UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR (ES):

Flores Vasquez, Leopoldo (orcid.org/0000-0002-2416-6967)

Varas Valles, Tony (orcid.org/0000-0002-1021-4315)

ASESORA:

Dra. Mescua Ampuero, Lizeth Erly (orcid.org/0000-0003-2748-479X)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE ACCIÓN DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico,empleo y emprendimiento

TARAPOTO – PERÚ

2023

Dedicatoria

Dedicamos este proyecto a todas las personas que han sido parte fundamental de nuestro camino académico. A nuestros padres por su inquebrantable apoyo y amor incondicional. A nuestros docentes, cuyos conocimientos y orientación han sido mi fuente de inspiración. A los amigos, por su constante ánimo. Por sus guía y consejos expertos que han enriquecido este trabajo. A todos aquellos que creyeron en nosotros y nos alentaron a perseguir nuestros sueños, este proyecto es el reflejo de su confianza en nosotros. ¡Gracias!

Los autores

Agradecimiento

En el camino hacia la realización de este proyecto, hubo numerosas personas cuyo apoyo, orientación y contribuciones desempeñaron un papel fundamental en nuestro éxito académico. A todos ellos les expreso mi más sincero agradecimiento:

A nuestra asesora, Dra. Mescua Ampuero, Lizeth Erly, por su paciencia, conocimiento y dedicación. Su guía constante y valiosos consejos fueron cruciales en la culminación de este proyecto.

Agradecemos a nuestra a mi familia, especialmente a nuestros padres, por su amor incondicional, sacrificio y apoyo continuo sin su respaldo emocional, este logro no habría sido posible.

Agradezco a mis docentes y mentores que compartieron sus conocimientos y experiencias, ayudándonos a crecer tanto académica como personalmente.

Al Hospital II 1 Moyobamba, por su generoso apoyo en recursos que facilitaron la realización de esta investigación.

A todos los participantes del estudio, cuya colaboración fue esencial para la recopilación de datos y el éxito de la investigación.

Finalmente, agradecemos a todas las personas que de una forma u otra formaron parte de este viaje académico. Sus contribuciones y ánimos fueron esenciales para alcanzar este hito en nuestra vida.

Este logro no solo es de nosotros, sino también de todos aquellos que creyeron y nos respaldaron en este emocionante viaje académico.

¡Gracias a todos!

Los autores

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, LIZETH ERLY MESCUA AMPUERO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - TARAPOTO, asesor de Tesis titulada: "Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023", cuyos autores son FLORES VASQUEZ LEOPOLDO, VARAS VALLES TONY, constato que la investigación tiene un índice de similitud de 15.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

TARAPOTO, 23 de Noviembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
LIZETH ERLY MESCUA AMPUERO **DNI:** 42694079 **ORCID:** 0000-0003-2748-479X	Firmado electrónicamente por: MAMPUEROL8 el 23-12-2023 12:35:37

Código documento Trilce: TRI - 0663088

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Originalidad de los Autores

Nosotros, FLORES VASQUEZ LEOPOLDO, VARAS VALLES TONY estudiantes de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - TARAPOTO, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. Hemos mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	**Firma**
LEOPOLDO FLORES VASQUEZ **DNI:** 76676131 **ORCID:** 0000-0002-2416-6967	Firmado electrónicamente por: LFLORESV11 el 23-11-2023 00:54:12
TONY VARAS VALLES **DNI:** 44116672 **ORCID:** 0000-0002-1021-4315	Firmado electrónicamente por: TVARAS el 23-11-2023 00:57:15

Código documento Trilce: TRI - 0663078

INVESTIGA UCV

Índice de contenidos

Dedicatoria ii
Agradecimiento iii
Declaratoria de autenticidad del asesor v
Declaratoria de originalidad del autor(es) vi
Índice de contenidos vii
Índice de tablas ix
Resumen x
Abstract xi
I. INTRODUCCIÓN 1
II. MARCO TEÓRICO 5
III. METODOLOGÍA 12
3.1. Tipo y diseño de investigación 12
3.2. Variables y operacionalización 12
3.3. Población (criterios de selección) muestra, muestreo y unidad de análisis 13
3.4. Técnicas e instrumentos de recolección de datos 14
3.5. Procedimientos 16
3.6. Método de análisis de datos 16
3.7. Aspectos éticos 17
IV. RESULTADOS 18
V. DISCUSIÓN 24
VI. CONCLUSIONES 28

VII. RECOMENDACIONES 29

REFERENCIAS 30

ANEXOS 38

Índice de tablas

Tabla 1. Validación de instrumentos 155

Tabla 2. Confiabilidad del instrumento 166

Tabla 3. Prueba de normalidad el acceso restringido 188

Tabla 4. Prueba de normalidad del acceso restringido y transmisión segura. 188

Tabla 5. Prueba de normalidad para evaluar el almacenamiento protegido. 1919

Tabla 6. Prueba de normalidad para evaluar las políticas y procedimientos..... 1919

Tabla 7. Prueba de normalidad para evaluar la auditoría y monitoreo. 200

Tabla 8. Prueba de Wilcoxon para medir el Acceso Restringido..... 211

Tabla 9. Prueba de Wilcoxon para medir la transmisión segura. 211

Tabla 10. Prueba de Wilcoxon para medir el Almacenamiento protegido. 222

Tabla 11. Prueba de Wilcoxon para medir las Políticas y procedimientos 233

Tabla 12. Prueba de Wilcoxon para medir la Auditoria y monitoreo..... 233

Resumen

En el presente estudio de investigación titulado “Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023”. El objetivo general fue implementar un plan de gobierno de datos para mejorar la confidencialidad de la información en establecimientos de salud de la Región San Martín periodo 2023. El tipo de investigación que se utilizó fue aplicado con diseño pre experimental longitudinal, se contó con una población y muestra de 50 colaboradores, quienes fueron encuestados con un pretest y posttest. Los resultados evidenciaron que la implementación de un gobierno de datos mejora el acceso restringido a la información, la transmisión segura de los datos, el almacenamiento protegido de los datos, las política y procedimientos en establecimientos de salud y la auditoria y monitoreo en establecimientos de salud (0,000 < 0,05). Se llegó a concluir que la implementación de un plan de gobierno de datos mejora la confidencialidad de la información en establecimientos de salud de la Región San Martín 2023 (0,000 < 0,05).

Palabras clave: Implementación, gobierno, garantizar, confidencialidad, información

Abstract

In the present research study titled “Implementation of a data governance plan to guarantee the confidentiality of information in a health facility, San Martín 2023”. The general objective was to implement a data governance plan to improve the confidentiality of information in a health facility in the San Martín Region for the period 2023. The type of research used was applied with a longitudinal pre-experimental design, there was a population and sample of 50 employees, who were surveyed with a pretest and posttest. The results showed that the implementation of data governance improves restricted access to information, secure transmission of data, protected storage of data, policies and procedures in a health facility, and auditing and monitoring in a facility. health (0.000 < 0.05). It was concluded that the implementation of a data governance plan improves the confidentiality of information in a health facility in the San Martín 2023 Region (0.000 < 0.05).

Keywords: Implementation, government, guarantee, confidentiality, information

I. INTRODUCCIÓN

En los últimos tiempos hubo muchos cambios en la ciencia de datos ha traído al área de salud, sobre todo con el aumento de la tecnología y la cantidad de datos electrónicos, lo que hace cada vez más difícil garantizar la confidencialidad. Así, Latinoamérica debe afrontar un gran reto para administrar esos datos debido a los problemas estructurales que caracterizan a la región. Uno de los problemas relevantes en los establecimientos de salud fue implementar una política de datos es el tema de la seguridad, esto se debió a que muchas veces las personas encargadas de manejar los datos no son conscientes de los estándares de seguridad existentes, especialmente en lo que respecta a la recopilación, almacenamiento y transmisión de datos personales. Muchas veces los dispositivos de almacenamiento no son seguros, lo que a su vez permite a los hackers y a los criminales obtener acceso a los datos sin autorización. Además, a veces, los establecimientos de salud no tienen un plan para asegurar la intimidad y el secreto de los datos. Por lo tanto, es necesario que los establecimientos de salud adquieran un software especializado y proporcionen entrenamientos para garantizar que los trabajadores manejen información confiable (Rosa y Frutos, 2022)

A nivel nacional, uno de los problemas en el gobierno de datos que puede afectar la garantía de confidencialidad de datos en el sector salud en Perú es la falta de una legislación adecuada y robusta referente a la protección de datos en salud. Asimismo, carecen de normativas especificas lo que lleva a lagunas legales, por falta de claridad sobre cómo se deben manejar y proteger los datos sensibles de los pacientes. Sumado a ello, la falta de conciencia y capacitación sobre cómo se puede manejar la información de manera segura en los establecimientos de salud. Lo que resulta en un manejo inadecuado de los datos y la escasez de protección de los mismos. Otro problema común es la falta de recursos financieros y técnicos para implementar sistemas de seguridad de la información adecuada. Los establecimientos de salud carecen de infraestructura tecnológica suficiente, datos seguros y sin la protección en su calidad. Por último, la escasa coordinación y colaboración entre los que manejan los datos en los establecimientos de salud

también genera problemas manejo eficiente de los procesos para cumplir las metas. Si no hay un enfoque unificado y una clara responsabilidades, es más probable que se produzcan errores, descubiertos o negligentes en la preservación de los datos secretos (Banco de Desarrollo de América Latina, 2021)

La región San Martín no es ajena a la problemática nacional referente al problema que enfrentan los hospitales de la región debido a un deficiente plan de gobierno de datos, reflejado en la escacez de sistemas y procedimientos adecuados que terminan afectando directamente la protección de la información, así como el acceso a dichos datos del personal de salud. Se considera un problema, ya que los datos de los pacientes pueden ser vulnerados. Esto es particularmente preocupante debido al continuo aumento del volumen de datos personales confidenciales que necesitan ser manejados adecuadamente para salvaguardar la seguridad de los datos. En los establecimientos de salud de Moyobamba y Jerillo, existen una serie de amenazas a la confidencialidad de datos, y si no se implementan los controles y mecanismos de seguridad adecuados, tales datos podrían caer en manos equivocadas y causar serios problemas. Además, los métodos obsoletos de almacenamiento de las unidades locales no cumplen con los nuevos estándares nacionales de seguridad de datos, los que le convierten en riesgo importante, que deberían ser tratadas y reducir de manera significativa la probabilidad de su ocurrencia.

De todo de lo anterior mencionado el presente proyecto se plantea como problema general: ¿En qué medida la implementación de un plan de gobierno de datos mejora la confidencialidad de la información en establecimientos de salud de la Región San Martín 2023? Y como problemas específicos: a. ¿Cómo la implementación de un plan de gobierno de datos mejora **el acceso restringido** en establecimientos de salud de la Región San Martín 2023? b. ¿Cómo la implementación de un plan de gobierno de datos mejora **la transmisión segura** en establecimientos de salud de la Región San Martín 2023? c. ¿Cómo la implementación de un plan de gobierno de datos mejora el **almacenamiento protegido** en establecimientos de salud de la Región San Martín 2023? d. ¿Cómo la implementación de un plan de gobierno de

datos mejora las **políticas y procedimientos** en establecimientos de salud de la Región San Martín 2023?. e. ¿Cómo la implementación de un plan de gobierno de datos mejora la **auditoría y monitoreo** en establecimientos de salud de la Región San Martín 2023?

Así también la presente investigación resultó conveniente, ya que los establecimientos de salud tratan datos sensibles y, por tanto, su confidencialidad debe garantizarse. De lo contrario, se corre el peligro de que los datos sean utilizados para fines indebidos, como el acoso, y correrían el riesgo de exponer la información de los pacientes a la ligera, así también socialmente, el establecimiento de un plan de gobierno de datos, los establecimientos de salud también se beneficiaron de los avances tecnológicos para lograr una mejor eficiencia en el tratamiento de los pacientes, asimismo en cuanto al valor teórico la implementación de un plan de gobierno de datos brinda la necesaria tranquilidad a los usuarios, garantizando la confidencialidad de los datos alcanzando diversos niveles de seguridad digital. El Plan de Gobierno de Datos para la Región San Martín, del año 2023 brindó una cobertura exhaustiva que abarcó tanto la legislación vigente como los requisitos para el cifrado de datos, control de acceso y auditoría.

Referente a la justificación práctica, el establecimiento de un plan de gobierno de datos ayudó a garantizar que la información sea procesada correctamente y de manera segura, evitando fraudes y usos indebidos de la información. con el uso de tecnologías modernas, y tratar la información de forma mejor planificada con buenas prácticas de ciberseguridad. Y finalmente en términos metodológicos La presente investigación aporta un instrumento para la Implementación de un plan de gobierno de datos y la confidencialidad de la información en establecimientos de salud Región San Martín, el cual será de ayuda para otras investigaciones, pues este fue validado mediante el criterio de jueces.

De acuerdo a lo propuesto, el objetivo general de la investigación fue: Implementar un plan de gobierno de datos para mejorar la confidencialidad de la información en establecimientos de salud de la Región San Martín periodo 2023 y los objetivos

específicos fueron: Mejorar **el acceso restringido** en establecimientos de salud de la Región San Martín 2023. Mejorar **la transmisión segura** en establecimientos de salud de la Región San Martín 2023. Mejorar el **almacenamiento protegido** en establecimientos de salud de la Región San Martín 2023. Mejorar las **políticas y procedimientos** en establecimientos de salud de la Región San Martín 2023. Mejorar en la **Auditoría y monitoreo** en establecimientos de salud de la Región San Martín 2023.

Finalmente se planteó la hipótesis, que la implementación de un plan de gobierno de datos mejora la confidencialidad de la información en establecimientos de salud de la Región San Martín 2023. Y como hipótesis específicas: El plan de gobierno de datos mejora **el acceso restringido** en establecimientos de salud de la Región San Martín 2023. El plan de gobierno de datos mejora **la transmisión segura** en establecimientos de salud de la Región San Martín 2023. El plan de gobierno de datos mejora el **almacenamiento protegido** en establecimientos de salud de la Región San Martín 2023. El plan de gobierno de datos mejora las **políticas y procedimientos** en establecimientos de salud de la Región San Martín 2023. El plan de gobierno de datos mejora la **auditoría y monitoreo** en establecimientos de salud de la Región San Martín 2023.

II. MARCO TEÓRICO

Tras un análisis minucioso de la información disponible en las diferentes plataformas digitales, se han seleccionado varios documentos como a nivel internacional: Morales (2022), en el estudio de tipo propositiva, diseño no experimental, tomando como población a la Empresa Universitaria de Salud EUS – EP. Concluyó que, la Empresa Universitaria de Salud EUS – EP carecía de una Gobernanza de Datos implementada. Esto fue debido a que no se habían formalmente identificado los responsables de los datos, ni se contaba con un gobierno de datos aprobado. Además, los medios previamente elaborados ya no eran adecuados para la realidad actual de la entidad, que había experimentado un crecimiento significativo en el último año. Por ello, se hizo necesario elaborar una Guía Metodológica para aplicar una Gobernanza de datos en la EUS-EP.

De acuerdo con Orozco et al. (2021). En su trabajo descriptivo y diseño explicativo, sin manipular variables, en la cual se analizaron a 12 hospitales, en la cual se empleó la técnica de observación y una ficha observacional. Concluyó que, en los establecimientos de salud, existe deficiencia en la gobernanza de datos, incluso la normativa es general para acceder y usar los datos. Tampoco hay mecanismos de control efectivos para controlar la calidad y la transparencia en su manejo, perdiendo información muchas veces, usarla incorrectamente, hasta incluso no usarla para cumplir los objetivos.

De la misma forma, Hernández (2021). Se desarrolló un estudio tipo aplicado, si n manipular variables, y nivel descriptivo, donde tomaron como población a los datos clínicos de los pacientes, por lo que se empleó una ficha de observación. Por tanto, los autores concluyeron que, se ha comprobado que el 80% de los hospitales que reciben profesionales y/o estudiantes de medicina, y otras profesiones afines, han implementado medidas para salvaguardar la intimidad y privacidad de la información de los pacientes, estas normas cumplen con las reglas de privacidad establecidas para crear un entorno seguro y proteger la dignidad de los pacientes involucrados. Así, el sistema de atención a los pacientes puede ser mejorado de

manera eficaz y segura, permitiendo la realización de importantes investigaciones que puedan ser aplicadas a la mejora del servicio para los pacientes.

Ante lo expuesto por Morejón et al. (2020). Se realizó un trabajo descriptivo, buscando ampliar conocimientos, sin llegar a manipular varaibles, cuya población fue el personal asistencial y personal informático, a quienes se les aplicó la encuesta y entrevista para el recojo de información. Llegaron a la conclusión que, después de una exhaustiva implementación de un sistema hospitalario en varias organizaciones de salud, los resultados indican que el 89% de los centros de salud estaban mejor preparados para prestar servicios con la nueva aplicación, esto demuestra que la implantación del sistema hospitalario fue un éxito y proporcionó a las organizaciones de salud un aumento significativo en la eficacia de la prestación de servicios.

Solà, et al. (2023). Se llevó a cabo una investigación descriptiva, transversal, sin manipulación de variables; teniendo como población especifica a los establecimientos de salud, se utilizaron guías de entrevista. Dicho autor concluyó que, existe una brecha significativa en la confidencialidad de la información en los establecimientos de salud. Se identificaron varias deficiencias en las prácticas actuales de seguridad de los datos, como la falta de políticas claras, la limitada formación de los colaboradores y la falta de medidas tecnológicas adecuadas. Por lo que, un plan de gobierno de datos podría ser una estrategia efectiva para abordar estas deficiencias.

De esta manera se precisa aspectos teóricos relacionados a la variable plan de gobierno, donde se tomará información de autores como. García-Ahumada y León-Jiménez (2020), definen que el plan de gobierno de datos para el sector salud se concentra en brindar buenos servicios sanitarios a los ciudadanos, esto se puede lograr a través de la implementación de varias políticas dirigidas a la transformación digital, estas políticas incluyen inversiones en tecnología para mejorar la capacidad de almacenamiento de gran volumen de datos. Además, Nissán (2019) indica que el plan de gobierno en el sector, visibiliza el acceso oportuno y sin costo de servicios de salud, promoviendo la salud de los habitantes mediante el fortalecimiento de la

atención primaria, la vacunación, los programas sanitarios y aumentar la cantidad de equipos médicos de última generación para mejorar los tratamientos (Zinelli, 2022).

Sisalema-Rivera et al. (2022), sostienen que el sistema de información hospitalario está orientado a almacenar, procesar los datos médicos y las historias clínicas de los pacientes, esto para mejorar la calidad de atención que ofrecen los hospitales, ya que estos sistemas tienen la capacidad de monitorear y ayudar a realizar seguimiento a los servicios ofrecidos dentro de un hospital, como consultas externas, sala de emergencias, pruebas de diagnóstico, farmacéuticos, registros médicos, seguridad de la información, entre otros (Flores y Barbarán, 2021; Tanwar et al., 2020).

