



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733 - 2023

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Naira Guerrero, Elmer (orcid.org/0000-0002-0405-2583)

Paredes Bocanegra, Christian Anthony (orcid.org/0000-0001-6969-9153)

ASESOR:

Mg. More Valencia, Ruben Alexander (orcid.org/0000-0002-7496-3702)

LÍNEA DE INVESTIGACIÓN:

Sistema de Información y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

PIURA - PERÚ

2023

DEDICATORIA

Dedicatoria de Elmer

El presente trabajo está dedicado principalmente a mis padres, hermanas y sobrinos quienes siempre han sido mi fuente inagotable de apoyo y sabiduría. Agradezco su constante aliento, paciencia y amor incondicional que me han permitido llegar hasta este momento. En segundo lugar, a mis compañeros de trabajo, amigos y seres queridos quienes han compartido conmigo este viaje académico, brindándome su comprensión y motivación.

Dedicatoria de Christian Anthony

Este trabajo está dedicado a mis familiares que, por su insistencia, apoyo, y buenos consejos estoy logrando un objetivo más en mi vida.

AGRADECIMIENTO

Agradecimiento de Elmer

agradezco a Dios por otorgarnos la sabiduría necesaria para emprender este camino de aprendizaje y crecimiento.

A mi madre por apoyarme de forma incondicional en todo momento.

A mi familia quienes han sido un sólido soporte emocional y logístico en cada etapa de mi vida.

El Mg. Rubén Alexander More Valencia, asesor de tesis. por su dedicación y disponibilidad para lograr con éxito el desarrollo de este proyecto.

Agradecimiento de Christian Anthony

Agradezco a Dios por brindarnos sabiduría. A la Universidad César Vallejo, a los docentes, en especial a nuestro asesor Mg. More Valencia Rubén Alexander por compartir su experiencia y conocimientos en la realización de esta investigación. A mis amigos que motivaron, apoyaron y alentaron el inicio, el proceso y la culminación de mi carrera, mi más sincero agradecimiento.

Índice de Contenidos

DEDICATORIA.....	ii
AGRADECIMIENTO	iii
RESUMEN.....	ix
ABSTRACT	x
I. INTRODUCCIÓN	1
II. MARCO TEÓRICO.....	6
III. METODOLOGÍA.....	16
3.1. Tipo y diseño de investigación.....	16
3.2. Variables y operacionalización	16
3.3. Población, Muestra y Muestreo	17
3.4. Técnicas e instrumentos de recolección de datos.....	19
3.5. Procedimientos	21
3.6. Método de análisis de datos	22
3.7. Aspectos Éticos.....	23
IV. RESULTADOS.....	25
4.1. Análisis descriptivo.	25
4.2. Análisis Inferencial.....	33
V. DISCUSIÓN	44
VI. CONCLUSIONES.....	48
VII. RECOMENDACIONES	50
REFERENCIAS	51
ANEXOS	58

Índice de Tablas

Tabla 1. Población.....	17
Tabla 2. Métodos y herramientas para recopilar datos.....	19
Tabla 3. Confiabilidad del instrumento “Cuestionario”	21
Tabla 4. Descripción estadística del indicador proteger la confidencialidad de los datos antes y después de la implementación.....	26
Tabla 5. Descripción estadística del indicador de confidencialidad de los datos tanto antes como después de la implementación.....	27
Tabla 6. Descripción estadística del indicador garantizar la integridad de los datos antes y después de la implementación	28
Tabla 7. Descripción estadística del indicador de Integridad antes y después de la implementación	29
Tabla 8. Descripción estadística del indicador garantizar la disponibilidad de los datos antes y después de la implementación.....	31
Tabla 9. Descripción estadística del indicador disponibilidad antes y después de la implementación	32
Tabla 10. prueba de normalidad para el indicador Proteger la confidencialidad de los datos pre test y post test.....	33
Tabla 11. Correlación de los datos en antes (pre test) y después (post test) de la implementación	34
Tabla 12. prueba de normalidad para el indicador de confidencialidad antes y después de la implementación	35
Tabla 13. prueba de normalidad del indicador garantizar la integridad de los datos antes y después de la implementación	36
Tabla 14. Correlación de los datos en antes y después de la implementación	37
Tabla 15. prueba de normalidad para el indicador de Integridad antes y después de la implementación	37
Tabla 16. prueba de normalidad del indicador garantizar la disponibilidad de los datos antes y después de la implementación.....	38
Tabla 17. Correlación de los datos en pre test y post test	39
Tabla 18. prueba de normalidad del indicador de disponibilidad antes y después de la implementación	40
Tabla 19. prueba de rangos de Wilcoxon para confidencialidad.....	41

Tabla 20. prueba de rangos de Wilcoxon para integridad.	42
Tabla 21. prueba de rangos de Wilcoxon en Disponibilidad.	43

Índice de Figuras

Figura 1. Pretest y posttest-----	16
Figura 2. Histograma del indicador proteger la confidencialidad de los datos – Pre Test.-----	26
Figura 3. Histograma del indicador proteger la confidencialidad de los datos – Post Test.-----	26
Figura 4. Gráfico comparativo del indicador de confidencialidad antes y después de la implementación.-----	27
Figura 5. Gráfico de Histograma de los datos en el indicador garantizar la integridad antes de la implementación – Pre Test.-----	28
Figura 6. Gráfico de Histograma de los datos en el indicador garantizar la integridad antes de la implementación – Post Test.-----	29
Figura 7. Gráfico comparativo del indicador de Integridad antes y después de la implementación.-----	30
Figura 8. Gráfico de Histograma de los datos en el indicador garantizar la disponibilidad de los datos antes de la implementación – Pre Test.-----	31
Figura 9. Gráfico de Histograma de los datos en el indicador garantizar la disponibilidad de los datos después de la implementación – Post Test.-----	31
Figura 10. Gráfico comparativo del indicador de Disponibilidad antes y después de la implementación.-----	32
Figura 11. gráfico de cuantiles-cuantiles en el indicador Proteger la confidencialidad de los datos (pre test).-----	34
Figura 12. gráfico de cuantiles-cuantiles en el indicador Proteger la confidencialidad de los datos (post test).-----	34
Figura 13. Histograma de prueba de normalidad de la métrica de confidencialidad antes y después de la implantación.-----	35
Figura 14. gráfico de cuantiles-cuantiles en el indicador garantizar la integridad de los datos (pre test).-----	36
Figura 15. gráfico de cuantiles-cuantiles en el indicador garantizar la integridad de los datos (post test).-----	37
Figura 16. Histograma de prueba de normalidad de la métrica de integridad antes y después de la implantación.-----	38

Figura 17. gráfico de cuantiles-cuantiles para el indicador de garantizar la integridad de los datos (pre test).-----	39
Figura 18. gráfico de cuantiles-cuantiles para el indicador de garantizar la integridad de los datos (post test).-----	39
Figura 19. Histograma de prueba de normalidad de la métrica de disponibilidad antes y después de la implantación.-----	40

RESUMEN

El proyecto de investigación titulado **"Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733 – 2023"** busca fortalecer la seguridad de datos en una Unidad de Gestión Educativa Local mediante la aplicación de controles según la legislación peruana. Con un enfoque cuantitativo y diseño aplicado experimental, el estudio se centra en diseñar controles de seguridad para proteger información confidencial, garantizar la integridad y disponibilidad de datos a través de un sistema de planillas. Los resultados, obtenidos mediante análisis pre y post-test, respaldan la eficacia de la implementación, indicando mejoras significativas en la protección de datos personales, alineándose con la Ley 29733. Se destaca la importancia de normativas y estándares internacionales, como la norma ISO, en procesos esenciales para entidades y empresas. En conclusión, la implementación del sistema refuerza la relevancia de medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de datos, recalcando la necesidad de adherirse a estándares normativos para cumplir con las exigencias legales y proteger la información sensible en entornos educativos.

Palabras clave: Sistema de planillas, controles de seguridad, protección de datos personales, Ley Peruana 29733, NTP ISO /IEC 27001.

ABSTRACT

The research project entitled "**Implementation of a spreadsheet system based on security controls for the protection of personal data applying Peruvian Law 29733 - 2023**" seeks to strengthen data security in a Local Educational Management Unit through the application of controls according to Peruvian legislation. With a quantitative approach and applied experimental design, the study focuses on designing security controls to protect confidential information, ensure data integrity and availability through a spreadsheet system. The results, obtained through pre- and post-test analysis, support the effectiveness of the implementation, indicating significant improvements in the protection of personal data, in line with Law 29733. The importance of international norms and standards, such as ISO, in essential processes for entities and companies is highlighted. In conclusion, the implementation of the system reinforces the relevance of security measures to protect the confidentiality, integrity and availability of data, emphasizing the need to adhere to regulatory standards to comply with legal requirements and protect sensitive information in educational environments.

Keywords: Payroll system, security controls, personal data protection, Peruvian Law 29733, NTP ISO /IEC 27001.

I. INTRODUCCIÓN

Las empresas y organizaciones de hoy en día se han transformado en sociedades de la información, dado el volumen considerable de datos que procesan, almacenan y transmiten. Estas entidades reconocen que la información y los datos son activos de vital importancia y, por ende, los sitúan en un lugar prioritario. En este contexto, la gestión eficaz de la seguridad de los datos se convierte en un aspecto crucial, con el propósito de garantizar la integridad, confidencialidad y disponibilidad de la información, pues estos principios fundamentales son esenciales para salvaguardar el acceso a datos personales. La seguridad informática se basa en la aplicación de medidas técnicas destinadas a preservar la seguridad de los datos sensibles dentro de estas entidades (Linares, 2022).

Naciones altamente desarrolladas, como Japón, Francia, Canadá, Dinamarca, Estados Unidos e Inglaterra, ocupan las posiciones de liderazgo a nivel mundial en ciberseguridad, tanto en sus sectores públicos como privados. Estas naciones continúan realizando inversiones sustanciales en sistemas diseñados con un enfoque centrado en la garantía de una experiencia ciudadana eficiente y segura, permitiendo la confiable protección de sus datos (Wouilloz 2023).

De acuerdo con un estudio llevado a cabo en 2022 por la empresa de ciberseguridad Symantec, que evaluó a 157 países en todo el mundo utilizando ocho parámetros de medición que incluyeron ataques de red, cryptojacking, ransomware, ataques web, malware, hosts de phishing, spam y bots, se llegó a la conclusión de que países como Venezuela, México y Brasil están entre las naciones más vulnerables a los ataques cibernéticos (Barrales 2016).

En Perú, tras realizar encuestas a 2,363 entidades públicas acerca de la implementación de medidas de seguridad digital, se reveló que solo 117 de estas instituciones han incorporado dichas medidas. Destacan entre las principales instancias públicas con planes de seguridad digital implementados el CONCYTEC, la Fuerza Aérea del Perú, la Contraloría General, la Autoridad Nacional PDP, el Congreso de la República y el Despacho Presidencial, entre otros.

Es importante subrayar que, si bien ninguna arquitectura de ciberseguridad es infalible, ya que todas presentan tanto debilidades como fortalezas que requieren un estudio detenido para su mejora y sofisticación, es esencial reconocer que una infraestructura tecnológica desactualizada o con niveles bajos de seguridad puede dejar a un país altamente expuesto a las amenazas de delitos cibernéticos.

En el contexto nacional, la normativa de proteger datos personales, identificada como la Ley Nro. 29733, es de aplicación tanto para entidades públicas como privadas. Esta legislación, promulgada el 3 de julio de 2011 a través del Diario Oficial El Peruano, tiene como objetivo principal garantizar la protección del derecho fundamental a la privacidad de los datos personales, tal como se establece en el Art. 2°, núm. 6) de la Constitución del Perú. Su propósito es asegurar la adecuada implementación de esta salvaguardia («Ley N.° 29733» [sin fecha]).

En respuesta a la creciente necesidad de proteger los datos sensibles, en el año 2014 se aprobó la NTP ISO/IEC 27001:2013. A partir del 2016, se hizo obligatorio su empleo en las entidades gubernamentales, lo que condujo a la implementación de sistemas de gestión de seguridad de la información en dichas organizaciones. Esta medida tenía como objetivo primordial la disminución de los riesgos vinculados a la gestión de la seguridad de la información. («Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001"» [sin fecha])

En la Región Piura las (UGEL) son entidades de naturaleza administrativa y supervisora, con operaciones a nivel local y un enfoque en la administración y mejora de la educación en sus respectivas jurisdicciones. La mayoría de estas entidades carece de un conjunto de procedimientos establecidos, directrices o planes de seguridad de la información que permitan una gestión adecuada de los datos personales. Un ejemplo concreto de esta falta de medidas se encuentra en el proceso de pago de planillas de personal bajo el Contrato Administrativo de Servicios (CAS) 1057. Esta situación expone la información a potenciales amenazas tanto desde fuentes externas como internas, y se han identificado **problemas específicos**, como la ausencia de regulaciones que restrinjan el uso de los datos, la falta de normativas que limiten la manipulación de la información y la carencia de regulaciones que supervisen la disponibilidad de la información.

Con el fin de abordar la problemática señalada previamente, proponemos implementar un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733, la propuesta consiste en establecer un esquema que permita definir y aplicar políticas de seguridad, integridad y disponibilidad de una manera efectiva en una Unidad de Gestión Educativa Local.

Se plasmó la **formulación del problema** de manera *general*: ¿Cómo un sistema de planillas basado en controles de seguridad permite proteger los datos personales en una Unidad de Gestión Educativa Local en el año 2023?; de manera *específica* surgen los siguientes problemas: 1 - ¿de qué manera un sistema de planillas basado en controles de seguridad contribuye a la protección de la información confidencial en una Unidad de Gestión Educativa Local en el año 2023?, 2 - ¿de qué manera un sistema de planillas basado en controles de seguridad garantiza la integridad de la información en una Unidad de Gestión Educativa Local en el año 2023?, 3 - ¿de qué manera un sistema de planillas basado en controles de seguridad garantiza la disponibilidad de la información en una Unidad de Gestión Educativa Local en el año 2023?

En el contexto de la investigación, **la justificación** es un componente fundamental en la cual se presentan de manera detallada las razones que sustentan la pertinencia y necesidad de llevar a cabo el estudio propuesto (Álvarez-Risco 2020). A continuación, se presentan las justificaciones de manera social, práctica, tecnológica y metodológica. **La Justificación social** se basa en la importancia de la privacidad como un aspecto de gran relevancia en el contexto de responsabilidad social de una Unidad de Gestión Educativa Local. Para abordar de manera proactiva esta cuestión, la institución demuestra su fuerte posición para respetar los derechos y la privacidad de las personas, que son pilares clave para promover el respeto y la convivencia justa en la sociedad. La seguridad y protección de los datos personales no sólo garantiza la integridad de las personas, sino que también contribuye a la creación de un entorno social que fomenta la confianza y fortalece la relación entre una institución y su comunidad educativa. de manera **práctica** se justifica esta iniciativa en virtud de una serie de factores esenciales que respaldan a su relevancia. En primer lugar, la mitigación de riesgos es un aspecto

fundamental, ya que la protección de datos personales reduce la posibilidad de vulnerabilidades y posibles problemas legales. La eficiencia en la gestión de datos es otro punto crucial, ya que permite un manejo más ágil y organizado de la información, mejorando así la toma de decisiones y la eficacia operativa. Respecto al cumplimiento normativo se erige como un imperativo, garantizando que la institución se ajuste a las regulaciones legales vigentes en cuanto a la privacidad y protección de datos. Esto no solo evita posibles sanciones, sino que también fortalece la imagen institucional y la confianza de la comunidad educativa, ya que demuestra un compromiso transparente y ético con la gestión de la información. De manera **tecnológica** se justifica por la necesidad de salvaguardar los datos sensibles, la prevención de brechas de seguridad, la gestión eficiente de accesos, el respaldo y recuperación de datos, así como la capacidad de mantenerse actualizado y cumplir con los requisitos normativos en evolución. De manera **metodológica** se justifica porque se aplicará los conocimientos requeridos para diseñar un sistema de planillas respaldado por medidas de seguridad, con el propósito de abordar un problema concreto relacionado con la confidencialidad, integridad y disponibilidad de la información. Además, porque permite a la entidad el cumplimiento de estándares, el análisis de riesgos, el diseño de controles de seguridad, la evaluación de impacto, capacitación y concientización del personal y el enfoque de monitoreo y mejora continua.

Para la investigación propuesta se propone como **objetivo general** de la tesis: Mejorar la protección de datos personales en una Unidad de Gestión Educativa Local mediante un sistema de planillas basado en controles de seguridad aplicando la Ley Peruana 29733 y como **objetivos específicos**: 1) Diseñar controles de seguridad adecuados para proteger la información confidencial. 2) Garantizar la integridad de los datos a través de la implementación un sistema de planillas basado en controles de seguridad. 3) Garantizar la disponibilidad de los datos a través de la implementación de un sistema de planillas basado en controles de seguridad.

Esta investigación, supone plantear la Hipótesis general de que la implementación de un sistema de planillas basado en controles de seguridad resultará en una mejora sustancial en la salvaguarda de los datos personales en una UGEL.

Asimismo, en cuanto a las hipótesis específicas relacionadas con las dimensiones, se plantea el siguiente enfoque. 1) La implementación de un sistema de planillas basado en controles de seguridad protegerá significativamente la información confidencial de los datos en una UGEL. 2) La implementación de un sistema de planillas basado en controles de seguridad garantiza significativamente la integridad de los datos en una UGEL. 3) La implementación de un sistema de planillas basado en controles de seguridad brinda significativamente la disponibilidad de los datos en una UGEL.

II. MARCO TEÓRICO.

En el año 2020, los autores Onyshchenko, Hlushko y Yanko publicaron un artículo que destacaba la creciente dificultad de garantizar la protección de la información en medio de una pandemia. El propósito principal de su investigación era fundamentar el papel crítico y la relevancia de la protección de la información en un entorno pandémico. El estudio se centró en la exploración de la base conceptual y categórica de la seguridad de la información, así como en la identificación de las prioridades estratégicas necesarias para reforzar la seguridad de la información en Ucrania. Los autores subrayaron que la amenaza de infección viral se había convertido en un desafío no solo para el sistema de atención médica, sino también para la capacidad de las autoridades públicas, los gobiernos locales y las empresas para hacer frente a desafíos y amenazas de tal magnitud. Este artículo proporciona un análisis en profundidad de las consecuencias de la pandemia de COVID-19. en diversos campos, incluida la economía global, la economía nacional y la seguridad general. La pandemia ha sido un factor disruptivo con graves impactos en muchos sectores, y los autores destacan la necesidad de abordar eficazmente la protección de la información en este entorno desafiante. El estudio reveló que la rápida expansión de los procesos de digitalización, impulsada por las restricciones de cuarentena, planteó preocupaciones significativas sobre la información y la seguridad cibernética en diversos niveles: desde los ciudadanos individuales hasta la sociedad en su conjunto y el país en su totalidad. Esto condujo al desarrollo de herramientas especializadas diseñadas para detectar y neutralizar contenidos perjudiciales en el vasto ciberespacio. Como resultado de este análisis, se logró identificar cuatro niveles de apoyo normativo y jurídico destinados a fortalecer la seguridad de la información. Estos niveles se derivaron de una evaluación del marco normativo vigente. Esto se debe a la creciente necesidad de mitigar los efectos nocivos de las ciberamenazas y abordar los desafíos que plantea la pandemia de COVID-19. En el ámbito de la seguridad de la información existe una necesidad urgente de optimizar las acciones legales y regulatorias. El aumento de la actividad en el ciberespacio, incluida la proliferación de redes sociales y el cambio a métodos de trabajo y aprendizaje remotos, justifica una mayor investigación. El propósito de este estudio es brindar una protección efectiva de la información,

tomando en cuenta los desafíos y amenazas generadas por la pandemia. En un contexto de cambios constantes, la seguridad de la información se perfila como un elemento importante que debe protegerse no sólo a nivel individual, sino también a nivel social y nacional. (Onyshchenko, Hlushko y Yanko 2020).

Los autores Pradana y Trianto en el 2018 señalan la importancia de conocer la normativa en Indonesia, que requiere que las organizaciones que manejan datos personales establezcan políticas internas para la protección y seguridad de estos datos. La identificación del nivel de impacto de la información según el Control de Seguridad y Privacidad de NIST SP800-53 parece ser un enfoque sólido para evaluar la importancia de la protección de datos. Es impresionante ver qué aspectos como la confidencialidad y la disponibilidad tienen un impacto alto, lo que refuerza la necesidad de medidas de seguridad sólidas. Es notable que, según el mapeo de Control de Seguridad y Privacidad de NIST SP800-53 revisión 5, se hayan identificado 57 controles relacionados con la privacidad en este contexto. Esto indica que se debe prestar atención a la privacidad de los datos personales y adoptar un enfoque riguroso para protegerlos. En general, Indonesia parece estar tomando medidas importantes para garantizar la seguridad de la información personal confidencial en la era digital. Los resultados de las evaluaciones de privacidad pueden ser valiosas sugerencias durante la elaboración de políticas destinadas a proteger la información de carácter personal dentro de una entidad. Un factor decisivo en este proceso es determinar el nivel de exposición a los sistemas de información de una organización en función de su política de privacidad para información de identificación personal (PII). Esta guía permite abordar la preservación de la privacidad de los datos personales en los sistemas de información de acuerdo con su nivel de impacto, lo que facilita la elección de los controles adecuados. Es relevante destacar que el resultado de la evaluación conforme al NIST SP 800-53 está intrínsecamente vinculado con la confidencialidad de la información, tal como se establece en ISO/IEC 27001. En este contexto, se llega a la conclusión de que el sistema de información de la organización encargada de gestionar datos personales, denominados Información de Identificación Personal, posee una categoría de seguridad alta. Dicha categoría alta se deriva de la valoración del nivel de impacto en el objetivo de seguridad, en donde la

confidencialidad presenta un impacto alto, la integridad un impacto moderado y la disponibilidad un impacto alto. De forma predeterminada, la categoría de alta seguridad incluye un total de 57 controles de privacidad, lo que destaca la importancia y el alcance de las medidas implementadas para garantizar la privacidad. Estos controles son importantes para mantener la integridad y confidencialidad de la información en un entorno de gestión de datos personales (Pradana y Trianto 2018a).

