UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
ESCUELA DE POSGRADO
INGENIERÍA DE SISTEMAS, MENCIÓN EN TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN UN ESTÁNDAR DE SEGURIDAD EN EL PROGRAMA JUNTOS, HUÁNUCO

LÍNEA DE INVESTIGACIÓN: OPTIMIZACIÓN DE PROCESOS

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS, MENCIÓN EN TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

TESISTA: POZO MEZA DALI RAFAEL
ASESORA: MG. REYES AYALA YESSICA RAQUEL

HUÁNUCO – PERÚ
2023

DEDICATORIA

A Dios con mucha gratitud y con todo mi amor a mi esposa Yessica.

A mis adorados hijos Xiomy, Paul, Leonardo, Valentina e Ivanna siendo los motores y motivos.

A mis adorados padres Héctor y Belia.

A mis hermanos Ketty, Vladimir, Nydia, Mayra, Janet, Marisol, Nita, Jorge y Héctor (+).

A mis suegros Teófilo y Maura.

AGRADECIMIENTO

A Dios, por acompañarme día a día y enfrentar los retos que se presentan.

A la UNHEVAL por albergarme en sus aulas con un selecto grupo de profesionales que nos brindaron sus conocimientos y experiencias para seguir adelante.

A la Mg. Yessica Reyes Ayala asesora de tesis.

A mis colegas.

A mis padres y hermanos que creyeron y siguen creyendo en mí, quienes me brindaron su apoyo en todo momento.

A mi esposa e hijos, siempre motivo de aliento y superación siendo parte y compañía en este camino por alcanzar nuestros objetivos.

Muchísimas gracias, Mi Dios por TODO.

RESUMEN

La presente investigación tuvo como objetivo general el de determinar en qué medida el diseño propuesto de un SGSI basado en el estándar ISO/IEC 27001:2013 mejorará la seguridad de la información en el Programa Nacional de Apoyo Directo a los más Pobres (PNADP) – JUNTOS Huánuco. La investigación presenta un enfoque de tipo cuantitativo de nivel explicativo, en la búsqueda de identificar las causas de los fenómenos sociales y/o físicos. La muestra es de tipo no probabilística y está constituida por los trabajadores de la Unidad Territorial Huánuco – JUNTOS; siendo 31 personas del total de 128. La muestra ha sido de tipo probabilístico intencional. Para la recopilación de la información era muy necesario usar la técnica de la encuesta para las variables, así como el instrumento que se usó ha sido el cuestionario. Para el procesamiento de los datos se emplearon los programas IBM SPSS Statistics V21.0 y Excel Microsoft 365, permitieron el proceso y la muestra de los datos a través de tablas de frecuencias y figuras de una manera más clara y precisa. Teniendo como conclusión principal y según refiere Wilcoxon se tiene un resultado con un valor de 0.033; que es un valor menor que 0.05 (0.000<0.05) por ese motivo se procedió a rechazar la hipótesis nula y aceptar la hipótesis alterna.

Palabras Claves: Sistemas, Programa JUNTOS, Diseño, Políticas.

ABSTRACT

The general objective of this research was to determine to what extent the proposed design of an ISMS based on the ISO/IEC 27001:2013 standard will improve information security in the National Direct Support Program for the Poorest (PNADP) - JUNTOS Huánuco. The research presents a quantitative approach of an explanatory level, in the search to identify the causes of social and/or physical phenomena. The sample is of a non-probabilistic type and is made up of the workers of the Huánuco Territorial Unidad – JUNTOS; being 31 people out of a total of 128. The sample has been of an intentional probabilistic type. For the collection of information, it was very necessary to use the survey technique for the variables, as well as the instrument that was used has been the questionnaire. For the data processing, the IBM SPSS Statistics V21.0 and Excel Microsoft 365 programs were used, allowing the processing and display of the data through frequency tables and figures in a clearer and more precise way.Having as main conclusion and according to Wilcoxon, there is a result with a value of 0.033; which is a value less than 0.05 (0.000<0.05) for this reason we proceeded to reject the null hypothesis and accept the alternate hypothesis.

Keywords: Systems, JUNTOS Program, Design, Policies.

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

El Programa Nacional de Asistencia Directa a los más Pobres JUNTOS (PNADP) carece actualmente de un plan de sistema de gestión de seguridad de la información (SGSI) en todo el Perú, particularmente en el departamento de Huánuco. En el departamento de Huánuco, existen numerosos sistemas, controles y tareas manuales que impiden la gestión eficiente que requiere el Programa JUNTOS. Uno de los retos que enfrenta el Programa JUNTOS para salvaguardar sus datos de amenazas tanto internas como externas, es la ausencia de ciertas normas, planes y acciones relacionadas a la seguridad de la información. Con el fin de apoyar los procesos misionales, es importante construir un SGSI basado en la norma ISO/IEC 27001:2013, y se desarrollará un documento que incluya las políticas de seguridad de la información.

Se tiene como objetivo en el proyecto determinar en qué medida el diseño propuesto de un Sistema de Gestión de la Seguridad de la Información basado en la norma o estándar ISO/IEC 27001:2013 mejorará la seguridad de la información en el PNDAP – JUNTOS en el departamento de Huánuco.

Por la cual y para un mejor estudio se dividió la investigación de acuerdo con la estructura de la escuela de posgrado en cinco capítulos de la manera siguiente:

Capítulo I: Aspectos básicos del problema de investigación. Fundamentación del problema de investigación, Descripción y formulación del problema, formulación de objetivos.

Capítulo II: Sistema de Hipótesis. Donde se presenta la formulación de hipótesis, operacionalización de variables y la definición de términos operacionales.

Capítulo III: Marco Teórico. Espacio que nos permitirá plantear el marco conceptual de la investigación.

Capítulo IV: Marco Metodológico. Apreciaremos acá: el ámbito, tipo y nivel de investigación, muestra y población, técnicas e instrumentos para el procesamiento de datos.

Capítulo V: Resultados y discusión.

CAPÍTULO I: ASPECTOS BÁSICOS DEL PROBLEMA DE INVESTIGACIÓN

1.1. Fundamentación del Problema de Investigación

El estudio contempla la fase de diseño de un sistema de gestión de seguridad de la información, el cual está aparejado con la adhesión a la norma ISO/IEC 27001:2013 y se ajusta a las necesidades institucionales, pero no su implementación. El presente estudio se realiza en el programa JUNTOS en el departamento de Huánuco con la finalidad de ofrecer una alternativa de solución y mejoras en las preocupaciones relacionadas a la seguridad de la información. Esto debido a la magnitud del PNADP en Perú.

Con el fin de satisfacer los criterios establecidos en la política de calidad de la institución para la mejora continua de los procesos técnicos y administrativos, la satisfacción de la población interesada y el cumplimiento del marco legal vigente, los valores y principios institucionales, el diseño se enmarca en la norma ISO/IEC 27001:2013, que incluye los estándares de seguridad de los sistemas de información.

Todo esto ha causado a responder si ¿El diseño propuesto de un SGSI basado en ISO/IEC 27001:2013 mejorará la seguridad de la información en el Programa Nacional de Apoyo Directo a los Más Pobres JUNTOS – Huánuco?

1.2. Justificación e importancia de la investigación

El PNADP – JUNTOS en el departamento de Huánuco; como toda organización cuenta con planes estratégicos para la gestión administrativa en la cual se encuentra definida la visión, misión, política y objetivos estratégicos a lograrse en un determinado periodo. Sin embargo, con el horizonte de una mejora continua se requiere monitorear y supervisar de manera efectiva el accionar de los involucrados del Programa JUNTOS frente a los diferentes procesos de sistemas de información implementados a la actualidad.

Según Pallas (2009), donde menciona y dice que la seguridad de la información debe controlarse, debe tener un objetivo específico, criterios generales de evaluación y decisión, y debe ser mensurable. No es un activo que se pueda comprar ni un objetivo en sí mismo.

Debe evaluarse y controlarse con criterios fijos porque es un sistema dinámico que evoluciona constantemente. Esto nos permite evaluar con conocimiento de causa y de la forma más objetiva posible las distintas posibilidades y llegar a conclusiones sobre los riesgos a los que nos enfrentamos y los recursos de que disponemos.

La etapa de diseño o planificación es la piedra angular de los sistemas de gestión porque establece las normas que regirán las fases posteriores, fijando el alcance, las políticas y los objetivos generales. Los sistemas de gestión son procesos en mejora continua y se componen de etapas. En consecuencia, el Sistema de Gestión de seguridad de la Información basada en el estándar ISO/IEC 27001:2013 la fase de diseño será el punto de partida para una implementación posterior, el cual permitirá que el Programa JUNTOS en la UT Huánuco utilizando un enfoque metódico, se pueden detectar y reducir los riesgos potenciales para los activos informáticos sin dejar de cumplir los requisitos legales y normativos, e incluso reduciendo costes.

1.3. Viabilidad de la investigación

En PNADP JUNTOS, la información es un recurso de crucial importancia, por lo que deben existir métodos, procesos y acciones que aseguren su protección. Además de utilizar filtros y otros métodos para proteger el acceso a los datos y limitarlo únicamente a las personas autorizadas para procesarlos, la seguridad lógica también incluye la seguridad física. El PNADP JUNTOS en Huánuco no practica adecuadamente una metodología de gestión de la seguridad de la información para reducir el riesgo de pérdida, cambio o manipulación y robo de la información.

El sector privado en Perú cuenta con un sistema de gestión de la seguridad de la información; según Telefónica Empresas y Nextel S.A., los temas de seguridad de la información rara vez se centran únicamente en cuestiones técnicas, sino más bien en cómo integrar la tecnología con los objetivos estratégicos de la organización.

Dado que la información puede imprimirse o escribirse en papel, almacenarse electrónicamente, enviarse por correo o medios electrónicos, mostrarse en vídeo o hablarse en una conversación, debe protegerse adecuadamente independientemente de cómo se comparta o almacene. Ante esto se optó por diseñar un SGSI en el PNADP JUNTOS – Huánuco con la cual se pretende proteger la información de un amplio rango de amenazas.

El presente estudio permitirá identificar los activos de información del programa JUNTOS muy importantes para el desarrollo y crecimiento del programa, buscando para tal fin métodos y técnicas adecuadas para la salvaguarda y protección de la información.

1.4. Formulación del Problema

1.4.1. Problema general:

¿El diseño propuesto de un SGSI basado en ISO/IEC 27001:2013 mejorará la seguridad de la información en el Programa Nacional de Apoyo Directo a los Más Pobres JUNTOS – Huánuco?

1.4.2. Problemas específicos:

- ✓ ¿Cuál es el estado actual del Sistema de Seguridad de la Información en PNDAP – JUNTOS en el Departamento de Huánuco?
- ✓ ¿Cuál es el análisis del SGSI basado en el estándar ISO/IEC 27001:2013 en el PNDAP – JUNTOS en el Departamento de Huánuco?
- ✓ ¿Cuál es el tipo adecuado del SGSI basado en el estándar ISO/IEC 27001:2013 para la seguridad de la información en el PNDAP – JUNTOS en el Departamento de Huánuco?

- ✓ ¿Con la propuesta del SGSI basado en el estándar ISO/IEC 27001:2013 se mejorará la seguridad de la información en el PNADP – JUNTOS en el Departamento de Huánuco?