El objetivo del sistema hospitalario es proveer servicios de alta calidad a pacientes de la comunidad con enfermedades o lesiones médicas, prevenir la aparición de enfermedades, brindar tratamiento y rehabilitación, educar a la comunidad sobre la salud y respaldar la investigación médica (Mat et al., 2021). Además, mejorar la educación médica, prevenir enfermedades, proporcionar información y atención a la comunidad, realizar investigación para el desarrollo de mejores prácticas médicas y promover los programas de bienestar (Gutierrez et al., 2020; Abraham et al., 2019)

El gobierno de datos en el sector salud es crucial asegurar los datos y su calidad de los pacientes, así como para asegurar la precisión, la coherencia y la adecuación de los datos (Attaran, 2020). Los gobiernos de datos en el sector salud pueden ayudar a mejorar los datos clínicos, el control de la calidad del cuidado y la toma de opciones. También, facilitan la ejecución de las regulaciones de resguardo y confidencialidad de los datos de salud federales y estatales (Janssen & Brous, 2020). Al proporcionar una implementación eficaz y soluciones de gobierno de datos de confianza, transparencia, privacidad, seguridad y la accesibilidad, el gobierno de datos puede ayudar a proporcionar un cuidado inteligente y velar por la salud y protección de los pacientes (Preciado et al., 2021; (Reddy et al., 2020)

Además, Aguerre (2020), menciona los principios de gobernanza de datos en el

sector salud: 1) Compromiso y responsabilidad, las organizaciones de salud deben establecer y fortalecer sus compromisos con la gobernanza de los datos de salud como una responsabilidad compartida entre la administración, las áreas técnicas y los usuarios (Li et al., 2022; Benfeldt et al., 2020). 2) Enfoque estratégico, la gobernanza de datos debe ser parte integral de los procesos, estrategias, directrices y decisiones del ámbito de la salud. 3) Accesibilidad e Interoperabilidad, es necesario promover un acceso amplio y sin obstáculos a los datos de salud en ambos sentidos, esto significa asegurar que los datos permanezcan accesibles a todos aquellos que los necesiten, manteniendo criterios de seguridad y privacidad adecuados (Jayabalan & Jeyanthi, 2022). 4) Calidad, seguridad y confiabilidad de los datos, el cual garantiza la correcta administración de los datos, la mejora de su calidad y su seguridad. 5) Responsable uso y divulgación de los datos, es fundamental conocer cómo los datos se utilizan, enmarcado en criterios profesionales y éticos, el cual incluye la responsable administración de los mismos, acorde a los principios legales, ético-morales, protección de la privacidad, uso responsable y apropiado de los datos (Dubovitskaya et al., 2022; Peng-Ting et al., 2020).

Con respecto, a la variable confidencialidad de la información, se precisa aspectos teóricos tomando de autores relacionados a la misma, donde Solá-Morales el all (2023), indica que la confidencialidad de los datos se refiere al hecho de que los datos se mantienen seguros y se procesan de forma segura (Wu et al., 2022). Esto significa que los datos solamente se comparten entre aquellas personas autorizadas a verlos. Esto también incluye proteger datos sensibles y la adopción de procesos para asegurar los datos, y evitar accesibilidad no autorizado a dichos datos (Caruccio et al., 2020).

La confidencialidad de datos es importante en la salvaguardia de los datos y la confidencialidad. Kumar et al. (2021), esto es especialmente importante cuando se trata de procesar datos personales relacionados con temas sensibles como el carácter, la salud, la religión o la orientación sexual. La confidencialidad de los datos también es importante para proteger a los usuarios de la vulnerabilidad y el abuso

y evitar situaciones fraudulentas (Zinelli, 2022).

Según Preciado et al. (2021), los elementos clave dentro de la confidencialidad de los datos son el control, la verificación, la verificación, la seguridad de la información y la confidencialidad. Estos elementos son necesarios para garantizar que los datos estén seguros y protegidos. El control implica la regulación obligatoria de la gestión de los datos que se usan y con los que se comparte (Ávalos y Fernández, 2020; Kandabongee et al., 2022). La verificación requiere que los usuarios demuestren quiénes son antes de acceder a los datos. La autenticación se refiere al proceso de verificación de la identidad de un usuario. Mella et al. (2020), menciona que la seguridad de la información implica el uso de procedimientos, tecnologías y procesos para mantener los datos seguros. La privacidad significa que los usuarios tienen control sobre quién tiene acceso a sus datos (Santiago-González et al., 2019).

Además, Hernández (2019), menciona que existe métodos para proteger datos e información en los establecimientos de salud, tales como: 1) Implementación de procedimientos de la seguridad de la información, los establecimientos de salud deben desarrollar políticas y protocolos de la protección de la información para proteger la confidencialidad de los datos de los pacientes (Lema y Cuenca, 2020). 2) Uso obligatorio de credenciales para el acceso a cualquier equipo de tecnología de información: Los trabajadores de salud deben tener una identificación única para poder acceder a los sistemas de información (Vega, 2021). 3) Utilización de tecnologías de cifrado y autenticación de dos factores, se deben utilizar métodos de seguridad avanzados, como el cifrado y la autenticación de dos factores, para garantizar la integridad de la información (Francisco y Yarad, 2020). 4) Prohibición de compartir datos de los pacientes, los dispositivos móviles como computadoras portátiles y tablets no deben ser usados para compartir información de los pacientes debido a su vulnerabilidad a la intrusión (Rosales et al., 2020). 5) Formación a los empleados de los establecimientos de salud, los profesionales y otros empleados de los establecimientos de salud deben recibir formación para comprender y respetar los protocolos y la legislación relacionada a proteger la información valiosa

en las instituciones (Miranda et al., 2019; Mohammad et al., 2020).

Así mismo, según Morales (2022), indica que la gestión de datos tiene las siguientes dimensiones. a. Gestión de datos maestros, está relacionado con la forma en cómo se prevé la cantidad de datos, su calidad, seguridad, el cumplimiento normativo, la arquitectura de datos y los roles de quién los maneja. b) Calidad de datos, está basada en la en el aseguramiento y privacidad, las violaciones de datos, el cumplimiento de seguridad, la sensibilidad y confidencialidad o confidencialidad encriptados. c) Seguridad y privacidad de los datos, está basado en el cumplimiento de regulaciones, número de auditorías y el tiempo en responder los incumplimientos de los mismos. d) Cumplimiento normativo, relacionado con las consultas de datos, porcentaje de registros y tiempo promedio de resolución de problemas relacionados. e) Arquitectura de datos, puntos de integración de datos, diseño e implementación de datos y problemas o errores relacionados a datos identificados o resueltos. f). Responsabilidad y roles, relacionados la calidad de integridad de datos.

Holguín (2023), también concuerda que las dimensiones del gobierno de dato, tiene que ver con el proceso de garantizar que los datos sean usados de manera efectiva, segura, coherente. Siguiendo la gestión de datos, su calidad, la seguridad y privacidad, cumplimiento normativo, arquitectura de datos, y responsabilidad de roles.

Dentro de los documentos normativos, se tiene el Decreto Legislativo (D.L.) N° 1412, en su Art. 1 muestra en el marco de la gobernanza del gobierno digital de datos, para una adecuada gestión, arquitectura, Inter operatividad y seguridad de datos digitales de las entidades públicas en sus tres niveles. Además, contempla la privacidad del diseño de datos, su usabilidad, corporación digital, datos abiertos y el grado de confidencialidad de datos personales (El Peruano, 2023).

También se encuentra la ley 29733, ley de protección de datos personales, está enmarcada en los derechos a los dueños de datos personales, sus principios y las condiciones en que se deben aplicar respectivamente, así como su tratamiento. Le acompaña el decreto supremo D.S. 003-2013-JUS, que regula y ayuda a proteger

los datos e información de las instituciones, regulando su forma y su registro en el régimen que sanciona su violación, la inobservancia o normatividad al respecto (Defensoría del Pueblo, 2029).

Además, está la ley N°30096, en su art. 4., indica la regulación y sanciones a delitos informáticos, donde incluyen la información personal y la protección de las instituciones públicas, incluyendo sanciones al acceso de manera ilegal a datos no autorizados (El Peruano, 2019).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

La investigación fue de tipo aplicada, dado que buscó la solución de la problemática encontrada, mediante la aplicación de conocimientos existentes, relacionada con el gobierno de datos para garantizar una información confiable, como una investigación que aborda el campo tecnológico en materia de información de tecnologías, con miras a tener una mejor administración de los datos y la eficiencia de los servicios de salud. Un estudio de tipo aplicada, que busca entender los problemas, desarrollar soluciones y establecer políticas para mejorar la vida de los ciudadanos (Concytec, 2018).

Diseño de investigación

Arias y Covinos (2021) propusieron un diseño pre-experimental para evaluar el impacto de un plan de gobierno de datos en términos de confidencialidad de la información. Para esto, se recurrió a técnicas de investigación cuantitativa para recopilar datos sobre la confidencialidad de la información antes y después de la implementación de dicho plan. Una vez recopilados los datos, se compararon para verificar si el plan de gobierno de datos produjo cambios en la confidencialidad.

Representación:

M ------- O1 --------- X -------- O2

Dónde:

M: es la muestra

O1: Pre evaluación del plan de gobierno de datos

O2: Post evaluación de la confidencialidad de la información

X: Aplicación de la propuesta

3.2. Variables y operacionalización

Variable 1. Plan de gobierno de datos

Variable 2: Confidencialidad de la información

Nota: La operacionalización de variables está en la sección de anexos.

3.3. Población (criterios de selección) muestra, muestreo y unidad de análisis

Población

Al referirse a establecimientos de salud, la investigación abordó particularmente a dos establecimientos: el Hospital de Moyobamba y el centro de salud Jerillo. El primero, contó con una población de 35 trabajadores del área de informática y estadística, por su parte el centro de salud Jerillo, participó del estudio con la colaboración de 15 trabajadores también del área de informática y estadística. Por lo tanto, a nivel general, la población del estudio estuvo compuesta por 50 trabajadores encargados de manejar directamente la información institucional de los establecimientos de salud de Moyobamba y Jerillo.

- Criterios de inclusión:
    - Se incluyó al personal que maneja la información con una antigüedad laboral mayor a 5 meses.
    - Personal del área de informática y estadística
    - Personal perteneciente al Hospital de Moyobamba y del centro de salud Jerillo.
- Criterios de exclusión:
    - Se excluyeron al personal con antigüedad menor a 5 meses, dado que no manejan la información histórica
    - Personal que no pertenezca al área de informática y estadística.
    - Personal de otros establecimientos de Salud.

Muestra

Se consideró al 100 % de la población, por lo que fueron los 35 trabajadores del área

de informática y estadística del Hospital de Moyobamba y los 15 del centro de salud Jerillo. De manera que la muestra total fueron 50 trabajadores entre los dos establecimientos de salud de la región San Martín.

Muestreo

Debido a que la muestra fue censal, es decir, toda la población, no se aplicó ninguna técnica de muestreo.

Unidad de análisis

01 personal del área de informática y estadística de Hospital de Moyobamba o el centro de salud Jerillo.

3.4. Técnicas e instrumentos de recolección de datos

Como técnica, se usó la encuesta. Esta técnica implicó la formulación de preguntas dirigidas a un grupo de individuos específico con el fin de recabar información relevante sobre el asunto en consideración. En cuanto al instrumento, se empleó el cuestionario, el cual estuvo compuesto por ítems, que permitieron conocer como percibe el personal de salud sobre la confidencialidad de la información antes y después de la implementación del plan de gobierno de datos.

Validación y confiabilidad

Validez

En cuanto a la validez, se llevó a cabo una evaluación del instrumento mediante la participación de tres expertos. Estos expertos se encargaron de evaluar el instrumento y llevar a cabo su correspondiente validación. Es importante destacar que se consideraron dos aspectos principales: la validez del contenido y la validez de la estructura. Los expertos emitieron su juicio al respecto, el cual quedo registrado en un informe donde confirmaron que el instrumento cumple con las condiciones necesarias para su ejecución.

A continuación, en la siguiente tabla, se expone el informe de la validación según variables:

Tabla 1

Validación de instrumentos

Variable	N.º	Especialidad	Promedio de validez	Opinión del experto
Plan de gobierno de datos	1	Mg. Henry Lolan Vásquez Tuanama Especialista en Gestión de Proyectos Informáticos.	4	Bueno
	2	Dr. Miguel Ángel Valles Coral Ing. Sistemas. Doctor en GPyG	4	Bueno
	3	Mg. Miguel Ángel Román Martínez García Ing. Sistemas. Maestro en GP.	4	Bueno
Confidencialidad de la información	1	Mg. Henry Lolan Vásquez Tuanama Especialista en Gestión de Proyectos Informáticos.	4	Bueno
	2	Dr. Miguel Ángel Valles Coral Ing. Sistemas. Doctor en GPyG	4	Bueno
	3	Mg. Miguel Ángel Román Martínez García Ing. Sistemas. Maestro en GP.	4	Bueno

Fuente. Elaboración propia

La tabla muestra la validez de expertos sobre los instrumentos de investigación, de las cuales se contó con una docente metodóloga y dos ingenieros de sistemas con doctorado en gestión pública y gobernabilidad y maestría en gestión pública y gobernabilidad. Teniendo un promedio de validez de 4 y una opinión de bueno para ambas variables de estudio.

Confiabilidad

En esta fase, se empleó el método estadístico conocido como Prueba Alfa de Cronbach. Este método se utilizará para evaluar la confiabilidad de los instrumentos a fin de que puedan aplicarse. En consecuencia, los resultados obtenidos a partir de las respuestas proporcionadas reflejaron la capacidad de dichos instrumentos para ser considerados válidos y coherentes.

Tabla 2

Confiabilidad del instrumento

Variables	**Coeficiente Alfa de cronbach**	**Nivel de consistencia**
Gobierno de datos	0.8146	Alta confiabilidad
Confidencialidad de la información	0.8034	Alta confiabilidad

Fuente. Elaboración propia

Para la variable Gobierno de datos, se obtuvo un coeficiente alfa de Cronbach de 0.8146. Para la variable de confidencialidad de información se consiguió un alfa de Cronbach de 0.8034. Concluyendo que los instrumentos tuvieron alta confiabilidad para su aplicación en la investigación.

3.5. Procedimientos

En cuanto a los procedimientos, se realizó una evaluación de la confidencialidad de la información antes y después del plan de gobierno de datos. Pre-test: Se llevó a cabo una prueba preliminar para evaluar cuanto conoce el personal de los establecimientos de salud acerca de la confidencialidad de la información antes de iniciar la investigación. Post-test: Se realizó una prueba posterior con la finalidad de evaluar el grado de entendimiento del personal de los establecimientos de salud sobre la confidencialidad de la información después de llevar a cabo la investigación.

3.6. Método de análisis de datos

La recopilación de la información se llevó a cabo usando los instrumentos validados por expertos respecto al hospital de Moyobamba y centro de salud Jerillo. Se aplicó una encuesta a los responsables de manejar la información confidencial de pacientes, trabajadores e institución. Para procesar los datos, se tuvo en cuenta el uso de Excel, el cual permitió tabular los datos recolectados mediante los instrumentos. Posteriormente, los resultados se presentaron en tablas específicas que se ajustan a las variables y dimensiones correspondientes.

3.7. Aspectos éticos

Con el propósito de garantizar la rigurosidad científica de la investigación, se tuvo en cuenta los criterios de beneficencia. El trabajo tuvo en cuenta los principios y conductas aceptables en la investigación, utilizando las normas el ISO para las citas respectivas y la normativa de la Universidad César Vallejo. También se promovió el bienestar general de la población a la cual se aplicó la investigación. Esto implica garantizar la utilidad de los datos recopilados para el avance del estudio, así como la difución de los hallazgos para beneficiar a la comunidad en general. En relación con el criterio de no maleficencia, los investigadores se aseguraron de que los involucrados no sufran ningún perjuicio como resultado de su participación. Esto garantizó la precisión de los datos recopilados y de que estos no se utilizan con fines diferentes a los previstos. Además, se respetó la autonomía de los participantes, proporcionándoles datos acerca los riesgos y ventajas de la investigación, permitiéndoles decidir libremente si desean participar o no. Por último, se garantizó la justicia en la investigación, tratando a los participantes de manera equitativa, sin discriminación.

IV. RESULTADOS

Prueba de normalidad

Por tener una muestra no mayor a 50, se empleó la prueba estadística Shapiro Wilk. Para que exista normalidad en los datos, estos deberán superar el nivel de significancia asumida del 5 % ($p > 0,05$), caso contrario, se asume que los datos no tienen una distribución normal ($p < 0,05$).

Dimensión 1: Acceso Restringido

Tabla 3

Prueba de normalidad el acceso restringido

	Shapiro-Wilk		
	Estadístico	gl	Sig.
ARYTS_Pretest	,865	50	,000
ARYTS_PosTest	,765	50	,000

Fuente: Datos propio del estudio

Los valores obtenidos de la tabla 3 en la dimensión acceso restringido en el pre-test fue de 0,000 (< 0.05), y en el post-test indica que el valor fue de 0,000 (< 0.05), de esta forma se evidenció que la variable cumple con la distribución no normal.

Dimensión 2: Transmisión segura

Tabla 4

Prueba de normalidad del acceso restringido y transmisión segura.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
ARYTS_Pretest	,880	50	,000
ARYTS_PosTest	,802	50	,000

Fuente: Datos propio del estudio

Los valores obtenidos de la tabla 4 en la dimensión acceso y restringido y transmisión segura en el pre-test fue de 0,000 (< 0.05), y en el post-test indica que el valor fue de 0,000 (< 0.05), de esta forma se evidenció que la variable cumple con la distribución no normal.

Dimensión 3: Almacenamiento protegido

Tabla 5

Prueba de normalidad para evaluar el almacenamiento protegido.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
AP_Pretest	,871	50	,000
AP_PosTest	,793	50	,000

Fuente: Datos propio del estudio

Los valores obtenidos de la tabla 5 en la dimensión almacenamiento protegido en el pre-test fue de 0,000 (< 0.05), y en el post-test indica que el valor fue de 0,000 (< 0.05), de esta de esta forma se evidenció que la variable cumple con la distribución no normal.

Dimensión 4: Políticas y procedimientos

Tabla 6

Prueba de normalidad para evaluar las políticas y procedimientos

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PYP_Pretest	,862	50	,000
PYP_PosTest	,803	50	,000

Fuente: Datos propio del estudio

Los valores obtenidos de la tabla 6 en la dimensión políticas y procedimiento en el pre-test fue de 0,000 (< 0.05), y en el post-test indica que el valor fue de 0,000 (< 0.05), de esta de esta forma se evidenció que la variable cumple con la distribución no normal.