En la edición de la revista CAEN 2020 los autores plantean evaluar el Sistema Nacional de Seguridad Cibernética en relación a los ataques cibernéticos como un riesgo para la Seguridad Nacional. El estudio busca generar contribuciones que ayuden a abordar esta problemática. El objetivo principal de la indagación fue examinar el Sistema de Seguridad Cibernética Nacional en relación a los ataques cibernéticos como un riesgo para la Seguridad Nacional. En lo que respecta a la metodología empleada, se empleó un enfoque descriptivo y un diseño correlacional no experimental. Los resultados destacan la importancia de fortalecer la formación académica y formación profesional de los expertos en ciberseguridad. Además, se recomienda fomentar la conciencia sobre la incorporación de medidas de seguridad cibernética durante todo el proceso de la educación y desarrollo profesional de los ciudadanos. El propósito de este análisis es ofrecer contribuciones que ayuden a abordar la problemática que se plantea en este contexto (Revista de Ciencia e Investigación en Defensa - CAEN 2020).

Según los investigadores Iván B. Moore, Rodrigo, Elías y Medrano en su artículo denominado: las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales, tienen como propósito revisar los últimos documentos legislativos y jurisprudenciales en lo que concierne a la salvaguarda de la información personal en casos específicos de uso tecnológico en el campo laboral, Además, se busca evaluar los casos considerando los principios estipulados en la legislación actual y los criterios fundamentales sobre las responsabilidades relacionadas con el derecho a la protección de datos personales que se derivan de las leyes nacionales. El nivel de investigación del artículo fue descriptivo y el tipo de investigación fue aplicada, los indagadores comentaron que partir de los avances en la legislación y los precedentes judiciales, surgen en la actualidad más

interrogantes que soluciones con respecto a los límites y alcance en relación al derecho de resguardar la información personal en el contexto laboral, como resultados se tiene que se realizó un amplio análisis sobre la LPDP en el marco legal de nuestro país y los antecedentes en los progresos en el ámbito jurídico de forma nacional e internacional, también se brindó principios fundamentales que sustentan la normativa de protección de datos personales y la divulgación de las responsabilidades de los empleadores en cuanto a la salvaguarda de la información confidencial de sus empleados. (Iván Blume Moore 2021).

También, Alvarado en su artículo Information Security Management in the Peruvian Personal Data Protection Regime plasma como propósito proporcionar información sobre la normativa vigente en Perú relacionada con la protección de datos personales, sobre la regulación aplicable, se establece que los encargados de almacenamiento de datos en Perú están obligados a cumplir con las acciones para resguardar la seguridad especificadas en los documentos normativos emitidos por las autoridades competentes. El objetivo es ampliar el conocimiento sobre la extensión de estas medidas en el ámbito empresarial y de individuos cuya gestión económica o social involucra la protección de los datos confidenciales. Esto se debe a que dichas entidades están sujetas a la vigilancia y regulación ejercida por las autoridades competentes. El nivel de investigación fue descriptivo, y el tipo de investigación aplicada, de lo analizado en el presente artículo se concluye que, en la actualidad, el interés público en la protección de datos personales ha aumentado debido al creciente riesgo de pérdida de confidencialidad, integridad o disponibilidad debido al tratamiento automatizado de dichos datos. En nuestro país, se ha promulgado una ley especial que establece el principio de seguridad, lo cual impone la obligación a los administradores de almacenamiento de datos personales y encargados de su procesamiento de documentar las medidas de seguridad implementadas. Esto aplica tanto a la información digital como al almacenamiento de documentación no automatizada, con el propósito de minorar o prevenir el riesgo humano o técnico de adulteración, pérdida o desviación de información, así como cualquier tipo de tratamiento ilegal. Los hallazgos obtenidos en el estudio es que se desarrolló un enfoque de gestión del riesgo sobre la protección de información personal en nuestro país (Alvarado 2016).

Asimismo, Sánchez Campos en el 2022, elaboró una propuesta de un Modelo de seguridad informática para la Protección de datos en una entidad municipal, plantea como objetivo de la investigación Mejorar la protección de datos de una entidad municipal mediante modelo de seguridad informática, utilizó la metodología aplicada y el diseño preexperimental debido al manejo no directo de la data muestral. Como resultados obtuvo: La implementación del modelo de seguridad informática del gobierno local ha supuesto mejoras significativas en la prevención de la divulgación no autorizada de información. Se trata de un aumento de 3,26 puntos, lo que corresponde a una mejora del 69,40%. La prueba comenzó con una media pretest de 1,51 y finalizó con una media de 4,77. Estos resultados demuestran el efecto positivo de implementar medidas de seguridad informática en términos de protección de la información confidencial en los municipios. Se han realizado mejoras significativas para evitar cambios no autorizados en los datos municipales. Esto representa un aumento de 3,19 puntos, o un aumento del 65,20%. La prueba comenzó con una puntuación promedio de 1,67 en la prueba previa y terminó con una puntuación promedio de 4,86 en la prueba posterior, todo como resultado de la implementación del modelo de seguridad de TI por parte del departamento de la ciudad. Se han logrado avances significativos en la prevención del acceso no autorizado a la información a nivel municipal. Este avance se refleja en un aumento de 3,23 puntos, lo que corresponde a un aumento del 67,30%. La prueba comenzó con una puntuación media de 1,60 en el pretest y finalizó con una puntuación media de 4,93 en el posttest. Todo es resultado de la implementación por parte del gobierno local de un modelo de seguridad informática. Estos resultados demuestran el impacto positivo de implementar medidas de seguridad TI en la protección de la información y la reducción de interrupciones no autorizadas en el entorno Municipal (Sanchez Campos 2022).

Por otro lado, Garro Murillo & Navarro Torres en el 2022, en su tesis plasmo como propósito Fortalecer la seguridad de los datos en las transacciones de ventas mediante el sistema de encriptación homomórfica en Lugar Expresivo SAC, El investigador empleó la ficha de recopilación de datos tanto en el pretest como en el posttest como instrumento de estudio. El tesista concluye que en lo que respecta al índice de Disponibilidad, se observó un incremento positivo del 90.00% en esta

dimensión al comparar la medición de la Media del pretest, que registró una diferencia del 10.00% con respecto a la Media del índice posttest, que alcanzó el 100.00%. Para el índice de Integridad, la evaluación de los resultados indicó una mejora positiva del 90.00% en esta dimensión. Esto se refleja en la diferencia del 10.00% entre la medición de la Media en el pretest y la Media en el índice pos test, que alcanzó el 100.00%. En el índice de Confidencialidad, el examen de los resultados arrojó un resultado positivo, mostrando una mejora del 100% en esta dimensión. Esto se evidencia en que no hubo diferencia (0.00%) entre la medición de la Media en el pretest y la Media en el índice pos test, que alcanzó el 100%. (Garro Murillo y Navarro Torres 2022)

Finalmente, Rojas Jaén en el 2019, en su investigación evaluó el aumento de la seguridad de los datos tras la implementación de la norma ISO 27001 en la Subgerencia de Gestión de Bases de Datos del RENIEC. El tipo de investigación fue aplicada - pre experimental, el instrumento utilizado para el tratamiento de datos fue la ficha de registro. El investigador indica que con la implementación de la norma ISO 27001 hubo mejoras significativas en los indicadores de seguridad de los datos. La adhesión a los controles establecidos por la norma, junto con la implementación de nuevos mecanismos de gestión enfocados en la seguridad de la información, ha tenido un impacto favorable en el aumento de los resultados en las áreas de seguridad de datos, lo que muestra que ha se mejorado significativamente el índice de integridad, disponibilidad y confidencialidad de la información (Rojas Jaén 2019).

Teóricamente un **sistema de planillas** es un instrumento utilizado por las empresas para administrar y procesar la información relacionada con los salarios y pagos a los empleados. Este sistema automatiza y simplifica el proceso de cálculo de las remuneraciones, los descuentos, las deducciones y otros conceptos relacionados con la nómina de pago (Zepeda Coronado y Talavera Flores 2004). En cambio Zapata Rosales el 2018, señala que un sistema de planillas ayuda a mejorar la administración de los servidores de una determinada entidad u empresa ya que permite tener un control en tiempo real de los ingresos de sus empleados, asimismo generar oportunamente reportes como boletas de pago, (Zapata Rosales 2019).

Conceptualmente, los **Controles de Seguridad** abarcan las acciones y disposiciones adoptadas con el fin de resguardar la integridad de la información y los activos del sistema frente a diversas amenazas y riesgos de seguridad. Estas medidas se estructuran para evitar accesos no autorizados, identificar potenciales intrusiones y gestionar de manera eficaz cualquier incidente relacionado con la seguridad (Li, Hu y Liu 2011). Los controles de seguridad más comunes en un sistema son: Control de acceso, Autenticación y autorización, Encriptación, Firewalls y sistemas de detección de intrusiones, Copias de seguridad y recuperación de desastres, Auditorías y registros de actividad, Actualizaciones y parches de seguridad, Concientización y capacitación en seguridad.

En cambio, Terán Terranova el 2021 señala que los **controles de seguridad** se refieren a un enfoque o conjunto de medidas diseñadas para proteger los activos, información y procesos de una organización contra posibles amenazas y riesgos de seguridad. Estos controles son mecanismos implementados para prevenir, detectar, mitigar y responder a incidentes de seguridad, con el propósito de resguardar la Disponibilidad, confidencialidad, e integridad de los recursos organizativos. Estos controles pueden incluir políticas, procedimientos, tecnologías y prácticas específicas que se implementan y mantienen para garantizar un nivel adecuado de seguridad de la información y la infraestructura (Terán Terranova 2021).

La **Protección de datos personales** implica la aplicación de medidas y prácticas destinadas a asegurar la privacidad y seguridad de la información personal de los individuos. Los datos personales engloban toda información que tenga la capacidad de identificar a un ser humano, así como sus pre nombres, domicilio, N° telefónico, email, datos financieros, historial médico, etc.(Romansky et al. 2020).

Alvarado en su artículo de opinión del año 2016, aplica la protección de información personal, enfocada en la regulación que exige a las entidades o empresas que manejan bases de datos, poner en marcha las medidas de seguridad establecidas en el marco normativo emitido por las autoridades nacionales (Alvarado 2016).

Moore en cambio aplica la protección de datos personales revisando los cambios significativos introducidos por la implementación de la Ley de Protección de Datos Personales (Ley 29733) en el sistema legal de Perú (Iván Blume Moore 2021).

En el Perú la **Ley N° 29733** tiene por objetivo asegurar el derecho esencial a la salvaguarda de los datos de carácter confidencial, establecido en el Art. 2, num. 6) de la Constitución Política del Perú. Esto se logrará mediante el manejo adecuado de los datos, dentro de un marco que respete los demás derechos esenciales establecidos en dicha Constitución. Según la investigación de Calisaya Sana y Tarrillo Villegas, en Perú, todas las empresas o entidades del estado que traten con datos personales deben cumplir con dicha Ley. (Calisaya Sana y Tarrillo Villegas 2018).

La **Ciberseguridad** abarca una serie de medidas y acciones diseñadas para salvaguardar los sistemas informáticos, redes y datos frente a amenazas cibernéticas, como la intrusión no autorizada, la revelación indebida, la manipulación o la destrucción de información. En la sociedad actual, la ciberseguridad desempeña un papel fundamental debido a la creciente sofisticación y frecuencia de las amenazas y los ataques provenientes del ámbito digital (León 2021).

Chatchalermpun y Daengsi en el año 2021, indican que contar con un conocimiento sólido en ciberseguridad puede incrementar el grado de sensibilidad sobre la importancia de la seguridad cibernética dentro de una institución, la cual constituye un objetivo atractivo para los atacantes. Al aumentar el nivel de concienciación entre todos los empleados, se puede contribuir a la reducción de los riesgos y amenazas, además de fomentar la posibilidad de que una posible víctima informe sobre casos sospechosos, lo que permitirá activar una respuesta adecuada y oportuna ante un incidente, mitigando así los posibles daños. (Chatchalermpun y Daengsi 2021).

Respecto de las **Tecnologías de la información** son herramientas, sistemas y aplicaciones utilizadas para gestionar, procesar, almacenar y transmitir información de manera eficiente. Las TI contienen una diversa gama de áreas y tecnologías que se utilizan en diversas industrias y sectores (Huidobro 2007).

Pradana y Trianto, en 2018, comparten en cierta medida y hacen referencia al hecho de que las Tecnologías de la Información y la Comunicación (TIC) comprenden un conjunto diverso de recursos, herramientas, dispositivos, software,

medios utilizados, redes y aplicaciones. Estos tienen la finalidad de recopilar, procesar, almacenar y transmitir una variedad de información, que abarca voz, datos, texto, video e imágenes. (Pradana y Trianto 2018b).

La norma **ISO 27001**, que forma parte de la serie ISO/IEC 27000, tiene como objetivo definir los requisitos fundamentales para la instauración, ejecución, conservación y perfeccionamiento constante de un Sistema de Gestión de Seguridad de la Información (SGSI) en una entidad (Ladino, Villa y López 2011).

Mirtsch et al, en el año 2021 utilizo datos de una encuesta realizada a 125 empresas de Alemania que cuentan con certificación ISO/IEC 27001. Dado que los índices de adopción varían entre Las compañías del ámbito de las TIC y las que no lo son, destacan que hubo variaciones significativas relacionadas con cada uno de los sectores (Mirtsch et al. 2021).

Los **datos personales** son registros o datos que, ya sea de manera independiente o en conexión con otra información, puede revelar la identidad de un individuo. (Garriga Domínguez 2016).

La **Confidencialidad** implica preservar la privacidad de la información personal de las personas y salvaguardarla contra accesos no permitidos. Esto implica asegurarse de que los datos personales recolectados y guardados por una entidad u organización se manejen de forma segura y solo se compartan con personas o entidades autorizadas (Álvarez 2017).

La **Integridad** implica asegurar que la información personal permanezca exacta, completa y libre de modificaciones no autorizadas. Este principio tiene como objetivo proteger los datos personales contra cualquier forma de manipulación, alteración o corrupción (Arellano Veloz 2023).

La **Disponibilidad** implica asegurar que la información personal esté siempre accesible y lista para ser utilizada por las personas autorizadas en el momento en que la requieran. Este principio se centra en garantizar que los datos estén

disponibles de manera confiable y oportuna, para asegurar su uso efectivo y adecuado (Olguín Decencier 2023).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

- **Tipo de investigación:**

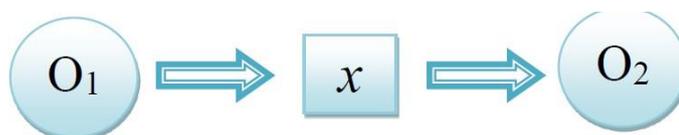
Aplicada, porque se basa en el uso de métodos y herramientas previamente probados y utilizados para resolver un problema específico.

- **Diseño de investigación**

Se emplea un diseño **preexperimental**, seleccionado cuando la gestión indirecta de los datos muestrales es necesaria por motivos de conveniencia práctica.

Dónde:

Figura 1. Pretest y posttest



Fuente: Elaboración Propia

- O1: Estado actual del manejo de planillas y datos personales en la Unidad de Gestión educativa Local.
- X: Implementación de un sistema de planillas basado en controles de seguridad.
- O2: Estado posterior del manejo de planillas y datos personales en la Unidad de Gestión educativa Local.

3.2. Variables y operacionalización

Variables:

Independiente: Sistema basado en controles de seguridad

Definición conceptual:

Un sistema basado en controles de seguridad se refiere a un enfoque o conjunto de medidas diseñadas para proteger los activos, información y procesos de una organización contra posibles amenazas y riesgos de seguridad. Los controles de seguridad abarcan políticas, procedimientos,

tecnologías y prácticas para mantener la seguridad de la información y la infraestructura (Terán Terranova 2021).

Definición operacional:

El sistema basado en controles de seguridad contempla medidas para evitar, identificar, reducir y tomar medidas frente a incidentes de seguridad, teniendo como objetivo de salvaguardar la confidencialidad, integridad y disponibilidad.

Dependiente: Protección de data personal.

Definición conceptual:

Se refiere a las medidas y prácticas adoptadas para proteger la integridad, disponibilidad y confidencialidad de la información personal de los individuos. Se refiere a las medidas para salvaguardar la información que identifica o puede identificar a una persona física, como su N° celular, dirección, DNI, email, información financiera, datos de salud, entre otros.

Definición operacional:

Se implementan políticas y procedimientos establecidos para utilizar mecanismos técnicos de apoyo con el objetivo de resguardar la información almacenada en el sistema, asegurando así el cumplimiento de las formalidades necesarias.

Operacionalización:

El cuadro de operatividad de las variables de estudio se encuentra en el anexo 02.

3.3. Población, Muestra y Muestreo

Población:

Los participantes del estudio fueron los empleados de una UGEL en cargos directivos, jefaturas, administrativos y operativos.

Tabla 1. Población

Cargo o Puesto	Cantidad
Directora	1
Jefes (as) de Área	3
Técnicos	5

Secretaria	3
Total	12

N = 12 personas

Fuente: Elaboración Propia

A nivel conceptual es un conjunto previamente definido de elementos con los que se va a trabajar, con el objetivo de determinar su número y características, así como el tipo de información que se necesita recopilar en general (Pastor 2019).

En relación al comentario previo, se estableció que la población objetiva de esta investigación será de 12 fichas de registros de incidencias pertenecientes a la UGEL.

Muestra:

Una muestra se elige con el propósito de realizar inferencias o generalizaciones sobre la población en su conjunto. La muestra se elige de forma aleatoria o mediante algún otro método de muestreo específico, con el objetivo de garantizar que sea representativa de la población de interés (Quispe et al. 2020).

Como el tamaño de la población es menor que 30, la muestra es igual a la población.

n = 12 personas

Para el estudio, se empleó una muestra de 12 fichas de registros de incidencias, debido a la similitud con la población. Los datos serán recolectados durante un mes, siguiendo la ocurrencia observada en los registros correspondientes con lo que respecta a la confidencialidad, integridad y disponibilidad.

Muestreo:

Es el proceso de seleccionar y analizar una muestra que sea representativa de una población con el propósito de realizar inferencias o generalizaciones sobre dicha población (Hernández-Ávila y Escobar 2019).

Dado que la población es pequeña, se tomó una muestra de 12 trabajadores, lo que dio pie a la obtención de 12 fichas de registro de incidencias para el análisis.

3.4. Técnicas e instrumentos de recolección de datos

Tabla 2. Métodos y herramientas para recopilar datos

Indicadores	Técnica	Instrumentos
Confidencialidad	 Encuesta  Observación	<ul style="list-style-type: none">• Cuestionario• Ficha de Observación
Integridad	 Encuesta  Observación	<ul style="list-style-type: none">• Cuestionario• Ficha de Observación
Disponibilidad	 Encuesta  Observación	<ul style="list-style-type: none">• Cuestionario• Ficha de Observación

Fuente: Elaboración Propia

Encuesta:

Se trata de una metodología de obtención de datos utilizada para obtener información de un conjunto de individuos o una muestra representativa de una población. Implica la elaboración de una serie de interrogantes estructuradas, ya sea de manera oral o escrita, con la finalidad de obtener datos acerca de opiniones, actitudes, comportamientos u otras características relevantes (Useche et al. 2019).

Con el propósito de realizar la investigación, se aplicó un cuestionario al personal directivo, jefaturas, personal administrativo y operativo de una UGEL, a fin de evaluar cómo se maneja y utiliza la información y las herramientas tecnológicas. El objetivo es medir el cumplimiento de los estándares y directrices de seguridad que se utiliza para proteger los datos y la información confidencial dentro de la entidad.

La Observación:

es una estrategia empleada en la investigación científica para recolectar datos. Implica recopilar información de forma sistemática y directa al observar y documentar los comportamientos, eventos y fenómenos

relevantes en un entorno específico. Para ello se debe tener en cuenta, la definición de los objetivos, diseño del protocolo de la observación, Observación participante o no participante, Registro de datos, Observación estructurada o no estructurada, evitar sesgos y análisis de datos (Martínez 2022).

Cuestionario:

Es un instrumento para recolectar datos utilizada para obtener información particular de los participantes que forman parte del estudio. Se trata de un grupo de interrogantes estructuradas y estandarizadas que se plantean de manera uniforme a todos los participantes con el fin de recopilar datos cuantitativos o cualitativos relevantes para la investigación (Pozzo, Borgobello y Pierella 2018).

Guía de observación:

Es una herramienta utilizada en la investigación cualitativa para recopilar datos mediante la observación directa de eventos, situaciones o comportamientos. La guía de observación proporciona una estructura y pautas para el investigador, detallando los aspectos a observar, las categorías de análisis y los indicadores relevantes. Esta guía ayuda a dirigir la atención del observador hacia los elementos específicos que se pretenden investigar, facilitando la recolección sistemática y organizada de datos observacionales (Useche et al. 2019).

Ficha de Registro:

Una ficha de registro, como instrumento de investigación, es un documento creado con el propósito de recopilar y registrar datos específicos durante un estudio o proyecto de investigación. Su objetivo es facilitar la recolección de información de forma organizada y sistemática, lo cual permite analizar y referenciar posteriormente los datos obtenidos (Tafur y Izaguirre 2022).