1.5. Formulación de Objetivos

1.5.1. Objetivo general:

Determinar en qué medida el diseño propuesto de un SGSI basado en el estándar ISO/IEC 27001:2013 mejorará la seguridad de la información en el PNADP – JUNTOS en el Departamento de Huánuco.

1.5.2. Objetivos específicos:

- ✓ Describir el Sistema de Seguridad de la Información en PNDAP – JUNTOS en el Departamento de Huánuco.
- ✓ Diagnosticar el Sistema de Seguridad de la Información en el PNDAP – JUNTOS en el Departamento de Huánuco.
- ✓ Elaborar las políticas del SGSI basado en el estándar ISO/IEC 27001:2013 en el PNDAP – JUNTOS en el Departamento de Huánuco.

- ✓ Evaluar las políticas propuestas para el SGSI basado en el estándar ISO/IEC 27001:2013 para la seguridad de la información en el PNDAP – JUNTOS en el Departamento de Huánuco.

CAPÍTULO II. SISTEMA DE HIPÓTESIS

2.1. Formulación de Hipótesis

2.1.1. Hipótesis general:

H1: El Diseño propuesto de un SGSI basado en el estándar ISO/IEC 27001:2013 mejorará el sistema de gestión de seguridad de la información en el programa JUNTOS – Huánuco.

H0. El Diseño propuesto de un SGSI basado en el estándar ISO/IEC 27001:2013 no mejorará la seguridad de la información en el PNADP – JUNTOS en el Departamento de Huánuco.

2.1.2. Hipótesis específica:

H_1i: Mediante la descripción del Sistema de Seguridad de la Información se logró conocer la situación real en el PNDAP – JUNTOS en el Departamento de Huánuco.

$H_1$0: Mediante la descripción del Sistema de Seguridad de la Información no logramos conocer la situación real en el PNDAP – JUNTOS en el Departamento de Huánuco.

H_2i: Se logró diagnosticar el sistema de Seguridad de la Información en el PNDAP – JUNTOS mediante el ISO/IEC 27001:2013.

$H_2$0: No se logró diagnosticar el sistema de Seguridad de la Información en el PNDAP – JUNTOS mediante el ISO/IEC 27001:2013.

H_3i: La propuesta de políticas de seguridad de la información de un SGSI se desarrolló mediante el estándar ISO/IEC 27001:2013 en el PNDAP – JUNTOS en el Departamento de Huánuco.

H_30: La propuesta de políticas de seguridad de la información de un SGSI no se desarrolló mediante el estándar ISO/IEC 27001:2013 en el PNDAP – JUNTOS en el Departamento de Huánuco.

H_4i: Mediante las políticas propuestas de la seguridad de la información de un SGSI se logrará mejorar mediante el estándar ISO/IEC 27001:2013 en el PNDAP – JUNTOS en el Departamento de Huánuco.

H_40: Mediante las políticas propuestas de la seguridad de la información de un SGSI se logrará mejorar mediante el estándar ISO/IEC 27001:2013 en el PNDAP – JUNTOS en el Departamento de Huánuco.

2.2. Operacionalización de Variables

Tabla 1: Operacionalización de las variables de investigación

Variable	Dimensión	Indicadores
	✓ A5. Políticas de la seguridad de la información.	- ¿Existe un manual de funciones de la seguridad de la información?
	✓ A6. Organización de la seguridad de la información.	- ¿TI está monitoreando tu computador asignado? - ¿La computadora asignada para su labor cuenta con antivirus y actualizado? - ¿En el trabajo usan software original o legal?
	✓ A7. Seguridad de los Recursos Humanos.	- ¿Capacita al personal en temas de seguridad de información?

VI: Diseño de SGSI mediante estándar ISO/IEC 27001:2013		- ¿Se cuenta con sistemas de alarma con detectores de humo y humedad?
	✓ A8. Gestión de Activos.	- ¿Se realizan mantenimiento preventivo y correctivo a la red de datos y wifi? - ¿Se realiza mantenimiento preventivo del computador? - ¿Se realiza mantenimiento preventivo del celular y/o Tablet?
	✓ A9. Control de Acceso.	- ¿Existen zonas restringidas de acceso al personal en determinadas áreas de trabajo? - ¿Existe vigilancia en la entrada del edificio?
	✓ A10. Criptografía.	- ¿Existen políticas para el cambio frecuente de las contraseñas del email y el acceso a dispositivos electrónicos asignados? - ¿Existe control sobre el uso de correo electrónico?
	✓ A11. Seguridad física y del entorno.	- ¿Realizan copias de seguridad de los datos almacenados en tu computadora? - ¿Realizan copias de seguridad de los datos almacenados en tu Tablet y/o celular? - ¿Los lugares dónde están los equipos de cómputo cuentan con aire acondicionado y funcionando?

	✓ A12. Seguridad de las Operaciones.	- ¿Existe algún control para navegar en Internet?
	✓ A13. Seguridad de las comunicaciones	- ¿El SITC presenta problemas cuando se trabaja en campo?
	✓ A16. Gestión de incidentes de seguridad de la información	- ¿Cuándo ocurre un evento relacionado con seguridad de la información sabes a quién reportarlo?
	✓ A18. Cumplimiento	- ¿Cuentan con seguro los equipos informáticos de uso diario?
La seguridad de la información en el PNADP JUNTOS – Huánuco	✓ Confidencialidad	- Control de acceso - Autenticación - Autorización
	✓ Integridad	- Seguridad de la comunicación - Seguridad en los procesos - Protección de los datos
	✓ Disponibilidad	- Continuidad del servicio - Acceso en el tiempo - Acceso a la información

2.3. Definición de términos operacionales

Tabla 2: Definición operacional de las variables

VARIABLE / DIMENSIÓN	DEFINICIÓN OPERACIONAL
VI: Diseño de SGSI mediante estándar ISO/IEC 27001:2013	Según (redcedia, 2014 p.34) Proteger la información y los sistemas de información del acceso, uso, divulgación o destrucción ilegales es el objetivo del Sistema de Gestión de la Seguridad de la Información, o SGSI.

VD: La Seguridad de la Información en el PNDAP de JUNTOS – Huánuco.	Se puede caracterizar como el mantenimiento de la integridad y accesibilidad de la información en una variedad de formatos, incluidos los medios escritos, orales, impresos y otros según (Dejan Kosutic, 2014 p.19)

CAPÍTULO III: MARCO TEÓRICO

3.1. Antecedentes

3.1.1. Investigaciones Extranjeras

- La investigación presentada por (Giraldo Cepeda, 2016) sobre el "*Análisis para la Implementación de un Sistema de Gestión de la Seguridad de la Información según la Norma ISO 27001 en la Empresa SERVIDOC S.A.*," realizada en el país de Colombia.

  Conclusión: Luego de investigaciones realizadas en la empresa Servidoc S.A. se pudo concluir lo siguiente:

  - ✓ A través de entrevistas no estructuradas y observaciones directas se recogió información y se conoció el funcionamiento de las actividades que son llevadas a cabo en la empresa Servidoc S.A. en Santiago de Cali - Colombia.
  - ✓ Se logró identificar los focos problemáticos que presentaba en las estaciones de trabajo, áreas de contabilidad, facturación e historias clínicas, lo que permitió la elaboración de los documentos que son llevados a cabo en las diferentes etapas del proyecto.

- La investigación presentada por (Pallas Megas, 2009) sobre la "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico" realizada en Uruguay.

  Conclusión**:** Este estudio examina la implantación de un SGSI de enfoque mixto para un grupo empresarial. Aunque las actividades se desarrollan localmente, es decir, en cada una de las empresas que componen el grupo empresarial, el autor pretende que la gestión esté centralizada. Pallas Megas afirma concluyendo: cuando los riesgos son compartidos, el enfoque mixto permitirá unificar criterios y optimizar recursos.

- La investigación presentada por (Bueñano Quintana & Granda Luces, 2009) sobre la "*Planeación y diseño de un Sistema de Gestión de Seguridad de la Información basado en las normas ISO / IEC 27001 – 27002*" realizada en Ecuador.

  Conclusión: Donde La Universidad Politécnica Salesiana Guayaquil es objeto de un estudio de riesgos para este proyecto, que se centra en las amenazas a la prestación de servicios y la continuidad de las actividades. Los autores llegaron a la conclusión de que la Universidad se ha vuelto extremadamente vulnerable a los ataques informáticos como consecuencia del desarrollo tecnológico que ha experimentado. El objetivo de este análisis es reducir el riesgo, para lo cual se ha definido la aplicación de controles centrados en la infraestructura y la documentación. Al aplicar la norma ISO/IEC 27001 - 27002 y la técnica de análisis de riesgos MAGERIT, este trabajo supone una aportación teórica sustancial a la investigación.

3.1.2. Investigaciones Nacionales.

- La investigación presentada por (Cordova Rodriguez, 2003) sobre el "*Plan de seguridad informática para una entidad financiera"*, se desarrolló en Lima, Perú.

  Conclusión: Esta tesis tiene como objetivo diagnosticar el estado existente de la seguridad de la información que actualmente supervisa el Banco ABC y crear un plan de seguridad de la información (PSI) que permita el desarrollo de operaciones seguras basadas en normas y directrices inequívocas que sean comprendidas por todos los empleados del banco. El presente trabajo también tiene en cuenta la descripción de la estrategia y las tareas más cruciales que deben llevarse a cabo antes de poder completar el Plan de Implementación.

- La investigación presentada por (Aguirre Mollehuanca, 2014) sobre el "*Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A.",* se desarrolló en la Ciudad de Lima.

  Conclusión: El objetivo de este estudio ha sido diseñar un sistema de gestión de la seguridad de la información para SERPOST en consonancia con las normas NTP ISO/IEC 27001:2008 y NTP-ISO/IEC 17999:2007.

3.1.3. Investigaciones locales

- El proyecto realizado por (Torres Suarez, 2015) sobre "La Norma Técnica Peruana ISO/IEC 27001:2014 y las Políticas de Seguridad de la Información en la Dirección de Administración del Proyecto Especial CORAH", se desarrolló en la ciudad de Aguaytía, 2015.

  Conclusión: El presente estudio encuentra una ALTA correlación entre la gestión de las políticas de seguridad de la información en la Dirección de Administración del Proyecto Especial de Control y Reducción de Cultivos Ilícitos en el Alto Huallaga (CORAH), 2015, y la norma técnica peruana ISO/IEC 27001:2014. Esta correlación demuestra la importancia de realizar adecuadamente las fases de implementación de un Sistema de Gestión de Seguridad de la Información y apegarse a las recomendaciones realizadas por la norma técnica peruana.

- Vilca (2017, p.3) en su trabajo de investigación "Diseño e implementación de un sistema de gestión de seguridad de la información ISO 27001 para la mejora de la seguridad del área de Recursos Humanos de la empresa Geosurvey de la ciudad de Lima". El objetivo de la tesis de grado de Ingeniero en Sistemas e Informática de la Universidad de Huánuco fue conocer la mejor forma de implementar un sistema de gestión de seguridad de la información para la seguridad de la división de Recursos Humanos de la empresa Geosurvey S.A. Metodología: El estudio utilizó un diseño pre-experimental y una metodología cuantitativa.