Dimensión 5: Auditoria y monitoreo

Tabla 7

Prueba de normalidad para evaluar la auditoría y monitoreo.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
AYM_Pretest	,627	50	,000
AYM_PosTest	,481	50	,000

Fuente: Datos propio del estudio

Los valores obtenidos de la tabla 7 en la dimensión auditoria y monitoreo en el pre-test fue de 0,000 (< 0.05), y en el post-test indica que el valor fue de 0,000 (< 0.05), de esta de esta forma se evidenció que la variable cumple con la distribución no normal.

Prueba de hipótesis

Para el contraste de la hipótesis de la investigación se trabajó con la prueba no paramétrica Wilcoxon, debido a que los datos inmersos en el análisis no siguen una distribución normal y debido a que la información pertenece a muestras relacionadas, es decir, los mismos en el pre y post test.

Nivel de significación:

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

Regla de decisión

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

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

Prueba de hipótesis específica 1

Ha: El plan de gobierno de datos mejora el acceso restringido en establecimientos de salud de la Región San Martín 2023.

Ho: El plan de gobierno de datos no mejora el acceso restringido en establecimientos

de salud de la Región San Martín 2023.

Tabla 8

Prueba de Wilcoxon para medir el Acceso Restringido

Estadísticos de prueba[a]	
	Acceso Restringido_PreTest Acceso Restringido _PostTest
Z	-5,224[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

En la tabla 8, al aplicar la estadística se obtuvo un p-valor de (p=0,000 que es menor a α= 0.05), obteniendo como evidencia para rechazar la hipótesis nula, lo que nos lleva afirmar que existe una mejora significativa en el acceso restringido en los establecimientos se salud de la región San Martin periodo 2023, después de la implementación del plan de gobierno de datos.

Prueba de hipótesis específica 2

Ha: El plan de gobierno de datos mejora la transmisión segura en establecimientos de salud de la Región San Martín 2023.

Ho: El plan de gobierno de datos no mejora la transmisión segura en establecimientos de salud de la Región San Martín 2023.

Tabla 9

Prueba de Wilcoxon para medir la transmisión segura.

Estadísticos de prueba[a]	
	Transmisión Segura_PreTest Transmisión Segura _PostTest
Z	-5,202[b]
Sig. asintótica(bilateral)	,000

Fuente: Datos propio del estudio

En la tabla 9, al aplicar la estadística se obtuvo un p-valor de (p=0,000 que es menor

a α= 0.05), obteniendo como evidencia para rechazar la hipótesis nula, lo que nos lleva afirmar que existe una mejora significativa de la transmisión segura de datos en los establecimientos se salud de la región San Martin periodo 2023, después de la implementación del plan de gobierno de datos.

Prueba de hipótesis específica 3

Ha: El plan de gobierno de datos mejora el almacenamiento protegido en establecimientos de salud de la Región San Martín 2023.

Ho: El plan de gobierno de datos no mejora el almacenamiento protegido en establecimientos de salud de la Región San Martín 2023.

Tabla 10

Prueba de Wilcoxon para medir el Almacenamiento protegido.

Estadísticos de prueba[a]	
	Almacenamiento protegido_PreTest Almacenamiento protegido _PostTest
Z	-4,998[b]
Sig. asintótica(bilateral)	,000

Fuente: Datos propio del estudio

En la tabla 10, al aplicar la estadística se obtuvo un p-valor de (p=0,000 que es menor a α= 0.05), obteniendo como evidencia para rechazar la hipótesis nula, lo que nos lleva afirmar que existe una mejora en el almacenamiento protegido en establecimientos de salud se salud de la región San Martin periodo 2023, después de la implementación del plan de gobierno de datos.

Prueba de hipótesis específica 4

Ha: El plan de gobierno de datos mejora las políticas y procedimientos en establecimientos de salud de la Región San Martín 2023.

Ho: El plan de gobierno de datos no mejora las políticas y procedimientos en establecimientos de salud de la Región San Martín 2023.

Tabla 11

Prueba de Wilcoxon para medir las Políticas y procedimientos

Estadísticos de prueba[a]	
	Políticas y procedimientos_PreTest Políticas y procedimientos _PostTest
Z	-5,846[b]
Sig. asintótica(bilateral)	,000

Fuente: Datos propio del estudio

En la tabla 11, al aplicar la estadística se obtuvo un p-valor de (p=0,000 que es menor a α= 0.05), obteniendo como evidencia para rechazar la hipótesis nula, lo que nos lleva afirmar que existe una mejora significativa en las políticas y procedimientos en establecimientos de salud de la región San Martin periodo 2023, después de la implementación del plan de gobierno de datos.

Prueba de hipótesis específica 5

Ha: El plan de gobierno de datos mejora la auditoría y monitoreo en establecimientos de salud de la Región San Martín 2023.

Ho: El plan de gobierno de datos no mejora la auditoría y monitoreo en establecimientos de salud de la Región San Martín 2023.

Tabla 12

Prueba de Wilcoxon para medir la Auditoria y monitoreo

Estadísticos de prueba[a]	
	Auditoria y monitoreo _PreTest Auditoria y monitoreo_PostTest
Z	-6,263[b]
Sig. asintótica(bilateral)	,000

Fuente: Datos propio del estudio

En la tabla 12, al aplicar la estadística se obtuvo un p-valor de (p=0,000 que es menor a α= 0.05), obteniendo pruebas contundentes para descartar la hipótesis nula, lo que nos lleva afirmar el plan de gobierno de datos mejora la auditoría y monitoreo en establecimientos de salud de la Región San Martín 2023.

V. DISCUSIÓN

En el primer objetivo específico, se buscó mejorar el acceso restringido en establecimientos de salud de la región San Martín durante el periodo 2023. Los resultados obtenidos en esta investigación muestran discrepancias en comparación con los obtenidos por Orozco et al. (2021), quienes identificaron deficiencias en la gobernanza de datos en 12 hospitales. Según sus hallazgos, la normativa para acceder y utilizar los datos es general, y carecen de mecanismos efectivos de control para supervisar la calidad y transparencia en su manejo, es decir, no cuentan con un acceso restringido a los datos. Asimismo, Morales (2022), En su estudio se evidencia que en la dimensión de Gobierno de Datos se registró un promedio de 1.53. El puntaje mínimo posible por dimensión es de 1, por lo tanto, el resultado obtenido es muy bajo. Los participantes señalaron que no hay un Gobierno de Datos o que desconocen su existencia, careciendo de información sobre sus funciones, responsabilidades y posibles implicaciones dentro de la empresa. Estos hallazgos son análogos a los de la investigación actual, ya que el personal de algunos establecimientos de salud en la región de San Martín desconoce la existencia de un Gobierno de Datos y, por ende, no comprenden su importancia ni los beneficios que podrían obtener al implementarlo.

En el segundo objetivo, se buscó mejorar la transmisión segura en establecimientos de salud de la Región San Martin periodo 2023. Asimismo, se observaron diferencias con los resultados obtenidos por Morales (2022), quien señala que la Empresa Universitaria de Salud EUS – EP carecía de una Gobernanza de Datos implementada. Además, La privacidad significa que los usuarios tienen control sobre quién tiene transmisión a sus datos (Santiago-González et al., 2019).

En el tercer objetivo, se buscó mejorar el almacenamiento protegido de datos en establecimientos de salud de la Región San Martin periodo 2023. Asimismo, los resultados obtenidos muestran coincidencias con los resultados de los autores García-Ahumada y León-Jiménez (2020) señalan que el plan de gobierno de datos para el sector salud se enfoca en proporcionar servicios sanitarios de calidad a los

ciudadanos. Esto se puede alcanzar mediante la ejecución de diferentes políticas orientadas a la transformación digital, las cuales abarcan inversiones en tecnología para mejorar la capacidad de almacenamiento de grandes volúmenes de datos. El gobierno de datos en el sector salud es crucial para garantizar la seguridad y calidad de la información de los pacientes, así como para asegurar la precisión, coherencia y adecuación de la información (Attaran, 2020).

En el cuarto objetivo, se buscó mejorar las políticas y procedimientos en establecimientos de salud de la Región San Martin periodo 2023. Estos resultados muestran diferencia con la investigación Solà, et al. (2023), cuyos resultados evidenciaron varias deficiencias en las prácticas actuales de protección de la información, como por mencionar algunas políticas claras, la escasa capacitación del personal y la ausencia de medidas tecnológicas adecuadas. Indicando que un plan de gobierno de datos podría ser una estrategia efectiva para abordar estas deficiencias y que existe una brecha significativa en la confidencialidad de la información en establecimientos de salud. Además, Hernández (2019), menciona que existe diferentes métodos para proteger los datos de la información en los establecimientos de salud uno de ellos es desarrollar políticas y protocolos de protección de datos. Asimismo, en esta investigación muestra similitudes con el estudio de Morejón et al. (2020). quienes evidenciaron que, tras la implementación de un sistema hospitalario en diversas organizaciones de salud, los resultados indicaron que el 89% de los centros de salud estaban mejor preparados para ofrecer servicios con la nueva aplicación. Esto demuestra que la implantación del sistema hospitalario fue exitosa y proporcionó a las organizaciones de salud un aumento significativo en la eficacia de la prestación de servicios. En la investigación realizado por (Avalo, Fernández, 2020) Presentan similitudes con los resultados obtenidos, donde se demuestra que más del 92% de los centros informan tener medidas técnicas para prevenir el acceso o divulgación no autorizados de datos por parte de terceros. También señalan que el personal está al tanto de sus responsabilidades en relación con la protección de datos. Es relevante destacar que este hallazgo contrasta con el porcentaje de hospitales que proporcionan capacitación a su

personal sobre protección de datos, el cual es solo del 74%. En términos de otras medidas de seguridad, el 96% de los hospitales requieren que los usuarios se autentifiquen con una clave y contraseña para acceder a los datos, y en el 95% de los casos, el personal solo puede acceder a datos o recursos autorizados. Resultados similares a la presente investigación.

En el objetivo cinco, se buscó mejorar la auditoria y monitoreo en los establecimientos de salud de la Región San Martin periodo 2023. Los resultados obtenidos en la presente investigación arrojaron una meda de 4,10 (valores: mínimo 3 y máximo de 5) después de la implementación del gobierno de datos. Estos resultados muestran similitudes con la investigación de Hernández (2021), quien encontró que 80 % de los hospitales han implementado medidas para garantizar la confidencialidad y privacidad de los datos de los pacientes. Estas medidas cumplen con las normas de privacidad establecidas, creando un entorno seguro y protegiendo la dignidad de los pacientes involucrados. Además, señala que el sistema de atención a los pacientes puede mejorarse de manera eficaz y segura, lo que permite llevar a cabo investigaciones significativas aplicables a la mejora del servicio para los pacientes. Además, Morales (2022) indica que la gestión de datos cuenta con dimensiones y una de ellas es la protección y privacidad de la información, está basado en el cumplimiento de regulaciones, número de auditorías y el tiempo en responder los incumplimientos de los mismos. En la investigación realizado por (Avalo, Fernández, 2020) presentan similitudes con los resultados obtenidos, evidencian que únicamente el 25% de los centros llevaba a cabo auditorías para verificar si el personal autorizado utilizaba los datos de acuerdo con la finalidad justificada para acceder a ellos. Además, el 45% de los centros había realizado la auditoría bienal necesaria para garantizar la seguridad del Fichero de Historias Clínicas. No obstante, como aspecto positivo, el 95% de los centros aseguraba que los locales que albergaban los dispositivos de almacenamiento se cerraban cuando no había personal de la organización para su custodia. Asimismo, Morales (2022), Los resultados promedio de la investigación reflejan valoraciones bajas en las diferentes dimensiones, en mayor parte inferiores a dos en una escala

de cuatro puntos. A excepción de la dimensión “Gestión de datos empresariales e inteligencia de negocio", donde los resultados indican la ausencia de un seguimiento o monitoreo al diseño de los datos o procesos creados. Aunque tienen un proceso para el almacenamiento de datos, no se llevan a cabo evaluaciones que verifiquen el cumplimiento y permitan, identificar mejoras o realizar mejoramientos. Estos hallazgos se asemejan a los de la investigación actual, ya que en algunos centros de salud de la región San Martin no existe un monitoreo o seguimiento para asegurar el cumplimiento del gobierno de datos.

VI. CONCLUSIONES

Se concluye que, con la implementación de un plan de gobierno para garantizar la privacidad de los datos en establecimientos de salud, se logró mejorar el acceso restringido a la información en establecimientos de salud. Con un p-valor de 0.000, inferior a 0.05, concluyendo así que se ha cumplido con el objetivo establecido.

Con la implementación de un plan de gobierno para garantizar la confidencialidad de la información en establecimientos de salud, se logró mejorar la transmisión segura de los datos en establecimientos de salud. Con un p-valor de 0.000, inferior a 0.05, concluyendo así que se ha cumplido con el objetivo establecido.

Con la implementación de un plan de gobierno para garantizar la confidencialidad de la información en establecimientos de salud, se logró mejorar el almacenamiento protegido de los datos en establecimientos de salud. Con un p-valor de 0.000, inferior a 0.05, concluyendo así que se ha cumplido con el objetivo establecido.

Con la implementación de un plan de gobierno para garantizar la confidencialidad de la información en establecimientos de salud, se logró mejorar las políticas y procedimientos en establecimientos de salud. Con un p-valor de 0.000, inferior a 0.05, concluyendo así que se ha cumplido con el objetivo establecido.

Con la implementación de un plan de gobierno para garantizar la confidencialidad de la información en establecimientos de salud, se logró mejorar la auditoria y monitoreo en establecimientos de salud. Con un p-valor de 0.000, inferior a 0.05, concluyendo así que se ha cumplido con el objetivo establecido.

VII. RECOMENDACIONES

Se sugiere continuar fortaleciendo el plan de gobierno implementado para garantizar la confidencialidad de la información en los establecimientos de salud investigados. Esto asegurará la consolidación y mejora continua de las medidas de seguridad, promoviendo así un entorno confiable en la gestión de la información.

Se sugiere fortalecer el acceso restringido a los datos en los establecimientos de salud estudiados. Esta acción contribuirá a mejorar la seguridad y confidencialidad de los datos, fortaleciendo así la integridad del sistema de gestión de la información en el ámbito sanitario.

Se sugiere continuar fortaleciendo el almacenamiento protegido de datos en los establecimientos de salud investigados. Esta medida contribuirá a garantizar una mayor seguridad y confidencialidad en el manejo de la información, consolidando así prácticas efectivas en el resguardo de los datos sensible.

Se recomienda proporcionar capacitación al personal sobre la relevancia de mantener la confidencialidad de la información en los establecimientos de salud. Esto garantizará que el personal esté consciente de la trascendencia de proteger la privacidad de los pacientes y evitar la divulgación no autorizada de información sensible. Esta capacitación asegurará una comprensión profunda de la relevancia de mantener la confidencialidad, fortaleciendo así la seguridad y protección de los datos en el entorno sanitario.

Se sugiere realizar auditorías y monitoreo de datos en los establecimientos de salud investigados de salud para asegurar la efectividad en la implementación del plan de gobierno y garantizar la confidencialidad de la información Esto permitirá evaluar y fortalecer continuamente las medidas de seguridad, creando así un entorno confiable y protegido para la administración de la información en el ámbito de la salud. Esta medida ayudará a evaluar y mejorar constantemente las medidas de seguridad, garantizando un entorno seguro y confiable para la administración de la información en el campo de la salud.

REFERENCIAS

Abraham, R., Schneider, J., & Brocke, J. v. (2019). Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management, 49(1), 424-438. doi:https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Aguerre, C. (2020). Estrategias nacionales de IA y gobernanza de datos en la región. Revista CeTyS, 1(1), 1-27. https://proyectoguia.lat/wp-content/uploads/2020/05/Aguerre-Estrategias-nacionales-de-IA-y-gobernanza-de-datos-en-la-region.pdf

Arias, J. L., & Covinos, M. (2021). Diseño y metodología de la investigación. Arequipa: Enfoques Consulting EIRL. https://repositorio.concytec.gob.pe/handle/20.500.12390/2260

Attaran, M. (2020). Blockchain-enabled healthcare data management: a potential for COVID-19 outbreak to reinforce deployment. International Journal of Business Information Systems, 1(1), 1-21. doi:http://dx.doi.org/10.1504/IJBIS.2020.10034132

Ávalos, S., & Fernández, N. (2020). Evolución histórica del cumplimiento de la normativa de protección de datos en hospitales públicos de España. Scielo, 14(1), 1-16. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1988-348X2020000100014

Banco de Desarrollo de América Latina. (2021). Gobernanza de datos y capacidades estatales para la pospandemia. https://scioteca.caf.com/bitstream/handle/123456789/1765/Gobernanza%20de%20datos%20y%20capacidades%20estatales%20para%20la%20pospandemia.pdf?sequence=1&isAllowed=y

Benfeldt, O., Stouby, J., & Madsen, S. (2020). Data Governance as a Collective Action

Problem. Information Systems Frontiers, 22(1), 299–313. doi:https://doi.org/10.1007/s10796-019-09923-z

Caruccio, L., Desiato, D., & Polese, G. (2020). GDPR Compliant Information Confidentiality Preservation in Big Data Processing. 8, 205034-205050. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9252876

Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica. (2020). Reglamento de calificación, clasificación y registro de los Investigadores del sistema nacional de ciencia, tecnología e innovación tecnológica - Reglamento RENACYT. Lima, Perú: CONCYTEC. https://cdn.www.gob.pe/uploads/document/file/1423550/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20LA%20FORMULACI%C3%93N%20Y%20EJECUCI%C3%93N%20%20DE%20PROYECTOS%20DE%20INVESTIGACI%C3%93N%20Y%20DESARROLLO-04-11-2020.pdf.pdf

Defensoría del Pueblo (2019). Manual de protección de datos personales. Lima, Perú. https://www.defensoria.gob.pe/wp-content/uploads/2019/11/Manual-de-Protecci%C3%B3n-de-Datos-Personales.pdf

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Sushil, P., Swaminathan, A., Wang, F. (2022). ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. J Med Internet Res, 22(8), e13598. doi:https://doi.org/10.2196/13598

El Peruano (16 de Junio del 2023). Decreto Legislativo 1412, que aprueba la ley de gobierno digital. Lima, Perú. https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1/

EL PERUANO. Ley de Ciberdefensa. (27 de Agosto del 2019). Lima, Perú. https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-30999-1801519-5/

Flores, J., & Barbarán, H. (2021). Gestión Hospitalaria: una mirada aldesarrollo de sus

procesos. Revista Científica Multidisciplinar, 5(2), 1527-1545. doi:https://doi.org/10.37811/cl_rcm.v5i2.368

Francisco, X., & Yarad, P. (2020). Análisis de las características del sector microempresarial en latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información. Revista Científica ECOCIENCIA, 7(1), 1-26. https://revistas.ecotec.edu.ec/index.php/ecociencia/article/view/303/233

