1	1	1
20	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1
21	2	1	2	2	1	1	1	1	1	2	1	1	1	1	2	1	1	1	2	1	1	2	1	1	1
22	2	1	1	2	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	2	1	1	2	1	1
23	3	2	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
24	1	1	1	2	1	1	2	1	1	1	1	2	1	1	1	1	1	1	2	2	1	2	2	1	1
25	2	1	1	2	1	1	1	1	1	2	1	1	1	1	2	2	1	1	1	1	1	1	1	2	1
26	1	1	1	1	2	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
27	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	2	1
28	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	2	2	1	1	2	1	1	1	2
29	2	1	2	2	2	2	1	2	2	2	2	2	2	1	2	2	2	3	2	2	2	2	2	2	1
30	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1

	Capacitación y Concienciación en Ciberseguridad					Respuesta ante Incidentes de Seguridad															Total				
	Evaluación de la efectividad de las capacitaciones					Tiempo de respuesta ante incidentes					Contención y mitigación de amenazas					Recuperación y continuidad operativa									
	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	D1	D2	D3	D4	Total
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	16	17	15	0	48
2	1	1	1	2	1	2	1	2	1	2	1	2	1	1	1	1	2	1	1	1	19	20	20	0	59
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	15	17	16	0	48
4	1	1	1	1	2	1	1	2	2	1	1	2	1	1	1	1	2	1	1	1	20	16	19	0	55
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	16	15	15	0	46
6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	20	17	15	0	52
7	2	1	1	2	1	1	1	2	1	1	2	1	1	2	1	2	1	1	2	1	20	20	20	0	60
8	1	1	2	1	2	2	1	1	2	1	1	1	2	1	1	1	1	2	1	1	16	21	19	0	56
9	2	1	2	1	1	1	2	1	1	1	1	2	1	1	1	1	2	1	1	1	19	22	18	0	59
10	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	18	15	17	0	50
11	1	1	1	1	1	2	1	1	1	1	1	1	2	1	2	1	1	2	1	2	16	16	20	0	52
12	1	1	1	2	1	2	1	1	1	1	1	1	1	2	1	1	1	1	2	1	17	20	18	0	55
13	2	1	1	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1	1	1	18	20	17	0	55
14	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	17	15	16	0	48
15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15	15	15	0	45
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	18	15	15	0	48
17	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	15	19	16	0	50
18	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	15	16	16	0	47
19	1	1	1	2	1	1	2	1	1	1	1	1	2	1	2	1	1	1	1	1	16	18	18	0	52
20	1	1	1	1	1	1	2	1	2	2	1	2	1	1	1	1	2	1	1	1	16	17	20	0	53
21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	20	17	17	0	54
22	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	19	18	16	0	53
23	1	2	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	1	2	19	16	18	0	53
24	1	2	1	1	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1	1	18	20	17	0	55
25	1	2	1	1	1	1	1	2	1	2	2	1	1	1	1	2	1	1	1	1	19	18	19	0	56
26	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	2	1	1	18	15	18	0	51
27	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1	2	1	2	16	18	19	0	53
28	1	1	1	2	1	2	1	1	1	1	1	1	1	2	1	1	1	1	2	1	17	20	18	0	55
29	2	2	2	2	2	2	2	2	2	2	3	3	1	2	2	1	1	1	1	1	27	30	26	0	83
30	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	17	15	16	0	48

EVALUACIÓN DEL IMPACTO DE LA CIBERSEGURIDAD EN LA PROTECCIÓN DE DATOS SENSIBLES (POS TEST)