Validez y confiabilidad:

Para asegurar la validez y confiabilidad del uso del instrumento para recopilar datos, como el cuestionario, se someterá a un proceso de validación y aprobación mediante una evaluación de especialistas. Esta evaluación se basará en la participación de tres miembros con experiencia en el campo, quienes evaluarán y confirmarán, mediante su firma y rúbrica, la validez y confiabilidad del cuestionario y la ficha de registro. Esto garantizará que la encuesta se realice de manera correcta y precisa, proporcionando resultados precisos y fiables.

La herramienta utilizada en la investigación fue evaluada y analizada mediante el método estadístico Alfa de Cronbach para medir su confiabilidad. Para el análisis, se empleó el software R, el cual permitió aplicar el método de manera eficiente y obtener resultados precisos sobre la confiabilidad del instrumento (Quispe et al. 2020).

Tabla 3. Confiabilidad del instrumento "Cuestionario"

	Estadística de fiabilidad
Alfa de Cronbach	N° de elementos
0.857	12

Fuente: Elaboración Propia

3.5. Procedimientos

El estudio incluyó tres objetivos específicos, cuyo desarrollo e implementación engloba las siguientes actividades:

Objetivo específico 1: Diseñar controles de seguridad adecuados para proteger la información confidencial. se recopiló los datos relacionados con la gestión de la confidencialidad de la información de una UGEL, para ello se solicitó el permiso correspondiente y se manejó la técnica de la encuesta y observación. Para la técnica de encuesta, se empleó un cuestionario personalizado que consta de cinco preguntas o ítems y para la técnica de observación se manejó la ficha de registro de incidentes. para observar en detalle los instrumentos revisar los anexos 3, 4, 5, 6, 7, 8 y 9. En busca de salvaguardar la información de carácter confidencial, se aplicaron controles según el estándar ISO 27001.

Objetivo específico 2: Garantizar la integridad de los datos a través de la implementación un sistema de planillas basado en controles de seguridad. Fue necesario recopilar los datos relacionados con la gestión de la integridad de la información de una UGEL, para ello se solicitó el permiso correspondiente y se aplicó la técnica de la encuesta y observación. Para la técnica de encuesta, se empleó un cuestionario personalizado que consta de cinco preguntas o ítems y para la técnica de observación se manejó la ficha de registro de incidentes. para observar en detalle los instrumentos revisar los anexos 3, 4, 5, 6, 7, 8 y 9. Para cautelar y mejorar la integridad de la información se aplicó controles del estándar ISO 27001.

Objetivo específico 3: Garantizar la disponibilidad de los datos a través de la implementación de un sistema de planillas basado en controles de seguridad. Fue necesario recopilar los datos relacionados con la disponibilidad de la información en una UGEL. Se solicitó el permiso respectivo, y se utilizó la técnica de la encuesta y observación. Para la técnica de la encuesta, se empleó un cuestionario personalizado que consta de cinco preguntas o ítems y para la técnica de observación se manejó la ficha de registro de incidentes. para observar en detalle los instrumentos revisar los anexos 3, 4, 5, 6, 7, 8 y 9. Para mejorar la disponibilidad de la información se aplicará procedimientos, normativa y controles del estándar ISO 27001

3.6. Método de análisis de datos

Se utilizó estadística descriptiva para visualizar y tabular gráficamente la situación antes (pre-test) y después (post-test) de la implementación de la solución propuesta, con la misma población antes y después de la implementación propuesta. Esta técnica permitió visualizar de forma clara y concisa los cambios y mejoras obtenidas.

Se aplicó estadística inferencial para evaluar la normalidad de cada indicador utilizado en la investigación, acorde con los objetivos específicos establecidos. La técnica también se representó gráfica y tubularmente, proporcionando información relevante sobre la distribución de los datos y permitiendo sacar inferencias y conclusiones más precisas.

Basándonos en lo señalado en el párrafo previo, la estadística inferencial se enfoca en el análisis de técnicas y procedimientos, en el estudio, se empleó el método t de Student cuyo propósito fue realizar la comparación entre dos muestras provenientes de una misma población. Esta elección se debe al hecho de que la población en cuestión es de menor tamaño. Además, se empleó el método deductivo, el cual es común en investigaciones cuantitativas. Este enfoque se fundamenta en la aplicación de generalidades y principios generales para llegar a conclusiones y resultados específicos. En este caso, se partió de conceptos y teorías establecidas para analizar y comprender los datos recolectados en el estudio.

En resumen, se utilizó métodos de estadística descriptiva e inferencial en el procesamiento de los datos recopilados. La estadística descriptiva mostrara la situación antes y después de la intervención, mientras que la estadística inferencial evaluara la normalidad de los indicadores. En consecuencia, se empleó el método deductivo para realizar el análisis cuantitativo en base a principios generales.

3.7. Aspectos Éticos

Los aspectos éticos considerados durante el proceso de investigación incluyen metas universitarias, valores, lineamientos éticos, responsabilidades, política de creatividad, derechos de autor, etc. Estas disposiciones rigen los derechos y responsabilidades de los investigadores y tienen como objetivo garantizar que la investigación se lleve a cabo de acuerdo con los estándares establecidos por la institución académica en materia de seguridad y calidad.

La elaboración de la declaración de autoría evidencia el reconocimiento por parte de los autores de que la investigación es de su autoría.

La creación de la declaración de originalidad certifica la aprobación del asesor de que la investigación es única y propiedad de los autores.

Para la creación del informe de similitud mediante el empleo de Turnitin confirma la utilización de un programa anti plagio para asegurar la originalidad del trabajo.

Además, se ha considerado el consentimiento informado como un procedimiento ético y legal. En este proceso, las personas con plena capacidad mental otorgan su aprobación de manera voluntaria y consciente para participar en intervenciones médicas, tratamientos, investigaciones u otros procedimientos que puedan afectar su salud, privacidad o derechos.

Por otra parte, el estudio se llevó a cabo siguiendo el formato ISO-690, el cual es un requisito obligatorio de la Universidad para la presentación de la investigación. Es fundamental resaltar que el trabajo de investigación será de elaboración propia y original, por lo tanto, se debe respetar los derechos de autor para asegurar la legitimidad y autenticidad de la investigación.

IV. RESULTADOS

El propósito del estudio de investigación, desea comprobar, que tanto influyen los controles de seguridad en la operatividad del proceso de planillas. En esta situación, vamos a demostrar que la implementación de un sistema de planillas centrado en medidas de seguridad en una UGEL puede tener impactos positivos o negativos en la protección de la información personal, abarcando los aspectos de confidencialidad, integridad y disponibilidad.

Con el fin de demostrar los resultados, se realizó un análisis exhaustivo tanto descriptivo como inferencial de la cantidad de datos recolectados mediante los instrumentos de recopilación. Según (Rendón-Macías, Villasís-Keever y Miranda-Navales 2016), la estadística descriptiva se utiliza con el propósito de simplificar y resumir los datos que han sido procesados y convertidos en información, permitiendo así la adaptación de modelos a la realidad que se está investigando. En cuanto a la estadística inferencial, opera en sentido contrario, ya que, a partir del análisis de frecuencias de una variable, busca inferir el modelo probabilístico que ha dado origen a los datos (Llinás Solano 2018).

4.1. Análisis descriptivo.

En el contexto de este análisis, nos proponemos condensar la información recopilada en nuestra muestra para obtener una visión general y caracterizar a los participantes en el estudio. Dado que estamos tratando con variables numéricas, utilizamos medidas de tendencia central como la media, la moda y la mediana. Es importante señalar que, en el contexto de este estudio, el conjunto de datos es el mismo que el de la muestra. Para lograrlo, monitoreamos el desempeño de nuestros indicadores dos veces: antes y después de la implementación de un sistema de planillas basado en controles de seguridad. Tal como lo establecen los objetivos específicos de la investigación:

OE1. Diseñar controles de seguridad adecuados para proteger la información confidencial.

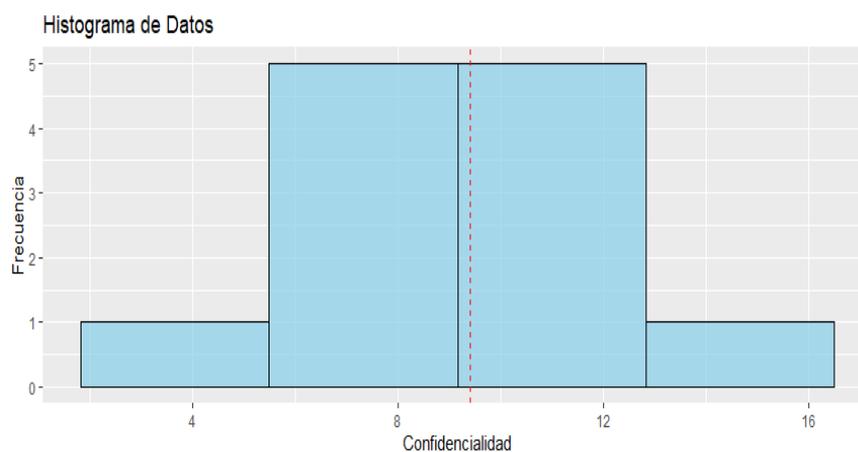
4.1.1. Indicador 1.- Proteger la confidencialidad de los datos

Tabla 4. Descripción estadística del indicador proteger la confidencialidad de los datos antes y después de la implementación

	Media	Mediana	Moda	Desviación Estándar	Mínimo	Máximo	Coefficiente de Variación
PRE	9.417	10	6	3.315	5	16	35.209
POST	23.333	24	25	1.723	20	25	7.385

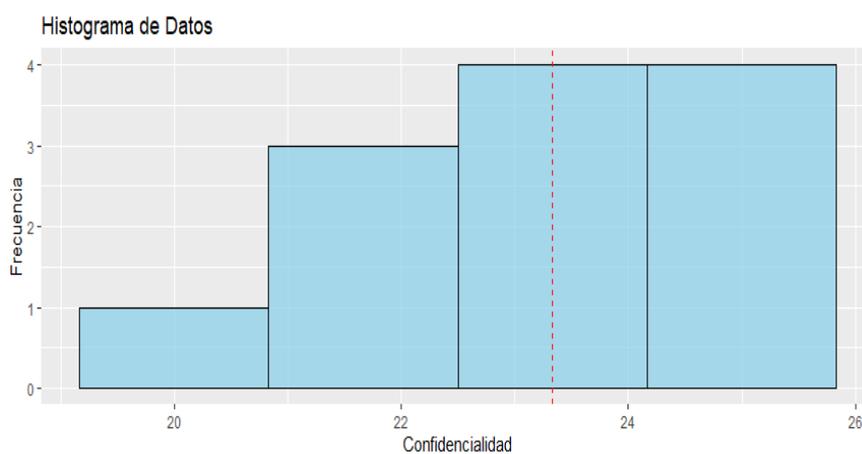
Fuente: Elaboración Propia

Figura 2. Histograma del indicador proteger la confidencialidad de los datos – Pre Test.



Fuente: Elaboración Propia

Figura 3. Histograma del indicador proteger la confidencialidad de los datos – Post Test.



Fuente: Elaboración Propia

El análisis revela una disparidad en las medias. En el pretest, fue de 9.417, en contraste con una media en el post test de 23.33. Esto sugiere que la introducción de la variable independiente tuvo un impacto en el momento de su implementación. En términos de protección de la confidencialidad de los datos, se encontró que el mínimo era 5 antes de la implementación y 20 después de la implementación. La variabilidad de la protección de la confidencialidad de los datos disminuyó del 35,20% al 7,38%.

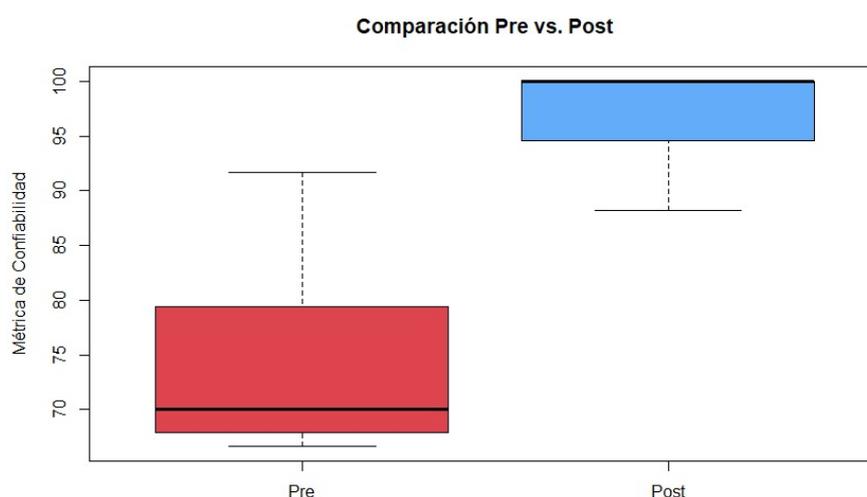
4.1.2. Indicador 2.- Métrica de Confidencialidad

Tabla 5. Descripción estadística del indicador de confidencialidad de los datos tanto antes como después de la implementación.

	Media	Mediana	Moda	Desviación Estándar	Mínimo	Máximo	Coefficiente de Variación
PRE	74.910	70	66.667	9.277	66.667	91.667	12.384
POST	97.589	100	100	3.813	88.235	100	3.908

Fuente: Elaboración Propia

Figura 4. Gráfico comparativo del indicador de confidencialidad antes y después de la implementación.



Fuente: Elaboración Propia

El análisis muestra una disparidad en las medias. La media de la métrica previo a la implementación se situó en 74.91, en contraste con una

media la métrica posterior a la implantación de 97.59. Esto indica que la variable independiente ejerció un efecto significativo una vez que se puso en marcha. En cuanto a la métrica de confidencialidad, se observó que el valor mínimo antes de la implantación fue de 66, en comparación con la métrica de confidencialidad posterior, que alcanzó 88. La dispersión de la métrica de confidencialidad disminuyó de 12.3% a 3.90%, lo que sugiere que la variabilidad en los datos no experimentó un cambio sustancial. En consecuencia, se determina que la comparación de los valores promedio es adecuada.

OE2. Garantizar la integridad de los datos a través de la implementación un sistema de planillas basado en controles de seguridad.

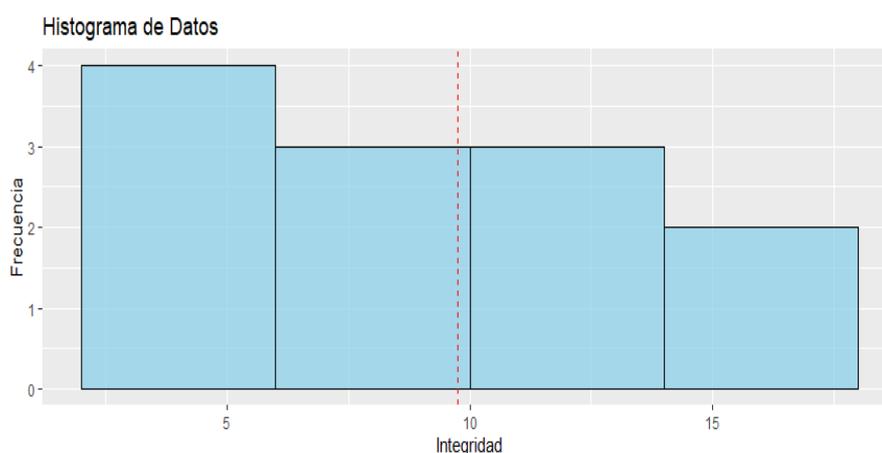
4.1.3. Indicador 3.- Garantizar la integridad de los datos

Tabla 6. Descripción estadística del indicador garantizar la integridad de los datos antes y después de la implementación

	Media	Mediana	Moda	Desviación Estándar	Mínimo	Máximo	Coefficiente de Variación
PRE	9.417	10	6	3.315	5	16	35.209
POST	23.333	24	25	1.723	20	25	7.385

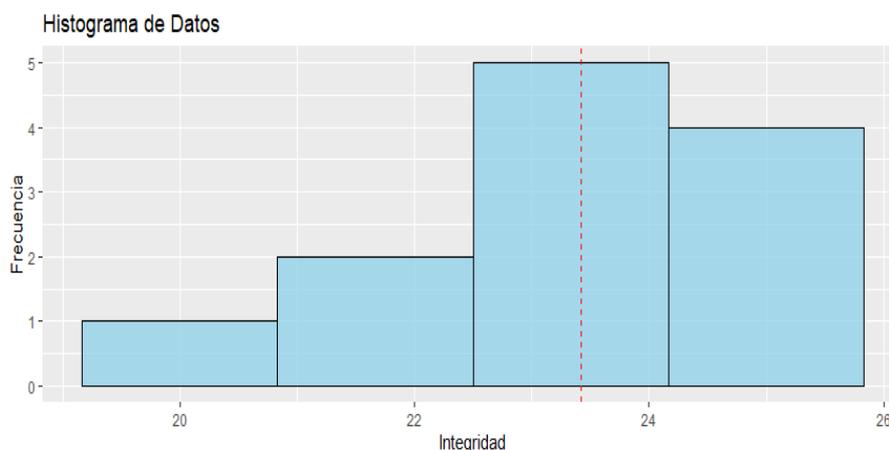
Fuente: Elaboración Propia

Figura 5. Gráfico de Histograma de los datos en el indicador garantizar la integridad antes de la implementación – Pre Test.



Fuente: Elaboración Propia

Figura 6. Gráfico de Histograma de los datos en el indicador garantizar la integridad antes de la implementación – Post Test.



Fuente: Elaboración Propia

Como muestra el análisis, existen diferencias en las medias. en el pre test fue de 9.417, en contraste con una media del post test de 23.33. Esto sugiere que la variable independiente ejerció un impacto en el momento de su implementación. En cuanto a garantizar la integridad de los datos, se observó que el valor mínimo antes de la implementación fue de 5 y después de la implementación fue 20. La dispersión de garantizar la integridad de los datos disminuyó del 35.20% a 7.38%.

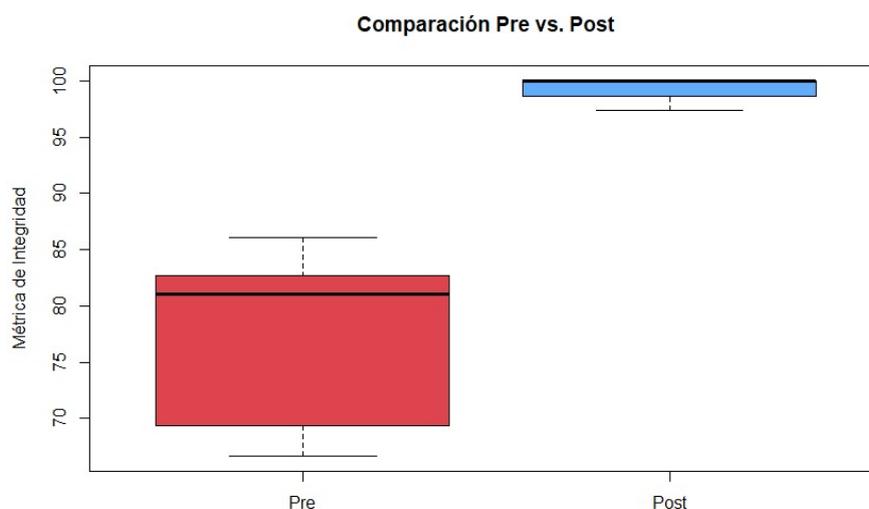
4.1.4. Indicador 4.- Métrica de Integridad

Tabla 7. Descripción estadística del indicador de Integridad antes y después de la implementación

	Media	Mediana	Moda	Desviación Estándar	Mínimo	Máximo	Coficiente de Variación
PRE	76.885	81.034	83.333	7.299	66.667	86.076	9.493
POST	99.262	100	100	0.920	97.414	100	0.927

Fuente: Elaboración Propia

Figura 7. Gráfico comparativo del indicador de Integridad antes y después de la implementación.



Fuente: Elaboración Propia

El análisis puso de manifiesto una diferencia en las medias. La media de la métrica antes de la implementación fue de 76.88, en contraste con una media de la métrica posterior de 99.26. Esto señala que la variable independiente ejerció un impacto en el momento de su implementación. En cuanto a la métrica de integridad, se observó que el valor mínimo antes de la implementación fue de 66, en comparación con la métrica de integridad posterior, que alcanzó 97. La dispersión de la métrica de integridad disminuyó de 9.49% a 0.92%, lo que sugiere que la variabilidad en los datos no experimentó un cambio sustancial. Por lo tanto, se estima que la confrontación de los promedios es adecuada.

OE3. Garantizar la disponibilidad de los datos a través de la implementación de un sistema de planillas basado en controles de seguridad.