Conclusión: El sistema de gestión de la seguridad de la información de la empresa Geosurvey en su departamento de Recursos Humanos mejoró gracias a la intervención.

No existe investigación alguna en la Universidad Nacional Agraria de la Selva

3.2. Bases Teóricas

Diseño de SGSI mediante estándar ISO/IEC 27001:2013

El mundo actual está dominado por las tecnologías de la información (TI), que han penetrado tanto en el ámbito personal como en el comercial. Hoy en día, las empresas utilizan bases de datos para guardar información sobre sus clientes, usuarios y proveedores y comunicarse con ellos por correo electrónico, videoconferencias en directo, etc. Desde que pasó de ser un área que los accionistas descuidaban a ser crucial para las operaciones empresariales y la creación de nuevas perspectivas como elemento diferenciador para obtener una ventaja competitiva, la TI ha desempeñado un papel importante en el éxito de las empresas. Teniendo esto en cuenta, las TI no sólo apoyan las estrategias comerciales actuales de una empresa, sino que también desarrollan otras nuevas, mejorando los productos y servicios de la organización.

No solo la seguridad atañe a grandes empresas y corporaciones de carácter privado, sino también la seguridad debe de ser parte de instituciones públicas, ya que la información que se maneja es muy delicada e importante para el estado y para el usuario.

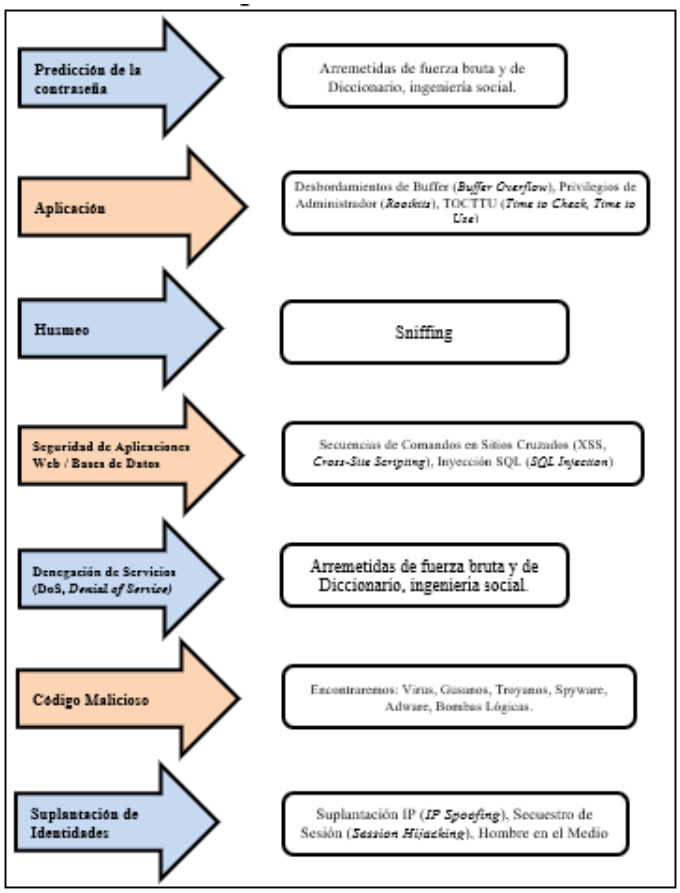
3.2.1. Amenazas a la Seguridad de la Información.

Los activos conforman la infraestructura informática de una organización. Cualquier cosa que pueda producir valor para la empresa u organización y que ésta sienta la necesidad de proteger se denomina activo o recurso informático. Hardware, routers, switches, hubs, firewalls, antenas,

ordenadores, software, sistemas de información, bases de datos, sistemas operativos, así como personal operativo y ubicaciones físicas, son ejemplos de activos.

Estos activos son vulnerables a las amenazas, que pueden proceder tanto de fuentes internas como externas y suponer un riesgo para los activos o para la seguridad de la información en su conjunto. Entre estos peligros se encuentran los siguientes:

Tabla 3. Amenazas a la seguridad de la información.



3.2.2. Sistemas de Gestión de Seguridad de la Información

También se dice que un Sistema de Gestión de Seguridad de la Información (SGSI[1]), según ISO 27001, va a consistir en el cuidado de la confidencialidad, integridad y disponibilidad de la información mediante el uso de un proceso de gestión de riesgos y brindará a las partes interesadas confianza sobre la adecuada gestión de los riesgos (AENOR, 2014).

La información se define como cualquier conjunto organizado de datos que posee una entidad y es valioso para ella, independientemente de cómo se haya creado (internamente dentro de la organización o a partir de fuentes externas), de dónde proceda (por escrito, en imágenes, oralmente, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o correo electrónico, etc.), de cómo se almacene o transmita o de lo reciente que sea su creación o elaboración[2].

Para gestionar la seguridad de la información debe utilizarse un método organizado y documentado que sea conocido en toda la empresa.

Uso de un Sistema de Gestión de Seguridad de la Información:

La información es uno de los recursos más valiosos de una organización, junto con los sistemas y procedimientos que la utilizan. La disponibilidad, el secreto y la integridad de la información sensible pueden llegar a ser cruciales para mantener los niveles de competitividad, rentabilidad, cumplimiento legal e imagen corporativa necesarios para cumplir los objetivos de la empresa y garantizar los beneficios financieros.

Beneficios de un Sistema de Gestión de Seguridad de la Información:

- La creación y establecimiento de una metodología para la gestión de la seguridad siendo clara y estructurada.

[1] Puede encontrarse también como ISMS por sus siglas en inglés de Information Security Management System.
[2] http://www.iso27000.es/index.html

- Reducir el riesgo de pérdida, robo o corrupción de la información.
- Acceso a la información a través de medidas de seguridad.
- Revisión continúa de los riesgos y sus controles.
- Gracias al control de calidad y la confidencialidad empresarial, los consumidores y los socios estratégicos confían.
- Periódicamente, las auditorías externas ayudan a detectar fallos del sistema y posibles áreas de mejora.
- Integración a futuro con otros sistemas de gestión como (ISO 9001, ISO 14001, OHSAS 18001…).
- Cumplimiento de las leyes y reglamentos vigentes en materia de datos personales, propiedad intelectual y otras cuestiones.
- Reconocimiento internacional de la marca de la empresa y ventaja competitiva.
- Mayor confianza y reglas claras para las personas en la organización.
- Menores costes y mejora de los procesos y servicios.
- Mayor motivación y satisfacción al personal.
- Mayor seguridad basada en la gestión de procesos frente a la adquisición metódica de productos y tecnología.

El ciclo Planificar, Hacer, Comprobar, Actuar (PDCA), habitual en los sistemas de gestión de la calidad, se utiliza para establecer y poner en funcionamiento un SGSI. Esta técnica ha demostrado su eficacia y ha permitido desarrollar la mejora continua en empresas de todo tipo. Para medir el estado actual del sistema y realizar mejoras continuas, este modelo consta de cuatro fases:

- ***Planear (Plan)***: Se construye o planifica el SGSI, especificando las políticas generales de seguridad de la organización, los objetivos deseados y cómo apoyarán el cumplimiento de los objetivos de la misión. Se crea la lista de activos y se elige el enfoque de riesgos que se utilizará de acuerdo con los objetivos y directrices propuestos.
- ***Hacer (Do)***: En esta fase, el SGSI se pone en marcha utilizando los controles de seguridad seleccionados, designando a los responsables y aplicando los procedimientos.
- ***Verificar (Check)***: Es durante la fase de supervisión del SGSI cuando se confirma y audita la aplicación de los controles, políticas y procedimientos de seguridad para garantizar que se siguen según lo previsto.
- ***Actuar (Act)***: Durante esta fase se mejora el SGSI y se ponen en marcha medidas correctoras.

  La fase de Actuación conduce de nuevo a la fase de Planificación para iniciar un nuevo ciclo de las cuatro etapas, ya que el PDCA es un ciclo de vida continuo. Cabe señalar que las fases no tienen que completarse necesariamente en el orden indicado; por ejemplo, las actividades de ejecución pueden estar en marcha, aunque otras actividades de planificación aún no hayan finalizado, o los controles pueden supervisarse, aunque aún no se hayan implantado por completo[3].

La seguridad de la información en el PNADP JUNTOS – Huánuco

3.2.3. Programa Nacional de Apoyo Directo a los Más Pobres – JUNTOS

Es un programa de transferencias monetarias condicionadas que fue creado el 7 de abril de 2005 mediante el Decreto Supremo N.º 032–2005–PCM en el que se detalla su finalidad, fuentes de financiamiento y estructura operativa.

El Programa Juntos contribuye a la reducción de la pobreza y evita que las nuevas generaciones se formen en ambientes limitados y de poca participación

[3] http://www.iso27000.es/sgsi_implantar.html#seccion1

social. A través de la entrega de incentivos, Juntos atiende temas sociales como la salud, nutrición y educación; esto bajo un enfoque de restitución de derechos básicos, con la participación organizada y la vigilancia de los dirigentes sociales de las comunidades.

La subvención que otorga Juntos conlleva al cumplimiento de compromisos asumidos por el afiliado, los cuales garantizan el acceso y participación de los hogares en extrema pobreza conformados por niños, niñas, adolescentes hasta los 19 años y gestantes. Del mismo modo la selección de usuarios se realiza en base a la composición de los hogares, obteniendo mejores resultados e impulsando de forma ágil, la producción del capital humano.

3.2.3.1. Misión y visión

Misión:

Contribuir al desarrollo humano y al desarrollo de capacidades especialmente de las generaciones futuras. Mediante incentivos económicos busca promover servicios de calidad en materia de educación, salud, nutrición e identidad, así como restituir los derechos básicos de los usuarios.

Visión

Ser el programa de ayuda económica sostenible que permita restituir totalmente los derechos básicos de los hogares en situación de pobreza y extrema pobreza a nivel nacional. Se pretende disminuir la pobreza, mejorar la calidad de vida de los peruanos e impulsar el desarrollo del capital humano.

3.2.3.2. Marco Normativo

a) Lineamiento de la Política Social

1. **Según el "Acuerdo Nacional"** (22.07.2002), acá se establecen los principios que deberán respetar y guiar las

políticas nacionales del país, que son: (1) Democracia y Estado de derecho; (2) Equidad y justicia social; (3) Competitividad del país; y (4) Estado eficiente, transparente y descentralizado. A partir de los principios señalados en el 'Acuerdo Nacional', se establecen una serie de políticas nacionales vinculadas a la política social, como son: el fortalecimiento del régimen democrático y del Estado de derecho; la descentralización política, económica y administrativa para el desarrollo integral, armónico y sostenido del Perú; la reducción de la pobreza; la promoción de la igualdad de oportunidades sin discriminación; el acceso universal a una educación pública gratuita y de calidad, a los servicios de salud y de seguridad social y al empleo pleno, digno y productivo; la promoción de la seguridad alimentaria y nutrición; el fortalecimiento de la familia, promoción y protección de la niñez, la adolescencia y la juventud; la búsqueda de la competitividad, productividad y formalización de la actividad económica; el desarrollo sostenible y la gestión ambiental; el desarrollo de la vivienda e infraestructura; la política de desarrollo agrario y rural; y la afirmación de un Estado transparente y eficiente.