García-Ahumada, F., & León-Jiménez, F. (2020). Mortalidad hospitalaria en un centro de alta complejidad del Ministerio de Salud, LambayequePerú, 2014-2018. Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo, 13(2), 175-182. doi:https://doi.org/10.35434/rcmhnaaa.2020.132.669

Gutierrez, D., Chávez, G., Santizo, N., García, Y., Morasen, E., & Duany, L. (2020). La importancia del gobierno de datos en el sector sanitario La importancia del gobierno de datos en el sector sanitario. Revista Cubana de tecnología de la salud, 11(1), 49-56. https://revtecnologia.sld.cu/index.php/tec/article/view/1818/1391

Hernández, E., & Mancilla, P. (2021). Confidencialidad de datos en un hospitales cuela dedicado a la investigación. Revista Latinoamericana de Bioética, 21(2), 41-55. doi:https://doi.org/10.18359/rlbi.5111

Hernández-Mier, C. (2019). Acceso al expediente clínico en Establecimientos de Atención Médica en México con fines de investigación. Revista Conamed, 24(2), 57-63. https://www.medigraphic.com/pdfs/COMPLETOS/conamed/2019/con192.pdf#page=5

Janssen, M., & Brous, P. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. Government Information Quarterly, 37(3), 101493. doi:https://doi.org/10.1016/j.giq.2020.101493

Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS

storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing, 164, 152-167. doi:https://doi.org/10.1016/j.jpdc.2022.03.009

Kandabongee, P., Muhammad, A., Luyi, S., & Bian, Y. (2022). Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development. Advancing digital Health & Open Science, 9(2), 1-9. Obtenido de https://humanfactors.jmir.org/2022/2/e30050/

Kumar, S., Sunitha, T., Manda, S., Ratnam, V., & Chidurala, S. (2021). Maintaining confidentiality when sharing health information with CloudLet. International Journal of Computational Intelligence in Control, 13(2), 176-186. Obtenido de https://www.mukpublications.com/resources/15.%20Maintaining%20confidentiality%20when%20sharing%20health%20information%20with%20CloudLet_pagenumber.pdf

Lema, C., & Cuenca, J. (2020). Plan de gestión de seguridad de la información. Journal of Science and Research: Revista Ciencia e Investigación, 5(4), 62-75. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7634599

Li, V., Ma, L., & Wu, X. (2022). COVID-19, policy change, and post-pandemic data governance: a case analysis of contact tracing applications in East Asia. Policy and Society, 41(1), 129–142. doi:https://doi.org/10.1093/polsoc/puab019

Mat, S., Chow, K., Nawi, N., Hooi-Ten, D., & Maarop, N. (2021). Mejores prácticas para implementar un gobierno de datos. Revista Internacional Abierta de Informática (OIJI), 9(2), 7–12. doi:https://doi.org/10.11113/oiji2021.9n2.154

Mella, M., Velázquez, T., Aranaz, J., Ramos, G., & Compañ, A. (2020). Análisis de la cultura de seguridad del paciente en un hospital universitario. Gaceta Sanitaria, 34(5), 500-513. doi:https://dx.doi.org/10.1016/j.gaceta.2018.10.004

Miranda, O., Ortiz, T., & Yuen, V. (2019). Nuevos retos en la protección de la vida y salud de las mujeres. Revista Peruana de Ginecología y Obstetricia, 65(3), 293-298. doi:https://doi.org/10.31403/rpgo.v66i2184

Mohammad, S., Landman, A., & Gordon, W. (2020). Telemedicine, privacy, and information security in the age of COVID-19. Journal of the American Medical Informatics Association, 28(3), 671–672. Obtenido de https://watermark.silverchair.com/ocaa310.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAAsMwggK_BgkqhkiG9w0BBwaggggKwMIICrAIBADCCAqUGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMDrcWmufVAYbidV3KAgEQgIICdo2fSbcIbAHT8cZhPoLerWkesigu0METu2mzDG6uknSQ02N

Morales, A. D. (2022). Guía metodológica para la implementación de gobernanza de datos en la Empresa Universitaria de Salud EUS – EP de la Universidad de Cuenca. Tesis de maestría, Pontificia Universidad Católica del Ecuador, Quito, Ecuador. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/21177/Trabajo%20titulaci%c3%b3n%20Gobernanza%20de%20Datos%20EUS-EP.pdf?sequence=1&isAllowed=y

Morejón, M., Ramírez, J., Pérez, A., & Ramírez, A. (2020). Estrategia para la implantación del Sistema XAVIA HIS en instituciones hospitalarias. Revista Cubana de Informática Médica, 12(1), 3-19. Obtenido de https://www.medigraphic.com/pdfs/revcubinfmed/cim-2020/cim201b.pdf

Morón, K.R. (2023). Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C. (Tesis de pre grado, Universidad Señor de Sipán). Repositorio de Señor de Sipán. https://repositorio.uss.edu.pe/handle/20.500.12802/10629

Nissán, E. (2019). Hacia un nuevo modelo de gobernanza para la promoción de la salud. Buen Gobierno, 1(46), 1-28. Obtenido de https://www.redalyc.org/journal/5696/569660606002/html/

Olguin, M.A. (2023). Modelamiento e implementación de un plan de gobierno de datos en la universidad de chile utilizando el framework dama. (Tesis de pre grado,

Universidad de Chile). Repositorio de la universidad de Chile. https://repositorio.uchile.cl/bitstream/handle/2250/193748/Modelamiento-e-implementacion-de-un-plan-de-gobierno-de-datos-en-la-Universidad-de-Chile-utilizando-el-framework-DAMA.pdf?sequence=1&isAllowed=y

Orozco, F., Guaygua, S., Lopez, D. H., Muñoz, F., & Urquia, M. L. (2021). Vinculación de datos administrativos y su utilidad en salud pública: el caso de Ecuador/Vinculacion de datos administrativos y su utilidad en salud publica: el caso de Ecuador. Revista Panamericana de Salud Pública, 45, 1. Obtenido de https://go.gale.com/ps/i.do?id=GALE%7CA663200393&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=10204989&p=HRCA&sw=w&userGroupName=anon%7E9ff09c74&aty=open+web+entry

Peng-Ting, C., Chia-Li, L., & Wan-Ning, W. (2020). Big data management in healthcare: Adoption challenges and implications. International Journal of Information Management, 53(1), 102078. doi:https://doi.org/10.1016/j.ijinfomgt.2020.102078

Preciado, A., Valles, M., & Lévano, D. (2021). Importancia del uso de sistemas de información en la automatización de historiales clínicos, una revisión sistemática. Revista Cubana de Informática Médica, 13(1), 1-11. Obtenido de http://scielo.sld.cu/pdf/rcim/v13n1/1684-1859-rcim-13-01-e417.pdf

Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in health care. Journal of the American Medical Informatics Association, 27(3), 491–497. doi:https://doi.org/10.1093/jamia/ocz192

Rosa, J., & Frutos, E. (2022). Ciencia de datos en salud: desafíos y oportunidades en América Latina. Revista Médica Clínica Las Condes, 33(6), 591-597. Obtenido de https://pdf.sciencedirectassets.com/312299/1-s2.0-S0716864022X00072/1-s2.0-S0716864022001183/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEIz%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJHMEUCICGvOgXuiaYhi3Ef%2FIy0iPU5eLUs4gtQEqmcdCm4hdWGAiEA3YD7brnJCl

Rosales, M., Gómez, M., & Borré, F. (2020). Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit. Revista Aglala, 11(1), 227–245. Obtenido de https://revistas.curn.edu.co/index.php/aglala/article/view/1579

Santiago-González, N., Morales-García, D., Ibarra-Cerón, M., & López-Jacinto, E. (2019). Cultura de seguridad del paciente en un hospital de alta especialidad. Revistade enfeRmeRía neuRológica, 18(3), 115-123. doi:https://doi.org/10.51422/ren.v18i3.288

Sisalema-Rivera, K. L., Esteves-Fajardo, Z. I., Quito-Esteves, A. C., & Melgar-Ojeda, K. A. (2022). Modelo de gobierno abierto para la calidad del servicio en hospitales. CIENCIAMATRIA, 8(3), 558-569. doi:https://doi.org/10.35381/cm.v8i3.789

Solà-Morales, O., Sigurðardóttir, K., Akehurst, R., Murphy, L. A., Mestre-Ferrandiz, J., Cunningham, D., & Pouvourville, G. (2023). Data Governance for Real-World Data Management: A Proposal for a Checklist to Support Decision Making. Value in Health, 26(4), 32-42. doi:https://doi.org/10.1016/j.jval.2023.02.012

Tanwar, S., Parekh, K., & Evansb, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Revista de Seguridad de la Información y Aplicaciones, 50, 102407. doi:https://doi.org/10.1016/j.jisa.2019.102407

Vega, E. (2021). Seguridad de la información. Area sw Innovacion y Desarrollo S.L. Obtenido de https://books.google.es/books?hl=es&lr=&id=nx4uEAAAQBAJ&oi=fnd&pg=PA79&dq=metodos+de+seguridad+de+la+informaci%C3%B3n+en+un+hospital+&ots=Dcsgh6nNvA&sig=oUqRq4gVUa7PZe1YV4212r3STig#v=onepage&q=metodos%20de%20seguridad%20de%20la%20informaci%C3%B3n%20en%20u

Wu, Z., Xuan, S., Lin, C., & Lu, C. (2022). How to ensure the confidentiality of electronic

medical records on the cloud: A technical perspective. Computers in Biology and Medicine, 147, 1-10. doi:https://doi.org/10.1016/j.compbiomed.2022.105726

Zinelli, H. (2022). Gestión hospitalaria de un modelo de asociaciones público privadas y un modelo tradicional en dos hospitales del Callao. Revista De La Facultad De Medicina Humana, 22(2), 280-286. doi:https://revistas.urp.edu.pe/index.php/RFMH/article/view/4796

ANEXOS

Matriz operacionalización de variables

Variable	Definición conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Gobierno de datos	Para Power Data, está relacionada con la capacidad de que una institución tenga información y sepa gestionarla, sobre todo el conocimiento que tenga de la información, el registro, origen, resguardo y modo de uso (Como se citó en Olguín, 2023).	Tiene que ver con el proceso de garantizar que los datos sean usados de manera efectiva, segura, coherente. Siguiendo la gestión de datos, su calidad, la seguridad y privacidad, cumplimeinto normativo, arquitectura de datos, y responsabilidad de roles.	Gestión de datos maestros	Calidad de los datos: -Porcentaje de registros -duplicados en los datos maestros. -Porcentaje de registros con errores o -inconsistencias. Tiempo promedio de respuesta para resolver -problemas de calidad de datos. Número de -incidentes de calidad de datos reportados.	ordinal
			Calidad de datos	Seguridad y privacidad de los datos: -Número de violaciones de seguridad de datos. -Nivel de cumplimiento de políticas de seguridad y privacidad. -Tiempo promedio de respuesta ante incidentes de seguridad. -Porcentaje de datos sensibles o confidenciales encriptados.	

			Seguridad y privacidad de los datos	Cumplimiento normativo: -Porcentaje de cumplimiento de regulaciones y leyes relevantes. -Número de auditorías de datos exitosas. -Porcentaje de políticas y procedimientos documentados y actualizados. -Tiempo promedio de respuesta para abordar incumplimientos identificados.	
			Cumplimiento normativo	Gestión de datos maestros: -Porcentaje de datos maestros completos y actualizados. -Número de solicitudes o consultas relacionadas con datos maestros. -Porcentaje de registros de datos maestros correctamente vinculados y referenciados. -Tiempo promedio para la resolución de problemas o	

				solicitudes relacionadas con datos maestros.	
			Arquitectura de datos	Arquitectura de datos: -Porcentaje de aplicaciones y sistemas integrados con la arquitectura de datos. -Número de puntos de integración implementados con éxito. -Tiempo promedio para el diseño e implementación de cambios en la arquitectura de datos. -Número de problemas o errores relacionados con la arquitectura de datos identificados y resueltos.	
			Responsabilidades y roles	La calidad y la integridad de los datos que son responsables de la propiedad y el uso de los datos.	

Matriz de operacionalización de la variable Confidencialidad de la información

Variable	Definición conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de Medición
Confidencialidad de la información	Según Chopra y Chaudhary, indica que la confidencialidad tiene que ver con la protección de la información, para el no acceso a la información de personas no autorizadas, dado que la información es preciada para que las autoridades tomen decisiones (Como se citó en Morón, 2023).	La confidencialidad de la información se refiere a la protección y privacidad de los datos sensibles y privilegiados, evitando su divulgación o acceso no autorizado. Implica mantener la información en secreto y limitar su	acceso restringido	1. Acceso restringido	Ordinal
			Transmisión segura.	2. Encriptación	
			Almacenamiento protegido	3. Auditoría y registro de actividades	
			Políticas y procedimientos	4. Protección contra malware y ataques cibernéticos	
			Auditoría y monitoreo	5. Políticas y procedimientos	
				6.Seguridad física	
				7. Protección de la información durante su ciclo de vida	

Instrumento de recolección de datos

CUESTIONARIO

Gobierno de datos

Buenos (as) días (tardes), como estudiante de la escuela de posgrado de la Universidad César Vallejo hago presente este cuestionario diseñado con fines académicos con el propósito de Implementar un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023. Es por ello que solicito a usted responder de manera sincera marcando con un aspa (X) en el recuadro que contenga la alternativa más certera, considerando lo presentado a continuación:

Escala	
Muy bajo	1
Bajo	2
Regular	3
Alto	4
Muy alto	5

Enunciado	MA	A	R	B	MB
Dimensión Gestión de datos maestros	5	4	3	2	1
1. Valore la calidad de datos duplicados en los datos maestros					
2. Valore el nivel de registros de datos con errores o inconsistencias.					
3. Valores el tiempo para resolver problemas de datos referentes a la calidad					
4. Valore el nivel de incidentes de calidad de datos reportados					

Calidad de datos					
5. Califique el nivel de violaciones de datos de seguridad en la institución					
6. Califique el nivel de incumplimiento a las políticas de seguridad y privacidad de los datos					
7. Califique el promedio de respuesta ante incidentes de seguridad de datos					
8. Califique el porcentaje de datos sensibles confidenciales o encriptados					
Seguridad y privacidad de los datos					
9. Califique el porcentaje de cumplimiento de regulaciones y leyes relevantes.					
10. Califique el número de auditorías de datos exitosos.					
11. Califique el nivel de políticas de procedimientos documentados y actualizados					
12. Califique el tiempo promedio de respuesta para abordar el incumplimiento de identificación de datos					
Cumplimiento normativo					
13. Califique el porcentaje de datos maestros actualizados.					
14. Califique el nivel de solicitudes consultadas respecto a los datos maestros					
15. Califique el registro de datos maestros correctamente vinculados y referenciados					
16. Califique el tiempo promedio para la resolución de problemas o solicitudes con datos maestros					
Arquitectura de datos					
17. Valore las aplicaciones y sistemas integrados con la arquitectura de datos.					
18. Califique los puntos de integración implementados con					

éxito.					
19. Valore el diseño e implementación de cambios en la arquitectura de datos.					
20. Valore el nivel de problemas o errores relacionados con la arquitectura de datos identificados y resueltos					
Responsabilidades y roles					
21. Valores la calidad y la integridad de los datos que son responsables de la propiedad y el uso de los datos					

CUESTIONARIO

Confidencialidad de la información

Buenos (as) días (tardes), como estudiante de la escuela de posgrado de la Universidad César Vallejo hago presente este cuestionario diseñado con fines académicos con el propósito de Implementar un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023. Es por ello que solicito a usted responder de manera sincera marcando con un aspa (X) en el recuadro que contenga la alternativa más certera, considerando lo presentado a continuación:

Escala	
Muy bajo	1
Bajo	2
Regular	3
Alto	4
Muy alto	5

N.°		**Escala**				
		1	**2**	**3**	**4**	**5**
D1	**Acceso restringido**					
1.	¿Cómo evalúa el nivel de acceso restringido de datos?					
D2	**Transmisión segura.**					
2.	¿Cómo valora el nivel de encriptación de los datos?					
D3	**Almacenamiento protegido**					
3.	¿Cómo califica el proceso de auditoría y registro de actividades?					
D4	**Políticas y procedimientos**					
4.	Como valora la protección contra malware y ataques cibernéticos					
D5	**Auditoría y monitoreo**					

5.	Como califica las políticas y procedimiento					
6.	Seguridad física					
7.	Cómo valora la protección de la información durante su ciclo de vida.					

Gracias por su valiosa participación.

Anexo 03. Solicitud de validación de los instrumentos y validación

Moyobamba, 10 de junio de 2023

Mg. Henry Lolan Vásquez Tuanama

Asunto: Evaluación de cuestionario

Espero que al recibir está carta se encuentre bien. Me complace escribirle para solicitar su colaboración en la validación de expertos para mi proyecto titulado "**Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023**". Como especialista en gestión de proyectos informáticos, creo que tu experiencia y conocimientos son esenciales para garantizar la calidad y la relevancia de mi investigación.

Mi proyecto se centra en implementar un plan de gobierno de datos y la confidencialidad de la información, y su contribución como experto en este campo sería inestimable. Tu revisión y evaluación crítica de mi trabajo ayudarán a asegurar que mis hallazgos sean precisos, sólidos y que estén alineados con las mejores prácticas en la confidencialidad de la información.

Agradezco de antemano tu consideración de esta solicitud y estaré encantado de proporcionarte cualquier información adicional que puedas necesitar sobre mi proyecto. Si decides colaborar, tus comentarios y sugerencias serán reconocidos en los agradecimientos de mi proyecto.

Aprecio mucho tu tiempo y consideración. Tu apoyo sería de gran valor para el éxito de mi proyecto de tesis.

Atentamente

TONY VARAS VALLES
DNI: 44116672

LEOPOLDO FLORES VASQUEZ
DNI: 76676131

Adjunto:

- Título de la investigación
- Matriz operatividad de variables
- Instrumento

CARTA A EXPERTOS PARA EVALUACIÓN DE GUIA DE OBSERVACIÓN

Tarapoto, 10 de junio de 2023

Dr. Miguel Ángel Valles Coral

Asunto: Evaluación de cuestionario

Espero que al recibir está carta se encuentre bien. Me complace escribirle para solicitar su colaboración en la validación de expertos para mi proyecto titulado "**Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023**". Como especialista en gestión pública y gobernabilidad, tu experiencia y conocimientos son esenciales para garantizar la calidad y la relevancia de mi investigación.

Mi proyecto se centra en implementar un plan de gobierno de datos y la confidencialidad de la información, y su contribución como experto en este campo sería inestimable. Tu revisión y evaluación crítica de mi trabajo ayudarán a asegurar que mis hallazgos sean precisos, sólidos y que estén alineados con las mejores prácticas en la confidencialidad de la información.

Agradezco de antemano tu consideración de esta solicitud y estaré encantado de proporcionarte cualquier información adicional que puedas necesitar sobre mi proyecto. Si decides colaborar, tus comentarios y sugerencias serán reconocidos en los agradecimientos de mi proyecto.