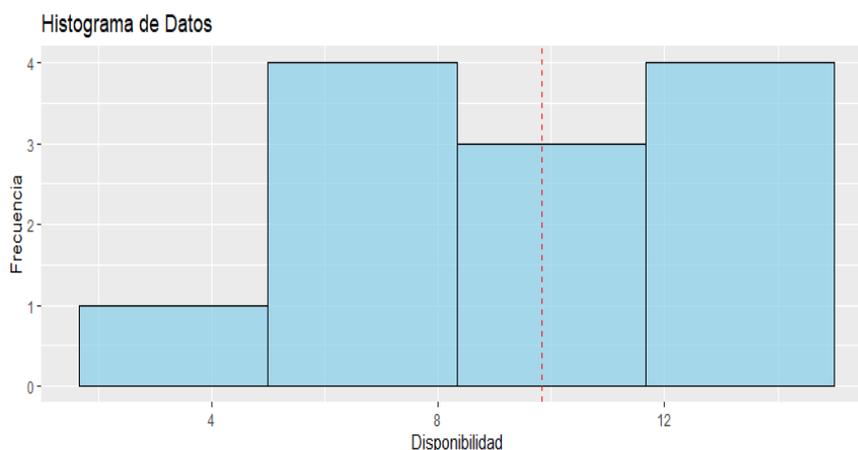
4.1.5. Indicador 5.- Garantizar la Disponibilidad de los datos

Tabla 8. Descripción estadística del indicador garantizar la disponibilidad de los datos antes y después de la implementación

	Media	Mediana	Moda	Desviación Estándar	Mínimo	Máximo	Coefficiente de Variación
PRE	9.833	10.5	7	3.407	5	15	34.645
POST	23.583	23.5	23	1.084	22	25	4.595

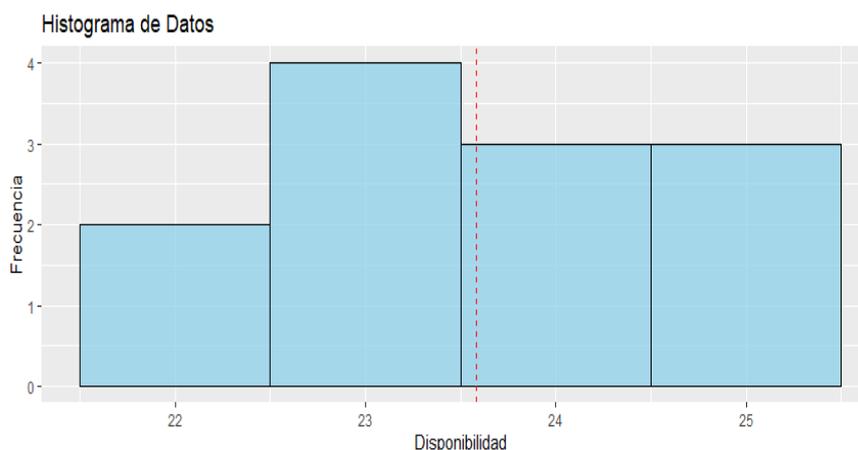
Fuente: Elaboración Propia

Figura 8. Gráfico de Histograma de los datos en el indicador garantizar la disponibilidad de los datos antes de la implementación – Pre Test.



Fuente: Elaboración Propia

Figura 9. Gráfico de Histograma de los datos en el indicador garantizar la disponibilidad de los datos después de la implementación – Post Test.



Fuente: Elaboración Propia

El análisis evidencia una diferencia en las medias. en el pre test fue de 9.83, en contraste con una media del post test de 23.58. Esto sugiere

que la variable independiente tuvo un impacto en el momento de su implementación. En cuanto a garantizar la integridad de los datos, se observó que el valor mínimo antes de la implementación fue de 5 y después de la implementación fue 22. La dispersión de garantizar la disponibilidad de los datos disminuyó de 34.64% a 4.59%.

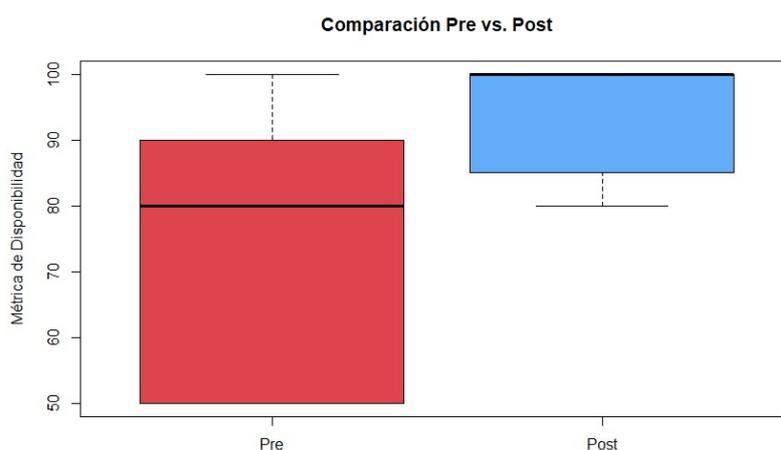
4.1.6. Indicador 6.- Métrica de Disponibilidad

Tabla 9. Descripción estadística del indicador disponibilidad antes y después de la implementación

	Media	Mediana	Moda	Desviación Estándar	Mínimo	Máximo	Coficiente de Variación
PRE	74.667	80	50	20.307	50	100	27.197
POST	93.333	100	100	8.997	80	100	9.640

Fuente: Elaboración propia

Figura 10. Gráfico comparativo del indicador de Disponibilidad antes y después de la implementación.



Fuente: Elaboración propia

El análisis reveló una disparidad en las medias. La media de la métrica antes de la implantación fue de 74.66, en contraste con una media de 93.33 para la métrica posterior. Esto sugiere que la variable independiente ejerció un efecto en el momento de su implementación. En lo que respecta a la métrica de disponibilidad, se observó que el valor mínimo antes de la implantación fue de 50, en comparación con una métrica de disponibilidad posterior de 80. La dispersión de la métrica de disponibilidad disminuyó de 27.19% a 9.64%, lo que sugiere que la

variabilidad en los datos no experimentó un cambio significativo. Por tanto, se considera apropiado comparar valores medios.

4.2. Análisis Inferencial.

4.2.1. Prueba de Normalidad

Según lo indicado por (Tapia y Cevallos 2021), el estadístico de Shapiro - Wilks se emplea para llevar a cabo la evaluación de la normalidad cuando el tamaño de las muestras es inferior a 30. En la situación actual de este estudio, se dispone de conjuntos de datos con un máximo de 15 observaciones que serán sujetos a este tipo de análisis estadístico.

Se utilizó como indicador de estimación un nivel de confianza del 5%. Esto significa que el valor de significancia cumple con la siguiente regla: Sig. ≥ 0.05 , nos encontraremos con una distribución que sigue un patrón normal.

Sig. < 0.05 , nos encontraremos con una distribución que sigue un patrón no normal.

OE1. Diseñar controles de seguridad adecuados para proteger la información confidencial.

4.2.1.1 Indicador 1.- Proteger la confidencialidad de los datos.

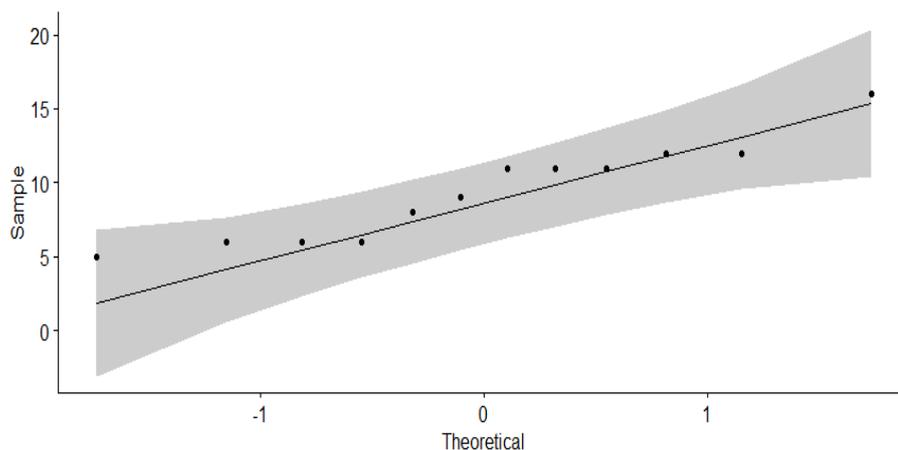
Tabla 10. prueba de normalidad para el indicador Proteger la confidencialidad de los datos pre test y post test

	Estadístico	gl.	Sig.
PRE	0.9216	12	0.3
POST	0.8729	12	0.0713

Fuente: Elaboración Propia

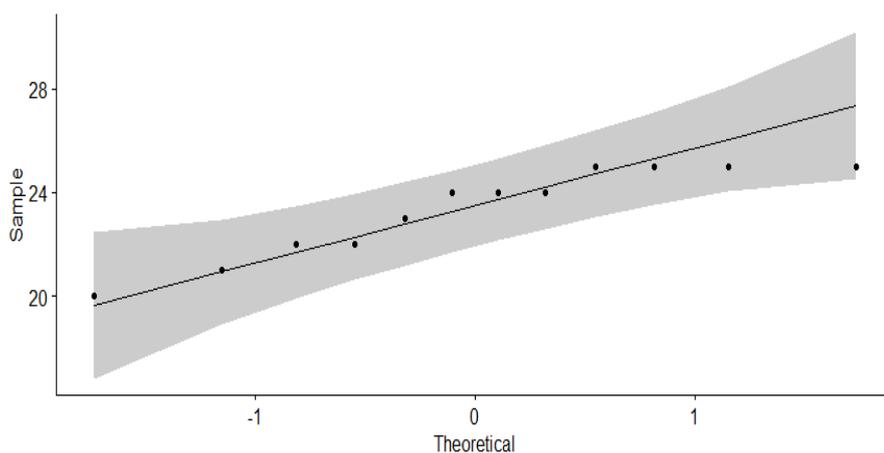
Los resultados obtenidos del indicador Proteger la confidencialidad de los datos arrojaron un valor de Sig. igual a 0.3 en antes de la implementación y un valor de Sig. Igual a 0.0713 posterior a la implementación. Según el nivel de confiabilidad establecido, esta cifra indica que nos encontramos ante una distribución normal tanto en la fase de pre-test como en la de post-test. Esto implica que se utilizara una prueba paramétrica.

Figura 11. gráfico de cuantiles-cuantiles en el indicador Proteger la confidencialidad de los datos (pre test).



Fuente: Elaboración Propia

Figura 12. gráfico de cuantiles-cuantiles en el indicador Proteger la confidencialidad de los datos (post test).



Fuente: Elaboración Propia

Tabla 11. Correlación de los datos en antes (pre test) y después (post test) de la implementación

Test	Sig(p)	Rho
Prueba de Correlación de Spearman	0.9641	0.0146

Fuente: Elaboración Propia

De acuerdo a la información proporcionada en la tabla número 11, se observa que el p es 0.0146, lo que sugiere una correlación muy baja o prácticamente nula. Por lo tanto, se acepta que hubo un cambio

significativo en el post influenciado por la implementación del sistema de planillas basado en controles de seguridad.

4.2.1.2 Indicador 2.- Métrica de Confidencialidad.

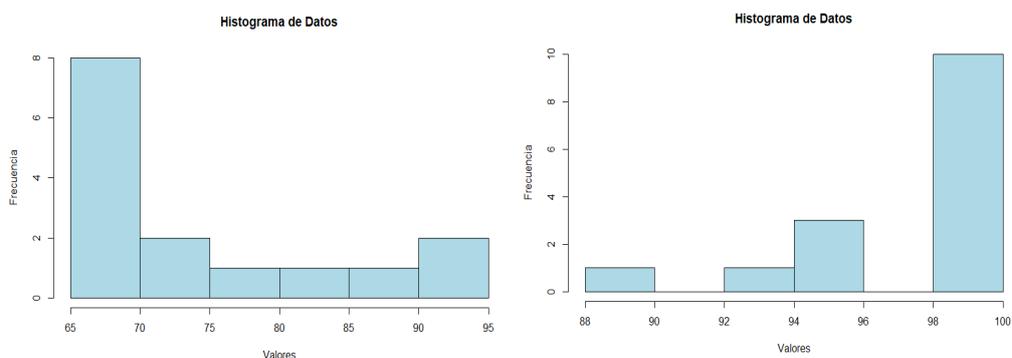
Tabla 12. prueba de normalidad para el indicador de confidencialidad antes y después de la implementación

	Estadístico	gl	Sig
PRE	0.803	15	0.00397
POST	0.687	15	0.00018

Fuente: Elaboración Propia

Los resultados conseguidos para el indicador de Confidencialidad arrojaron un valor de Sig. igual a 0.003 en la métrica antes de la implantación y un valor de Sig. Igual a 0.00018 en la métrica después de la implementación. Según el nivel de confiabilidad establecido, esta cifra indica que nos encontramos ante una distribución no normal tanto en la fase de pre-test como en la de post-test. Esto implica que optaremos por utilizar una prueba no paramétrica.

Figura 13. Histograma de prueba de normalidad de la métrica de confidencialidad antes y después de la implantación.



Fuente: Elaboración Propia

OE2. Garantizar la integridad de los datos a través de la implementación un sistema de planillas basado en controles de seguridad.

4.2.1.3 Indicador 3.- Garantizar la integridad de los datos.

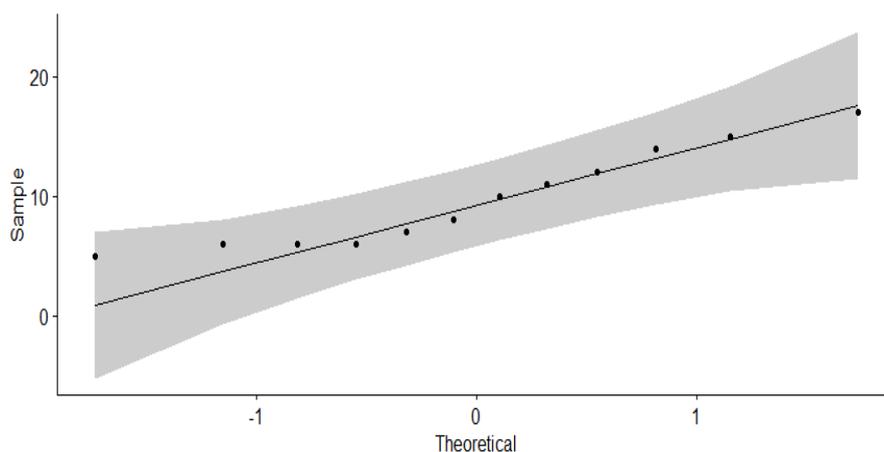
Tabla 13. prueba de normalidad del indicador garantizar la integridad de los datos antes y después de la implementación

	Estadístico	gl	Sig
PRE	0.9121	12	0.2271
POST	0.8844	12	0.0998

Fuente: Elaboración Propia

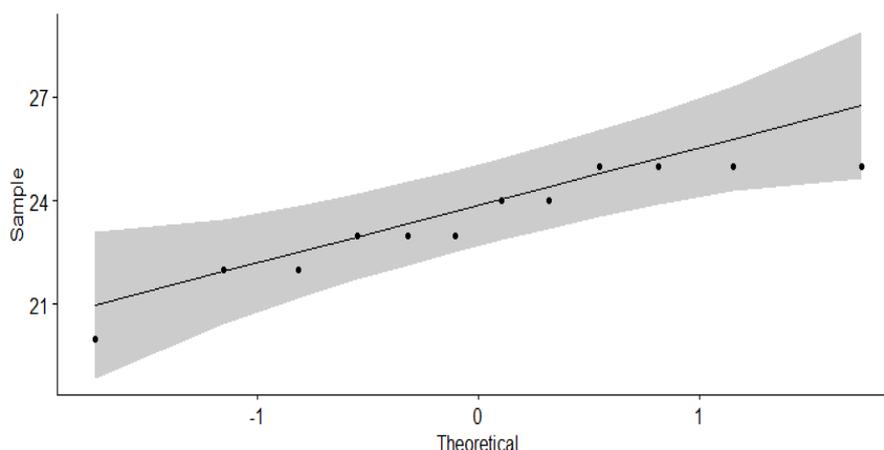
Los resultados logrados para el indicador de garantizar la integridad de los datos arrojaron un valor de Sig. igual a 0.227 en antes de la implementación y un valor de Sig. Igual a 0.0998 posterior a la implementación. Según el nivel de confiabilidad establecido, esta cifra indica que nos encontramos ante una distribución normal tanto en la fase de pre-test como en la de post-test. Esto implica que se utilizara una prueba paramétrica.

Figura 14. gráfico de cuantiles-cuantiles en el indicador garantizar la integridad de los datos (pre test).



Fuente: Elaboración Propia

Figura 15. gráfico de cuantiles-cuantiles en el indicador garantizar la integridad de los datos (post test).



Fuente: Elaboración Propia

Tabla 14. Correlación de los datos en antes y después de la implementación

Test	Sig(p)	Rho
Prueba de Correlación de Spearman	0.1819	0.3721

Fuente: Elaboración Propia

Según la información proporcionada en la tabla número N° 12, se observa que el ρ es 0.372, lo que sugiere una correlación muy baja o prácticamente nula. Por lo tanto, se acepta que hubo un cambio significativo en el post influenciado por la implementación del sistema de planillas basado en controles de seguridad.

4.2.1.4 Indicador 4.- Métrica de Integridad.

Tabla 15. prueba de normalidad para el indicador de Integridad antes y después de la implementación

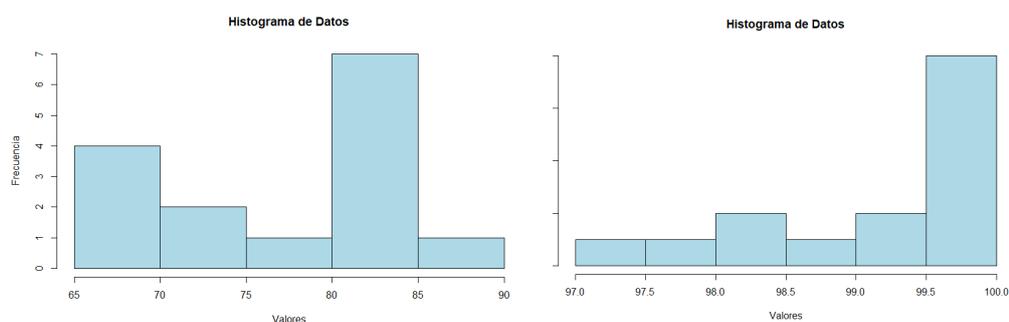
	Estadístico	gl	Sig
PRE	0.854	15	0.01962
POST	0.792	15	0.00287

Fuente: Elaboración Propia

Los resultados alcanzados para el indicador de Integridad arrojaron un valor de Sig. igual a 0.019 en la métrica antes de la implantación y un valor de Sig. Igual a 0.002 en la métrica después de la implementación.

Según el nivel de confiabilidad establecido, esta cifra indica que nos encontramos ante una distribución no normal tanto en la fase de pre-test como en la de post-test. Esto implica que optaremos por utilizar una prueba no paramétrica.

Figura 16. Histograma de prueba de normalidad de la métrica de integridad antes y después de la implantación.



Fuente: Elaboración Propia

OE3. Garantizar la disponibilidad de los datos a través de la implementación de un sistema de planillas basado en controles de seguridad.

4.2.1.5 Indicador 5.- Garantizar la disponibilidad de los datos.

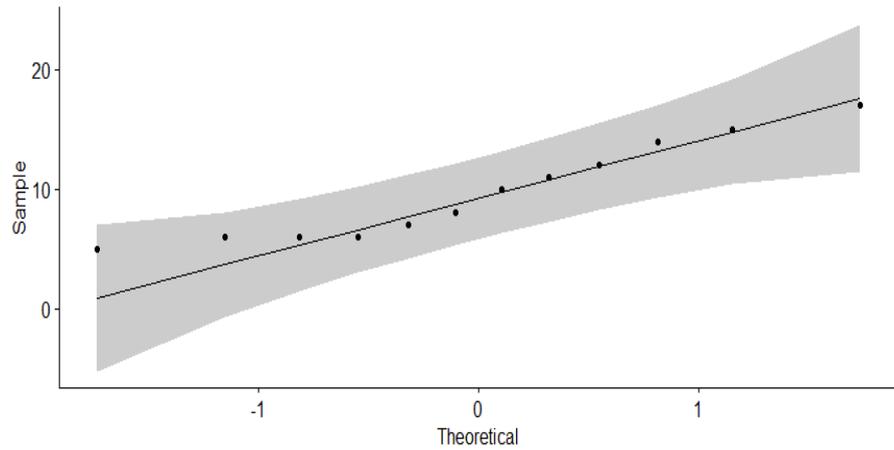
Tabla 16. prueba de normalidad del indicador garantizar la disponibilidad de los datos antes y después de la implementación

	Estadístico	gl	Sig.
PRE	0.9194	12	0.2817
POST	0.8901	12	0.1182

Fuente: Elaboración Propia

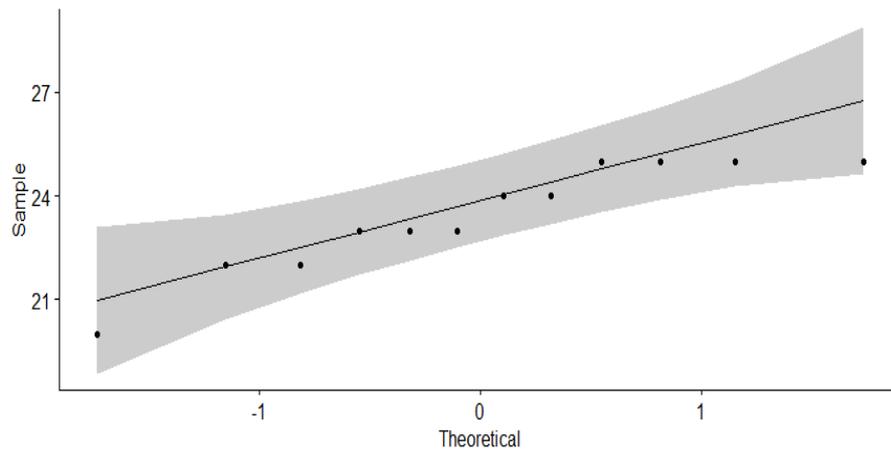
Los resultados conseguidos para el indicador de Garantizar la disponibilidad de los datos arrojaron un valor de Sig. igual a 0.281 en antes de la implementación y un valor de Sig. Igual a 0.1182 posterior a la implementación. Según el nivel de confiabilidad establecido, esta cifra indica que nos encontramos ante una distribución normal tanto en la fase de pre-test como en la de post-test. Esto implica que se utilizara una prueba paramétrica.