2. **Y la "Declaración del Milenio"** (13.09.2000), suscrita por 189 Estados miembros de las Naciones Unidas, entre los que se encuentra el Perú. Se fundamenta en principios tales como libertad, igualdad, solidaridad, tolerancia, respeto a la naturaleza y responsabilidad común pero diferenciada, y establece ocho "Objetivos de Desarrollo del Milenio": (1) Erradicar la pobreza extrema y el hambre; (2) lograr la enseñanza básica universal; (3) promover la igualdad de género y el empoderamiento de la mujer; (4) reducir la mortalidad infantil; (5) mejorar la salud materna; (6) combatir el VIH/SIDA, el paludismo y otras enfermedades;

(7) garantizar la sostenibilidad del medio ambiente; y (8) fomentar una alianza mundial para el desarrollo, cuyas metas deberán ser exhibidas entre el 2010 y el 2015.

3. **Según el Plan Bicentenario:** el Perú hacia el 2021, aprobado por el Acuerdo Nacional.

b) Normas de origen y organización

Siendo las siguientes:

1) Ley n.º 29792, Creación y organización de Midis.

2) Decreto Supremo n.º032-2005-PCM**,** Creación del programa JUNTOS.

3) Decreto de Urgencia n.º094-2009 (02-oct-2009)**,** Aprueba y facilita la intervención de los programas sociales y otras entidades en la zona VRAEM.

4) Decreto Supremo n.º009-2012-Midis**,** de fecha 06/07/2012 "Ampliación de la atención del Programa Nacional de Asistencia Solidaria Pensión 65 y del Programa Nacional de Apoyo Directo a los Más Pobres – JUNTOS".

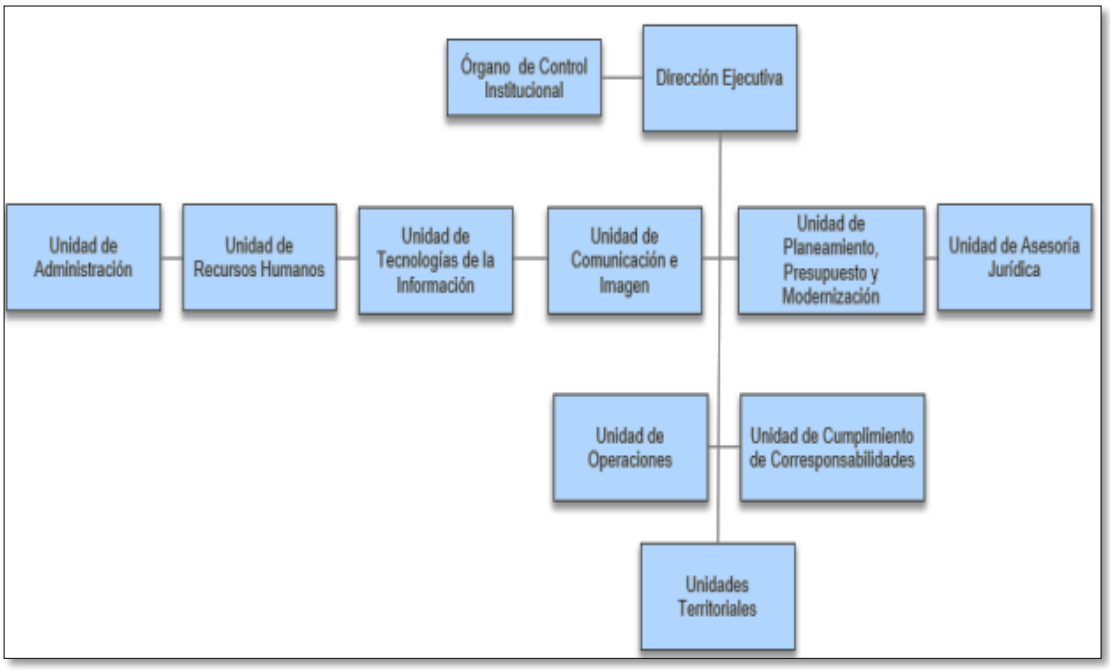
3.2.3.3. Organización y Procesos

Organigrama:

El Ministerio de Desarrollo e Inclusión Social aprueba el Manual de Operaciones (MOP) con la Resolución Ministerial N° 157-2016-MIDIS del 26 de julio del 2016, en la cual se detalla las mejoras funcionales de las unidades del Programa, la creación de la Unidad de Recursos Humanos, la inclusión de las Nuevas Unidades Territoriales (UT), con el fin de mejorar la cobertura y acercamiento a los hogares usuarios.

Siguiendo las recomendaciones para la modernización de la gestión pública, el Programa JUNTOS ha mejorado su gestión por procesos. El Programa JUNTOS cuenta con la siguiente estructura organizacional para llevar a cabo los procesos que le competen.

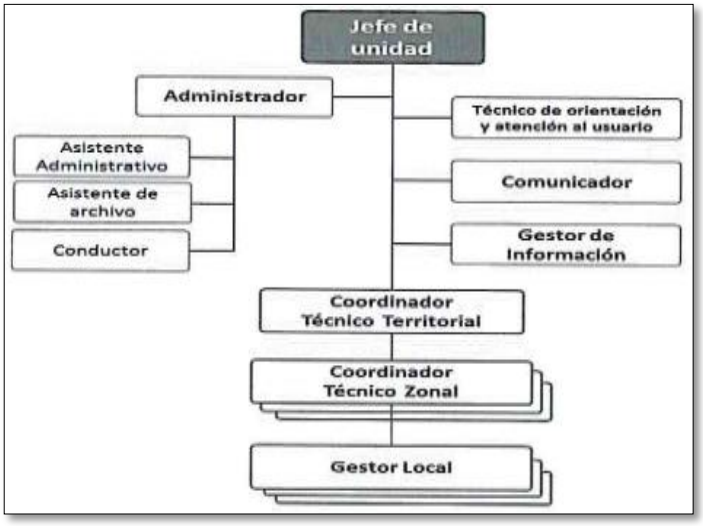
Figura 1: Estructura orgánica del Programa Juntos.



Fuente: Según el (RDE N.° 278-2017-MIDIS) del Manual de Operaciones del Programa Nacional de Apoyo a los Más Pobres Juntos

La Unidad Territorial (UT) son las encargadas de ejecutar en los departamentos del Perú donde exista JUNTOS, para el logro de los objetivos del programa cuentan con profesionales y teniendo un ámbito de intervención, las actividades relacionadas con los procesos operativos, además de articular las acciones necesarias con las instituciones y organizaciones locales y siendo de la manera siguiente:

Figura 2: Estructura de cargos de una Unidad Territorial



Fuente: Según (RDE N.° 278-2017-MIDIS) del Manual de Operaciones del Programa Nacional de Apoyo a los Más Pobres Juntos

3.2.3.4. Procesos del Programa

Van a incluir:

- Procesos Estratégicos,
- Procesos Misionales y
- Procesos de Apoyo.

1) **Los Procesos Estratégicos**, controlan cómo se toman las decisiones sobre la planificación de la organización, las mejoras de sus operaciones y las relaciones con el entorno. Estos procesos se encargan de analizar las necesidades y condicionantes y de emitir las directrices adecuadas al resto de procesos organizativos para asegurar que se satisfacen dichas necesidades y condicionantes. Permiten diseñar e implantar la estrategia, las políticas y los objetivos del programa. Y estos comprenden los procesos siguientes:
   - Gestión del Programa Presupuestal.
   - Gestión de la mejora continua.
   - Gestión de las comunicaciones.

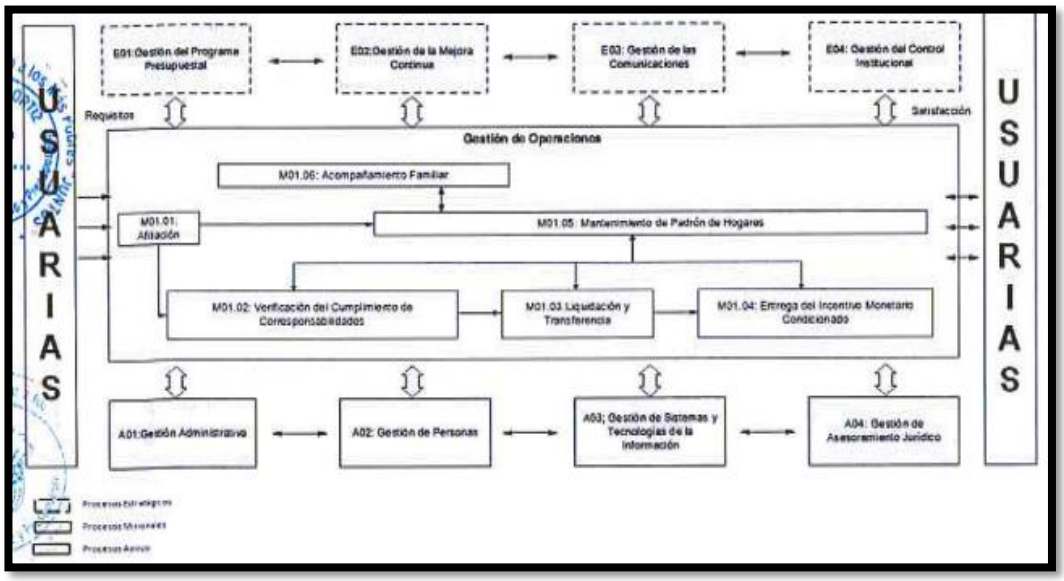
- Gestión del Control Institucional.

2) **Procesos Misionales**, son procedimientos que controlan las acciones que dan lugar a la prestación del servicio a los hogares usuarios. De ellos depende que se satisfagan adecuadamente sus necesidades y aspiraciones.

   Los procesos misionales comprenden:

   - El proceso de Afiliación.
   - EL proceso de Verificación del cumplimiento de corresponsabilidades.
   - El proceso de Liquidación y transferencia.
   - El proceso de Entrega del incentivo monetario condicionado.
   - El proceso de Mantenimiento de padrón de hogares.
   - El proceso de Acompañamiento familiar.

Figura3: **Mapa de Interacción de Procesos**



Fuente: Según (RDE N.° 278-2017-MIDIS) del Manual de Operaciones del Programa Nacional de Apoyo a los Más Pobres Juntos.

3.2.3.5. Asignación presupuestaria del Programa Juntos 2018:

La asignación presupuestaria del programa JUNTOS se da de acuerdo y con la aprobación de la Ley N° 30693, que es la Ley de Presupuesto del Sector Público para el año 2018, incluye la asignación de recursos presupuestarios para el Midis y para sus Programas Sociales adscritos a él, siendo el Presupuesto Institucional de Apertura (PIA) para el año 2022 del Programa Juntos la suma de S/. 1227 millones de soles, el cual se detalla a continuación su desagregación a nivel de genérica de gasto.

S/ 1227 millones para el Programa Nacional de Apoyo Directo a los más pobres (JUNTOS), con lo cual se atenderá a 704 432 hogares. Adicionalmente, para el 2023, se han previsto S/ 150 millones en el presupuesto para financiar el potencial incremento de beneficiarios de los programas sociales[4].