Aprecio mucho tu tiempo y consideración. Tu apoyo sería de gran valor para el éxito de mi proyecto de tesis.

Atentamente,

TONY VARAS VALLES
DNI: 44116672

LEOPOLDO FLORES VASQUEZ
DNI: 76676131

Adjunto:

- Título de la investigación
- Matriz operatividad de variables
- Instrumento

CARTA A EXPERTOS PARA EVALUACIÓN DE GUIA DE OBSERVACIÓN

Moyobamba, 10 de junio de 2023

Mg. Miguel Ángel Román Martínez García

Asunto: Evaluación de cuestionario

Espero que al recibir está carta se encuentre bien. Me complace escribirle para solicitar su colaboración en la validación de expertos para mi proyecto titulado "**Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023**". Como especialista en ingeniería de sistemas tu experiencia y conocimientos son esenciales para garantizar la calidad y la relevancia de mi investigación.

Mi proyecto se centra en implementar un plan de gobierno de datos y la confidencialidad de la información, y su contribución como experto en este campo sería inestimable. Tu revisión y evaluación crítica de mi trabajo ayudarán a asegurar que mis hallazgos sean precisos, sólidos y que estén alineados con las mejores prácticas en la confidencialidad de la información.

Agradezco de antemano tu consideración de esta solicitud y estaré encantado de proporcionarte cualquier información adicional que puedas necesitar sobre mi proyecto. Si decides colaborar, tus comentarios y sugerencias serán reconocidos en los agradecimientos de mi proyecto.

Aprecio mucho tu tiempo y consideración. Tu apoyo sería de gran valor para el éxito de mi proyecto de tesis.

Atentamente,

TONY VARAS VALLES
DNI: 44116672

LEOPOLDO FLORES VASQUEZ
DNI: 76676131

Adjunto:

- Título de la investigación
- Matriz operatividad de variables
- Instrumento

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento **Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023**.". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	**HENRY LOLAN VÁSQUEZ TUANAMA**
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (x) Organizacional ( )
Áreas de experiencia profesional:	**Especialista en Gestión de Proyectos informáticos**
Institución donde labora:	**Universidad César Vallejo**
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en Investigación Psicométrica: (si corresponde)	Trabajo(s) psicométricos realizados Título del estudio realizado.

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala (Colocar nombre de la escala, cuestionario o inventario)

Nombre de la Prueba:	**Cuestionario sobre gobierno de datos**
Autores:	**Leopoldo Flores Vasquez – Tony Varas Valles**
Procedencia:	**Elaboración Propia**
Administración:	
Tiempo de aplicación:	
Ámbito de aplicación:	**Salud**
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

UNIVERSIDAD CÉSAR VALLEJO

4. **Soporte teórico**

Escala/ÁREA	Subescala (dimensiones)	Definición
Ordinal		

5. **Presentación de instrucciones para el juez:**

A continuación, a usted le presento el cuestionario **sobre gobierno de datos** elaborado por Leopoldo Flores Vásquez y Tony Varas Valles. en el año 2023. De acuerdo con lossiguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento: Gestión de datos maestros, Calidad de datos, Seguridad y privacidad de los datos, Cumplimiento normativo, Arquitectura de datos, Responsabilidades y roles.

- Primera dimensión: (Gestión de datos maestros)

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Porcentaje de registros -duplicados en los datos maestros.	Valore la calidad de datos duplicados en los datos maestros	4	4	3	Sí cumple
		4	4	4	Sí cumple
-Porcentaje de registros con errores o -inconsistencias.	Valore el nivel de registros de datos con errores o inconsistencias…	4	4	4	Sí cumple
		3	4	4	Sí cumple
Tiempo promedio de respuesta para resolver -problemas de calidad de datos.	Valores el tiempo para resolver problemas de datos referentes a la calidad	4	4	3	Sí cumple
Número de -incidentes de calidad de datos reportados	Valore el nivel de incidentes de calidad de datos reportados	4	4	4	Sí cumple

- Segunda dimensión: Calidad de datos

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Número de violaciones de seguridad de datos.	Califique el nivel de violaciones de datos de seguridad en la institución	4	4	3	Sí cumple
Nivel de cumplimiento de políticas de seguridad y privacidad.	Califique el nivel de incumplimiento a las políticas de seguridad y privacidad de los datos	3	4	4	Sí cumple
Tiempo promedio de respuesta ante incidentes de seguridad.	Califique el promedio de respuesta ante incidentes de seguridad de datos	4	4	3	Sí cumple
Porcentaje de datos sensibles o confidenciales encriptados.	Califique el porcentaje de datos sensibles confidenciales o encriptados	4	4	4	Sí cumple

- Tercera dimensión: Seguridad y privacidad de los datos

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
-Porcentaje de cumplimiento de regulaciones y leyes relevantes.	Califique el porcentaje de cumplimiento de regulaciones y leyes relevantes.	4	4	3	Sí cumple
-Número de auditorías de datos exitosas.	Califique el número de auditorías de datos exitosos.	4	4	3	Sí cumple
-Porcentaje de políticas y procedimientos documentados y actualizados.	Califique el nivel de políticas de procedimientos documentados y actualizados	4	4	4	Sí cumple
Tiempo promedio de respuesta para abordar incumplimientos identificados	Califique el tiempo promedio de respuesta para abordar el incumplimiento de identificación de datos	4	4	3	Sí cumple

- Cuarta dimensión: Cumplimiento normativo

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Porcentaje de datos maestros completos y actualizados.	Califique el porcentaje de datos maestros actualizados.	4	4	3	Sí cumple
-Número de solicitudes o consultas relacionadas con datos maestros.	Califique el nivel de solicitudes consultadas respecto a los datos maestros	4	4	4	Sí cumple
-Porcentaje de registros de datos maestros correctamente vinculados y referenciados	Califique el registro de datos maestros correctamente vinculados y referenciados	4	4	3	Sí cumple
Tiempo promedio para la resolución de problemas o solicitudes relacionadas con datos maestros	Califique el tiempo promedio para la resolución de problemas o solicitudes con datos maestros	3	4	4	Sí cumple

- Quinta dimensión: Arquitectura de datos

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Porcentaje de aplicaciones y sistemas integrados con la arquitectura de datos.	Valore las aplicaciones y sistemas integrados con la arquitectura de datos.	4	4	3	Sí cumple

-Número de puntos de integración implementados con éxito.	Califique los puntos de integración implementados con éxito.	4	4	3	Sí cumple
-Tiempo promedio para el diseño e implementación de cambios en la arquitectura de datos.	Valore el diseño e implementación de cambios en la arquitectura de datos.	4	4	4	Sí cumple
-Número de problemas o errores relacionados con la arquitectura de datos identificados y resueltos.	Valore el nivel de problemas o errores relacionados con la arquitectura de datos identificados y resueltos	4	4	3	Sí cumple

- Sexta dimensión: Responsabilidades y roles

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
La calidad y la integridad de los datos que son responsables de la propiedad y el uso de los datos	Valores la calidad y la integridad de los datos que son responsables de la propiedad y el uso de los datos	3	4	4	Sí cumple

Firma del evaluador

DNI **41327678**

Pd.: el presente formato debe tomar en cuenta:

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento **Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023**.". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	**HENRY LOLAN VÁSQUEZ TUANAMA**
Grado profesional:	Maestría (x) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (x) Organizacional ( )
Áreas de experiencia profesional:	**Docente investigadora**
Institución donde labora:	**Universidad César Vallejo**
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala Ordinal, gobierno de datos

Nombre de la Prueba:	**Cuestionario sobre gobierno de datos**
Autores:	**Leopoldo Flores Vasquez – Tony Varas Valles**
Procedencia:	**Elaboración Propia**
Administración:	
Tiempo de aplicación:	
Ámbito de aplicación:	**Salud**
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

UNIVERSIDAD CÉSAR VALLEJO

4. **Soporte teórico**

Escala/ÁREA	Subescala (dimensiones)	Definición
Ordinal		

5. **Presentación de instrucciones para el juez:**

A continuación, a usted le presento el cuestionario **sobre gobierno de datos** elaborado por Leopoldo Flores Vásquez y Tony Varas Valles. en el año 2023. De acuerdo con lossiguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento: Dimensión acceso restringido y transmisión segura, almacenamiento protegido, políticas y procedimientos, auditoria y monitoreo.

- Primera dimensión: **Acceso restringido y Transmisión segura**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Acceso restringido	¿Cómo evalúa el nivel de acceso restringido de datos?	4	4	3	Sí cumple
Encriptación	¿Cómo valora el nivel de encriptación de los datos?	4	4	4	Sí cumple

- Segunda dimensión: **Almacenamiento protegido**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Auditoría y registro de actividades	Cómo califica el proceso de auditoría y registro de actividades	4	4	3	Sí cumple

- Tercera dimensión: **Políticas y procedimientos.**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Protección contra malware y ataques cibernéticos	Como valora la protección contra malware y ataques cibernéticos	4	4	3	Sí cumple

- Cuarta dimensión: **Auditoría y monitoreo.**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Políticas y procedimientos	Como califica las políticas y procedimiento	4	4	3	Sí cumple
Seguridad física	Seguridad física	4	4	4	Sí cumple
Protección de la información durante su ciclo de vida	Cómo valora la protección de la información durante su ciclo de vida.	4	4	3	Sí cumple

Firma del evaluador

DNI 41327678

Pd.: el presente formato debe tomar en cuenta:

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento **Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023**.". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	**MIGUEL ANGEL ROMAN MARTINEZ GARCÍA**
Grado profesional:	Maestría (X) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (X)
Áreas de experiencia profesional:	**Asistente de Sistemas**
Institución donde labora:	**Corte Superior de Justicia de San Martin**
Tiempo de experiencia profesional en el área:	2 a 4 años (X) Más de 5 años ( )
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala Ordinal, gobierno de datos

Nombre de la Prueba:	**Cuestionario sobre gobierno de datos**
Autores:	**Leopoldo Flores Vasquez – Tony Varas Valles**
Procedencia:	**Elaboración Propia**
Administración:	
Tiempo de aplicación:	
Ámbito de aplicación:	**Salud**
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

UNIVERSIDAD CÉSAR VALLEJO

4. Soporte teórico

Escala/ÁREA	Subescala (dimensiones)	Definición
Ordinal		

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el cuestionario **sobre gobierno de datos** elaborado por Leopoldo Flores Vásquez y Tony Varas Valles. en el año 2023. De acuerdo con lossiguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento: Dimensión Gestión de datos maestros, Calidda de datos, Seguridad y privacidad de los datos, Cumplimiento normativo, Arquitectura de datos, Responsabilidades y roles

- Primera dimensión: Dimensión Gestión de datos maestros,

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Porcentaje de registros -duplicados en los datos maestros.	Valore la calidad de datos duplicados en los datos maestros	3	3	4	Sí cumple
		4	3	4	Sí cumple
-Porcentaje de registros con errores o -inconsistencias.	Valore el nivel de registros de datos con errores o inconsistencias…	4	4	3	Sí cumple
		4	4	4	Sí cumple
Tiempo promedio de respuesta para resolver -problemas de calidad de datos.	Valores el tiempo para resolver problemas de datos referentes a la calidad	3	4	4	Sí cumple
Número de -incidentes de calidad de datos reportados	Valore el nivel de incidentes de calidad de datos reportados	4	4	3	Sí cumple

- Segunda dimensión: **Calidad de datos**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Número de violaciones de seguridad de datos.	Califique el nivel de violaciones de datos de seguridad en la institución	4	4	3	Sí cumple
Nivel de cumplimiento de políticas de seguridad y privacidad	Califique el nivel de incumplimiento a las políticas de seguridad y privacidad de los datos	4	4	4	Sí cumple
Tiempo promedio de respuesta ante incidentes de seguridad.	Califique el promedio de respuesta ante incidentes de seguridad de datos	4	3	4	Sí cumple
Porcentaje de datos sensibles o confidenciales encriptados.	Califique el porcentaje de datos sensibles confidenciales o encriptados	4	4	4	Sí cumple

- Tercera dimensión: Seguridad y privacidad de los datos.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
-Porcentaje de cumplimiento de regulaciones y leyes relevantes.	Califique el porcentaje de cumplimiento de regulaciones y leyes relevantes.	4	4	3	Sí cumple
-Número de auditorías de datos exitosas.	Califique el número de auditorías de datos exitosos.	4	4	3	Sí cumple
-Porcentaje de políticas y procedimientos documentados y actualizados.	Califique el nivel de políticas de procedimientos documentados y actualizados	4	4	4	Sí cumple
Tiempo promedio de respuesta para abordar incumplimientos identificados	Califique el tiempo promedio de respuesta para abordar el incumplimiento de identificación de datos	4	4	4	Sí cumple

- Cuarta dimensión: Cumplimiento normativo.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Porcentaje de datos maestros completos y actualizados.	Califique el porcentaje de datos maestros actualizados.	4	4	3	Sí cumple
-Número de solicitudes o consultas relacionadas con datos maestros.	Califique el nivel de solicitudes consultadas respecto a los datos maestros	4	4	4	Sí cumple
-Porcentaje de registros de datos maestros correctamente vinculados y referenciados	Califique el registro de datos maestros correctamnete vinculados y referenciados	4	4	3	Sí cumple
Tiempo promedio para la resolución de problemas o solicitudes relacionadas con datos maestros	Califique el tiempo promedio para la resolución de problemas o solicitudes con datos maestros	4	3	4	Sí cumple

- Quinta dimensión: **Arquitectura de datos.**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Porcentaje de aplicaciones y sistemas integrados con la arquitectura de datos.	Valore las aplicaciones y sistemas integrados con la arquitectura de datos.	4	4	3	Sí cumple
-Número de puntos de integración	Califique los puntos de integración	4	4	3	Sí cumple

implementados con éxito.	implementados con éxito.				
-Tiempo promedio para el diseño e implementación de cambios en la arquitectura de datos.	Valore el diseño e implementación de cambios en la arquitectura de datos.	4	4	4	Sí cumple
-Número de problemas o errores relacionados con la arquitectura de datos identificados y resueltos.	Valore el nivel de problemas o errores relacionados con la arquitectura de datos identificados y resueltos	3	4	4	Sí cumple

- Sexta dimensión: **Responsabilidades y roles.**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
La calidad y la integridad de los datos que son responsables de la propiedad y el uso de los datos	Valores la calidad y la integridad de los datos que son responsables de la propiedad y el uso de los datos	4	4	4	Sí cumple

Mg. Miguel Ángel Román Martínez García
DNI N° 45709398
CIP-CDSM N° 222504
ORCID: 0000-0003-1302-1575
Firma del experto informante

Firma del evaluador
DNI **45709398**

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento **Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023**.". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	**MIGUEL ANGEL ROMAN MARTINEZ GARCÍA**
Grado profesional:	Maestría (x) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (x)
Áreas de experiencia profesional:	**Asistente de Sistemas**
Institución donde labora:	**Corte Superior de Justicia de San Martin**
Tiempo de experiencia profesional en el área:	2 a 4 años (x) Más de 5 años ( )
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala Ordinal, gobierno de datos

Nombre de la Prueba:	**Cuestionario sobre gobierno de datos**
Autores:	**Leopoldo Flores Vasquez – Tony Varas Valles**
Procedencia:	**Elaboración Propia**
Administración:	
Tiempo de aplicación:	
Ámbito de aplicación:	**Salud**
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

4. Soporte teórico

Escala/ÁREA	Subescala (dimensiones)	Definición
Ordinal		

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el cuestionario **sobre gobierno de datos** elaborado por Leopoldo Flores Vásquez y Tony Varas Valles. en el año 2023. De acuerdo con lossiguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento: Dimensión acceso restringido y transmisión segura, almacenamiento protegido, políticas y procedimientos, auditoria y monitoreo.

- Primera dimensión: **Acceso restringido y Transmisión segura**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Acceso restringido	¿Cómo evalúa el nivel de acceso restringido de datos?	4	3	4	Sí cumple
Encriptación	¿Cómo valora el nivel de encriptación de los datos?	3	4	4	Sí cumple

- Segunda dimensión: **Almacenamiento protegido**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Auditoría y registro de actividades	Cómo califica el proceso de auditoría y registro de actividades	4	4	4	Sí cumple

- Tercera dimensión: **Políticas y procedimientos.**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Protección contra malware y ataques cibernéticos	Como valora la protección contra malware y ataques cibernéticos	4	4	3	Sí cumple

- Cuarta dimensión: **Auditoría y monitoreo.**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Políticas y procedimientos	Como califica las políticas y procedimiento	4	3	4	Sí cumple
Seguridad física	Seguridad física	4	4	4	Sí cumple
Protección de la información durante su ciclo de vida	Cómo valora la protección de la información durante su ciclo de vida.	3	4	3	Sí cumple

Mg. Miguel Ángel Román Martínez García
DNI N° 45709398
CIP-CDSM N° 222504
ORCID 0000-0003-1302-1575
Firma del experto informante

Firma del evaluador
DNI 45709398

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento **Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023**.". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	**MIGUEL ANGEL VALLES CORAL**
Grado profesional:	Maestría ( ) Doctor (x)
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (x)
Áreas de experiencia profesional:	**Docente investigador**
Institución donde labora:	**Universidad Nacional de San Martín**
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:
Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala Ordinal, gobierno de datos

Nombre de la Prueba:	**Cuestionario sobre gobierno de datos**
Autores:	**Leopoldo Flores Vasquez – Tony Varas Valles**
Procedencia:	**Elaboración Propia**
Administración:	
Tiempo de aplicación:	
Ámbito de aplicación:	**Salud**
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

4. Soporte teórico

Escala/ÁREA	Subescala (dimensiones)	Definición
Ordinal		

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el cuestionario **sobre gobierno de datos** elaborado por Leopoldo Flores Vasquez y Tony Varas Valles. en el año 2023. De acuerdo con lossiguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento: Dimensión Gestión de datos maestros, Calidda de datos, Seguridad y privacidad de los datos, Cumplimiento normativo, Arquitectura de datos, Responsabilidades y roles

- Primera dimensión: Dimensión Gestión de datos maestros,

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Porcentaje de registros -duplicados en los datos maestros.	Valore la calidad de datos duplicados en los datos maestros	4	4	4	Sí cumple
		4	4	3	Sí cumple
-Porcentaje de registros con errores o -inconsistencias.	Valore el nivel de registros de datos con errores o inconsistencias…	4	4	3	Sí cumple
		4	3	4	Sí cumple
Tiempo promedio de respuesta para resolver -problemas de calidad de datos.	Valores el tiempo para resolver problemas de datos referentes a la calidad	4	4	3	Sí cumple
Número de -incidentes de calidad de datos reportados	Valore el nivel de incidentes de calidad de datos reportados	4	4	4	Sí cumple