Figura 17. gráfico de cuantiles-cuantiles para el indicador de garantizar la integridad de los datos (pre test).



Fuente: Elaboración Propia

Figura 18. gráfico de cuantiles-cuantiles para el indicador de garantizar la integridad de los datos (post test).



Fuente: Elaboración Propia

Tabla 17. Correlación de los datos en pre test y post test

Test	Sig(p)	Rho
Prueba de Correlación de Spearman	0.7597	0.0989

Fuente: Elaboración Propia

Según la información proporcionada en la tabla número N° 15, se observa que el p es 0.0989, lo que sugiere una correlación muy baja o prácticamente nula. Por lo tanto, se acepta que hubo un cambio

significativo en el post influenciado por la implementación del sistema de planillas basado en controles de seguridad.

4.2.1.6 Indicador 6.- Métrica de Disponibilidad.

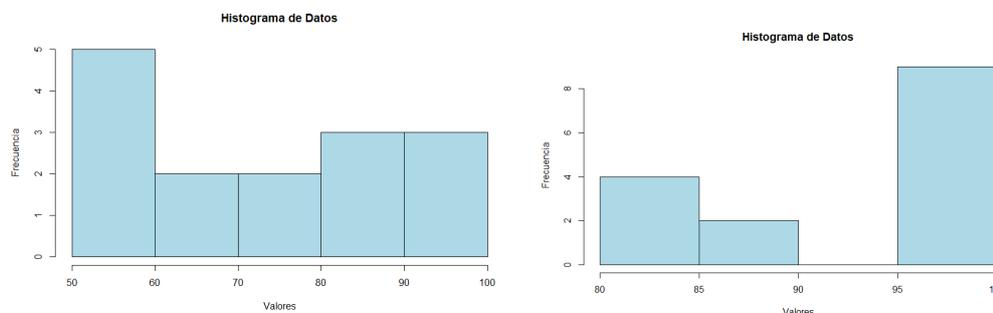
Tabla 18. prueba de normalidad del indicador de disponibilidad antes y después de la implementación

	Estadístico	gl	Sig.
PRE	0.846	15	0.01511
POST	0.686	15	0.00018

Fuente: Elaboración Propia

Los resultados que muestra la tabla 18 corresponden al indicador de disponibilidad, lo cuales arrojaron un valor de Sig. igual a 0.015 en la métrica antes de la implantación y un valor de Sig. Igual a 0.00018 en la métrica después de la implementación. Según el nivel de confiabilidad establecido, esta cifra indica que nos encontramos ante una distribución no normal tanto en la fase de pre test como en la de post test. Esto implica que optaremos por utilizar una prueba no paramétrica.

Figura 19. Histograma de prueba de normalidad de la métrica de disponibilidad antes y después de la implantación.



Fuente: Elaboración Propia

4.2.2 Prueba de Hipótesis

H1: La implementación de un sistema de planillas basado en controles de seguridad optimizara significativamente la protección de la información en una UGEL.

a) Hipótesis de investigación 01

I1 = Indicador de confidencialidad

Variables:

MCa: Métrica de confidencialidad antes de la implementación del sistema.

MCd: Métrica de confidencialidad después de la implementación del sistema.

H10: La implementación de un sistema de planillas basado en controles de seguridad no protege la información confidencial de los datos.

H1a: la implementación de un sistema de planillas basado en controles de seguridad protege significativamente la información confidencial de los datos.

H10: $MCd \leq MCa$, la Métrica después de la implementación es menor o igual que la métrica antes de la implementación.

H1a: $MCd > MCa$, la Métrica después de la implementación es mayor que la métrica antes de la implementación.

Tabla 19. prueba de rangos de Wilcoxon para confidencialidad.

Test	Sig. (p)
Prueba de Rangos Wilcoxon	0.00072

Fuente: Elaboración Propia

Según la información de la Tabla 19, el valor de significancia (Sig.) es 0.00072, el cual se encuentra en la zona de rechazo. Razón por la que, se descarta la hipótesis nula (H10), y se da por aceptada y válida la hipótesis alternativa (H1a), que prescribe: “la implementación de un sistema de planillas basado en controles de seguridad protege significativamente la información confidencial de los datos”.

b) Hipótesis de investigación 02

I2 = Indicador de Integridad

Variables:

MIa: Métrica de integridad antes de la implementación del sistema.

MId: Métrica de Integridad después de la implementación del sistema.

H10: La implementación de un sistema de planillas basado en controles de seguridad no garantiza la integridad de los datos.

H1a: la implementación de un sistema de planillas basado en controles de seguridad garantiza significativamente la integridad de los datos.

H10: $MC_d \leq MC_a$, la Métrica después de la implementación es menor o igual que la métrica antes de la implementación.

H1a: $MC_d > MC_a$, la Métrica después de la implementación es mayor que la métrica antes de la implementación.

Tabla 20. prueba de rangos de Wilcoxon para integridad.

Test	Sig. (p)
Prueba de Rangos Wilcoxon	0.00073

Fuente: Elaboración propia

Según la información de la Tabla 20, se observa que el valor de la significancia (Sig.) es 0.00073, se ubica en la zona de rechazo.

Razón por la cual, se descarta la hipótesis nula (H10), y se da por aceptada la hipótesis alternativa (H1a), que prescribe:

“la implementación de un sistema de planillas basado en controles de seguridad garantiza significativamente la integridad de los datos”.

c) Hipótesis de investigación 03

I3 = Indicador de Disponibilidad

Variables:

MIa: Métrica de Disponibilidad antes de la implementación del sistema.

MId: Métrica de Disponibilidad después de la implementación del sistema.

H10: La implementación de un sistema de planillas basado en controles de seguridad no brinda disponibilidad de los datos.

H1a: la implementación de un sistema de planillas basado en controles de seguridad brinda significativamente la disponibilidad de los datos.

H10: $MC_d \leq MC_a$, la Métrica después de la implementación es menor o igual que la métrica antes de la implementación.

H1a: $MC_d > MC_a$, la Métrica después de la implementación es mayor que la métrica antes de la implementación.

Tabla 21. prueba de rangos de Wilcoxon en Disponibilidad.

Test	Sig (p)
Prueba de Rangos Wilcoxon	0.01037

Fuente: Elaboración Propia

Según la información de la Tabla 21, se observa que el valor de la significancia (Sig.) es 0.01037, se ubica en la zona de rechazo. En consecuencia, se descarta la hipótesis nula (H10), y se acepta como válida la hipótesis alternativa (H1a), que prescribe: “la implementación de un sistema de planillas basado en controles de seguridad garantiza significativamente la Disponibilidad de los datos”.

V. DISCUSIÓN

Los resultados obtenidos en este estudio apoyan la idea de que la implementación de un sistema de planillas basado en controles de seguridad en una UGEL ofrece mejoras significativas en la seguridad de los datos personales de acuerdo con lo establecido en la ley peruana 29733. Este descubrimiento indica que los documentos normativos y los estándares internacionales, como la norma ISO, desempeñan un papel crucial en procesos esenciales dentro de una entidad o empresa. Además, se demuestra que estas normativas tienen un impacto positivo en el control y la gestión de procesos, creando un entorno seguro y confiable.

Con respecto a las investigaciones propuestas por los autores Onyshchenko, Hlushko & Yanko que plantearon garantizar la protección de la información confidencial en medio de una pandemia, asimismo con la investigación de Pradana y Trianto 2018 los cuales identificaron cuatro niveles de apoyo normativo y jurídico destinados a fortalecer la seguridad de la información, tomando en consideración los retos y amenazas que han surgido en el contexto de una pandemia, las organizaciones que manejan datos personales deben establecer políticas internas para la protección y seguridad de los datos. Para ello identificaron 57 controles de privacidad relacionados a la confidencialidad, integridad y disponibilidad de los datos en las empresas y organizaciones. Para ello sugieren implementar herramientas tecnológicas que permitan gestionar de manera eficiente la información y los datos (Onyshchenko, Hlushko y Yanko 2020), (Pradana y Trianto 2018a) e (Iván Blume Moore 2021).

En la presente investigación se aplicó la ley peruana 29733 y su reglamento para diseñar una herramienta tecnológica basada en controles de seguridad para proteger los datos y la información confidencial en la Unidad de Gestión Educativa Local. sin embargo, existen ciertas limitaciones debido a que no se aplica a cabalidad dicha Ley. Esto responde a uno de los objetivos específicos que es diseñar controles de seguridad adecuados para proteger la información confidencial.

La investigación realizada por Sánchez Campos aborda de manera integral la implementación de un modelo de seguridad informática en una Municipalidad

para la protección de datos. Enfocándose en las dimensiones de confidencialidad, integridad y disponibilidad, el proyecto busca prevenir la divulgación, modificación y la interrupción no autorizada de la información. Al implementar este modelo, se observa un impacto significativo en la prevención de la divulgación no autorizada de la información municipal. La mejora del 69.40%, representando un aumento de 3.26 puntos, demuestra la eficacia de la propuesta. Partiendo de una puntuación promedio en la preprueba de 1.51 puntos, el proyecto concluye con una puntuación promedio en la posprueba de 4.77 puntos, evidenciando de manera notable el éxito de la intervención.

En cuanto a la modificación no autorizada de la información, se evidencia un incremento del 65.20%, equivalentes a 3.19 puntos adicionales. Desde una puntuación promedio de 1.67 puntos en la etapa inicial hasta 4.86 puntos al finalizar, el proyecto logra un avance significativo en la protección contra alteraciones no autorizadas de datos.

El tercer componente, la prevención de la interrupción no autorizada de la información municipal, también experimenta una mejora sustancial del 67.30%. Con un aumento de 3.23 puntos, desde un promedio de 1.60 puntos en la fase inicial hasta 4.93 puntos después de la implementación del modelo, los resultados indican una mayor robustez en la seguridad contra interrupciones no autorizadas (Sanchez Campos 2022).

La investigación propuesta destaca por el diseño de controles de seguridad que garantizan la confidencialidad, integridad y disponibilidad de los datos. La implementación de un sistema de planillas basado en controles de seguridad ha demostrado ser efectiva. En cuanto a la protección de la confidencialidad, se observa un incremento significativo del indicador, pasando de un pre test de 9.14 a un post test de 23.33, señalando una mejora sustancial en la salvaguarda de la información confidencial. Similarmente, la garantía de la integridad de los datos también experimenta una mejora notable, con un aumento de la puntuación de 9.417 en el pre test a 23.33 en el post test. Finalmente, en lo que respecta a la disponibilidad de los datos, se observa un cambio significativo, evidenciado por el aumento de la puntuación de 9.83 en el pre test a 23.58 en el post test. Estos resultados indican cambios sustanciales tras la implementación del sistema de

planillas basado en controles de seguridad en la ugel. La propuesta no solo se traduce en mejoras estadísticas, sino que respalda la seguridad integral de los datos municipales, estableciendo un precedente valioso para futuras iniciativas en este ámbito.

El trabajo de Garro Murillo y Navarro Torres para implementar un sistema de cifrado homomórfico para mejorar la seguridad de los datos en las transacciones de ventas en Lugar Expresivo SAC se distingue por su enfoque integral en los aspectos clave de integridad, disponibilidad y confidencialidad. Se observó un impresionante aumento del 90,00 % en las medidas de accesibilidad, lo que supone una mejora significativa con respecto a la prueba preliminar. Después de las pruebas, el índice promedio alcanzó el 100,00%, lo que muestra el progreso general de la disponibilidad comercial. La evaluación de la integridad de los datos también mostró una mejora positiva del 90,00%, reflejada por una diferencia del 10,00% entre los valores medios previos y posteriores a la prueba, que también alcanzaron el 100,00%. Estos resultados muestran que la implementación del sistema tiene un impacto positivo en la retención y coherencia de los datos. En cuanto a la medida de protección de la privacidad, el análisis de los resultados mostró que el valor medio previo a la prueba y el valor medio del índice posterior a la prueba alcanzaron el 100%, que fue 0,00% igual, lo que resultó en una mejora del 100,00%. Este resultado fortalece la eficacia del cifrado homomórfico en la protección de información confidencial.

Para la investigación propuesta se utilizó métricas específicas para evaluar la confidencialidad, integridad y disponibilidad de los datos en las planillas de pago. Los resultados muestran mejoras significativas en todas las áreas después de la implementación de la herramienta tecnológica.

En la métrica de confidencialidad, el índice de incidentes de confidencialidad presenta un notable aumento, pasando de 74.71 en el pretest a 97.59 en el postest. Esto indica una mayor seguridad en el manejo de datos confidenciales. La métrica de integridad, evaluada a través del número de registros correctos en las planillas de pago, también experimenta un avance sustancial. Iniciando con un pretest de 76.88, alcanza un post test de 99.26, indicando una mejora significativa en la integridad de los datos procesados. En cuanto a la métrica de

disponibilidad, que considera el tiempo diario de disponibilidad de los servicios de información, se observa un incremento notable. Desde un pretest de 74.66, la métrica concluye con un post test de 93.33, denotando una mayor disponibilidad de datos durante el periodo evaluado.

En resumen, la investigación no solo ofrece resultados cuantificables que respaldan la efectividad del sistema propuesto, sino que también destaca su impacto positivo en la seguridad de datos y la eficiencia operativa en Lugar Expresivo SAC. La metodología aplicada y los resultados obtenidos ofrecen una valiosa contribución al campo de la seguridad de la información.

En última instancia, conforme a las perspectivas de autores como Iván Blume Moore y Alvarado 2016, emerge la imperiosa necesidad de aplicar medidas de protección de datos en las entidades y empresas regidas por la ley 29733. Estos expertos enfatizan la urgencia de emprender acciones inmediatas para resguardar la información confidencial, poniendo de relieve la crítica importancia de la seguridad de datos en un entorno normativo específico.

En sintonía con estas premisas, la investigación que aquí se presenta ha alcanzado un hito significativo al concebir controles de seguridad diseñados meticulosamente. Estos controles no solo posibilitan una gestión eficiente de la protección de datos, sino que también aseguran la integridad de la información. Adicionalmente, la investigación ha dirigido sus esfuerzos a garantizar la disponibilidad de los datos, lo cual se ha logrado mediante la implementación de un sistema de planillas respaldado por controles de seguridad específicos (Iván Blume Moore 2021) y (Alvarado 2016).

VI. CONCLUSIONES

Con base en el análisis de la investigación y los resultados obtenidos se llegó a las siguientes conclusiones:

- 1) Se ha comprobado que la implementación del sistema de planillas basado en controles de seguridad en una UGEL mejora significativamente la protección de la información personal. La implementación de los controles previstos en la normativa junto con la introducción de nuevos controles de gestión orientados a la protección de datos personales tuvo un efecto positivo, incrementando significativamente los resultados de los indicadores propuestos para cada dimensión de la protección de datos.
- 2) Se ha alcanzado el objetivo de Diseñar controles de seguridad adecuados para proteger la información confidencial, El análisis ha proporcionado resultados favorables en la discrepancia de medias. La media del índice antes de la implementación fue de 74.91, mientras que la media posterior fue de 97.589. Esto sugiere que la introducción de la variable independiente tuvo un impacto significativo. El índice mínimo de confidencialidad antes de la implementación fue de 66.667, en contraste con el índice posterior de 88.235. La variabilidad en el índice de confidencialidad disminuyó del 12.384% al 3.908%, lo que indica que la dispersión de los datos no experimentó cambios sustanciales. Por lo tanto, se puede considerar apropiada la comparación de las medias.
- 3) Se ha alcanzado el objetivo de garantizar la Integridad de los datos, el análisis ha arrojado resultados positivos en la diferencia de medias. La media del índice antes de la implementación fue de 76,885 mientras que la media posterior fue de 99,262. Esto indica que la introducción de la variable independiente tuvo un impacto significativo. El índice mínimo de integridad antes de la implementación fue de 66.667, en contraste con el índice posterior de 97.414. La dispersión del índice de confidencialidad disminuyó del 9.493% al 0.927%, demostrando que la variabilidad de los datos no difiere considerablemente. Por lo tanto, se puede considerar apropiada la comparación de las medias.

4) Se ha alcanzado el objetivo de garantizar la disponibilidad de los datos, el análisis ha arrojado resultados positivos en la diferencia de medias. La media del índice pre implementación fue de 74,667 mientras que la media posterior fue de 93,333. Esto indica que la introducción de la variable independiente tuvo un impacto significativo. El índice mínimo de disponibilidad antes de la implementación fue de 50, en contraste con el índice posterior de 80. La dispersión del índice de confiabilidad disminuyó del 27.197% al 9.640%, demostrando que la variabilidad de los datos no difiere considerablemente. Por lo tanto, se puede considerar apropiada la comparación de las medias.

VII. RECOMENDACIONES

- a) Se sugiere a los investigadores que tienen interés en ampliar el estudio sobre la implementación de sistemas de seguridad de la información en unidades organizativas de tecnologías de la información (TI) o áreas de TI, que profundicen en aspectos específicos como la infraestructura, la seguridad perimetral y el desarrollo de software. Se recomienda integrar especialmente la seguridad de la información y de los datos en sus análisis.
- b) Se recomienda examinar cómo los sistemas de planillas pueden ser diseñados para cumplir no solo con la legislación peruana, sino también con normativas internacionales relevantes sobre privacidad y protección de datos.
- c) Se sugiere evaluar la eficacia de auditorías independientes y certificaciones de seguridad como un método para garantizar el cumplimiento de los controles de seguridad y la legislación peruana.

REFERENCIAS

ALVARADO, F.J., 2016. La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales. *Foro Jurídico*, no. 15, ISSN 2414-1720.

ÁLVAREZ, L.E., 2017. Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Foro: Revista de Derecho*, no. 27, ISSN 2631-2484.

ÁLVAREZ-RISCO, A., 2020. Justificación de la investigación. En: Accepted: 2020-04-27T19:49:53Z, *Repositorio Institucional - Ulima* [en línea], [consulta: 31 octubre 2023]. Disponible en: <https://repositorio.ulima.edu.pe/handle/20.500.12724/10821>.

Aprueban el uso obligatorio de la Norma Técnica Peruana «NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición», en todas las entidades integrantes del Sistema Nacional de Informática-RESOLUCION MINISTERIAL-Nº 004-2016-PCM. [en línea], [sin fecha]. [consulta: 8 julio 2023]. Disponible en: <http://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/>.

ARELLANO VELOZ, C.E., 2023. *Modelo de gestión de la seguridad de la información en una institución financiera cooperativa* [en línea]. masterThesis. S.I.: Pontificia Universidad Católica del Ecuador. [consulta: 18 julio 2023]. Disponible en: <https://repositorio.pucesa.edu.ec/handle/123456789/4033>.

BARRALES, O.G., 2016. CIBERSEGURIDAD, RETOS Y PROSPECTIVA. *Universita Ciencia*,

- CALISAYA SANA, C.Y. y TARRILLO VILLEGAS, M., 2018. Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799:2007. En: Accepted: 2018-09-24T22:25:55Z, *Universidad Peruana Unión* [en línea], [consulta: 2 julio 2023]. Disponible en: <https://repositorio.upeu.edu.pe/handle/20.500.12840/1380>.
- CHATCHALERMPUN, S. y DAENGSI, T., 2021. Improving cybersecurity awareness using phishing attack simulation. *IOP Conference Series: Materials Science and Engineering*. S.I.: IOP Publishing, pp. 012015. vol. 1088.
- GARRIGA DOMÍNGUEZ, A., 2016. Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua. *Nuevos retos para la protección de datos personales* [en línea], [consulta: 31 octubre 2023]. Disponible en: <https://www.torrossa.com/gs/resourceProxy?an=3125879&publisher=FZ1825>.
- GARRO MURILLO, G.A.V. y NAVARRO TORRES, L.R., 2022. Sistema de encriptación homomórfica para fortalecer la seguridad de datos en las transacciones de ventas en lugar Expresivo SAC. En: Accepted: 2023-02-21T21:21:29Z, *Repositorio Institucional - UCV* [en línea], [consulta: 1 noviembre 2023]. Disponible en: <https://repositorio.ucv.edu.pe/handle/20.500.12692/107120>.
- HERNÁNDEZ-ÁVILA, C.E. y ESCOBAR, N.A.C., 2019. Introducción a los tipos de muestreo. *Alerta, Revista científica del Instituto Nacional de Salud*, vol. 2, no. 1 (enero-junio),
- HUIDOBRO, J., 2007. Tecnologías de información y comunicación. *Universidad Politécnica de Madrid*, vol. 2,

- IVÁN BLUME MOORE, 2021. Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales. *THEMIS Revista de Derecho*, no. 79, ISSN 1810-9934. DOI 10.18800/themis.202101.025.
- KAYES, A.S.M., CHOWDHURY, M.J.M., MOHAMMED, F., NG, A., WATTERS, P. y SCOLYER-GRAY, P., 2019. Ethical Access Control in the Era of Data Breaches. ,
- LADINO, M.I., VILLA, P.A. y LÓPEZ, A.M., 2011. Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia et technica*, vol. 17, no. 47,
- LEÓN, J.Á.Q., 2021. Ciberseguridad y protección de datos personales en el Perú. *Advocatus*, no. 039, ISSN 2523-6261. DOI 10.26439/advocatus2021.n39.5114.
- Ley N.º 29733. [en línea], [sin fecha]. [consulta: 8 julio 2023]. Disponible en: <https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733>.
- LI, S.-H., HU, C.-C. y LIU, C.-C., 2011. Implement Privacy Protection Act in Human Payroll System. *2011 International Symposium on Computer Science and Society*. S.l.: s.n., pp. 369-372. DOI 10.1109/ISCCS.2011.88.
- LLINÁS SOLANO, H., 2018. *Estadística inferencial* [en línea]. S.l.: Universidad del Norte. [consulta: 5 noviembre 2023]. Disponible en: <https://books.google.es/books?hl=es&lr=&id=vXdaDwAAQBAJ&oi=fnd&pg=PP1&dq=estad%C3%ADstica+inferencial&ots=G0VLMF207o&sig=TWrLD47FAnkKZb2Cfmsq63cLC-U>.
- MARTÍNEZ, D.V.S., 2022. Técnicas e instrumentos de recolección de datos en investigación. *TEPEXI Boletín Científico de la Escuela Superior Tepeji del Río*, vol. 9, no. 17,
- MIRTSCH, M., BLIND, K., KOCH, C. y DUDEK, G., 2021. Information security management in ICT and non-ICT sector companies: A preventive innovation

- perspective. *Computers & Security*, vol. 109, ISSN 0167-4048. DOI 10.1016/j.cose.2021.102383.
- MORALES, M.N.Z., 2019. Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. *Revista peruana de computación y sistemas*, vol. 2, no. 2, ISSN 2617-2003. DOI 10.15381/rpcs.v2i2.17103.
- OLGUÍN DECENCIER, M.A., 2023. Modelamiento e implementación de un plan de gobierno de datos en la Universidad de Chile utilizando el framework DAMA. En: Accepted: 2023-05-24T15:43:03Z [en línea], [consulta: 18 julio 2023]. Disponible en: <https://repositorio.uchile.cl/handle/2250/193748>.
- ONYSHCHENKO, S., HLUSHKO, A. y YANKO, A., 2020. Role and Importance of Information Security in a Pandemic Environment. *Науковий журнал «Економіка і регіон»*, no. 2(77), ISSN 2414-0538. DOI 10.26906/EiR.2020.2(77).1954.
- PASTOR, B.F.R., 2019. Población y muestra. *PUEBLO CONTINENTE*, vol. 30, no. 1, ISSN 19915837.
- POZZO, M.I., BORGOBELLO, A. y PIERELLA, M.P., 2018. Uso de cuestionarios en investigaciones sobre universidad: análisis de experiencias desde una perspectiva situada. *Revista Latinoamericana de Metodología de las Ciencias Sociales* [en línea], vol. 8, no. 2, [consulta: 1 julio 2023]. Disponible en: <https://www.memoria.fahce.unlp.edu.ar/library?a=d&c=arti&d=Jpr9347>.
- PRADANA, F.Y. y TRIANTO, N., 2018a. Privacy Control for Personally Identifiable Information on the Information System (Case Study:XYZ Organization). *2018 International Conference on Applied Information Technology and Innovation (ICAITI)*. S.l.: s.n., pp. 50-55. DOI 10.1109/ICAITI.2018.8686766.
- PRADANA, F.Y. y TRIANTO, N., 2018b. Privacy Control for Personally Identifiable Information on the Information System (Case Study:XYZ Organization). *2018 International Conference on Applied Information Technology and Innovation (ICAITI)*. S.l.: s.n., pp. 50-55. DOI 10.1109/ICAITI.2018.8686766.