Tabla 4: Asignación presupuestaria del Programa JUNTOS 2018 (*2022).

Genéricas Del Gasto		PIA	Estructura %
2.3	Bienes y servicios	143,332,370	15.13%
2.5	Otros gastos	802,519,363	84.74%
2.6	Adquisición de activos no financieros	1,200,000	0.13%
Total		**947,051,733**	**100.0%**

Fuente: Oficio n.° 866-2017-MIDIS/PNADP-DE (28.09.2017) se remite a OGPPM del Midis el Presupuesto y POI 2018 de la UE 005 del Midis y Reporte B-4 "POI Consolidado con programación física" del aplicativo Ceplan V.01 (24/11/2017).
Elaboración: UPP

3.2.3.6. Convenios Interinstitucionales

PROGRAMA JUNTOS Y EL INSTITUTO NACIONAL DE SALUD

Con el presente convenio se pretende la implementación de un Programa de entrenamiento en Salud Pública en los lugares que

[4]https://www.mef.gob.pe/contenidos/presu_publ/pres_multi/Informe_Programacion_Multianual_2022_2024.pdf

interviene el Programa Juntos, el cual brinde competencias para el desarrollo de las actividades básicas y operativas en el campo de la promoción de la salud, la vigilancia epidemiológica, sanitaria y ambiental, que visibilice el aporte del sector MIDIS como componente estratégico de la respuesta social del Estado contribuyendo al bienestar social y la salud pública.

Suscrito: 16/12/2022

Suscrito: 02 años con renovación automática

EL MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL (MIDIS) Y EL PROGRAMA JUNTOS

Establecer relaciones de cooperación entre ambas entidades, a fin de cumplir con los objetivos propios de cada institución, a través de la asignación de un espacio físico en alguno de los locales de propiedad del Midis, con la finalidad de ubicar el acervo documentario y archivos del programa JUNTOS.

Suscrito: 2/03/2022

Suscrito: Hasta el cumplimiento de la cláusula tercera: objetivo del convenio contratación – No vigente

PROGRAMA JUNTOS Y EL MINISTERIO DE EDUCACIÓN

Este convenio tiene como objetivo establecer las condiciones necesarias para la colaboración entre ambas instituciones, a fin de realizar acciones conjuntas que promuevan la matrícula, acceso y permanencia al servicio educativo contribuyendo a la culminación de la educación básica en el marco de atención a la diversidad.

Suscrito: 5 de octubre de 2022

Vigencia: Tiene dos años, pudiendo ser renovado por igual plazo de común acuerdo entre las partes.

Gobierno Regional de Huánuco y JUNTOS

Convenio Modelo de Gestión de Corresponsabilidad Operativa de los Servicios de Educación entre el GOBIERNO REGIONAL DE HUANUCO y el PROGRAMA JUNTOS

El presente convenio tiene por objeto, la cooperación interinstitucional en la implementación del uso de equipos biométricos en las instituciones educativas públicas de la región de Huánuco, bajo la jurisdicción del gobierno regional.

Así como también se enlista otros de los convenios que realizó el programa JUNTOS con el objetivo de brindar mejores servicios a los ciudadanos.

PROGRAMA JUNTOS Y OSIPTEL

PROGRAMA JUNTOS Y PRONABEC

PROGRAMA JUNTOS Y MINISTERIO DE CULTURA

3.2.3.7. Infraestructura tecnológica

JUNTOS siempre ha estado de acorde al avance tecnológico y prueba de ello cuenta con una plataforma tecnológica:

- Centro de Datos

  Se encuentra ubicado en el 5to piso de la Sede Central, el cual cuenta con Centro de Datos propio, que alberga toda la información y se procesa los servicios informáticos que se procesa en las UT del Perú, además de ello tienen y forma parte de su soporte tecnológico:

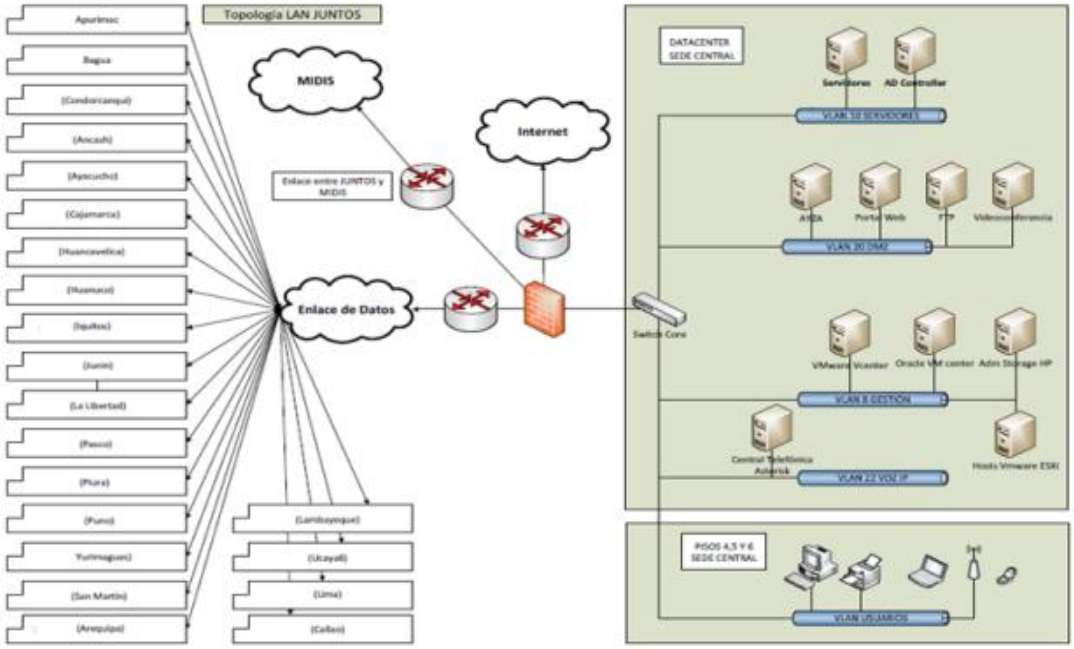
  - UPS.
  - Aire acondicionado de precisión.
  - Estabilizador de energía.
  - Acceso biométrico al local,
  - Cámaras de seguridad y videovigilancia
  - Control de visitantes, etc.

Tabla 5: Equipamiento informático

N.°	Equipo Informático	Cantidad	% operativo	% garantía	% obsolescencia *	Con Redundancia
1	Computadora	1433	85%	11%	81%	
2	Laptop	178	86%	12%	17%	
3	Impresora	236	63%	2%	68%	
4	Escáner	80	85%	16%	35%	
5	Servidor	50	44%	4%	80%	02 servidor Blade, a nivel de virtualización de 76 servidores
6	Storage	4	100%	0%	0%	
7	Firewall	19	53%	0%	100%	
8	Switch	150	39%	7%	69%	

Fuente: Según **UTI (**El Plan De Gobierno Digital Del Programa Juntos 2020 – 2022**)**

Figura 4: Diagrama topológico del programa JUNTOS



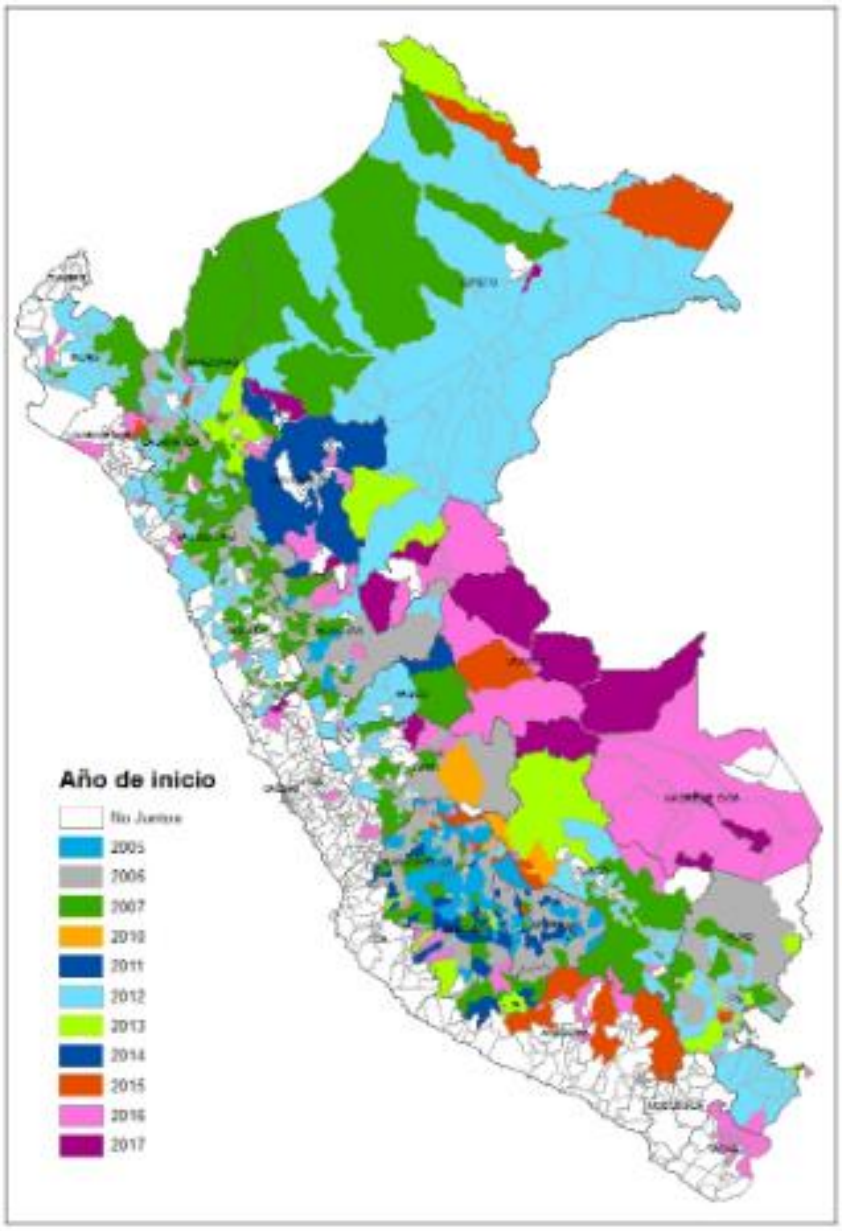
Fuente: Según **UTI (**El Plan De Gobierno Digital Del Programa Juntos 2020 – 2022**)**

3.2.3.8. Intervención y Cobertura geográfica

Para el ingreso de los hogares al Programa JUNTOS se determina de manera gradual y se basa en dos criterios de focalización:

1) Focalización Geográfica, determina si el Programa interviene o no en un distrito teniendo en consideración que debe ser de zonal rural.
2) Focalización de Hogares(SISFOH), Es determinado y se eligen los hogares según nivel de pobreza determinado por el SISFOH.

Figura 5: La intervención geográfica de hogares JUNTOS en Perú por años.