- Segunda dimensión: **Calidad de datos**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Número de violaciones de seguridad de datos.	Califique el nivel de violaciones de datos de seguridad en la institución	4	4	3	Sí cumple
Nivel de cumplimiento de políticas de seguridad y privacidad	Califique el nivel de incumplimiento a las políticas de seguridad y privacidad de los datos	4	4	4	Sí cumple
Tiempo promedio de respuesta ante incidentes de seguridad.	Califique el promedio de respuesta ante incidentes de seguridad de datos	4	4	3	Sí cumple
Porcentaje de datos sensibles o confidenciales encriptados.	Califique el porcentaje de datos sensibles confidenciales o encriptados	4	4	4	Sí cumple

- Tercera dimensión: Seguridad y privacidad de los datos.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
-Porcentaje de cumplimiento de regulaciones y leyes relevantes.	Califique el porcentaje de cumplimiento de regulaciones y leyes relevantes.	4	4	3	Sí cumple
-Número de auditorías de datos exitosas.	Califique el número de auditorías de datos exitosos.	4	4	3	Sí cumple
-Porcentaje de políticas y procedimientos documentados y actualizados.	Califique el nivel de políticas de procedimientos documentados y actualizados	4	4	4	Sí cumple
Tiempo promedio de respuesta para abordar incumplimientos identificados	Califique el tiempo promedio de respuesta para abordar el incumplimiento de identificación de datos	4	4	3	Sí cumple

- Cuarta dimensión: Cumplimiento normativo.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Porcentaje de datos maestros completos y actualizados.	Califique el porcentaje de datos maestros actualizados.	4	4	3	Sí cumple
-Número de solicitudes o consultas relacionadas con datos maestros.	Califique el nivel de solicitudes consultadas respecto a los datos maestros	4	4	4	Sí cumple
-Porcentaje de registros de datos maestros correctamente vinculados y referenciados	Califique el registro de datos maestros correctamente vinculados y referenciados	4	4	3	Sí cumple
Tiempo promedio para la resolución de problemas o solicitudes relacionadas con datos maestros	Califique el tiempo promedio para la resolución de problemas o solicitudes con datos maestros	4	4	3	Sí cumple

- Quinta dimensión: Arquitectura de datos.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Porcentaje de aplicaciones y sistemas integrados con la arquitectura de datos.	Valore las aplicaciones y sistemas integrados con la arquitectura de datos.	4	4	3	Sí cumple
-Número de puntos de integración	Califique los puntos de integración	4	4	3	Sí cumple

implementados con éxito.	implementados con éxito.				
-Tiempo promedio para el diseño e implementación de cambios en la arquitectura de datos.	Valore el diseño e implementación de cambios en la arquitectura de datos.	4	4	4	Sí cumple
-Número de problemas o errores relacionados con la arquitectura de datos identificados y resueltos.	Valore el nivel de problemas o errores relacionados con la arquitectura de datos identificados y resueltos	3	4	3	Sí cumple

- Sexta dimensión: Responsabilidades y roles.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
La calidad y la integridad de los datos que son responsables de la propiedad y el uso de los datos	Valores la calidad y la integridad de los datos que son responsables de la propiedad y el uso de los datos	3	4	4	Sí cumple

MIGUEL ANGEL VALLES CORAL
Dr. Gestión Pública y Gobernabilidad

Firma del evaluador

DNI **40810431**

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento **Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023**.". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	**MIGUEL ANGEL VALLES CORAL**
Grado profesional:	Maestría ( ) Doctor (x)
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (x)
Áreas de experiencia profesional:	**Docente investigador**
Institución donde labora:	**Universidad Nacional de San Martín**
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (x)
Experiencia en Investigación Psicométrica: (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la escala Ordinal, gobierno de datos

Nombre de la Prueba:	**Cuestionario sobre gobierno de datos**
Autores:	**Leopoldo Flores Vasquez – Tony Varas Valles**
Procedencia:	**Elaboración Propia**
Administración:	
Tiempo de aplicación:	
Ámbito de aplicación:	**Salud**
Significación:	Explicar Cómo está compuesta la escala (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

UNIVERSIDAD CÉSAR VALLEJO

4. **Soporte teórico**

Escala/ÁREA	Subescala (dimensiones)	Definición
Ordinal		

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el cuestionario **sobre gobierno de datos** elaborado por Leopoldo Flores Vasquez y Tony Varas Valles. en el año 2023. De acuerdo con lossiguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento: Dimensión acceso restringido y transmisión segura, almacenamiento protegido, políticas y procedimientos, auditoria y monitoreo.

- Primera dimensión: **Acceso restringido y Transmisión segura**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Acceso restringido	¿Cómo evalúa el nivel de acceso restringido de datos?	4	4	3	Sí cumple
Encriptación	¿Cómo valora el nivel de encriptación de los datos?	4	4	4	Sí cumple

- Segunda dimensión: **Almacenamiento protegido**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Auditoría y registro de actividades	Cómo califica el proceso de auditoría y registro de actividades	4	4	3	Sí cumple

- Tercera dimensión: **Políticas y procedimientos.**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Protección contra malware y ataques cibernéticos	Como valora la protección contra malware y ataques cibernéticos	4	4	3	Sí cumple

- Cuarta dimensión: **Auditoría y monitoreo.**

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Políticas y procedimientos	Como califica las políticas y procedimiento	4	4	3	Sí cumple
Seguridad física	Seguridad física	4	4	4	Sí cumple
Protección de la información durante su ciclo de vida	Cómo valora la protección de la información durante su ciclo de vida.	4	4	3	Sí cumple

UNIVERSIDAD CÉSAR VALLEJO

MIGUEL ANGEL VALLES CORAL
Dr. Gestión Pública y Gobernabilidad

Firma del evaluador

DNI 40810431

Pd.: el presente formato debe tomar en cuenta:
Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).
Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

CONSTANCIA DE JUICIO DE EXPERTO

Quien suscribe, La Mg. **HENRY LOLAN VÁSQUEZ TUANAMA** Especialista en gestión de proyecto, por medio de la presente hago constar que realice la revisión del instrumento elaborado por los estudiantes TONY VARAS VALLES Y LEOPOLDO FLORES VASQUEZ, estudiantes del décimo ciclo de la carrera de Ingeniería de sistemas de la universidad Cesar Vallejo; quien está realizando el trabajo de investigación titulado **"Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023".**

En tal sentido considero que el instrumento de investigación es válido para ser aplicado.

CONSTANCIA DE JUICIO DE EXPERTO

Quien suscribe, La Dr. Miguel Ángel Valles Coral como especialista en gestión pública y gobernabilidad , por medio de la presente hago constar que realice la revisión del instrumento elaborado por los estudiantes TONY VARAS VALLES Y LEOPOLDO FLORES VASQUEZ, estudiantes del décimo ciclo de la carrera de Ingeniería de sistemas de la universidad Cesar Vallejo; quien está realizando el trabajo de investigación titulado **"Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023".**

En tal sentido considero que el instrumento de investigación es válido para ser aplicado.

MIGUEL ANGEL VALLES CORAL
Dr. Gestión Pública y Gobernabilidad

CONSTANCIA DE JUICIO DE EXPERTO

Quien suscribe, La Mg. Miguel Ángel Román Martínez García como Ingeniero de Sistemas , por medio de la presente hago constar que realice la revisión del instrumento elaborado por los estudiantes TONY VARAS VALLES Y LEOPOLDO FLORES VASQUEZ, estudiantes del décimo ciclo de la carrera de Ingeniería de sistemas de la universidad Cesar Vallejo; quien está realizando el trabajo de investigación titulado **"Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023".**

En tal sentido considero que el instrumento de investigación es válido para ser aplicado.

Mg. Miguel Ángel Román Martínez García

DNI N° 45709398

CIP-CDSM N° 222504

ORCID: 0000-0003-1302-1575

Firma del experto informante

Anexo 04. Autorización de uso de información de Empresa

Universidad Cesar Vallejo

"AÑO DE LA INIDAD, LA PAZ Y EL DESARROLLO"

ASUNTO: Solicito autorización de uso de información de la Institución

Dr. ALDO ENRIQUE PINCHI FLORES
Director OGESS Alto Mayo

Yo, Leopoldo Flores Vasquez, identificado con DNI N° 76676131, con domicilio Jr. Emilio San Martin S/N Moyobamba. Ante usted respetuosamente me presente y expongo lo siguiente:

Que, estando cursando el décimo ciclo de la carrera profesional de Ingeniería de sistemas de la universidad Cesar Vallejo, solicito a Ud. Autorización para el uso de información para trabajo de investigación de recolección de datos como parte de mi proyecto de investigación.

Objetivo de la Investigación: mi investigación tiene como objetivo desarrollar una "implementación de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud de la región San Martin 2023", este plan proporcionara mejoras en la confidencialidad de la información, transmisión segura, almacenamiento protegido en los establecimientos de salud de la región San Martin 2023.

Métodos de recolección de datos: Para llevar a cabo esta investigación, utilizare la técnica de recolección de datos mediante la encuesta. Esto permitirá recopilar información sobre el gobierno de datos y la confidencialidad de la información, de esta manera poder identificar las falencias con las que cuenta la institución. Adjunto modelo de autorización solicitado por la universidad.

Agradezco de antemano su consideración y apoyo en esta solicitud.

Moyobamba, 15 de noviembre del 2023

OGESS - ALTO MAYO
RECIBIDO TRÁMITE
DOCUMENTARIO ÚNICO
15 NOV 2023
HORA: 3:25 pm
FIRMA:

Atentamente;

LEOPOLDO FLORES
VASQUEZ
DNI N°76676131

AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA

Yo Aldo Enrique Pinchi Flores identificado con DNI, 45774649 en mi calidad de director de la OGESS Alto Mayo, con R.U.C N° 20531320060, ubicada en el distrito de Moyobamba provincia de Moyobamba departamento de San Martin.

OTORGO LA AUTORIZACIÓN,

A los señores TONY VARAS VALLES Y LEOPOLDO FLORES VASQUEZ, Identificado(s) con DNI N° 44116672, DNI N° 76676131 de la Carrera profesional de Ingeniería de Sistemas, para que utilice la siguiente información del hospital II-I Moyobamba y centro de salud jerillo: información de encuesta aplicada a los trabajadores del área de TI, ESTADÍSTICA y HIS, con la finalidad de que pueda desarrollar su ( ) Informe estadístico, ( )Trabajo de Investigación, (x)Tesis para optar el Título Profesional.

(X) Publique los resultados de la investigación en el repositorio institucional de la UCV.
(X) Mantener en reserva el nombre o cualquier distintivo de la empresa; o
(X) Mencionar el nombre de la empresa.

El Estudiante declara que los datos emitidos en esta carta y en el Trabajo de Investigación, en la Tesis son auténticos. En caso de comprobarse la falsedad de datos, el Estudiante será sometido al inicio del procedimiento disciplinario correspondiente; asimismo, asumirá toda la responsabilidad ante posibles acciones legales que la empresa, otorgante de información, pueda ejecutar.

LEOPOLDO FLORES VASQUEZ
DNI: 76676131

TONY VARAS VALLES
DNI: 44116672

Anexo 5. Validación de contenido de la guía de Observación: Base de datos de Prueba piloto para la Confiabilidad

Variable GOBIERNO DE DATOS

Nro	Ítem 1	Ítem 2	Ítem 3	Ítem 4	Ítem 5	Ítem 6	Ítem 7	Ítem 8	Ítem 9	Ítem 10	Ítem 11	Ítem 12	Ítem 13	Ítem 14	Ítem 15	Ítem 16	Ítem 17	Ítem 18	Ítem 19	Ítem 20	Ítem 21
1	3	2	4	5	3	3	2	5	3	2	1	3	2	1	2	3	3	2	2	2	2
2	3	3	3	4	3	4	2	3	3	2	2	2	2	2	3	2	3	2	3	2	2
3	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	3	3	4
4	3	4	4	3	3	4	3	2	2	1	1	1	2	2	2	2	2	2	2	2	1
5	4	5	4	5	3	4	3	2	2	1	2	2	3	2	5	3	3	3	4	2	4
6	3	5	4	4	3	5	5	3	3	3	2	2	4	4	3	4	2	4	2	4	4
7	1	2	4	1	1	1	4	3	3	4	4	4	4	3	4	4	4	4	4	3	4
8	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
9	3	3	3	2	2	4	2	3	2	2	2	3	3	3	3	4	4	4	4	3	4
10	3	3	3	2	2	3	2	3	2	2	3	2	3	2	3	2	2	3	2	3	2
11	3	2	3	2	2	1	3	3	2	1	2	3	1	2	3	3	2	1	1	2	2
12	3	3	3	3	3	2	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3
13	4	4	3	3	2	3	3	4	2	3	4	3	3	4	3	4	3	3	3	3	3
14	3	4	3	2	3	4	3	3	4	3	3	4	4	3	3	2	2	3	4	3	3
15	4	3	3	2	2	2	2	3	2	1	3	1	3	3	3	2	3	3	4	4	3
16	2	3	2	3	3	2	3	2	2	2	3	2	3	2	2	2	2	2	2	3	2
17	2	3	4	3	4	3	2	3	3	2	3	3	2	3	4	3	3	4	3	2	2
18	3	2	2	2	2	2	3	2	2	3	2	2	2	2	3	2	2	3	2	2	2
19	2	2	2	3	5	4	3	2	2	1	3	1	3	3	2	3	3	2	3	3	2
20	1	2	2	2	2	2	2	3	2	3	2	3	2	2	3	2	3	3	3	3	2

Al calcular la fiabilidad con el alfa de Cronbach se obtiene como resultado 0.888 con este resultado podemos decir que es confiable nuestro instrumento de investigación.

Fiabilidad

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	20	100,0
	Excluido[a]	0	,0
	Total	20	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,888	21

Nro	Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	Item 7	Item 8	Item 9	Item 10	Item 11	Item 12	Item 13	Item 14	Item 15	Item 16	Item 17	Item 18	Item 19	Item 20	Item 21
1	3	2	4	5	3	3	2	5	3	2	1	3	2	1	2	3	3	2	2	2	2
2	3	3	3	4	3	4	2	3	3	2	2	2	2	2	3	2	3	2	3	2	2
3	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	3	3	4
4	3	4	4	3	3	4	3	2	2	1	1	1	2	2	2	2	2	2	2	2	1
5	4	5	4	5	3	4	3	2	2	1	2	2	3	2	5	3	3	3	4	2	4
6	3	5	4	4	3	5	5	3	3	3	2	2	4	4	3	4	2	4	2	4	4
7	1	2	4	1	1	1	4	3	3	4	4	4	4	3	4	4	4	4	4	3	4
8	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
9	3	3	3	2	2	4	2	3	2	2	2	3	3	3	3	4	4	4	4	3	4
10	3	3	3	2	2	3	2	3	2	2	3	2	3	2	3	2	2	3	2	3	2
11	3	2	3	2	2	1	3	3	2	1	2	3	1	2	3	3	2	1	1	2	2
12	3	3	3	3	3	2	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3
13	4	4	3	3	2	3	3	4	2	3	4	3	3	4	3	4	3	3	3	3	3
14	3	4	3	2	3	4	3	3	4	3	3	4	4	3	3	2	2	3	4	3	3
15	4	3	3	2	2	2	2	3	2	1	3	1	3	3	3	2	3	3	4	4	3
16	2	3	2	3	3	2	3	2	2	2	3	2	3	2	2	2	2	2	2	3	2
17	2	3	4	3	4	3	2	3	3	2	3	3	2	3	4	3	3	4	3	2	2
18	3	2	2	2	2	2	3	2	2	3	2	2	2	2	3	2	2	3	2	2	2
19	2	2	2	3	5	4	3	2	2	1	3	1	3	3	2	3	3	2	3	3	2
20	1	2	2	2	2	2	2	3	2	3	2	3	2	2	3	2	3	3	3	3	2

21	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	3	3	4
22	3	4	4	3	3	4	3	2	2	1	1	1	2	2	2	2	2	2	2	2	1
23	4	5	4	5	3	4	3	2	2	1	2	2	3	2	5	3	3	3	4	2	4
24	3	5	4	4	3	5	5	3	3	3	2	2	4	4	3	4	2	4	2	4	4
25	1	2	4	1	1	1	4	3	3	4	4	4	4	3	4	4	4	4	4	3	4
26	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
27	3	3	3	2	2	4	2	3	2	2	2	3	3	3	3	4	4	4	4	3	4
28	3	3	3	2	2	3	2	3	2	2	3	2	3	2	3	2	2	3	2	3	2
29	3	2	3	2	2	1	3	3	2	1	2	3	1	2	3	3	2	1	1	2	2
30	3	3	3	3	3	2	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3
31	4	4	3	3	2	3	3	4	2	3	4	3	3	4	3	4	3	3	3	3	3
32	3	4	3	2	3	4	3	3	4	3	3	4	4	3	3	2	2	3	4	3	3
33	4	3	3	2	2	2	2	3	2	1	3	1	3	3	3	2	3	3	4	4	3
34	3	4	4	3	3	4	3	2	2	1	1	1	2	2	2	2	2	2	2	2	1
35	4	5	4	5	3	4	3	2	2	1	2	2	3	2	5	3	3	3	4	2	4
36	3	5	4	4	3	5	5	3	3	3	2	2	4	4	3	4	2	4	2	4	4
37	1	2	4	1	1	1	4	3	3	4	4	4	4	3	4	4	4	4	4	3	4
38	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
39	3	3	3	2	2	4	2	3	2	2	2	3	3	3	3	4	4	4	4	3	4
40	3	3	3	2	2	3	2	3	2	2	3	2	3	2	3	2	2	3	2	3	2
41	3	2	3	2	2	1	3	3	2	1	2	3	1	2	3	3	2	1	1	2	2
42	3	3	3	3	3	2	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3
43	4	4	3	3	2	3	3	4	2	3	4	3	3	4	3	4	3	3	3	3	3
44	3	4	3	2	3	4	3	3	4	3	3	4	4	3	3	2	2	3	4	3	3
45	4	3	3	2	2	2	2	3	2	1	3	1	3	3	3	2	3	3	4	4	3
46	2	3	2	3	3	2	3	2	2	2	3	2	3	2	2	2	2	2	2	3	2

47	2	3	4	3	4	3	2	3	3	2	3	3	2	3	4	3	3	4	3	2	2
48	3	2	2	2	2	2	3	2	2	3	2	2	2	2	3	2	2	3	2	2	2
49	2	2	2	3	5	4	3	2	2	1	3	1	3	3	2	3	3	2	3	3	2
50	1	2	2	2	2	2	2	3	2	3	2	3	2	2	3	2	3	3	3	3	2

Al calcular la fiabilidad con el alfa de Cronbach se obtiene como resultado 0.891 con este resultado podemos decir que es confiable nuestro instrumento de investigación.