QUISPE, A.M., PINTO, D.F., HUAMAN, M.R., BUENO, G.M., VALLE-CAMPOS, A.,
QUISPE, A.M., PINTO, D.F., HUAMAN, M.R., BUENO, G.M. y VALLE-
CAMPOS, A., 2020. Metodologías cuantitativas: Cálculo del tamaño de
muestra con STATA y R. *Revista del Cuerpo Médico Hospital Nacional
Almanzor Aguinaga Asenjo*, vol. 13, no. 1, ISSN 2227-4731. DOI
10.35434/rcmhnaaa.2020.131.627.

RENDÓN-MACÍAS, M.E., VILLASÍS-KEEVER, M.Á. y MIRANDA-NOVALES, M.G.,
2016. Estadística descriptiva. *Revista Alergia México*, vol. 63, no. 4,

ROJAS JAÉN, M.C., 2019. Seguridad en los datos e implantación de la NTP-
ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del
RENIEC. En: Accepted: 2020-06-09T00:48:40Z, *Repositorio Institucional -
UCV* [en línea], [consulta: 1 noviembre 2023]. Disponible en:
<https://repositorio.ucv.edu.pe/handle/20.500.12692/43660>.

ROMANSKY, R.P., NONINSKA, I.S., ROMANSKY, R.P. y NONINSKA, I.S., 2020.
Challenges of the digital age for privacy and personal data protection. En:
Cc_license_type: cc_byPrimary_atype: Mathematical Biosciences and
EngineeringSubject_term: Research articleSubject_term_id: Research
article, *Mathematical Biosciences and Engineering*, vol. 17, no. 5, ISSN
1551-0018. DOI 10.3934/mbe.2020286.

SANCHEZ CAMPOS, K.E., 2022. Propuesta de un modelo de seguridad informática
para la protección de datos en la Municipalidad distrital de Pinra, Huánuco
2022. En: Accepted: 2022-12-12T17:55:46Z, *Repositorio Institucional - UCV*
[en línea], [consulta: 2 julio 2023]. Disponible en:
<https://repositorio.ucv.edu.pe/handle/20.500.12692/103456>.

Sistema de Seguridad Cibernética Nacional frente a los ciberataques como
amenaza a la seguridad nacional | Revista de Ciencia e Investigación en
Defensa - CAEN. [en línea], 2020. [consulta: 7 junio 2023]. Disponible en:
<https://www.recide.caen.edu.pe/index.php/recide/article/view/22>.

- SZCZEPANIUK, E.K., SZCZEPANIUK, H., ROKICKI, T. y KLEPACKI, B., 2020. Information security assessment in public administration. *Computers & Security*, vol. 90, ISSN 0167-4048. DOI 10.1016/j.cose.2019.101709.
- TAFUR, R. y IZAGUIRRE, M., 2022. *Cómo hacer un proyecto de investigación*. S.I.: Alpha Editorial.
- TAHERDOOST, H., 2022. Cybersecurity vs. Information Security. *Procedia Computer Science*, vol. 215, ISSN 1877-0509. DOI 10.1016/j.procs.2022.12.050.
- TAPIA, C.E.F. y CEVALLOS, K.L.F., 2021. Pruebas para comprobar la normalidad de datos en procesos productivos:: Anderson-darling, ryan-joiner, shapiro-wilk y kolmogórov-smirnov. *Societas*, vol. 23, no. 2,
- TERÁN TERRANOVA, Y.J., 2021. *Seguridad en la Gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: un Mapeo Sistemático* [en línea]. bachelorThesis. S.I.: s.n. [consulta: 2 julio 2023]. Disponible en: <http://dspace.ups.edu.ec/handle/123456789/20333>.
- USECHE, M.C., ARTIGAS, W., QUEIPO, B. y PEROZO, É., 2019. *Técnicas e instrumentos de recolección de datos cuali-cuantitativos*. [en línea]. S.I.: Universidad de la Guajira. [consulta: 1 julio 2023]. ISBN 978-956-603-704-0. Disponible en: <https://repositoryinst.uniguajira.edu.co/handle/uniguajira/467>.
- WOUILLOZ, M.F., 2023. *Las transformaciones tecnológicas en la gestión pública, a partir de la implementación de la política del Poder Ejecutivo Nacional de Gestión Documental Electrónica (GDE)* [en línea]. Master's Thesis. S.I.: Facultad de Ciencia Política y Relaciones Internacionales. [consulta: 1 noviembre 2023]. Disponible en: <http://rephip.unr.edu.ar/handle/2133/25484>.
- ZAPATA ROSALES, L.A. del C., 2019. Implementación de sistema para el pago de planillas en el Consorcio Arquidiocesano de Colegios Parroquiales de Piura. En: Accepted: 2019-05-08T21:41:30Z, *Universidad de Piura* [en línea], [consulta: 2 julio 2023]. Disponible en: <https://pirhua.udep.edu.pe/handle/11042/3976>.

ZEPEDA CORONADO, F.R. y TALAVERA FLORES, M.A., 2004. *Sistema de planilla*. PhD Thesis. S.I.: s.n.

ANEXOS

Anexo 01 Matriz de Consistencia

MATRIZ DE CONSISTENCIA											
Título	Pregunta General	Objetivo General	Preguntas específicas	Objetivos específicos	Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición	Diseño metodológico
Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley peruana 29733 en UGEL, 2023	¿Cómo un sistema de planillas basado en controles de seguridad permite proteger los datos personales?	Mejorar la protección de datos personales en una UGEL mediante un sistema de planillas basado en controles de seguridad aplicando la Ley Peruana 29733.	<p>¿de qué manera un sistema de planillas basado en controles de seguridad contribuye a la protección de la información confidencial en una Unidad de Gestión Educativa Local en el año 2023?,</p> <p>¿de qué manera un sistema de planillas basado en controles de seguridad garantiza la integridad de la información en una Unidad de Gestión Educativa Local en el año 2023?</p> <p>¿de qué manera un sistema de planillas basado en controles de seguridad puede brindar disponibilidad de la información en una Unidad de Gestión Educativa Local en el año 2023?</p>	<p>Diseñar controles de seguridad adecuados para proteger la información confidencial.</p> <p>Garantizar la integridad de los datos a través de la implementación un sistema de planillas basado en controles de seguridad.</p> <p>Garantizar la disponibilidad de los datos a través de la implementación de un sistema de planillas basado en controles de seguridad.</p>	Sistema basado en controles de Seguridad	Un sistema basado en controles de seguridad se refiere a un enfoque o conjunto de medidas diseñadas para proteger los activos, información y procesos de una organización contra posibles amenazas y riesgos de seguridad. Estos controles son mecanismos implementados para prevenir, detectar, mitigar y responder a incidentes de seguridad, con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de los recursos de la organización. Estos controles pueden incluir políticas, procedimientos, tecnologías y prácticas específicas que se implementan y mantienen para garantizar un nivel adecuado de seguridad de la información y la infraestructura. (Terán Terranova 2021)	El sistema basado en controles de seguridad contempla medidas para prevenir, detectar, mitigar y responder a incidentes de seguridad, con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad seguridad. Se utilizó como técnica la encuesta y observación y como instrumentos el cuestionario y ficha de observación				Muestra por conveniencia de 12 empleados de una UGEL

					Protección de data Personal	Se refiere a las medidas y prácticas adoptadas para salvaguardar la integridad y la privacidad de la información personal de los individuos. Se refiere a las medidas para salvaguardar la información que identifica o puede identificar a una persona física, como su número de teléfono, dirección, DNI, correo electrónico, información financiera, datos de salud, entre otros. (León 2021).	Se implementan políticas y procedimientos establecidos para utilizar mecanismos técnicos de apoyo con el fin de proteger los datos almacenados en el sistema, asegurando así el cumplimiento de las formalidades necesarias.	<p>Confidencialidad(Onyshchenko, Hlushko y Yanko 2020; Pradana y Trianto 2018a; Szczepaniuk et al. 2020).</p> <p>Integridad(Onyshchenko, Hlushko y Yanko 2020; Morales 2019; Taherdoost 2022).</p> <p>Disponibilidad (Pradana y Trianto 2018a; Taherdoost 2022; Kayes et al. 2019)</p>	<p>Proteger la confidencialidad de los datos.</p> <p>Métrica de confidencialidad.</p> <p>Garantizar la integridad de los datos.</p> <p>Métrica de integridad.</p> <p>Garantizar la Disponibilidad de los datos.</p> <p>Métrica de disponibilidad</p>	<p>Ordinal</p> <p>Escala de Likert</p> <p>Nunca (1) Rara vez (2) A veces (3) Casi siempre (4) siempre (5)</p> <p>Razón</p> <p>INCONF = ((TRS- N°IC)/TRS)%</p> <p>ININTE = (N° RC/N° R)%</p> <p>INCONT = ((TH – THSSI)/TH)%</p>	
--	--	--	--	--	-----------------------------	---	--	---	--	--	--

Anexo 02 Matriz de Operacionalización de Variables

VARIABLE	Definición conceptual	Dimensiones	Indicadores	Escala de medición
Sistema basado en controles de Seguridad	Un sistema basado en controles de seguridad se refiere a un enfoque o conjunto de medidas diseñadas para proteger los activos, información y procesos de una organización contra posibles amenazas y riesgos de seguridad. Estos controles son mecanismos implementados para prevenir, detectar, mitigar y responder a incidentes de seguridad, con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de los recursos de la organización. Estos controles pueden incluir políticas, procedimientos, tecnologías y prácticas específicas que se implementan y mantienen para garantizar un nivel adecuado de seguridad de la información y la infraestructura (Terán Terranova 2021)			
Protección de data Personal	Se refiere a las medidas y prácticas adoptadas para salvaguardar la integridad y la privacidad de la información personal de los individuos. Se refiere a las medidas para salvaguardar la información que identifica o puede identificar a una persona física, como su número de teléfono, dirección, DNI, correo electrónico, información financiera, datos de salud, entre otros. (León 2021).	Confidencialidad(Onyshchenko, Hlushko y Yanko 2020; Pradana y Trianto 2018a; Szczepaniuk et al. 2020).	<ul style="list-style-type: none"> • Proteger la confidencialidad de los datos. • Métrica de confidencialidad. 	Ordinal/Razón
Integridad(Onyshchenko, Hlushko y Yanko 2020; Morales 2019; Taherdoost 2022).		<ul style="list-style-type: none"> • Garantizar la integridad de los datos. • Métrica de integridad. 	Ordinal/Razón	
Disponibilidad(Pradana y Trianto 2018a; Taherdoost 2022; Kayes et al. 2019)		<ul style="list-style-type: none"> • Garantizar la Disponibilidad de los datos. • Métrica de disponibilidad. 	Ordinal/Razón	

Anexo 03 Instrumento de recolección de datos

Cuestionario aplicado a los trabajadores de una UGEL

A continuación, se presenta una lista de preguntas contenidas en doce (15) ítems que corresponden a su percepción sobre la protección de datos en una UGEL. Por favor, indique su apreciación objetiva marcando con una "X" sobre cualquier de los números 1, 2, 3, 4 o 5, dónde:

1	2	3	4	5
Nunca	Rara Vez	A veces	Casi siempre	Siempre

Variable	Dimensión	Items	Opción de respuesta				
			1	2	3	4	5
Protección de data personal	Confidencialidad	1. ¿Cree usted que se aplica la ley 29733 en la entidad para proteger los datos personales de los empleados?					
		2. ¿La entidad le brinda los recursos necesarios para mantener la información confidencial de forma segura?					
		3. ¿Considera usted que se toman medidas adecuadas para proteger la privacidad de los datos personales en tu entorno laboral?					
		4. ¿considera usted que los sistemas y herramientas tecnológicas se utilizan de manera correcta para proteger los datos de carácter confidencial?					
		5. ¿consideras confiable la información que se almacena en los sistemas o herramientas tecnológicas de la entidad?					
	Integridad	6. ¿Se mantiene un registro de cambios realizados en las planillas, incluyendo modificaciones, ajustes o correcciones?					
		7. ¿cree usted que los datos personales se actualizan y modifican solo con autorización y justificación adecuadas?					
		8. ¿El área en la que labora, realiza copias de seguridad de la información?					
		9. ¿cree usted que los cambios no autorizados o manipulaciones en los datos personales son reportados al jefe inmediato?					
		10. ¿Se realizan auditorías periódicas de las planillas de pago para verificar su integridad y precisión?					
	Disponibilidad	11. ¿Se te proporciona acceso a la información relacionada a las planillas y sistemas necesarios de manera oportuna y eficiente?					
		12. ¿has visto alguna vez que se supervisa y mide la disponibilidad de los sistemas y datos en tu entidad?					
		13. ¿Se realizan copias de seguridad periódicas para asegurar la disponibilidad de la información en caso de pérdida de datos?					
		14. ¿En la entidad que laboras aplican políticas específicas para garantizar la disponibilidad de la información a largo plazo?					
		15. ¿los empleados pueden acceder de forma rápida y eficiente a ver sus boletas de pago?					

Anexo 04 Instrumento de Ficha de Observación Pre test - Confidencialidad

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Confidencialidad		
INDICADOR	Métrica de confidencialidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Índice de confidencialidad		
FÓRMULA	INCONF = ((TRS-N°IC)/TRS) %		N° IC =Número de incidentes de confidencialidad
			TRS = Total de registros
			INCONF = Índice de confidencialidad
Periodo	setiembre	Año	2023
días	N° IC	TRS	INCONF
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Anexo 05 Instrumento de Ficha de Observación Post test - Confidencialidad

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Confidencialidad		
INDICADOR	Métrica de confidencialidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Índice de confidencialidad		
FÓRMULA	INCONF = ((TRS-N°IC)/TRS) %		N° IC =Número de incidentes de confidencialidad
			TRS = Total de registros
			INCONF = Índice de confidencialidad
Periodo	octubre	Año	2023
días	N° IC	TRS	INCONF
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Anexo 06 Instrumento de Ficha de Observación Pre test - Integridad

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Integridad		
INDICADOR	Métrica de integridad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre-test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de integridad		
FÓRMULA	ININTE = (N° RC/N° R) %		ININTE= Indicador de integridad
			N° R= Número de registros
			N° RC= Número de registros correctos
Mes	setiembre	Año	2023
Días	N° R	N° RC	ININTE
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Anexo 07 Instrumento de Ficha de Observación Post test – Integridad

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Integridad		
INDICADOR	Métrica de integridad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de integridad		
FÓRMULA	ININTE = (N° RC/N° R) %		ININTE= Indicador de integridad
			N° R= Número de registros
			N° RC= Número de registros correctos
Mes	octubre	Año	2023
Días	N° R	N° RC	ININTE
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Anexo 08 Instrumento de Ficha de Observación Pre test – disponibilidad

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Disponibilidad		
INDICADOR	Métrica de disponibilidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre-test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de disponibilidad de la base de datos		
FÓRMULA	INCONT = ((TH – THSSI) /TH) %		INCONT = Indicador de continuidad de servicio
			TH = Total de horas diarias
			THSSI = Total de horas sin servicios de información
Mes	setiembre	Año	2023
Días	TH	THSSI	INCONT
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Anexo 09 Instrumento de Ficha de Observación Post test – disponibilidad

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Disponibilidad		
INDICADOR	Métrica de disponibilidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de disponibilidad de la base de datos		
FÓRMULA	INCONT = ((TH – THSSI) /TH) %		INCONT = Indicador de continuidad de servicio
			TH = Total de horas diarias
			THSSI = Total de horas sin servicios de información
Mes	octubre	Año	2023
Días	TH	THSSI	INCONT
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Anexo 10 Consentimiento y/o asentimiento informado

Consentimiento Informado

Título de la investigación: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023.

Investigador (a) (es): Naira Guerrero Elmer y Paredes Bocanegra Christian Anthony.

Propósito del estudio

Le invitamos a participar de la investigación titulada "Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023", cuyo objetivo es Mejorar la protección de datos personales en la Unidad de Gestión Educativa Local mediante un sistema de planillas basado en controles de seguridad aplicando la Ley Peruana 29733.

Esta investigación es desarrollada por estudiantes de pregrado de la carrera profesional de Ingeniería de sistemas de la Universidad Cesar Vallejo del campus Piura, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la UGEL Huancabamba.

El impacto del problema de este proyecto de investigación esta relacionado con mejorar la protección de datos personales mediante un sistema de planillas basado en controles de seguridad, asimismo garantizar la integridad y disponibilidad de los datos. Hoy en día este proceso se hace manual y en muchos casos se genera divulgación, mal ingreso de datos a las planillas y poca disponibilidad de la información.

Con relación al sistema de planillas basado en controles de seguridad pretende mejorar la confidencialidad, integridad y disponibilidad de los datos. Para ello se aplicará el marco normativo de la Ley 29733 Ley de Protección de datos personales en el Perú.

Procedimiento

Si usted decide participar en la investigación se realizará los siguiente:

1. Se realizará una encuesta donde se recogerán datos en base a las preguntas formuladas sobre confidencialidad, integridad y disponibilidad de la información sobre la investigación denominada: "Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023".
2. Esta encuesta tendrá un tiempo aproximado de 10 minutos y se realizará en la UGEL de forma presencial, las respuestas del cuestionario serán codificadas usando un número de identificación y, por lo tanto, serán anónimas.

Participación voluntaria (principio de autonomía):

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzarán a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el Investigador (a) (es) Naira Guerrero Elmer y Paredes Bocanegra Christian, al email: enaira@ucvvirtual.edu.pe, cparedesbo@ucvvirtual.edu.pe y docente asesor y Docente asesor More Valencia, Rubén Alexander, email: rmore@ucv.edu.pe

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos:

Fecha y hora:

Anexo 11 autorización de la organización para publicar su identidad en los resultados de las investigaciones



AUTORIZACIÓN DE LA ORGANIZACIÓN PARA PUBLICAR SU IDENTIDAD EN LOS RESULTADOS DE LAS INVESTIGACIONES

Datos Generales

Nombre de la Organización:	RUC: 20526012071
UNIDAD DE GESTIÓN EDUCATIVA LOCAL DE HUANCABAMBA	
Nombre del Titular o Representante legal: Lourdes Consuelo La Madrid Benites	
Nombres y Apellidos Lourdes Consuelo La Madrid Benites	DNI: 03339133

Consentimiento:

De conformidad con lo establecido en el artículo 7º, literal "f" del Código de Ética en Investigación de la Universidad César Vallejo (*), autorizo [], no autorizo [] publicar LA IDENTIDAD DE LA ORGANIZACIÓN, en la cual se lleva a cabo la investigación:

Nombre del Trabajo de Investigación	
Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733 en UGEL Huancabamba, 2023.	
Nombre del Programa Académico: Ingeniería de Sistemas	
Autor: Nombres y Apellidos Elmer Naira Guerrero Christian Anthony Paredes Bocanegra	DNI: 70944387 72539033

En caso de autorizarse, soy consciente que la investigación será alojada en el Repositorio Institucional de la UCV, la misma que será de acceso abierto para los usuarios y podrá ser referenciada en futuras investigaciones, dejando en claro que los derechos de propiedad intelectual corresponden exclusivamente al autor (a) del estudio.