Fuente: Según el Plan De Gobierno Digital Del Programa Juntos 2020 – 2022

Tabla 6: Distritos de intervención del Programa JUNTOS

Periodo	Departamentos	Provincias	Distritos
2018 (V Bim.)	21	174	1,325
2017	21	174	1,325
2016	21	172	1,290
2015	18	159	1,178
2014	15	150	1,144
2013	14	140	1,097
2012	14	138	1,011
2011	14	116	700
2010	14	116	646
2009	14	115	638
2008	14	115	638
2007	14	115	638
2006	9	67	321
2005	4	26	70

3.3. Bases Conceptuales

3.3.1. Seguridad

De acuerdo con (Carletti Estrada, 2017) "Los individuos y las agrupaciones humanas tienen una necesidad básica de seguridad, que es también un derecho inalienable de los pueblos y las naciones. Implica las ideas de aseguramiento, protección, tranquilidad, confianza, prevención, previsión, preservación, defensa, control, paz y estabilidad de los individuos y grupos sociales, frente a las amenazas o presiones que atentan contra su existencia, su integridad, sus bienes, el respeto y ejercicio de sus derechos, etc. Seguridad viene del latín SECURITAS, que a su vez deriva del adjetivo SECURUS, sin cura, sin miedo".

"La seguridad implica la ausencia de peligros, un escenario extremadamente difícil de mantener en el mundo moderno, ya que las civilizaciones son cada vez más reacias al riesgo. La seguridad no puede considerarse como la ausencia de amenazas porque el componente de riesgo es permanente y confiere a los Estados y a las sociedades sus características singulares". (Kosutic, 2012).

3.3.2. Riesgos

Todos los esfuerzos humanos conllevan cierto nivel de riesgo. Esto explica por qué a lo largo de la historia el riesgo ha sido un tema común de discusión. Curiosamente, incluso con todo el discurso sobre el riesgo, sigue siendo un concepto muy ambiguo. Si le pidiera a alguien que le proporcione una definición de riesgo, es muy probable que le puedan proporcionar una respuesta razonable; Sin embargo, si pregunta a diez personas, o incluso a cien, probablemente recibirá una definición diferente de cada persona (Mark Ryan & Jason L., 2013).

Riesgo de seguridad de la información

En seguridad de la información, el riesgo se manifiesta en torno a tres conceptos importantes: amenazas, vulnerabilidades e impacto.

1. **La amenaza:** Es un evento, ya sea una acción o una inacción que conduce a una situación negativa o no deseada. Y estos eventos pueden causar daño, destrucción, alteración, pérdida o relevancia de activos que podrían impedir su uso, su acceso o prevenir su mantenimiento.
2. **Las vulnerabilidades**: Son debilidades o factores ambientales que aumentan la probabilidad de que la amenaza tenga éxito. Es una falla en los procedimientos, diseño, implementación o controles internos de un sistema de seguridad.
3. **El impacto**: Considerado como la pérdida o la posibilidad de una pérdida debido a la amenaza que aprovecha la vulnerabilidad.

Figura 6. Según Riesgos y conceptos de seguridad de la información.

Es crucial tener en cuenta que las entidades son responsables de crear las políticas, objetivos y estructuras de gestión de riesgos. Los planes estratégicos de cada empresa deben ajustarse a este marco.

Se aconseja tener en cuenta los siguientes factores para una gestión eficaz de los riesgos:

- La comunicación y consulta con la finalidad de tomar conciencia ante la presencia de riesgos.
- Alcance, contextos y criterios, así realizar una evaluación del riesgo y tener un plan de acción.
- Los riesgos en los procesos informáticos.
- La evaluación del riesgo y la afectación de los objetivos planteados.
- La valoración del riesgo y saber como actuar frente a ellos.
- Establecer los responsables a los diferentes procesos informáticos para minimizar el riesgo.
- Mejorar la confianza en la organización y los involucrados
- Uso eficaz de los recursos para la administración del riesgo.
- Mejoramiento de los controles.

3.3.3. Estándar UNE-ISO/IEC 27000

Según la norma española el estándar UNE-ISO/IEC 27000, se dice que las normas internacionales para los sistemas de gestión brindan un modelo a seguir para la implementación y operación de un sistema de gestión de la seguridad de la información. Este modelo trae consigo e incorpora características que los expertos acuerdan como un reflejo del estado del arte a nivel internacional. El subcomité SC27 del comité ISO/IEC JTC1 cuenta con un grupo de expertos dedicados a la elaboración de normas internacionales sobre sistemas de gestión de seguridad de la información, también conocido como familia de normas de Sistemas de Gestión de Seguridad de la Información (SGSI).

La familia de normas SGSI:

Esta familia tiene como fin, ayudar a organizaciones de todo tipo y tamaño a implementar y operar un SGSI. Las normas SGSI parta del título general de:

Tecnología de la Información. Técnicas de seguridad; y estas normas internacionales son:

- ✓ El ISO/IEC 27000, es el *Sistema de Gestión de Seguridad de la Información (SGSI). El cual enmarca la Visión de conjunto y vocabulario*.
- ✓ ISO/IEC 27001, Son los *Sistemas de Gestión de Seguridad de la Información (SGSI). Presenta a los Requisitos*.
- ✓ ISO/IEC 27002, contiene a los *Código de práctica para los controles de seguridad de la Información.*
- ✓ ISO/IEC 27003, Es la *Guía para la implementación de los Sistemas de Gestión de Seguridad de la Información (SGSI).*
- ✓ ISO/IEC 27004, En su interior tendremos a la *Gestión de Seguridad de la Información. Administra las Métricas*.
- ✓ ISO/IEC 27005, encargado de la *Gestión de riesgos de Seguridad de la Información*.
- ✓ ISO/IEC 27006, Contiene los *Requisitos para entidades que auditan y certifican Sistemas de Gestión de Seguridad de la Información (SGSI)*.
- ✓ ISO/IEC 27007, es una *Guía para la auditoría de los Sistemas de Gestión de Seguridad de la Información (SGSI)*.
- ✓ ISO/IEC 27010, *Gestión de Seguridad de la Información en comunicaciones intersectoriales e interorganizacionales*.
- ✓ ISO/IEC 27011 *Guía para la Gestión de Seguridad de la Información para las organizaciones de telecomunicaciones basada en la Norma ISO/IEC 27002.*
- ✓ ISO/IEC 27013 *Guía para la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1*.
- ✓ ISO/IEC 27014 *Gobernanza de la seguridad de la información*.
- ✓ ISO/IEC TR 27015 *Guía para la gestión de Seguridad de la Información para servicios financieros*.
- ✓ ISO/IEC TR 27016 *Gestión de Seguridad de la Información. Economía organizacional*.

3.3.4. Estándar UNE ISO/IEC 27001:2013

Un sistema de gestión de la seguridad de la información debe cumplir los criterios descritos en esta norma internacional para poder establecerse, mantenerse y mejorarse con el tiempo. La decisión deliberada de una organización de implantar un sistema de gestión de la seguridad de la información. Las exigencias y objetivos de una organización, las necesidades de seguridad, los procedimientos organizativos en uso, el tamaño y la estructura organizativa influyen en la creación e implantación de un sistema de gestión de la seguridad de la información. Es posible que, a lo largo del tiempo, todos estos elementos condicionantes cambien.

Las actividades y la estructura general de gestión de la organización deben integrarse con el sistema de gestión de la seguridad de la información, y la seguridad de la información debe tenerse en cuenta al diseñar los procesos, los sistemas de información y los controles. Se prevé que la instalación del sistema de gestión de la seguridad de la información se adapte a las exigencias de la empresa.

Según la Norma ISO/IEC 27000 ésta se van encargar de describir la visión de conjunto y el vocabulario de los sistemas de gestión de seguridad de la información, haciendo referencia a la familia de normas de sistemas de gestión de seguridad de la información (incluyendo las Normas ISO/IEC 27003, ISO/IEC 27004 e ISO/IEC 27005), junto con los términos y definiciones relacionados.

La estructura de alto nivel del “Anexo SL”, es la columna vertebral a la hora de revisar las principales normas ISO. Es una herramienta imprescindible, durante la implantación de los sistemas de gestión en las empresas, ya que facilita el trabajo de las organizaciones y de los auditores.

CAPÍTULO IV: MARCO METODOLOGICO

4.1. Ámbito de estudio

Según Sánchez et al. (2018) es considerado como el contexto donde se realizará el estudio. La presente investigación se realizó en el Programa Nacional de Apoyo Directo a los más Pobres JUNTOS – oficina de la Unidad Territorial Huánuco.

4.2. Tipo y nivel de investigación

4.2.1. Tipo de investigación

La presente investigación tiene un enfoque de tipo cuantitativo.

Hernández, Callado & Lucio (2010) define a la investigación cuantitativa como aquella que usa la recolección de datos para la comprobación de la hipótesis y para la cual se empleará la medición numérica y el análisis estadístico.

En este estudio se tiene la finalidad de recolectar la percepción de los trabajadores para diseñar un sistema de gestión de la seguridad de la información en el programa JUNTOS – Huánuco, y de esta manera probar la hipótesis planteada en base a la medición numérica o análisis estadístico.

4.2.2. Nivel de investigación

Explicativo, según Hernández, Callado & Lucio (2010) afirma que la investigación es de nivel explicativo es porque busca identificar las causas de los fenómenos físicos o sociales.

4.3. Población y muestra

4.3.1. Descripción de la población

La población conformada por los trabajadores del Programa Nacional de apoyo

directo a los más pobres JUNTOS – Huánuco, siendo un total de 128 trabajadores.

4.3.2. Muestra y método de muestreo

Es de tipo no probabilística la muestra y está constituido por los trabajadores del Programa Nacional de apoyo directo a los más pobres JUNTOS Huánuco; siendo 31 personas entre hombres y mujeres y con conocimientos en informática básico, medio y avanzado.

4.3.3. Criterio de inclusión y exclusión

Criterios de inclusión: Trabajadores del programa JUNTOS en la Unidad Territorial de Huánuco que actualmente están laborando en la entidad.

Criterios de Exclusión: Trabajadores del programa JUNTOS en la Unidad Territorial Huánuco que actualmente no están laborando en la entidad o presentan sanciones y/o permisos.

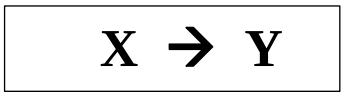
4.4. Diseño de la Investigación

El diseño para la presente investigación es no experimental transversal – causal.

Considerado de este tipo debido a que no hubo necesidad de manipular las variables de manera deliberada, realizándose la observación en su ambiente natural.

del mismo modo su diseño es transversal ya que la recopilación de la información de los encuestados se ejecutó en un mismo instante de tiempo.

Y cabe mencionar que es el causal porque tiene por objeto determinar la medida de la influencia entre las dos variables de estudio, siendo la estadística la herramienta principal de soporte cuya representación se muestra abajo:



Fuente: Elaboración propia.

Donde:

- ***X: Variable Independiente:*** "Diseño de SGSI mediante estándar ISO/IEC 27001:2013 en el PNDAP de JUNTOS – Huánuco"

- ***Y: Variable Dependiente:*** "Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001:2013, en el PNDAP de JUNTOS – Huánuco".