Fiabilidad

[ConjuntoDatos0]

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	50	100,0
	Excluido[a]	0	,0
	Total	50	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,891	21

Variable CONFIABILIDAD DE LA INFORMACION

Nro	Ítem 1	Ítem 2	Ítem 3	Ítem 4	Ítem 5	Ítem 6	Ítem 7
1	2	3	2	2	3	3	3
2	2	3	2	1	2	2	1
3	4	4	3	3	3	4	4
4	3	1	1	1	2	2	1
5	3	2	3	4	3	4	4
6	5	3	3	5	5	4	5
7	3	4	4	2	3	2	4
8	1	2	2	2	2	2	2
9	2	2	2	2	2	2	2
10	2	1	2	1	2	1	2
11	1	2	1	3	2	3	3
12	2	3	2	2	3	2	3
13	3	2	2	3	4	3	3
14	3	3	3	2	3	2	3
15	3	3	4	3	4	4	4
16	4	1	3	2	2	2	3
17	1	3	2	3	1	2	2
18	2	3	3	3	3	3	3
19	2	2	2	2	3	1	2
20	3	2	2	2	2	2	3

Al calcular la fiabilidad con el alfa de Cronbach se obtiene como resultado 0.885 con este resultado podemos decir que es confiable nuestro instrumento de investigación.

Fiabilidad

[ConjuntoDatos0]

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	20	100,0
	Excluido[a]	0	,0
	Total	20	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,885	7

Nro	Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	Item 7
1	2	3	2	2	3	3	3
2	2	3	2	1	2	2	1
3	4	4	3	3	3	4	4
4	3	1	1	1	2	2	1
5	3	2	3	4	3	4	4
6	5	3	3	5	5	4	5
7	3	4	4	2	3	2	4
8	1	2	2	2	2	2	2
9	2	2	2	2	2	2	2
10	2	1	2	1	2	1	2
11	1	2	1	3	2	3	3
12	2	3	2	2	3	2	3
13	3	2	2	3	4	3	3
14	3	3	3	2	3	2	3
15	3	3	4	3	4	4	4
16	4	1	3	2	2	2	3
17	1	3	2	3	1	2	2
18	2	3	3	3	3	3	3
19	2	2	2	2	3	1	2
20	3	2	2	2	2	2	3
21	4	4	3	3	3	4	4
22	3	1	1	1	2	2	1
23	3	2	3	4	3	4	4
24	5	3	3	5	5	4	5

25	3	4	4	2	3	2	4
26	1	2	2	2	2	2	2
27	2	2	2	2	2	2	2
28	2	1	2	1	2	1	2
29	1	2	1	3	2	3	3
30	2	3	2	2	3	2	3
31	3	2	2	3	4	3	3
32	3	3	3	2	3	2	3
33	3	3	4	3	4	4	4
34	4	1	3	2	2	2	3
35	1	3	2	3	1	2	2
36	4	4	3	3	3	4	4
37	3	1	1	1	2	2	1
38	3	2	3	4	3	4	4
39	5	3	3	5	5	4	5
40	3	4	4	2	3	2	4
41	1	2	2	2	2	2	2
42	2	2	2	2	2	2	2
43	2	1	2	1	2	1	2
44	1	2	1	3	2	3	3
45	2	3	2	2	3	2	3
46	3	2	2	3	4	3	3
47	3	3	3	2	3	2	3
48	3	3	4	3	4	4	4
49	4	1	3	2	2	2	3
50	1	3	2	3	1	2	2

Al calcular la fiabilidad con el alfa de Cronbach se obtiene como resultado 0.891 con este resultado podemos decir que es confiable nuestro instrumento de investigación.

Fiabilidad

[ConjuntoDatos0]

Escala: ALL VARIABLES

Resumen de procesamiento de casos

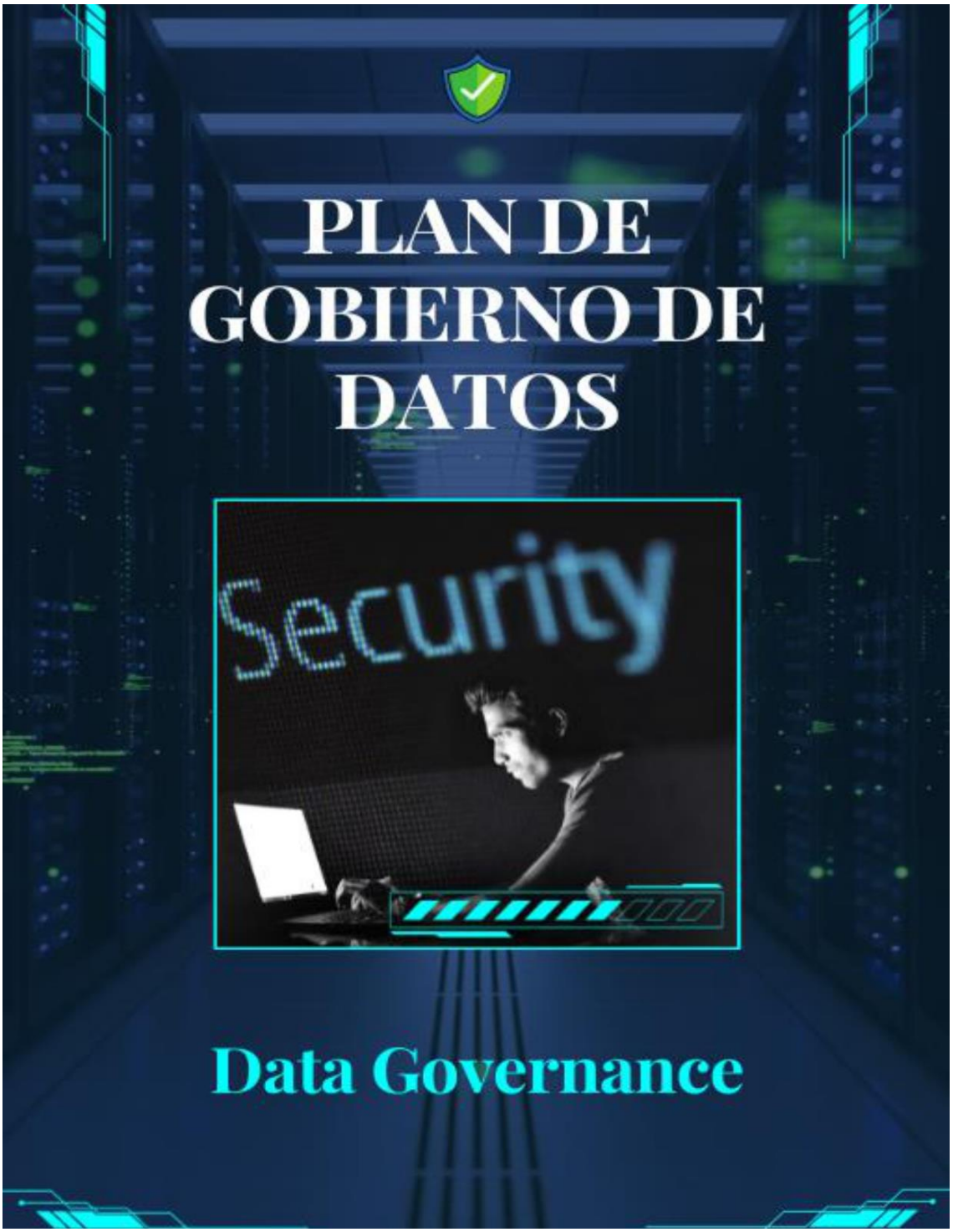
		N	%
Casos	Válido	50	100,0
	Excluido[a]	0	,0
	Total	50	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,892	7

Anexo Prototipo del sistema



.

I. DATOS GENERALES

HOSPITAL : MOYOBAMBA

UBICACIÓN : AV. GRAU

NIVEL : II-I

DIRECTOR : MED CRJ. DENIS PERES POSTIGO

RESPONSABLE : ALEX HERRERA CORONEL

II. EQUIPO RESPONSABLE.

- **LEOPOLDO FLORES VASQUEZ**
- **TONY VARAS VALLES**

III. PRESENTACIÓN.

En los hospitales y postas del alto mayo, surge la necesidad apremiante de integrar e implementar el gobierno de datos en el proceso de manejo de la información, motivada por el uso inadecuado del personal de los Hospitales y postas. El propósito primordial de la implantación del gobierno de datos en los establecimientos de los Hospitales y postas es capacitar a los usuarios que manejan la información confidencial, fortalecer los conocimientos de los usuarios en cargados del manejo de los datos confidenciales.

En la actualidad, nos encontramos inmersos en una era de revolución de la información y la tecnología, sin tener pleno conocimiento en la seguridad de los datos que manejamos y que nos rodea. Los cambios constantes exigen una actualización continua en conocimientos relacionados con las nuevas tecnologías de la información y leyes sobre gobierno de datos y confidencialidad de la información, cada vez más necesarias para el uso adecuado de los datos que se manejan a diario de los pacientes del Hospital. El uso de políticas de confidencialidad de la información se presenta como una necesidad ineludible en este contexto para el mejor manejo de los datos de los pacientes.

Los encargados del área de sistemas, estadística, desempeñan un papel crucial en la implementación exitosa de esta propuesta innovadora. Sus creencias y actitudes hacia los medios en general determinarán las posibilidades que estas

herramientas puedan desarrollar dentro del entorno del Hospital De ahí se deriva la necesidad de establecer un proceso continuo de capacitación para el uso adecuado de la confidencialidad de la información.

El Proyecto está dirigido principal mente a los encargados del área de sistemas, Estadística y los trabajadores en general del Hospital II-I en Moyobamba. Su enfoque principal es orientar a los trabajadores en el uso y la aplicación del gobierno de datos y confidencialidad de la información.

IV. Introducción

El propósito del presente Plan de Gobierno de Datos de los hospitales y postas del alto mayo tiene como objetivo principal mejorar la gestión y utilización de los datos en toda la organización. Este plan establece los principios, directrices y estrategias necesarios para garantizar la calidad de los datos, la seguridad de la información y el cumplimiento de las regulaciones aplicables.

V. Objetivos

Objetivo General

Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023.

Objetivos Específicos

- **Mejorar la calidad de los datos.** Reducir los errores en la documentación médica, como errores tipográficos, inexactitudes en la historia clínica y datos incorrectos del paciente.

- **Garantizar la seguridad y privacidad de la información.** Desarrollar y documentar políticas claras de privacidad y seguridad de datos que cumplan con las regulaciones aplicables, como HIPAA en los Estados Unidos.

- **Establecer una estructura de gobierno de datos efectiva.** Identificar y definir claramente los roles y responsabilidades de las personas involucradas en la gestión de datos, incluyendo un CDO (Chief Data Officer), DPO (Data Protection Officer), oficiales de cumplimiento y equipos de datos en los departamentos de salud.

VI. Base Legal.

El marco normativo aplicable para garantizar la confidencialidad de la información en establecimientos de salud en San Martín en 2023. Algunas de las regulaciones y leyes relevantes que deben ser consideradas son las siguientes.

NORMA	TEMA
Ley de protección de Datos Personales (Ley N°29733)	Esta ley regula el tratamiento de datos personales en Perú, estableciendo los principios de privacidad y los derechos de los individuos sobre sus datos personales. Las organizaciones de salud deben cumplir con los requisitos de esta ley al manejar datos personales de pacientes.
Reglamento de la Ley de Protección de Datos Personales (Decreto Supremo Nº 003-2013-JUS)	Este reglamento proporciona directrices más específicas sobre el tratamiento de datos personales y las obligaciones de las organizaciones para garantizar su protección.
Ley General de Salud (Ley Nº 26842): Esta	Esta ley regula el sistema de salud en Perú y establece las obligaciones y responsabilidades de los establecimientos de salud en la atención médica y la protección de la salud de los pacientes.
Norma Técnica de Historias Clínicas Electrónicas (Resolución Ministerial Nº 307-2018-MINSA):	Esta norma regula el manejo de historias clínicas electrónicas y establece pautas para garantizar la confidencialidad y seguridad de la información médica de los pacientes.
Ley de Telemedicina (Ley Nº 30947):	Esta ley regula la telemedicina en Perú, y las organizaciones de salud que utilizan esta modalidad deben cumplir con sus disposiciones,

	que incluyen medidas de seguridad de datos y confidencialidad.

VI. Metodología.

La metodología de la implementación será participativa y todas las actividades serán orientadas y supervisadas se desarrollarán por concientizaciones. Los talleres capacitación y los grupos de Inter aprendizaje (trabajadores por áreas), se realizarán en las horas, fechas fijas y acordadas previa coordinación, con sesiones mínimas de 60 minutos y máximas de 90 minutos. Los talleres tendrán un carácter Teórico, mediante Tutoriales y Separatas (Virtuales y Físicos).

ESTRATEGIA	DESCRIPCIÓN	RESPONSABLES
capacitación de Personal involucrado	**TEMÁTICA.** **-Evaluación de Riesgos y Activos:** Realiza una evaluación de riesgos para identificar y clasificar la información crítica y los activos de la organización. Comprender qué datos son más sensibles y valiosos es crucial para orientar las medidas de seguridad. - **Desarrollo de Políticas de Confidencialidad:** Establece políticas claras de confidencialidad que aborden aspectos como el manejo de datos sensibles, el acceso a la información, la transmisión segura y la disposición adecuada de la información al final de su ciclo de vida. - **Educación y Concientización del Personal:** Implementa programas de formación y concienciación para todo el personal. Los empleados deben comprender la importancia de la confidencialidad, cómo identificar y manejar la información sensible, y las mejores prácticas de seguridad. **-Control de Acceso:** Establece políticas y mecanismos de control de acceso. Asegúrate de que solo aquellos que necesitan acceso a información sensible tengan los permisos adecuados. Implementa autenticación multifactor cuando sea posible.	▪ LEOPOLDO FLORES VASQUEZ ▪ TONY VARAS VALLES
	- **Encriptación de Datos:** Utiliza la encriptación para proteger datos sensibles tanto en reposo como en tránsito. Esto es particularmente importante para la información que se almacena en dispositivos móviles,	▪ LEOPOLDO FLORES VASQUEZ ▪ TONY VARAS VALLES

	unidades USB y durante la transmisión a través de redes. - **Gestión de Identidades**: Implementa una sólida gestión de identidades y accesos (IAM) para garantizar que solo las personas autorizadas tengan acceso a la información confidencial. - **Monitoreo y Auditoría:** Establece sistemas de monitoreo y auditoría para realizar un seguimiento de las actividades de acceso a la información sensible. Esto permite la detección temprana de comportamientos inusuales o intentos no autorizados - **Protección contra Amenazas Internas:** Implementa medidas de seguridad específicas para mitigar las amenazas internas, como restricciones de acceso basadas en roles y la revisión regular de los privilegios de usuario. - **Actualizaciones y Parches de Seguridad:** Mantén actualizados los sistemas y aplicaciones con las últimas actualizaciones y parches de seguridad para proteger contra vulnerabilidades conocidas. - **Respuesta a Incidentes:** Desarrolla un plan de respuesta a incidentes que incluya acciones específicas en caso de violaciones de seguridad o pérdida de datos confidenciales. - **Cumplimiento Normativo:** Asegúrate de cumplir con las regulaciones y normativas de privacidad que afecten a tu industria y ubicación geográfica. **-Revisión y Mejora Continua:** Realiza revisiones periódicas de la estrategia, evalúa la efectividad de las medidas implementadas y realiza ajustes .	LEOPOLDO FLORES VASQUEZ TONY VARAS VALLES

VII Cronograma.

FASE 01: EVALUACION INICIAL			
	ACTIVIDADES	**DESCRIPCION**	**TIEMPO ESTIMADO**
1	- Recolección de Datos Actuales	Identificación y análisis exhaustivo de los sistemas de manejo de datos existentes. Revisión de las políticas de seguridad actuales. Evaluación de la estructura y calidad de los datos.	AGOSTO
2	- Identificación de Stakeholder	Identificación de partes interesadas clave, incluyendo personal médico, administrativo y otros actores relevantes. Programación de reuniones para comprender sus necesidades y preocupaciones respecto a la confidencialidad de los datos.	AGOSTO
FASE 02: DESARROLLO DEL PLAN			
1	- Diseño del plan de Gobierno de datos	Desarrollo de políticas y procedimientos detallados para el gobierno efectivo de datos. Definición de roles y responsabilidades en la gestión de datos. Establecimiento de métricas de rendimiento.	SETIEMBRE
2	- Capacitación del Personal	Creación de un programa de capacitación integral para el personal. Incluye sesiones informativas sobre las políticas y procedimientos de seguridad de datos, así como la formación en herramientas y prácticas seguras.	SETIEMBRE
FASE 03 IMPLEMENTACIÓN INICIAL			
1	- Implementación de Tecnologías de Seguridad	Instalación o actualización de sistemas de seguridad, como firewalls, antivirus y sistemas de detección de intrusiones. Configuración de protocolos de cifrado y autenticación.	OCTUBRE
2	- Desarrollo de Infraestructura	Aseguramiento de que la infraestructura de TI cumpla con los estándares de seguridad establecidos. Incluye actualizaciones de hardware y software según sea necesario.	

3	- Pruebas y Ajustes Iniciales	Realización de pruebas de seguridad exhaustivas para identificar posibles vulnerabilidades. Ajustes en el plan de gobierno de datos según los resultados de las pruebas.	OCTUBRE
FASE 04 DESPLIEGUE COMPLETO			
1	- Implementación de Procedimientos de Gobierno de datos.	Puesta en marcha completa de los procedimientos y políticas de gobierno de datos. Inicio de la monitorización continua.	NOVIEMBRE
2	- Monitoreo Continuo.	Implementación de herramientas de monitoreo continuo para identificar posibles violaciones de seguridad en tiempo real. Configuración de alertas y protocolos de respuesta.	NOVIEMBRE
FASE 05 EVALUACIÓN Y MEJORA CONTINUA			
1	- Auditorías Regulares	Programación de auditorías regulares para evaluar la efectividad del plan de gobierno de datos. Identificación de áreas de mejora.	DICIEMBRE
2	- Actualización del Plan	Revisión y actualización del plan de gobierno de datos según las auditorías y los cambios en la tecnología o regulaciones.	DICIEMBRE

VII. Partes Interesadas.

Las siguientes partes interesadas desempeñarán un papel fundamental en la implementación del plan de gobierno de datos:

Nombre del CEO	Denis Lewis Pérez Postigo
Nombre del CIO	Alex Herrera Coronel
Nombre del CDO (Chief Data Officer)	Alex Herrera Coronel
Nombre del Responsable de Seguridad de la Información	Alex Herrera Coronel
Nombre del responsable de Cumplimiento Normativo	Alex Herrera Coronel

VIII. Contenido

7.1 Misión.

Garantizar la confidencialidad, integridad y disponibilidad de la información en los establecimientos de salud de San Martín, promoviendo la privacidad de los pacientes y el cumplimiento de regulaciones, a través de la implementación de políticas, procedimientos y tecnologías de gestión de datos efectivos, y la promoción de una cultura de seguridad de datos entre el personal y la comunidad."