Lugar y Fecha: Huancabamba, 14 de julio de 2023

Firma:

(Titular o Representante legal de la Institución)

(*). Código de Ética en Investigación de la Universidad César Vallejo-Artículo 7º, literal "f" **Para difundir o publicar los resultados de un trabajo de investigación es necesario mantener bajo anonimato el nombre de la institución donde se llevó a cabo el estudio, salvo el caso en que haya un acuerdo formal con el gerente o director de la organización, para que se difunda la identidad de la institución. Por ello, tanto en los proyectos de investigación como en las tesis, no se deberá incluir la denominación de la organización, ni en el cuerpo de la tesis ni en los anexos, pero sí será necesario describir sus características.**



Anexo 12 Matriz Evaluación por juicio de expertos

EVALUACIÓN POR JUICIO DE EXPERTOS N° 01

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

N°	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSIÓN 1: Confidencialidad							
1	INDICADOR 1: Proteger la confidencialidad de los datos							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		
		Si	No	Si	No	Si	No	
	INDICADOR 2: Métrica de confidencialidad							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		

Observaciones (precisar si hay suficiencia): _____

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

Apellidos y nombres del juez validador: **More Valencia Rubén Alexander**

DNI: 02897931

Especialidad del validador: **Ingeniero Informático**

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

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

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

22 de setiembre del 2023

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


Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSIÓN 2: Integridad							
3	INDICADOR 1: Garantizar la integridad de los datos.							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		
		Si	No	Si	No	Si	No	
4	INDICADOR 2: Métrica de integridad							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		

Observaciones (precisar si hay suficiencia): _____

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

Apellidos y nombres del juez validador: **More Valencia Rubén Alexander**

DNI: 02897931

Especialidad del validador: **Ingeniero Informático**

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

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

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

22 de setiembre del 2023

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



Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSIÓN 3: Disponibilidad							
5	INDICADOR 1: Garantizar la Disponibilidad de los datos							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		
		Si	No	Si	No	Si	No	
6	INDICADOR 2: Métrica de disponibilidad							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		

Observaciones (precisar si hay suficiencia): _____

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

Apellidos y nombres del juez validador. **More Valencia Rubén Alexander**

DNI: 02897931

Especialidad del validador: **Ingeniero Informático**

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

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

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

22 de setiembre del 2023

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



 Firma del Experto Informante.

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: CUESTIONARIO – Dimensiones de Confidencialidad, integridad y disponibilidad.

I. DATOS GENERALES

Apellidos y Nombres del Experto: **More Valencia Rubén Alexander**
 Título y/o Grado Académico: **Ingeniero Informático / Magister en administración de la educación.**

Doctor () Magister (X) Ingeniero () Licenciado () Otro ().....

Universidad que labora: **Cesar Vallejo**
 Fecha : **22/09/2023**

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autores: Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.					100
OBJETIVIDAD	Esta expresado en conducta observable.					98
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					100
ORGANIZACION	Existe una organización lógica.					100
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					97
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					98
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					100
COHERENCIA	En los datos respecto al indicador.					99
METODOLOGIA	Responde al propósito de investigación.					100
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					100
TOTAL						992

III. PROMEDIO DE VALIDACIÓN

99.2

IV. OPCION DE APLICABILIDAD

- El instrumento puede ser aplicado, tal como está elaborado
 El instrumento debe ser mejorado antes de ser aplicado


FIRMA DEL EXPERTO

Cuestionario aplicado a los trabajadores de la Entidad

A continuación, se presenta una lista de preguntas contenidas en quince (15) ítems que corresponden a su percepción sobre la protección de datos Personales en una UGEL. Por favor, indique su apreciación objetiva marcando con una "X" sobre cualquier de los números 1, 2, 3, 4 o 5, dónde:

1	2	3	4	5
Nunca	Rara Vez	A veces	Casi siempre	Siempre

Variable	Dimensión	Items	Opción de respuesta				
			1	2	3	4	5
Protección de data personal	Confidencialidad	1. ¿Cree usted que se aplica la ley 29733 en la entidad para proteger los datos personales de los empleados?					
		2. ¿La entidad le brinda los recursos necesarios para mantener la información confidencial de forma segura?					
		3. ¿Considera usted que se toman medidas adecuadas para proteger la privacidad de los datos personales en tu entorno laboral?					
		4. ¿considera usted que los sistemas y herramientas tecnológicas se utilizan de manera correcta para proteger los datos de carácter confidencial?					
		5. ¿consideras confiable la información que se almacena en los sistemas o herramientas tecnológicas de la entidad?					
	Integridad	6. ¿Se mantiene un registro de cambios realizados en las planillas, incluyendo modificaciones, ajustes o correcciones?					
		7. ¿cree usted que los datos personales se actualizan y modifican solo con autorización y justificación adecuadas?					
		8. ¿El área en la que labora, realiza copias de seguridad de la información?					
		9. ¿cree usted que los cambios no autorizados o manipulaciones en los datos personales son reportados al jefe inmediato?					
		10. ¿Se realizan auditorías periódicas de las planillas de pago para verificar su integridad y precisión?					
	Disponibilidad	11. ¿Se te proporciona acceso a la información relacionada a las planillas y sistemas necesarios de manera oportuna y eficiente?					
		12. ¿has visto alguna vez que se supervisa y mide la disponibilidad de los sistemas y datos en tu entidad?					
		13. ¿Se realizan copias de seguridad periódicas para asegurar la disponibilidad de la información en caso de pérdida de datos?					
		14. ¿En la entidad que laboras aplican políticas específicas para garantizar la disponibilidad de la información a largo plazo?					
		15. ¿los empleados pueden acceder de forma rápida y eficiente a ver sus boletas de pago?					

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Métrica de Confidencialidad de la data personal

I. DATOS GENERALES

Apellidos y Nombres del Experto: **More Valencia Rubén Alexander**
 Título y/o Grado Académico: **Ingeniero Informático / Magister en administración de la educación.**

Doctor () Magister (X) Ingeniero () Licenciado () Otro ().....

Universidad que labora: **Cesar Vallejo**
 Fecha : **22/09/2023**

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autores: Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.					100
OBJETIVIDAD	Esta expresado en conducta observable.					98
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					100
ORGANIZACIÓN	Existe una organización lógica.					100
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					97
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					98
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					100
COHERENCIA	En los datos respecto al indicador.					99
METODOLOGIA	Responde al propósito de investigación.					100
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					100
TOTAL						99.2

III. PROMEDIO DE VALIDACIÓN

99.2

IV. OPCION DE APLICABILIDAD

- El instrumento puede ser aplicado, tal como está elaborado
- El instrumento debe ser mejorado antes de ser aplicado


FIRMA DEL EXPERTO

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Métrica de Integridad de la data personal

I. DATOS GENERALES

Apellidos y Nombres del Experto: **More Valencia Rubén Alexander**
 Título y/o Grado Académico: **Ingeniero Informático / Magister en administración de la educación.**

Doctor () Magister (X) Ingeniero () Licenciado () Otro ().....

Universidad que labora: **Cesar Vallejo**
 Fecha : **22/09/2023**

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autores: Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de items que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.					100
OBJETIVIDAD	Esta expresado en conducta observable.					98
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					100
ORGANIZACION	Existe una organización lógica.					100
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					97
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					98
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					100
COHERENCIA	En los datos respecto al indicador.					99
METODOLOGIA	Responde al propósito de investigación.					100
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					100
TOTAL						99.2

III. PROMEDIO DE VALIDACIÓN

99.2

IV. OPCION DE APLICABILIDAD

- (X) El instrumento puede ser aplicado, tal como está elaborado
 () El instrumento debe ser mejorado antes de ser aplicado


FIRMA DEL EXPERTO

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Integridad		
INDICADOR	Métrica de integridad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre test y post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de integridad		
FORMULA	$ININTE = (N^{\circ} RC / N^{\circ} R) \%$		ININTE= Indicador de integridad
			N° R= Número de registros
			N° RC= Número de registros correctos
Mes		Año	2023
Días	N° R	N° RC	ININTE
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

EVALUACIÓN POR JUICIO DE EXPERTOS N° 02

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

N°	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
1	INDICADOR 1: Proteger la confidencialidad de los datos							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		
		Si	No	Si	No	Si	No	
2	INDICADOR 2: Métrica de confidencialidad							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		

Observaciones (precisar si hay suficiencia): _____

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

Apellidos y nombres del juez validador. **Jaramillo Atoche Javier Eduardo**

DNI:40917312

Especialidad del validador: **Ingeniería de Sistemas**

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

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

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

27 de octubre del 2023

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



Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSIÓN 2: Integridad							
3	INDICADOR 1: Garantizar la integridad de los datos.							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		
		Si	No	Si	No	Si	No	
4	INDICADOR 2: Métrica de integridad							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		

Observaciones (precisar si hay suficiencia): _____

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

Apellidos y nombres del juez validador: **Jaramillo Atoche Javier Eduardo**

DNI: 40917312

Especialidad del validador: **Ingeniería de Sistemas**

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

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

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

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

27 de octubre del 2023



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSIÓN 3: Disponibilidad							
5	INDICADOR 1: Garantizar la Disponibilidad de los datos							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		
		Si	No	Si	No	Si	No	
6	INDICADOR 2: Métrica de disponibilidad							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		

Observaciones (precisar si hay suficiencia): _____

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

Apellidos y nombres del juez validador.

DNI: 40917312

Especialidad del validador: **Ingeniería de Sistemas**

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

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

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

27 de octubre del 2023

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



Firma del Experto Informante.

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: CUESTIONARIO – Dimensiones de Confidencialidad, integridad y disponibilidad.

I. DATOS GENERALES

Apellidos y Nombres del Experto: Jaramillo Atoche Javier Eduardo
 Título y/o Grado Académico: -Ingeniero de Sistemas / Magister en Dirección y Gestión de las TICs

Doctor () Magister (X) Ingeniero () Licenciado () Otro ().....

Universidad que labora: Universidad César Vallejo
 Fecha : 27/10/2023

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autores: Naira Guerrero, Elmer
 Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.					100
OBJETIVIDAD	Esta expresado en conducta observable.					100
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					100
ORGANIZACION	Existe una organización lógica.					100
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					100
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					98
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					100
COHERENCIA	En los datos respecto al indicador.					99
METODOLOGIA	Responde al propósito de investigación.					100
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					100
TOTAL						997

III. PROMEDIO DE VALIDACIÓN

99.7

IV. OPCIÓN DE APLICABILIDAD

- (X) El instrumento puede ser aplicado, tal como está elaborado
- () El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Cuestionario aplicado a los trabajadores de la Entidad

A continuación, se presenta una lista de preguntas contenidas en quince (15) ítems que corresponden a su percepción sobre la protección de datos Personales en la UGEL. Por favor, indique su apreciación objetiva marcando con una "X" sobre cualquier de los números 1, 2, 3, 4 o 5, dónde:

1	2	3	4	5
Nunca	Rara Vez	A veces	Casi siempre	Siempre

Variable	Dimensión	Ítems	Opción de respuesta				
			1	2	3	4	5
Protección de data personal	Confidencialidad	1. ¿Cree usted que se aplica la ley 29733 en la entidad para proteger los datos personales de los empleados?					
		2. ¿La entidad le brinda los recursos necesarios para mantener la información confidencial de forma segura?					
		3. ¿Considera usted que se toman medidas adecuadas para proteger la privacidad de los datos personales en tu entorno laboral?					
		4. ¿considera usted que los sistemas y herramientas tecnológicas se utilizan de manera correcta para proteger los datos de carácter confidencial?					
		5. ¿consideras confiable la información que se almacena en los sistemas o herramientas tecnológicas de la entidad?					
	Integridad	6. ¿Se mantiene un registro de cambios realizados en las planillas, incluyendo modificaciones, ajustes o correcciones?					
		7. ¿cree usted que los datos personales se actualizan y modifican solo con autorización y justificación adecuadas?					
		8. ¿El área en la que labora, realiza copias de seguridad de la información?					
		9. ¿cree usted que los cambios no autorizados o manipulaciones en los datos personales son reportados al jefe inmediato?					
		10. ¿Se realizan auditorías periódicas de las planillas de pago para verificar su integridad y precisión?					
	Disponibilidad	11. ¿Se te proporciona acceso a la información relacionada a las planillas y sistemas necesarios de manera oportuna y eficiente?					
		12. ¿has visto alguna vez que se supervisa y mide la disponibilidad de los sistemas y datos en tu entidad?					
		13. ¿Se realizan copias de seguridad periódicas para asegurar la disponibilidad de la información en caso de pérdida de datos?					
		14. ¿En la entidad que laboras aplican políticas específicas para garantizar la disponibilidad de la información a largo plazo?					
		15. ¿los empleados pueden acceder de forma rápida y eficiente a ver sus boletas de pago?					

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Métrica de Confidencialidad de la data personal

I. DATOS GENERALES

Apellidos y Nombres del Experto: Jaramillo Atoche Javier Eduardo
 Título y/o Grado Académico: Ingeniero de Sistemas / Magister en Dirección y Gestión de las TICs

Doctor () Magister (X) Ingeniero () Licenciado () Otro ().....

Universidad que labora: Universidad César Vallejo
 Fecha : 27/10/2023

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autor(es): Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.					100
OBJETIVIDAD	Esta expresado en conducta observable.					100
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					100
ORGANIZACION	Existe una organización lógica.					100
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					100
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					98
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					100
COHERENCIA	En los datos respecto al indicador.					99
METODOLOGIA	Responde al propósito de investigación.					100
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					100
TOTAL						997

III. PROMEDIO DE VALIDACIÓN

99,7

IV. OPCIÓN DE APLICABILIDAD

- (X) El instrumento puede ser aplicado, tal como está elaborado
- () El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Métrica de Integridad de la data personal

I. DATOS GENERALES

Apellidos y Nombres del Experto: Jaramillo Atoche Javier Eduardo
 Título y/o Grado Académico: -Ingeniero de Sistemas / Magister en Dirección y Gestión de las TICs

Doctor () Magister (X) Ingeniero () Licenciado () Otro ().....

Universidad que labora: Universidad César Vallejo
 Fecha : 27/10/2023

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autor(es): Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)
 Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.					100
OBJETIVIDAD	Esta expresado en conducta observable.					100
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					100
ORGANIZACION	Existe una organización lógica.					100
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					100
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					98
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					100
COHERENCIA	En los datos respecto al indicador.					99
METODOLOGIA	Responde al propósito de investigación.					100
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					100
TOTAL						997

III. PROMEDIO DE VALIDACIÓN

99.7

IV. OPCIÓN DE APLICABILIDAD

- (X) El instrumento puede ser aplicado, tal como está elaborado
- () El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Integridad		
INDICADOR	Métrica de integridad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre test y post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de integridad		
FORMULA	ININTE = (N° RC/N° R) %		ININTE= Indicador de integridad
			N° R= Número de registros
			N° RC= Número de registros correctos
Mes		Año	2023
Días	N° R	N° RC	ININTE
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Métrica de Disponibilidad de la data personal

I. DATOS GENERALES

Apellidos y Nombres del Experto: Jaramillo Atoche Javier Eduardo
 Título y/o Grado Académico: -Ingeniero de Sistemas / Magister en Dirección y Gestión de las TICs

Doctor () Magister (X) Ingeniero () Licenciado () Otro ().....

Universidad que labora: Universidad César Vallejo
 Fecha : 27/10/2023

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autor(es): Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.					100
OBJETIVIDAD	Esta expresado en conducta observable.					100
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					100
ORGANIZACION	Existe una organización lógica.					100
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					100
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					98
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					100
COHERENCIA	En los datos respecto al indicador.					99
METODOLOGÍA	Responde al propósito de investigación.					100
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					100
TOTAL						997

III. PROMEDIO DE VALIDACIÓN

99.7

IV. OPCIÓN DE APLICABILIDAD

- (X) El instrumento puede ser aplicado, tal como está elaborado
 () El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Disponibilidad		
INDICADOR	Métrica de disponibilidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre test y post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de disponibilidad de la base de datos		
FORMULA	$INCONT = ((TH - THSSI) / TH) \%$		INCONT = Indicador de continuidad de servicio
			TH = Total de horas diarias
			THSSI = Total de horas sin servicios de información
Mes		Año	2023
Días	TH	THSSI	INCONT
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

EVALUACIÓN POR JUICIO DE EXPERTOS N° 03

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

N°	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSIÓN 1: Confidencialidad							
1	INDICADOR 1: Proteger la confidencialidad de los datos							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X			X	X		
d	Comprende los aspectos de cantidad y calidad.	X			X	X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X			X	
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		
		Si	No	Si	No	Si	No	
2	INDICADOR 2: Métrica de confidencialidad							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.		X	X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X			X	X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X			X	
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación		X	X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir []** **No aplicable []**

Apellidos y nombres del juez validador. Iván Michell Castillo Jiménez

DNI: 02883813

Especialidad del validador: Ing. Informático

¹Pertinencia: El ítem corresponde al concepto teórico formulado.

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

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

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

22 de setiembre del 2023



Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSIÓN 2: Integridad							
3	INDICADOR 1: Garantizar la integridad de los datos.							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X			X	X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación		X		X	X		
		Si	No	Si	No	Si	No	
4	INDICADOR 2: Métrica de integridad							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.	X		X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X			X	
g	En los datos respecto al indicador.	X		X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir []** **No aplicable []**

Apellidos y nombres del juez validador: Iván Michell Castillo Jiménez

DNI: 02883813

Especialidad del validador: Ing. Informático

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

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

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

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

22 de setiembre del 2023



CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE:

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSION 3: Disponibilidad							
5	INDICADOR 1: Garantizar la Disponibilidad de los datos							
a	Es formulado con lenguaje apropiado.	X			X	X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X			X	
c	Existe una organización lógica.		X	X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X		X		
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X		X		X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.	X			X	X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación		X		X	X		
		Si	No	Si	No	Si	No	
6	INDICADOR 2: Métrica de disponibilidad							
a	Es formulado con lenguaje apropiado.	X		X		X		
b	Es adecuado el avance, la ciencia y tecnología.	X		X		X		
c	Existe una organización lógica.		X	X		X		
d	Comprende los aspectos de cantidad y calidad.	X		X			X	
e	Adecuado para valorar los aspectos del sistema metodológico y científico.	X			X	X		
f	Está basado en aspectos teóricos y científicos.	X		X		X		
g	En los datos respecto al indicador.		X	X		X		
h	Responde al propósito de investigación.	X		X		X		
i	El instrumento es adecuado al tipo de investigación	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable [x]** **Aplicable después de corregir []** **No aplicable []**

Apellidos y nombres del juez validador: Iván Michell Castillo Jiménez

DNI: 02883813

Especialidad del validador: Ing. Informático

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

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

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

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

22 de setiembre del 2023



Firma del Experto Informante.

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: CUESTIONARIO – Dimensiones de Confidencialidad, integridad y disponibilidad.

I. DATOS GENERALES

Apellidos y Nombres del Experto: CASTILLO JIMENEZ IVAN MICHELL
 Título y/o Grado Académico: TECNOLOGÍAS DE LA INFORMACION Y COMUNICACIONES

Doctor (X) Magister () Ingeniero () Licenciado () Otro ().....

Universidad que labora: UCV
 Fecha : 22/09/2023

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autores: Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.					90
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				75	
ORGANIZACION	Existe una organización lógica.					90
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				75	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					90
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				75	
COHERENCIA	En los datos respecto al indicador.				80	
METODOLOGIA	Responde al propósito de investigación.					90
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				75	
TOTAL					460	360

III. PROMEDIO DE VALIDACIÓN

82%

IV. OPCIÓN DE APLICABILIDAD

- (X) El instrumento puede ser aplicado, tal como está elaborado
- () El instrumento debe ser mejorado antes de ser aplicado



FIRMA DEL EXPERTO

Questionario aplicado a los trabajadores de la Entidad

A continuación, se presenta una lista de preguntas contenidas en quince (15) ítems que corresponden a su percepción sobre la protección de datos Personales en una UGEL. Por favor, indique su apreciación objetiva marcando con una "X" sobre cualquier de los números 1, 2, 3, 4 o 5, dónde:

1	2	3	4	5
Nunca	Rara Vez	A veces	Casi siempre	Siempre

Variable	Dimensión	Items	Opción de respuesta				
			1	2	3	4	5
Protección de data personal	Confidencialidad	1. ¿Cree usted que se aplica la ley 29733 en la entidad para proteger los datos personales de los empleados?					
		2. ¿La entidad le brinda los recursos necesarios para mantener la información confidencial de forma segura?					
		3. ¿Considera usted que se toman medidas adecuadas para proteger la privacidad de los datos personales en tu entorno laboral?					
		4. ¿considera usted que los sistemas y herramientas tecnológicas se utilizan de manera correcta para proteger los datos de carácter confidencial?					
		5. ¿consideras confiable la información que se almacena en los sistemas o herramientas tecnológicas de la entidad?					
	Integridad	6. ¿Se mantiene un registro de cambios realizados en las planillas, incluyendo modificaciones, ajustes o correcciones?					
		7. ¿cree usted que los datos personales se actualizan y modifican solo con autorización y justificación adecuadas?					
		8. ¿El área en la que labora, realiza copias de seguridad de la información?					
		9. ¿cree usted que los cambios no autorizados o manipulaciones en los datos personales son reportados al jefe inmediato?					
		10. ¿Se realizan auditorías periódicas de las planillas de pago para verificar su integridad y precisión?					
	Disponibilidad	11. ¿Se te proporciona acceso a la información relacionada a las planillas y sistemas necesarios de manera oportuna y eficiente?					
		12. ¿has visto alguna vez que se supervisa y mide la disponibilidad de los sistemas y datos en tu entidad?					
		13. ¿Se realizan copias de seguridad periódicas para asegurar la disponibilidad de la información en caso de pérdida de datos?					
		14. ¿En la entidad que laboras aplican políticas específicas para garantizar la disponibilidad de la información a largo plazo?					
		15. ¿los empleados pueden acceder de forma rápida y eficiente a ver sus boletas de pago?					