	Confidencialidad de los Datos															Integridad de los Datos														Disponibilidad de los Datos														Total				
	Control de acceso a datos sensibles					Políticas de privacidad y manejo de datos					Uso de cifrado en datos sensibles					Validación y control de cambios en los datos					Protección contra pérdida de datos					Monitoreo de la integridad de los datos					Acceso seguro y continuo a datos sensibles					Resiliencia ante ciberataques					Recuperación rápida de datos tras incidentes									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	D1	D2	D3	D4	Total
1	3	2	2	2	2	3	2	2	2	2	3	2	2	2	2	1	3	2	3	3	2	2	2	1	3	3	2	2	2	2	2	3	2	2	3	2	3	3	3	1	2	3	3	3	1	33	33	36	0	102
2	2	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	31	31	29	0	91
3	2	2	2	3	2	2	2	1	1	1	2	2	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	1	2	3	2	2	1	2	3	2	25	30	29	0	84
4	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	1	2	1	2	2	2	2	1	2	1	2	2	2	2	1	2	2	2	2	30	27	27	0	84
5	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	45	45	45	0	135
6	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	1	2	1	1	2	2	2	1	1	2	2	29	30	24	0	83
7	3	3	1	3	3	3	1	2	1	2	3	1	2	1	2	3	1	3	3	1	3	1	2	3	1	1	3	3	1	2	3	1	2	1	2	3	2	2	2	1	3	2	2	2	1	31	31	29	0	91
8	1	1	2	1	3	2	2	2	2	3	2	2	2	2	3	2	2	3	2	1	3	3	2	2	2	1	3	3	3	2	3	2	3	2	2	3	2	2	3	3	3	2	2	3	3	30	34	38	0	102
9	3	1	1	3	2	1	2	2	3	1	1	2	2	3	1	2	3	1	3	2	2	1	2	2	3	2	3	2	1	2	2	3	2	1	2	3	2	2	3	2	3	2	2	3	2	28	31	34	0	93
10	3	3	2	3	1	1	2	2	2	2	1	2	2	2	2	1	2	2	2	2	2	3	2	1	2	2	3	2	3	2	2	3	1	2	3	3	3	1	2	2	3	3	1	2	2	30	31	33	0	94
11	3	3	2	2	1	3	1	3	1	3	3	1	3	1	3	1	3	2	3	3	2	2	1	1	3	3	1	2	2	1	1	3	1	2	2	2	2	2	3	1	2	2	2	3	1	33	30	29	0	92
12	3	2	2	2	3	3	2	2	2	2	3	2	2	2	2	2	3	3	1	1	2	3	2	2	3	1	2	2	3	2	3	2	3	2	2	3	2	1	1	2	3	2	1	1	2	34	32	30	0	96
13	2	3	2	3	3	2	3	1	2	2	2	3	1	2	2	2	2	2	2	2	3	2	2	2	2	2	2	3	2	2	1	3	3	2	1	3	1	3	3	2	3	1	3	3	2	33	32	34	0	99
14	3	2	3	2	2	2	2	2	2	3	2	2	2	2	3	2	1	2	3	1	3	2	2	2	1	1	2	3	2	2	1	1	3	2	3	3	3	3	3	2	3	3	3	3	2	34	29	38	0	101
15	3	2	3	1	3	2	1	3	2	3	2	1	3	2	3	2	1	1	3	1	2	3	1	2	1	1	3	2	3	1	2	3	3	2	3	3	3	1	2	1	3	3	1	2	1	34	27	33	0	94
16	2	1	2	3	2	3	3	3	1	1	3	3	3	1	1	2	3	2	3	1	3	1	2	2	3	1	2	3	1	2	2	1	3	2	1	2	1	2	3	3	2	1	2	3	3	32	31	31	0	94
17	3	2	1	2	2	2	2	2	1	2	2	2	2	1	2	3	1	2	2	3	2	2	2	3	1	3	3	2	2	2	2	1	2	1	2	3	2	2	2	2	3	2	2	2	2	28	33	30	0	91
18	3	3	2	2	1	3	1	3	1	3	3	1	3	1	3	1	3	2	3	3	2	2	1	1	3	3	1	2	2	1	1	3	1	2	2	2	2	2	3	1	2	2	2	3	1	33	30	29	0	92
19	3	2	2	2	3	3	2	2	2	2	3	2	2	2	2	2	3	3	1	1	2	3	2	2	3	1	2	2	3	2	3	2	3	2	2	3	2	3	1	2	3	2	3	1	2	34	32	34	0	100
20	2	3	2	3	3	2	3	1	2	2	2	3	1	2	2	3	3	3	3	3	3	3	2	3	3	3	2	3	3	2	1	3	3	2	1	3	1	3	1	1	3	1	3	1	1	33	42	28	0	103
21	3	2	3	2	2	2	2	2	2	3	2	2	2	2	3	2	1	2	3	1	3	2	2	2	1	1	2	3	2	2	1	1	3	2	3	3	3	3	3	2	3	3	3	3	2	34	29	38	0	101
22	3	2	3	1	3	2	3	3	2	1	2	3	3	2	1	2	1	1	3	1	2	3	3	2	1	1	1	2	3	3	2	3	3	2	1	3	1	1	2	2	3	1	1	2	2	34	29	29	0	92
23	2	1	2	3	2	3	3	3	1	1	3	3	3	1	1	2	3	2	3	1	3	1	2	2	3	1	2	3	1	2	2	1	3	2	1	2	1	2	3	3	2	1	2	3	3	32	31	31	0	94
24	3	3	3	3	3	3	2	2	3	2	3	2	2	3	2	3	3	3	3	3	2	2	2	3	3	3	3	2	2	2	3	2	2	3	3	2	3	3	3	3	2	3	3	3	3	39	39	42	0	120
25	1	1	2	1	3	2	2	2	2	3	2	2	2	2	3	2	2	3	2	1	3	3	2	2	2	1	3	3	3	2	3	2	3	2	2	3	2	2	3	3	3	2	2	3	3	30	34	38	0	102
26	3	3	2	3	1	1	2	2	2	2	1	2	2	2	2	1	2	2	2	2	2	3	2	1	2	2	3	2	3	2	2	3	1	2	3	3	3	1	2	2	3	3	1	2	2	30	31	33	0	94
27	3	3	2	2	1	3	1	3	1	3	3	1	3	1	3	1	3	2	3	3	2	2	1	1	3	3	1	2	2	1	1	3	1	2	2	2	2	2	3	1	2	2	2	3	1	33	30	29	0	92
28	2	2	2	2	1	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	2	2	3	2	3	1	1	1	2	3	2	1	1	2	2	2	1	1	1	23	22	24	0	69
29	2	3	2	3	3	2	3	1	2	2	2	3	1	2	2	2	2	2	2	2	3	2	2	2	2	2	2	3	2	2	1	3	3	2	1	3	1	3	3	2	3	1	3	3	2	33	32	34	0	99
30	3	2	3	2	2	2	2	2	2	3	2	2	2	2	3	2	1	2	3	1	3	2	2	2	1	1	2	3	2	2	1	1	3	2	3	3	3	3	3	2	3	3	3	3	2	34	29	38	0	101