7.2 Visión.

"Convertirse en un referente regional en la protección de la confidencialidad de la información de pacientes y la gestión de datos de salud, mediante la implementación de prácticas de seguridad de datos de vanguardia, el cumplimiento riguroso de regulaciones y la promoción activa de una cultura de privacidad y confidencialidad, en aras de brindar a los pacientes una atención médica de calidad y segura."

7.3 Situación Actual.

Actualmente, el los Hospitales del alto mayo enfrentan desafíos relacionados con la calidad de los datos, la falta de una estructura de gobierno de datos formal y la necesidad de cumplir con regulaciones como como la designación de un responsable de desarrollar e implementar el gobierno de datos en la institución.

Antes de implementar un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud en San Martín 2023, es fundamental realizar un análisis exhaustivo de la situación actual. Este análisis proporcionará una base sólida para identificar las áreas que necesitan mejoras y diseñar un plan efectivo. A continuación, se presentan los elementos clave a considerar en el análisis de la situación actual:

-Evaluación de la Infraestructura de Datos:
Evaluar la infraestructura de tecnología de la información actual, incluyendo sistemas de gestión de registros médicos, bases de datos, almacenamiento de datos y sistemas de seguridad.

-Evaluación de la Calidad de Datos:
Realizar una revisión de la calidad de los datos existentes, identificando

problemas de precisión, integridad, consistencia y actualidad.

-Cumplimiento Regulatorio:
Evaluar el nivel de cumplimiento con las regulaciones de protección de datos y privacidad aplicables, como HIPAA, la Ley de Protección de Datos Personales u otras regulaciones locales y nacionales.

-Políticas y Procedimientos Actuales:
Revisar las políticas y procedimientos actuales de gestión de datos y privacidad para determinar su adecuación y efectividad.

-Recursos Humanos:

Evaluar las habilidades y capacitación del personal en materia de gestión de datos, seguridad y privacidad.

-Amenazas y Vulnerabilidades de Seguridad:

Identificar las amenazas y vulnerabilidades de seguridad que podrían poner en riesgo la confidencialidad de los datos, como ataques cibernéticos, accesos no autorizados o falta de controles de acceso.

-Interoperabilidad de Sistemas:

Evaluar la capacidad de los sistemas de salud para intercambiar datos de manera eficiente y coherente entre departamentos y organizaciones.

- Sistemas de Información.

Los sistemas de información son componentes esenciales en la gestión de datos y la operación de establecimientos de salud. Para garantizar la confidencialidad de la información en estos entornos, es importante contar con sistemas de información seguros y eficientes. Aquí hay una descripción de los tipos de sistemas de información comunes y su importancia en la atención médica:

AGRUPAMIENTO PRINCIPAL	AGRUPAMIENTO ESPECIFICO	SISTEMA	FUNCIÓN
HIS(Sistema de Información en salud)	GALENOS	Sistema Integrado de Gestión Hospitalaria	Registra información clínica y administrativa
	SGI(Sistema de Gestión Integrado)	RIS-PACS AJOVECO	Sistema de Radiología

	SEEM(Sistema de Información de Egresos y Emergencias)	Aplicativo de Captura de Datos	Es un Aplicativo de Captura de Dato de Diagnostico de egreso del paciente
	NOTI (Aplicativo para la Notificación de Casos de Enfermedades sujetas a vigilancia epidemiológica – NOTISP WEB		Identificar, cuantificar y monitorear las tendencias y patrones del proceso salud-enfermedad en las poblaciones.

7.4 Principios y Directrices.

Principios

-Calidad de Datos: Los datos deben ser precisos, completos y oportunos.

- Seguridad de Datos: Se deben implementar medidas de seguridad sólidas para proteger los datos.

- Privacidad de Datos: Se deben respetar las normativas de privacidad de datos.

- Cumplimiento Normativo: [Nombre de la Organización] se compromete a cumplir con todas las regulaciones aplicables.

Directrices

- Procedimientos de recopilación de datos estandarizados.

- Políticas de acceso y control de datos.

- Retención de datos de acuerdo con las regulaciones.

Estos principios y directrices proporcionan una base sólida para diseñar un plan de gobierno de datos efectivo que garantice la confidencialidad de la información en los establecimientos de salud de San Martín en 2023.

7.5 Metodología implementada por SAS.

Esta metodología se enfoca en un programa estándar de gobierno de datos. Los objetivos típicos de la gobernabilidad de datos incluyen siete componentes:

1. Mejorar la toma de decisiones y la coordinación.
2. Reducir los problemas internos.
3. Proteger a los interesados en los datos.
4. Adoptar las mejores prácticas para abordar los problemas de datos.
5. Construir procesos de información repetibles.
6. Reducir los costes y aumentar la eficacia.
7. Asegurar la transparencia de los procesos.

Los tres componentes principales de un gobierno de datos estándar son el patrocinio, la propiedad y la administración. El patrocinio implica el apoyo activo de la alta dirección y las unidades de negocio, mientras que la propiedad se refiere a la responsabilidad de garantizar la calidad de los datos. Por último, la administración implica comprender los requisitos y necesidades de los proveedores de datos y traducirlos en soluciones de datos.

El Data Governance Institute propone un marco de diez componentes para establecer un programa de gobierno de datos típico. Esto incluye definir la misión y el alcance de la gobernanza de datos, identificar el área de enfoque inicial y las métricas para el éxito, y establecer una estructura organizativa adecuada. Además, se debe considerar el establecimiento de controles de datos iniciales utilizando paneles de control, identificar a los interesados y revisar y formalizar los procesos básicos de gobierno de datos.

En resumen, un programa de gobierno de datos estándar se centra en mejorar la toma de decisiones, reducir problemas internos, proteger a los interesados en los datos, adoptar mejores prácticas, construir procesos repetibles, reducir costes, aumentar la eficacia y asegurar la transparencia de los procesos. Los componentes principales son el patrocinio, la propiedad y la administración. Además, se deben considerar aspectos como la estructura organizativa, los procesos y decisiones, y el plan operacional.

7.6 Estructura Organizacional.

Es importante establecer una estructura organizativa que permita la toma de decisiones eficiente y efectiva en el gobierno de los datos. Esto implica asignar roles y responsabilidades claras a los diferentes grupos y asegurar que tengan la autoridad necesaria para tomar decisiones colectivas sobre los activos de información.

Algunas de las actividades necesarias para establecer la estructura organizativa liviana son:

1. Confirmar la identidad del coordinador/administrador de la gestión de datos y determinar qué entidades (BU) deben estar representadas en la estructura de gestión.
2. Determinar qué roles dentro de las BU deben estar representados en los niveles de liderazgo e implementación.
3. Acordar el propósito, el alcance y el trabajo del gobierno de los datos, incluidos los roles y las responsabilidades dentro del esfuerzo presentado aquí.
4. Invitar a las personas que desempeñan funciones de gobierno (no involucradas) a convertirse en miembros de la política de datos o del comité de gestión de datos.
5. Programar una reunión de inicio para presentar (o volver a conocer) a los participantes con el propósito, el alcance y el trabajo del gobierno de los datos, incluida su función y responsabilidades dentro del esfuerzo.

6. Identificar un conjunto de KPI críticos (Activos de datos) con representantes de BU para definir un alcance de definición de datos inicial.

Estas actividades son fundamentales para establecer una estructura organizativa liviana y eficiente en el gobierno de los datos. Al confirmar la identidad del coordinador/administrador de la gestión de datos y determinar las entidades que deben estar representadas, se establece una base sólida para la toma de decisiones colectivas. Además, es importante acordar el propósito, alcance y trabajo del gobierno de los datos, así como invitar a las personas adecuadas a formar parte de la política de datos o el comité de gestión de datos. Por último, programar una reunión de inicio y definir KPI críticos ayudará a establecer un marco claro para el esfuerzo de gobierno de los datos.

7.2 Funciones y responsabilidades.

Es muy importante identificar los roles y las responsabilidades de todos los involucrados en el proceso de gobierno de datos. A menudo hay mucho miedo a lo desconocido y la información ayuda a todos a sentirse más cómodos.

Los sistemas de misión crítica, como el sistema EDW para recopilar información de los huéspedes, son cruciales para el éxito continuo de la organización en el cumplimiento de su misión. Estos sistemas deben proporcionar datos oportunos y precisos al tiempo que satisfacen las demandas de las necesidades diversificadas de los usuarios en toda la organización. Además, estos sistemas darán como resultado abundantes fuentes de datos, que brindan una vista integrada del huésped. Para que estos sistemas críticos funcionen sin problemas, es importante aclarar el papel y la contribución de cada uno.

7.7 Gerente de Gobernanza de Datos y Responsable de TI

El Gerente de Gobernanza de Datos y el responsable de TI tienen varias tareas que deben realizar en conjunto. Algunas de estas tareas incluyen coordinar el Comité de Gobierno de Datos, comunicarse efectivamente entre el Comité y la Administración superior, seguir los protocolos de la

organización, promover la gobernanza de datos, desarrollar una estrategia de gobernanza de la información, evaluar riesgos en los procesos comerciales, categorizar y mantener los activos de datos, utilizar herramientas de gobierno, mapear y documentar el flujo de información, implementar tecnologías para la gestión de datos, realizar evaluaciones de riesgos de privacidad, evaluar la efectividad de las políticas de gobernabilidad de la información, llevar a cabo la gestión de proyectos, recopilar y analizar métricas de gobernabilidad de la información, comprender los sistemas complejos, documentar la colección de derechos de decisión, facilitar el proceso de toma de decisiones y almacenar la colección de derechos de decisión.

7.5 Junta de Gobierno de Datos.

La junta proporciona supervisión al programa, emite políticas y resuelve problemas. También recopila y alinea reglas, abordando vacíos y superposiciones en los conjuntos de reglas. La junta establece pautas sobre cómo colocar las reglas encima de cada una y define responsabilidades claras sobre los datos. Además, establece derechos de decisión y define el desarrollo del proceso.

7.6 Consejo de Administración de Datos.

Los administradores de datos de la unidad de negocio se reúnen para tomar decisiones relacionadas con los datos. Pueden establecer políticas y estándares, o pueden hacer recomendaciones que sean consideradas por la Junta de Gobernanza de Datos de nivel superior. También resuelven problemas relacionados con los datos, escalando los problemas no resueltos al grupo de administración de datos y, en última instancia, a la Junta de Gobierno de Datos. Este grupo supervisa las reglas y es coordinado por el gestor de gestión de datos. Su función principal es armonizar las definiciones de datos y desarrollar estándares de datos.

El grupo de administración de datos recomienda cambios en los controles generales existentes, como la gestión de cambios, políticas, capacitación, SDLC y gestión de proyectos, para apoyar los objetivos de gobernabilidad y empresariales, y facilitar auditorías internas o externas. Explican cómo se

construyen los diferentes controles relacionados con los datos. Además, el grupo establece el alcance de la gestión de cambios y supervisa actividades como cambios en tablas de referencia, almacenes de datos físicos, modelos de datos, definiciones de datos, estructuras de datos, movimiento de datos, repositorios de metadatos, tipos de metadatos y responsabilidades de la data steward.

7.7 Fase de procesos y decisiones.

Se debe comenzar asignando niveles adecuados de autoridad a los sistemas de almacenamiento de datos mediante políticas y procedimientos. Es importante establecer una estructura organizativa con diferentes niveles de gobierno de datos, especificando roles y responsabilidades en cada nivel. El Gerente de DG y el responsable de TI identifican a los administradores de datos responsables de coordinar las actividades de gobernabilidad de datos y les otorgan la autoridad para corregir problemas de datos de manera eficiente. Mantener datos de alta calidad requiere un enfoque proactivo para el gobierno de datos, estableciendo estrategias para prevenir, detectar y corregir errores y usos incorrectos de los datos. Además, se deben desarrollar políticas iniciales, crear un inventario de datos y establecer una política escrita sobre los inventarios de datos.

VIII. Metodología para gobernanza de datos de Nicola Askham.

Según Nicola Askham, si no se utiliza un marco de trabajo adecuado, mantener la calidad de los datos en las organizaciones solo resultará en la pérdida de la visión de gobierno de la información y se limitará a la limpieza de datos. Para mantener una buena calidad de datos de manera constante, es necesario administrarlos de forma proactiva y asegurarse de capturarlos con precisión sin que su calidad se deteriore. Existe una estrecha relación entre el marco de gobierno de datos y la calidad de la información, ya que trabajan en conjunto. Sin esta interdependencia, muchos proyectos de mejora de calidad de datos solo ofrecen soluciones tácticas a corto plazo o no tienen un impacto significativo desde el principio. Esto se debe a que, sin la gobernanza de datos, los roles, las responsabilidades y los procesos organizacionales para gestionar proactivamente la calidad de los datos no se establecen ni se acuerdan. Por lo

tanto, es importante implementar un marco de gobernanza de datos que incluya políticas, procesos, roles y responsabilidades claras. Solo a través de este marco se pueden obtener beneficios sostenibles, pero es fundamental que se ajuste a la cultura, estructura y prácticas de la organización. Los componentes básicos de este marco se desarrollarán bajo tres lineamientos importantes: control, análisis y mejora.

Espero que esta respuesta resuma y parafrasee el texto de manera adecuada. Si tienes alguna otra pregunta, no dudes en hacerla.

8.1 Como crear soluciones en el gobierno de datos.

La pirámide de Askham simplifica la gobernanza de datos, haciendo que sea más accesible y fácil de implementar. Esta metodología estructurada permite adaptar los proyectos a la cultura organizacional y ser entendidos por todos los niveles de personal desde el principio. La Pirámide Askham desglosa los elementos clave de una implementación exitosa de gobernanza de datos, facilitando el trabajo en la iniciativa de gobernanza de datos de manera lógica.

IX. Metodología de gobierno de datos del DAMA: DMBOK

El Marco de Trabajo Funcional DAMA-DMBOK identifica nueve funciones importantes de la gestión de datos, cada una de ellas descrita a través de siete elementos ambientales. La figura 8 muestra gráficamente este marco de trabajo. Cada función se abordará en un capítulo específico en la Guía DAMA, donde se discutirán los siete elementos correspondientes. La profundidad de la discusión variará según las cuestiones particulares de cada capítulo. Cada capítulo seguirá una estructura consistente, que incluye una introducción a la función, descripción de conceptos y actividades, un resumen, una lista de lecturas recomendadas y una lista de las nueve funciones de gestión de datos. Estas funciones son: gobierno de datos, arquitectura, análisis y diseño de datos, gestión de la base de datos, gestión de la seguridad de los datos, gestión de la calidad de los datos, gestión de datos de referencia y maestros, gestión del almacenamiento de datos e inteligencia de negocio, gestión de documentos, registro y contenido, y gestión de metadatos.

Funciones de la Gestión de Datos	Elementos Ambientales						
	Metas y Principios	Actividades	Entregables	Roles & Responsabilidades	Tecnología	Prácticas y Técnicas	Organización y Cultura
Gobierno de Datos							
Arquitectura, Análisis y Diseño de Datos							
Gestión de la Base de Datos							
Gestión de la Seguridad de Datos							
Gestión de la Calidad de Datos							
Gestión de Datos Maestros y de Referencia							
Gestión del Almacenamiento de Datos e Inteligencia de Negocio							
Gestión de Documentos, Registro y Contenido							
Gestión de Meta Datos							

Figura Marco de trabajo funcional DAMA*

X. Metodología de ISACA

El gobierno de datos se refiere a establecer los derechos y responsabilidades para el manejo adecuado de la información en una organización. Esto implica definir procesos, roles, normas y métricas que aseguren el uso efectivo y eficiente de la información para alcanzar los objetivos de la organización. Algunas mejores prácticas incluyen priorizar con base en las necesidades del negocio, adoptar un enfoque simple y pragmático, ser flexible, comprometer a toda la organización y realizar un monitoreo continuo. El gobierno de datos debe ser capaz de cumplir con las normas y regulaciones, garantizar la calidad de los datos, incentivar resultados positivos, mapear la información, gestionar el significado de los datos, administrar clasificaciones, proteger la información, fomentar la administración adecuada de los datos, manejar requerimientos a largo plazo, gestionar retroalimentación, fomentar la innovación y controlar los datos de terceros.

XI. Aplicativos:

La implementación de medidas de seguridad de la información y la evaluación de la confidencialidad de los datos generalmente implica la utilización de varias herramientas y enfoques combinados. Aquí hay algunas categorías de herramientas y aplicativos que podrían ser útiles para los diferentes aspectos de la seguridad de la información:

10.1. Evaluación de Riesgos y Auditorías:

- Nessus: Una herramienta de escaneo de vulnerabilidades que ayuda a identificar posibles riesgos en la infraestructura de TI.

- OpenVAS: Una alternativa de código abierto para escaneo de vulnerabilidades y evaluación de riesgos.

10.2. Detección de Intrusiones y Monitoreo de Eventos:

- Snort: Un sistema de detección de intrusiones de código abierto.

- SIEM (Security Information and Event Management): Soluciones como Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), o ArcSight, que permiten recopilar, analizar y correlacionar eventos de seguridad.

10.3. Encriptación de Datos:

- itLocker (Windows) / FileVault (macOS): Herramientas integradas para la encriptación de discos.

- **VeraCrypt:**Una herramienta de código abierto para encriptación de archivos y discos.

10.4. Monitoreo de Acceso de Usuarios:

- Varonis: Una solución que ofrece monitoreo de acceso de usuarios y análisis de comportamiento.

- SolarWinds Access Rights Manager: Proporciona auditoría y monitoreo de permisos de usuario.

10.5. Pruebas de Penetración:

- **Metasploit:** Una herramienta de pruebas de penetración que ayuda a identificar y explotar vulnerabilidades.

- **OWASP ZAP (Zed Attack Proxy):** Una herramienta de seguridad de aplicaciones web.

10.6. Herramientas de Cumplimiento y Conformidad:

- Nipper (Rapid7): Ayuda en la evaluación de cumplimiento de seguridad.

- **OpenSCAP:** Herramienta de código abierto para evaluación de conformidad basada en estándares.

XI. RECURSOS:

MATERIALES:

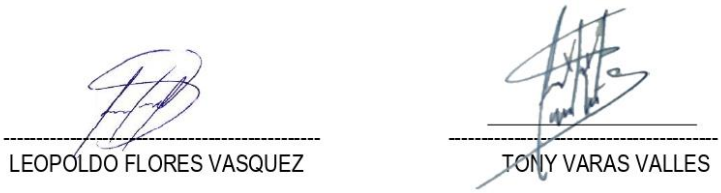
- Computadora personal (virtual).
- Materiales Didácticos Previamente Elaborados y Diseñados.
- Softwares.

HUMANOS:

- Personal de TI, SIS, HIS y otros.

XII. FINANCIAMIENTO:

Autofinanciado por los alumnos de X ciclo de la universidad Cesar Vallejo, en cuanto a recursos y equipamientos para las capacitaciones virtuales.



LEOPOLDO FLORES VASQUEZ

TONY VARAS VALLES