4.5. Técnicas e Instrumentos

4.5.1. Técnicas

La realización de la investigación nos permitió la recopilación de la información y para ello era muy necesario usar la técnica de la encuesta a los trabajadores del Programa Nacional de Apoyo Directo a los Más Pobres JUNTOS - Huánuco, ya que esto nos permitiría recabar información de acuerdo con la percepción que tienen los trabajadores sobre un sistema de seguridad de la información y la aplicación de políticas para el SGSI.

Según Bernal (2010 p. 194) afirma "la encuesta se fundamenta en un cuestionario o conjunto de preguntas que se preparan con el propósito de obtener información de las personas".

4.5.2. Instrumentos

Se diseñó un cuestionario con 20 preguntas con la herramienta formulario de Google Forms, los cuales tienen por objetivo recabar información que nos permitió conocer la situación de las variables en estudio. El cuestionario sobre

el sistema de seguridad de la información aplicado toma 11 de los 14 objetivos de control y controles de referencia del Anexo A de la Norma ISO/IEC 27001:2013.

4.5.2.1. Validación de los instrumentos para la recolección de datos

Para presente investigación se ha validado el instrumento que se aplicó a través de la opinión de expertos, los cuáles realizaron un análisis a las preguntas propuestas para determinar si tienen relación con los objetivos, variables, dimensiones y los indicadores. ***Ver Anexo 04.***

4.5.2.2. Confiabilidad de los instrumentos para la recolección de datos

Para la verificación de la confiabilidad de los instrumentos elaborados se usó el coeficiente de Alfa de Cronbanch teniendo en cuenta el siguiente rango:

Tabla 7: Nivel de confiabilidad del instrumento usando el rango para la valoración de Alfa de Cronbanch.

Valores	Nivel de Confiabilidad
0.53 a menos	Confiabilidad nula
0.54 a 0.59	Confiabilidad baja
0.60 a 0.65	Confiable
0.66 a 0.71	Muy confiable
0.72 a 0.99	Excelente confiabilidad
1.0	Confiabilidad perfecta

Fuente: Barraza (2007)

Tabla 8: Confiabilidad de la variable independiente.

Alfa de Cronbanch	N° de elementos	Nivel de confiabilidad
0.905	20	Excelente confiabilidad

Fuente: Resultados SPSS

4.6. Técnicas para el procesamiento y análisis de datos:

Para el procesamiento de los datos se emplearon los programas IBM SPSS Statistics V21.0 y Excel para Microsoft 365, estos programas permitieron el proceso y la muestra de los datos a través de tablas de frecuencias y figuras de una manera más clara y precisa.

4.7. Aspectos éticos

Según Begoña (2016), dice: se debe de garantizar que el tratamiento de la información no será manipulado por agentes externos al estudio. Asimismo, Google académico refiere la ética no solo alude a los datos personales también es importante para la información que se gestiona y se transmiten y por lo tanto es proteger contra el daño a los participantes que estén involucrados en la recolección de datos y garantizar que los datos recolectados eran creíbles y útiles".

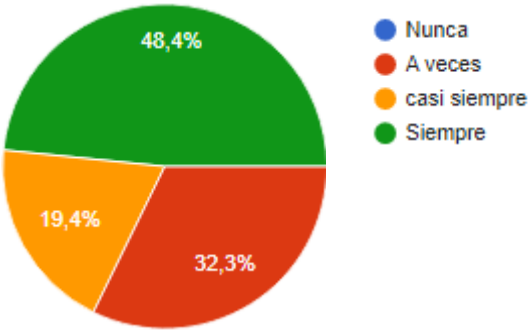
Teniendo en conocimiento lo antes mencionado en el presente estudio, los datos brindados por los participantes fueron protegidos. Se tuvo en consideración el consentimiento previo de los mismos para participar, asimismo, no se hace mención a nombres debido a que los resultados podrían no estar de acuerdo sus opiniones y percepción y se conservó intacto el contenido de las respuestas.

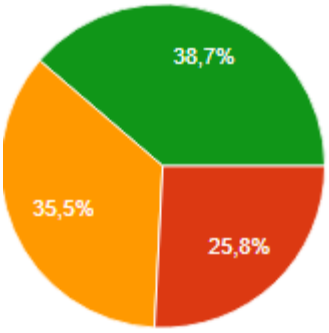
CAPITULO V. RESULTADOS Y DISCUSIÓN

5.1. Análisis Descriptivo

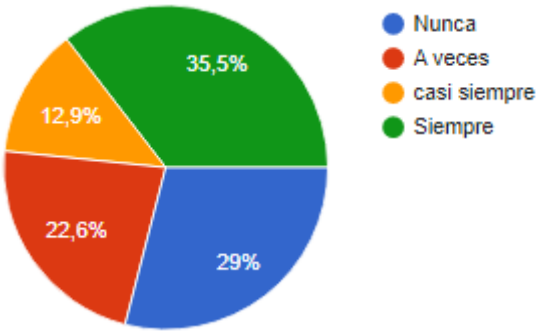
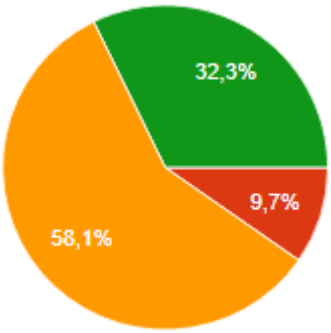
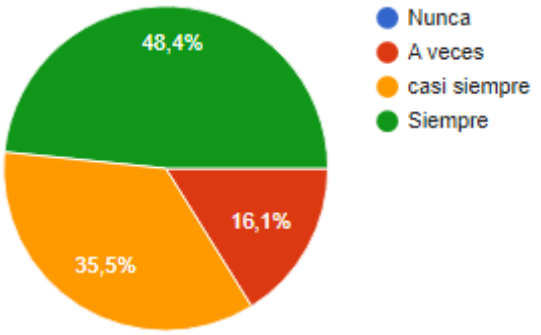
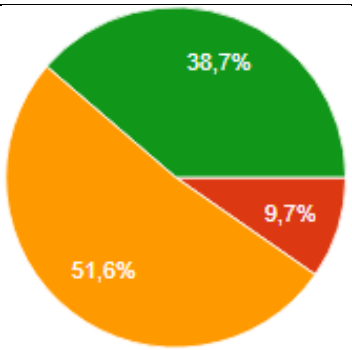
De acuerdo con el análisis de las encuestas realizadas al Programa Nacional de apoyo directo a los más pobres JUNTOS – Huánuco, trajo consigo información respecto a las variables en estudio, esto permitirá identificar si existe influencia entre ellas.

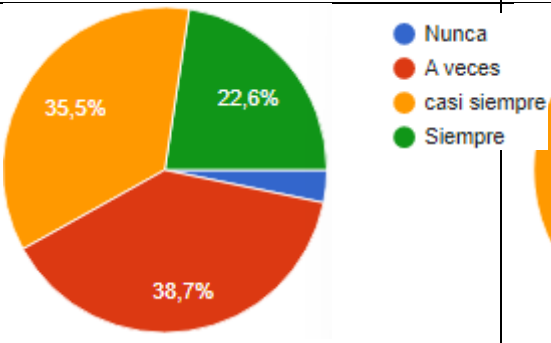
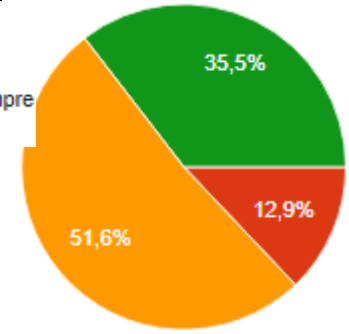
ANÁLISIS

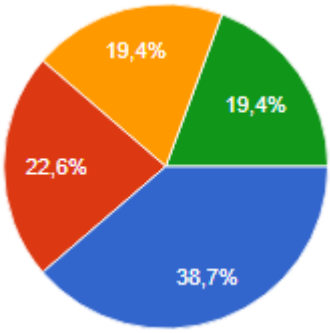
<table>
<tr><th>PRETEST</th><th>POSTEST</th></tr>
<tr><td>1) ¿El computador asignado para el desarrollo de sus actividades recibe mantenimiento preventivo?</td><td>1) ¿El computador asignado para el desarrollo de sus actividades recibiría mantenimiento preventivo?</td></tr>
<tr><td> 

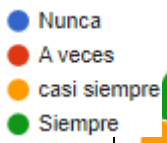
Interpretación: En la figura podemos apreciar que un 48,4% aseguran que se realizan mantenimiento a su computador asignado mientras que un 51,7% de ellos respondieron a veces o casi siempre.</td><td> 

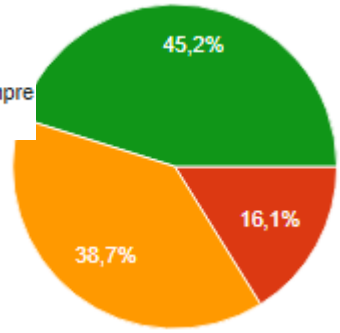
Interpretación: En la figura podemos apreciar que un 48,4% aseguran que se realizan mantenimiento a su computador asignado mientras que un 51,7% de ellos respondieron a veces o casi siempre.</td></tr>
<tr><td colspan="2">Análisis: Como podemos apreciar en los gráficos; en el prestest los trabjadores opinaron de forma positiva en un 67,8% y en el postest opinan positivamente en un 74,20% de lo cual podemos conlcuir que las políticas de un SGSI propuestas sobre el computador asignado para el desarrollo de sus actividades que recibirían mantenimiento, ésta mejoraría la opinión de los trabajadores en un 6,4%.</td></tr>
</table>

<table>
<tr><td>2) ¿La Tablet y/o celular asignado para el desarrollo de sus actividades recibe mantenimiento preventivo?</td><td>2) ¿La Tablet y/o celular asignado para el desarrollo de sus actividades recibiría mantenimiento preventivo?</td></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>Interpretación: En el gráfico siguiente podemos apreciar de las respuestas de los encuestados que un 35,5% siempre reciben mantenimiento la Tablet y celular, un 12,9% casi siempre, un 22,6% a veces y un 29% dicen que nunca recibir mantenimiento de su Tablet o celular.</td><td>Interpretación: En la figura podemos apreciar de la cantidad de encuestados que un 32,3% respondieron con la opción siempre reciben mantenimiento, y un 58,1% casi siempre reciben y un 9,7% a veces se les da mantenimiento a las tabletas y celulares.</td></tr>
<tr><td colspan="2">Análisis: Como podemos apreciar en el pretest los trabajadores opinaron de forma positiva en un 48,4% y en el postest opinan positivamente en un 90,4% de lo cual podemos concluir que las propuestas de las políticas de uns SGSI de la Tablet asignada recibirían mantenimiento y mejoraría en un 42%.</td></tr>
<tr><td>3) ¿Existe un manual de funciones de la Seguridad de la Información?</td><td>3) ¿Existiría un manual de funciones de la Seguridad de la Información?</td></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>Interpretación: Un 48,4% de los trabajadores respondieron que no existe un manual de funciones de la seguridad de</td><td>Interpretación: Un 38,7% de los trabajadores respondieron siempre existiría un manual de funciones de la</td></tr>
</table>

la información, así mismo un grupo representado por 35,5% dicen que casi siempre, y un 16,1% señalaron a veces.	seguridad de la información y un 51,6% respondieron con un casi siempre y no habiendo marcas de la opción nunca.
Análisis: Como apreciamos en el pretest opinaron de forma positiva en un 83,9% y en el postest opinan positivamente en un 90,3% de donde se puede concluir que las propuestas de las políticas para la existencia de un manual de funciones de la seguridad de la información mejoran la opinión de los usuarios en un 6,4%	
4) ¿Se capacita al personal en temas de Seguridad de la Información?	**4) ¿Se capacitarían al personal en temas de Seguridad de la Información?**
	