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Métrica de Confidencialidad de la data personal

I. DATOS GENERALES

Apellidos y Nombres del Experto:

CASTILLO JIMENEZ IVAN MICHELL
TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

Título y/o Grado Académico:

UCV
22/09/2023

Doctor (x) Magister () Ingeniero () Licenciado () Otro ().....

Universidad que labora:

UCV

Fecha :

22/09/2023

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autores: Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.					
OBJETIVIDAD	Esta expresado en conducta observable.					
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					
ORGANIZACION	Existe una organización lógica.					
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.					
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					
COHERENCIA	En los datos respecto al indicador.					
METODOLOGIA	Responde al propósito de investigación.					
PERTENENCIA	El instrumento es adecuado al tipo de investigación.					
TOTAL						

III. PROMEDIO DE VALIDACIÓN

--

IV. OPCIÓN DE APLICABILIDAD

- (x) El instrumento puede ser aplicado, tal como está elaborado
- () El instrumento debe ser mejorado antes de ser aplicado


FIRMA DEL EXPERTO

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Métrica de Integridad de la data personal

I. DATOS GENERALES

Apellidos y Nombres del Experto: **CASTILLO JIMENEZ IVAN MICHELL**
 Título y/o Grado Académico: **TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES**

Doctor () Magister () Ingeniero () Licenciado ()
 Otro ().....

Universidad que labora: **UCV**

Fecha : **22/09/2023**

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autores: Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.				80	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.					95
ORGANIZACION	Existe una organización lógica.					95
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.					95
COHERENCIA	En los datos respecto al indicador.					95
METODOLOGIA	Responde al propósito de investigación.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80	
TOTAL					480	380

III. PROMEDIO DE VALIDACIÓN

86%

IV. OPCIÓN DE APLICABILIDAD

- () El instrumento puede ser aplicado, tal como está elaborado
 () El instrumento debe ser mejorado antes de ser aplicado



FIRMA DEL EXPERTO

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Integridad		
INDICADOR	Métrica de integridad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre test y post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de integridad		
FORMULA	ININTE = (N° RC/N° R) %		ININTE= Indicador de integridad
			N° R= Número de registros
			N° RC= Número de registros correctos
Mes		Año	2023
Días	N° R	N° RC	ININTE
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS: Métrica de Disponibilidad de la data personal

I. DATOS GENERALES

Apellidos y Nombres del Experto: **CASTILLO JIMENEZ IVAN MICHELL**
 Título y/o Grado Académico: **TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES**

Doctor () Magister () Ingeniero () Licenciado ()
 Otro ()

Universidad que labora: **UCV**
 Fecha : **22/09/2023**

TESIS: Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023

Autores: Naira Guerrero, Elmer Paredes Bocanegra Christian Anthony

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACION				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.				80	
OBJETIVIDAD	Esta expresado en conducta observable.					95
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80	
ORGANIZACION	Existe una organización lógica.				80	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					95
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				80	
COHERENCIA	En los datos respecto al indicador.				80	
METODOLOGIA	Responde al propósito de investigación.				80	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80	
TOTAL					480	190

III. PROMEDIO DE VALIDACIÓN

67%

IV. OPCIÓN DE APLICABILIDAD

- () El instrumento puede ser aplicado, tal como está elaborado
 () El instrumento debe ser mejorado antes de ser aplicado



FIRMA DEL EXPERTO

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Disponibilidad		
INDICADOR	Métrica de disponibilidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre test y post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de disponibilidad de la base de datos		
FORMULA	$INCONT = ((TH - THSSI) / TH) \%$		INCONT = Indicador de continuidad de servicio
			TH = Total de horas diarias
			THSSI = Total de horas sin servicios de información
Mes		Año	2023
Días	TH	THSSI	INCONT
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Anexo 14 recolección de datos ficha de Observación (Confidencialidad, Integridad y Disponibilidad)

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Confidencialidad		
INDICADOR	Métrica de confidencialidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Índice de confidencialidad		
FÓRMULA	INCONF = ((TRS-N°IC)/TRS) %		N° IC =Número de incidentes de confidencialidad
			TRS = Total de registros
			INCONF = Índice de confidencialidad
Periodo	setiembre	Año	2023
días	N° IC	TRS	INCONF
1	3	9	66.67
2	3	10	70.00
3	4	13	69.23
4	2	11	81.82
5	1	10	90.00
6	4	14	71.43
7	4	12	66.67
8	3	13	76.92
9	3	12	75.00
10	3	10	70.00
11	1	11	90.91
12	6	18	66.67
13	5	15	66.67
14	3	10	70.00
15	1	12	91.67

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Confidencialidad		
INDICADOR	Métrica de confidencialidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Índice de confidencialidad		
FÓRMULA	INCONF = ((TRS-N°IC)/TRS) %		N° IC =Número de incidentes de confidencialidad
			TRS = Total de registros
			INCONF = Índice de confidencialidad
Periodo	octubre	Año	2023
días	N° IC	TRS	INCONF
1	0	11	100.00
2	0	11	100.00
3	2	17	88.24
4	0	13	100.00
5	0	10	100.00
6	0	8	100.00
7	1	17	94.12
8	0	10	100.00
9	0	9	100.00
10	1	18	94.44
11	0	11	100.00
12	0	10	100.00
13	1	13	92.31
14	1	19	94.74
15	0	14	100.00

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Integridad		
INDICADOR	Métrica de integridad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre-test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de integridad		
FÓRMULA	ININTE = (N° RC/N° R) %		ININTE= Indicador de integridad
			N° R= Número de registros
			N° RC= Número de registros correctos
Mes	setiembre	Año	2023
Días	N° R	N° RC	ININTE
1	84	71	84.52
2	97	79	81.44
3	121	92	76.03
4	104	85	81.73
5	95	78	82.11
6	134	90	67.16
7	116	94	81.03
8	123	88	71.54
9	118	79	66.95
10	90	75	83.33
11	100	67	67.00
12	96	80	83.33
13	79	68	86.08
14	102	68	66.67
15	113	84	74.34

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Integridad		
INDICADOR	Métrica de integridad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de integridad		
FÓRMULA	ININTE = (N° RC/N° R) %		ININTE= Indicador de integridad
			N° R= Número de registros
			N° RC= Número de registros correctos
Mes	octubre	Año	2023
Días	N° R	N° RC	ININTE
1	91	90	98.90
2	87	87	100.00
3	105	103	98.10
4	96	96	100.00
5	115	115	100.00
6	120	119	99.17
7	95	95	100.00
8	113	113	100.00
9	124	122	98.39
10	97	95	97.94
11	89	89	100.00
12	78	78	100.00
13	103	102	99.03
14	99	99	100.00
15	116	113	97.41

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Disponibilidad		
INDICADOR	Métrica de disponibilidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Pre test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de disponibilidad de la base de datos		
FÓRMULA	INCONT = ((TH – THSSI) /TH) %		INCONT = Indicador de continuidad de servicio
			TH = Total de horas diarias
			THSSI = Total de horas sin servicios de información
Mes	setiembre	Año	2023
Días	TH	THSSI	INCONT
1	10	2	80.00
2	10	0	100.00
3	10	5	50.00
4	10	3	70.00
5	10	1	90.00
6	10	0	100.00
7	10	1	90.00
8	10	2	80.00
9	10	5	50.00
10	10	0	100.00
11	10	5	50.00
12	10	3	70.00
13	10	5	50.00
14	10	1	90.00
15	10	5	50.00

FICHA DE OBSERVACIÓN			
DIMENSIÓN	Disponibilidad		
INDICADOR	Métrica de disponibilidad		
INVESTIGADORES	Naira Guerrero Elmer.	Tipo de prueba	Post test
	Paredes Bocanegra Christian.		
ENTIDAD	UGEL		
MEDICIÓN	Grado de disponibilidad de la base de datos		
FÓRMULA	INCONT = ((TH – THSSI) /TH) %		INCONT = Indicador de continuidad de servicio
			TH = Total de horas diarias
			THSSI = Total de horas sin servicios de información
Mes	octubre	Año	2023
Días	TH	THSSI	INCONT
1	10	0	100.00
2	10	2	100.00
3	10	2	80.00
4	10	2	80.00
5	10	0	80.00
6	10	0	100.00
7	10	0	100.00
8	10	2	80.00
9	10	0	100.00
10	10	0	100.00
11	10	1	90.00
12	10	0	100.00
13	10	0	100.00
14	10	1	90.00
15	10	0	100.00

Anexo 15 Implementación del sistema de planillas basado en controles de seguridad en la UGEL.

Interfaz de inicio de sesión

The screenshot shows a login form with a dark blue header containing the system name. Below the header, there is a white box with a dark blue border. Inside this box, the text 'Iniciar Sesión' is displayed next to a person icon. Below this, there are two input fields: 'USUARIO' with a placeholder 'Usuario' and 'CONTRASEÑA' with a placeholder 'Contraseña'. At the bottom of the form is a dark blue button with a white arrow and the text 'Login'.

Panel de administración del sistema de planillas

The screenshot shows a dashboard for 'SISTEMA DE PLANILLAS'. The top navigation bar includes the system name, a menu icon, and a user profile icon. The main content area is titled 'Panel de Administración' and features a sidebar on the left with the user 'Christian admin' and a list of menu items: 'Planillas', 'Empleados', 'Contratos', 'Administración', and 'Reportes'. The main area contains five cards: 'USUARIOS' (4), 'CONTRATOS' (82), 'EMPLEADOS' (103), 'PLANILLAS' (10), and 'Configuracion'.

Icono	Nombre	Cantidad
	USUARIOS	4
	CONTRATOS	82
	EMPLEADOS	103
	PLANILLAS	10
	Configuracion	-

Usuarios

SISTEMA DE PLANILLAS ☰ 👤

Christian
admin

- Planillas
- Empleados
- Contratos
- Administración
- Reportes

Usuarios

+ Mostrar 10 Entradas Buscar:

Id	Usuario	Nombres	Apellidos	Email
11	JRRHH	Miguel Augusto	Arambulo Garcia	miarambulo@yahoo.es
10	RPLANILLAS	John Wesley	Facundo Huamán	remufacundo2022@gmail.com
9	ENAIRA	Elmer	Naira Guerrero	elmernaira@gmail.com
1	admin	Christian	Paredes	admin@gmail.com

Mostrando 1 a 4 de 4 Entradas Anterior 1 Siguiente

Nuevo usuario

SISTEMA DE PLANILLAS

Christian
admin

- Planillas
- Empleados
- Contratos
- Administración
- Reportes

Nuevo Usuario

Usuario

Nombres

Apellidos

Email

Contraseña Confirmar Contraseña

Registrar Cancelar

1	admin	Christian	Paredes	admin@gmail.com
---	-------	-----------	---------	-----------------

Mostrando 1 a 4 de 4 Entradas Anterior 1 Siguiente

Gestión de contratos

SISTEMA DE PLANILLAS

Christian admin

Contratos

Mostrar 10 Entradas

Id	Cod Contrato	Empleado	Sueldo	Regimen Pensionario	Centro laboral	Cargo	RUC	Cuenta BIN	Inicio	Termino	Estado
1	30151	MIXY ARABELA	3500	INTEGRA M	UGEL HUANCABAMBA	ESPECIALISTA EN CONVIVENCIA ESCOLAR UGEL	10461954605	4754188079	2023-08-20	2023-11-20	Activo
2	30152	KARIN GUILIANA	2800	INTEGRA M	UGEL HUANCABAMBA	ITINERANTE DE CONVIVENCIA ESCOLAR	10721678771	4754165079	2023-08-20	2023-11-20	Activo
3	30153	MARIA ADELA	2800	INTEGRA M	UGEL HUANCABAMBA	ITINERANTE DE CONVIVENCIA ESCOLAR	10482546761	4309061018			Activo
4	30154	MIGUEL AUGUSTO	3800	SNP	UGEL HUANCABAMBA	ENCARGADO DE RECURSOS HUMANOS	1002663152	4631419807			Activo
5	30155	OTILIA MARIANELA	3800	INTEGRA F	UGEL HUANCABAMBA	ENCARGADA DE CONTABILIDAD	10028488080	4646396005			Activo
6	30156	CHRISTIAN RAMIRO	3000	INTEGRA M	UGEL HUANCABAMBA	ENCARGADO DE ESTADISTICA	10434820966	4631695189			Activo
7	30157	HENRY	4000	INTEGRA F	UGEL HUANCABAMBA	ENCARGADO DE PRESUPUESTO	10439441611	4662828306			Activo
8	30158	JOHN WESSLEY	4000	INTEGRA F	UGEL HUANCABAMBA	ENCARGADO DE REMUNERACIONES Y PLANILLAS	10414543184	4631666831			Activo
9	30159	HENRY ENRIQUE OMAR	4500	SNP	UGEL HUANCABAMBA	ENCARGADO DE ASESORIA JURIDICA	10439196772	4632352846			Activo

Nuevo Contrato

Nuevo Contrato

codigo

codigo del contrato

Empleado

Buscar Empleado

Centro Laboral

Buscar Centro

Cargo

Buscar Cargo

RUC

RUC

Regimen Pensionario

Buscar Regimen

Sueldo

Sueldo

CUSPP

CUSPP

Fecha de Inicio

16/11/2023

Fecha de Término

16/11/2023

Cuenta Bancaria

Cuenta Bancaria

Registrar Cancelar

Cargos

Cargos

Mostrar 10 Entradas

Buscar:

Id	Cargo	Estado
1	ESPECIALISTA EN CONVIVENCIA ESCOLAR UGEL	Activo
2	ITINERANTE DE CONVIVENCIA ESCOLAR	Activo
3	ENCARGADO DE RECURSOS HUMANOS	Activo
4	ENCARGADA DE CONTABILIDAD	Activo
5	ENCARGADO DE ESTADISTICA	Activo
6	ENCARGADO DE PRESUPUESTO	Activo
7	ENCARGADO DE REMUNERACIONES Y PLANILLAS	Activo
8	ENCARGADO DE ASESORIA JURIDICA	Activo
9	ENCARGADO DE ESCALAFON	Activo
10	ENCARGADO DE NEXUS	Activo

Régimen pensionario

Regimen Pensionario

Mostrar 10 Entradas

Buscar:

Id	Regimen	Comision	Prima	Aporte	Estado
1	INTEGRA M	0	1.84	10	Activo
2	SNP	0	0	13	Activo
3	INTEGRA F	1.55	1.84	10	Activo

Mostrando 1 a 3 de 3 Entradas

Anterior

Gestión de Empleados

SISTEMA DE PLANILLAS

Christian admin

Planillas

Empleados

Contratos

Administración

Reportes

Empleados

Mostrar 10 Entradas

Buscar:

Id	Dni	Nombre	Apellido Paterno	Apellido Materno	Sexo	Telefono	Email	Departamento	Provincia	Distrito	Estado
1	46195460	MIXY ARABELA	ADRIANZEN	GOMEZ	Femenino	935778436	mixya@gmail.com	Piura	Huancabamba	Sondor	Activo
2	72167877	KARIN GUILIANA	SANTIN	HUANCA	Femenino	944837738	PS.KARINSANTIN01@gmail.com	Piura	Huancabamba	La Laquiz	Activo
3	48254676	MARIA ADELA	SANDOVAL	DAMIAN	Femenino	953541082	mariaadelasandovaldamian@gmail	Piura	Huancabamba	San Miguel del Falque	Activo
4	03663152	MIGUEL AUGUSTO	ARAMBULO	GARCIA	Masculino	989452247	miguelgar5@gmail.com	Piura	Huancabamba	Sondorillo	Activo
5	02848808	OTILIA MARIANELA	CARRASCO	CASTILLO	Femenino	949873711	marianelacc4@hotmail.com	Piura	Huancabamba	El Carmen de la Frontera	Activo
6	43482096	CHRISTIAN RAMIRO	CHOQUEHUANCA	GARCIA	Masculino	947883576	chris14408@hotmail.com	Piura	Huancabamba	Huarmaca	Activo

Nuevo Empleado

Nuevo Empleado
✕

DNI

Nombre

Apellido Paterno

Apellido Materno

Teléfono Género:

Email

Departamento

Provincia

Distrito

Gestión de Planillas de Pago

SISTEMA DE PLANILLAS

Christian admin

Planillas

Empleados

Contratos

Administración

Reportes

Planillas

Mostrar 10 Entradas

Buscar:

Id	Tipo Planilla	Año	Mes	Periodo	Estado	Agregar Empleado
8	CAS SEDE PERSONAL ADMINISTRATIVO	2023	Septiembre	30	Activo	
9	PPR090 INTERVENCIONES PEDAGÓGICAS FOCALIZADAS (JEC)	2023	Septiembre	30	Activo	
11	PPR090 INTERVENCIONES PEDAGÓGICAS FOCALIZADAS - (JER)	2023	Septiembre	30	Activo	
12	ACCIONES CENTRALES MINEDU (CONVIVENCIA ESCOLAR)	2023	Septiembre	30	Activo	
13	ACCIONES CENTRALES MINEDU (RVM 026-2023 MINEDU)	2023	Septiembre	30	Activo	
14	CAS SEDE PERSONAL ADMINISTRATIVO	2023	Octubre	30	Activo	
15	PPR090 INTERVENCIONES PEDAGÓGICAS FOCALIZADAS (JEC)	2023	Octubre	30	Activo	
16	PPR090 INTERVENCIONES PEDAGÓGICAS FOCALIZADAS - (JER)	2023	Octubre	30	Activo	
17	ACCIONES CENTRALES MINEDU (CONVIVENCIA ESCOLAR)	2023	Octubre	30	Activo	
18	ACCIONES CENTRALES MINEDU (RVM 026-2023 MINEDU)	2023	Octubre	30	Activo	

Nueva Planillas

Nueva Planilla

Tipo Planilla

Año

Buscar Tipo

Año

Mes:

Periodo

Enero

Periodo

Registrar

Cancelar

Tipo de Planilla de pago según intervención

Tipo de Planilla

Mostrar 10 Entradas

Buscar:

Id	Tipo de Planilla	Estado
1	PPR090 INTERVENCIONES PEDAGÓGICAS FOCALIZADAS (JEC)	Activo
2	PPR090 INTERVENCIONES PEDAGÓGICAS FOCALIZADAS - (JER)	Activo
3	ACCIONES CENTRALES MINEDU (CONVIVENCIA ESCOLAR)	Activo
4	ACCIONES CENTRALES MINEDU (RVM 026-2023 MINEDU)	Activo
5	CAS SEDE PERSONAL ADMINISTRATIVO	Activo

Mostrando 1 a 5 de 5 Entradas

Anterior

Agregar empleados a la planilla

Agregar Empleado

Empleado:

Días Trabajados:

Descuento Administrativo:

Descuento Prestamo:

Descuento Judicial:

DS N° 311 - 2022 - EF:

Gratificación:

Registrar **Cancelar**

Creación del rubro de Descuentos

Descuentos

Mostrar 10 Entradas

Id	Nombre Descuento	Estado	
1	Descuento Prestamo	Activo	
2	Descuento c	Activo	

Mostrando 1 a 2 de 2 Entradas

Anterior 1 Siguiente

Otros ingresos

Otros Ingresos

Mostrar 10 Entradas

Id	Nombre de ingreso	Estado
No hay información		

Mostrando 0 to 0 of 0 Entradas

Anterior

Gestión de Reportes de las planillas de pago

Christian
admin

- Planillas >
- Empleados >
- Contratos >
- Administración >
- Reportes >

Empleados en planilla

Mostrar 10 Entradas



Buscar:

Id	CUSPP	APELLIDO PATERNO	APELLIDO MATERNO	NOMBRES	CARGO	CTA BACO	DNI	RUC	DIAS TRAB	MONTO DIARIO	MONTO BRUTO	-EF	GRATIFICACION	REGIMEN	DS Nº 311 2022
37		ADRIANZEN	GOMEZ	MIXY ARABELA	ESPECIALISTA EN CONVIVENCIA ESCOLAR UGEL	4754188079	46195460	10461954605	30	116.667	3500	64.19	0	INTEGRAM	
38	650320KSH7ND	SANTIN	HUANCA	KARIN GULLIANA	ITINERANTE DE CONVIVENCIA ESCOLAR	4754165079	72167877	10721678771	30	93.3333	2800	64.19	0	INTEGRAM	
39	344460MSDD1	SANDOVAL	DAMIAN	MARIA ADELA	ITINERANTE DE CONVIVENCIA ESCOLAR	4309061018	48254676	10482546761	30	93.3333	2800	64.19	0	INTEGRAM	

Mostrando 1 a 3 de 3 Entradas (Filtrado de 27 total entradas)

Anterior 1 Sigiente



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

Declaratoria de Autenticidad del Asesor

Yo, MORE VALENCIA RUBEN ALEXANDER, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, asesor de Tesis titulada: "Implementación de un sistema de planillas basado en controles de seguridad para la protección de datos personales aplicando la Ley Peruana 29733- 2023.", cuyos autores son PAREDES BOCANEGRA CHRISTIAN ANTHONY, NAIRA GUERRERO ELMER, constato que la investigación tiene un índice de similitud de 19.00%, 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.

PIURA, 08 de Diciembre del 2023

Apellidos y Nombres del Asesor:	Firma
MORE VALENCIA RUBEN ALEXANDER DNI: 02897931 ORCID: 0000-0002-7496-3702	Firmado electrónicamente por: RMOREV el 08-12- 2023 23:46:57

Código documento Trilce: TRI - 0689176