Interpretación: En la figura siguiente podemos apreciar del total de encuestados que un 38,7% nunca se capacitaron en temas de seguridad de la información, un 35,5% representan a un a veces y del mismo modo un 22,6% indican que siempre se capacitaron.	**Interpretación:** En la figura apreciamos que un 35,7% se capacitarían en temas de seguridad de la información, y un 51,6% representan a un casi siempre y del mismo modo un 12,9% indican a veces.
Análisis: Como podemos apreciar en el pretest los usuarios opinaron de forma positiva en 58.1% y en el postest opinan positivamente en un 87.1% de lo cual podemos concluir que propuestas sobre capacitación al personal en temas de seguridad de la información mejorar la opinión de los trabajadores en un 29%.	
5) ¿Existe políticas para el cambio frecuente de las contraseñas del email y el acceso a dispositivos electrónicos asignados?	**5) ¿Existirían políticas para el cambio frecuente de las contraseñas del email y el acceso a dispositivos electrónicos asignados?**







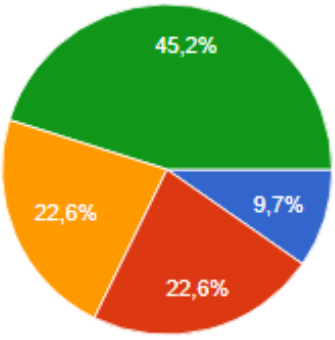
Interpretación: Como apreciamos los trabajadores del programa JUNTOS tienen una percepción de inseguridad, ya que solamente un 19,4% dicen que existe políticas para el cambio de contraseñas y el 61,3% no tiene una información contundente si es que existe o no las políticas para el cambio de las contraseñas

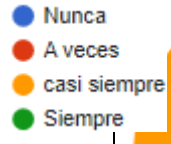
Interpretación: Como se puede ver un 45,2% de los trabajadores dicen que existirían políticas para el cambio de contraseñas y un 38,7% afirman casi siempre y un menor número 16,1% opina que a veces.

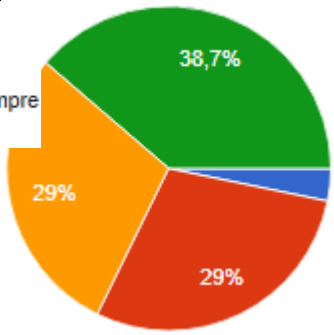
Análisis: Como apreciamos en el pretest opinaron de forma positiva en un 38,8% y en el postest opinan positivamente en un 83,90% de donde se puede concluir que las propuestas de las políticas para el cambio frecuente de las contraseñas del email y acceso a dispositivos electrónicos mejoran la opinión de los usuarios en un 45,1%

6) ¿TI está monitoreando tu computador asignado todo el tiempo?

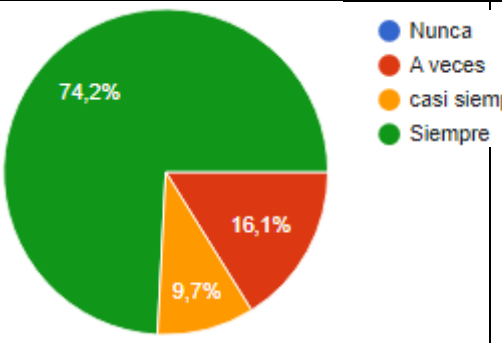
6) ¿TI estaría monitoreando tu computador asignado todo el tiempo?

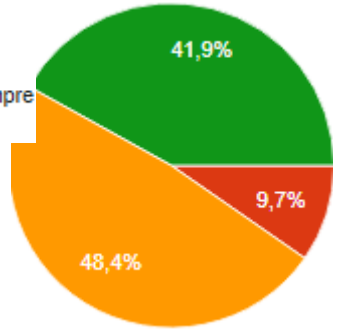




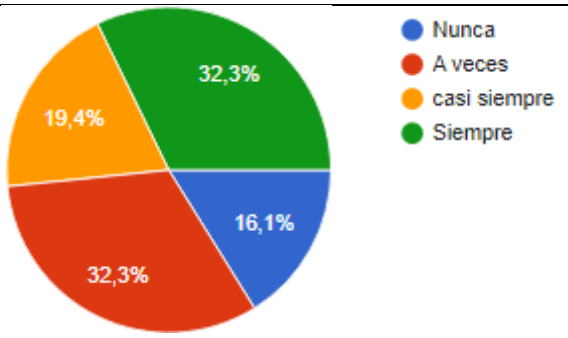


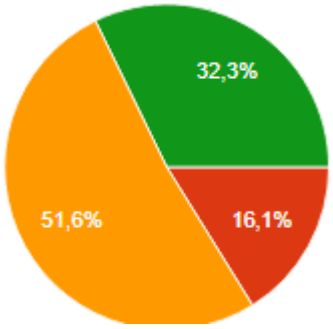
Interpretación: En la figura 6 podemos apreciar que 45,2% opina

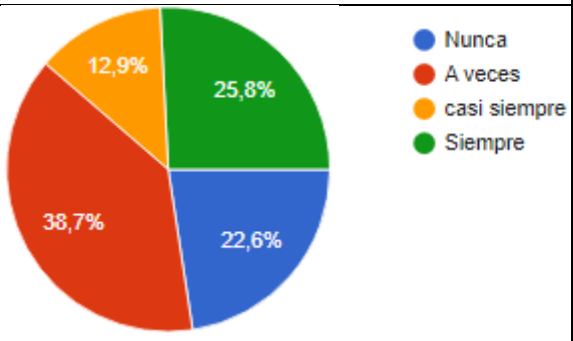
<table>
<tr><td>siempre y un 22,6% casi siempre, así como un 22,6% como los a veces y un 9,7% como nunca.</td><td>Interpretación: Aquí podemos apreciar que 38,7% opina siempre y un 29% casi siempre, así como un 29% como los a veces.</td></tr>
<tr><td colspan="2">Análisis: Como podemos apreciar en el pre test los usuarios opinaron de forma positiva en un 67,8% y en el post esto opinan positivamente en un 67,7% la opinión de los usuarios a bajado en un porcentaje menor al 0.1%.</td></tr>
<tr><td>7) ¿Si ocurriese un evento relacionado con seguridad de la información sabes a quien reportarlo?</td><td>7) ¿Si ocurriese un evento relacionado con seguridad de la información sabrías a quien reportarlo?</td></tr>
<tr><td> 

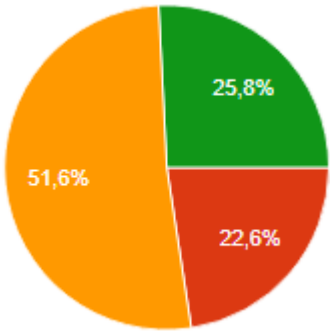
Interpretación: De la figura anterior se puede deducir que un 74,2% de los trabajadores saben a quién reportar un evento relacionado con la seguridad de la información asimismo los 25,8% reportan un a veces o casi siempre</td><td> 

Interpretación: De la figura anterior se puede deducir que un 41,9% de los trabajadores opinan siempre, un 48,4% dijeron casi siempre y los 9,7% reportan un a veces.</td></tr>
<tr><td colspan="2">Análisis: Como podemos apreciar en el pretest los trabajadores entrevistados opinaron de fort positiva en un 83.9% y en el postest opinan positivamente en un 90,3% de lo cual podem concluir que las propuestas de las políticas si ocurriese un evento relacionado con la segurid de la información, sabrían a quién reportarlo mejora la opinión de los usuarios en un 6.4%.</td></tr>
<tr><td>8) ¿Realizan copias de seguridad de los datos almacenados en tu computadora?</td><td>8) ¿Realizarían copias de seguridad de los datos almacenados en tu computadora?</td></tr>
</table>

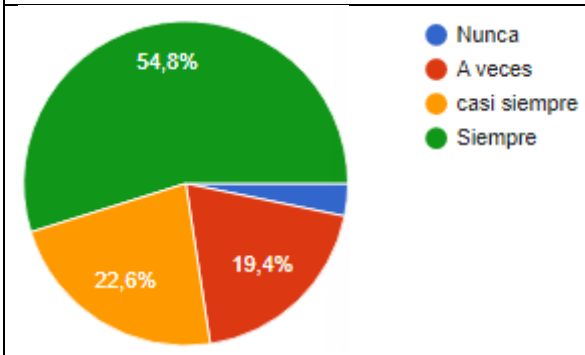
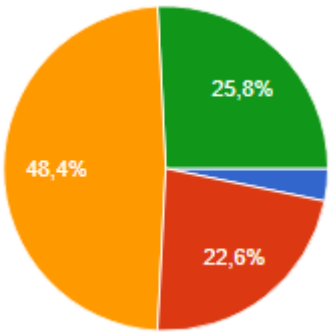
<table>
<tr>
<td> 

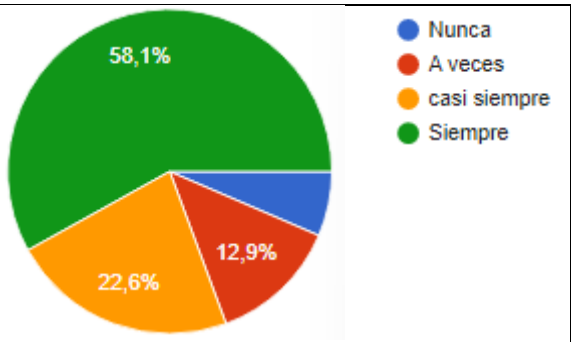
Interpretación: En la información de la figura anterior se observa que un 32,3% siempre realizan copias de seguridad, y un 67,8% el cual está representado por los que eligieron a veces, casi siempre o nunca realizan copias de seguridad de los datos almacenados en su computadora</td>
<td> 

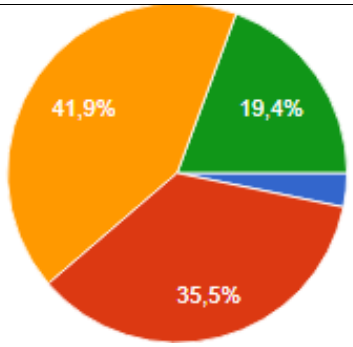
Interpretación: deducimos que un 32,3% de los trabajadores sabrían que realizarían copias de seguridad y asimismo los 51,6% lo harían casi siempre.</td>
</tr>
<tr>
<td colspan="2">Análisis: Apreciando en el pre test los trabajadores opinaron de forma positiva en un 51,7% y en el post test opinan positivamente con un 83,9% de lo cual podemos concluir que las propuestas de las políticas para la realización de copias de seguridad de los datos almacenados en tu computadora mejoran la opinión en un 32,2%.</td>
</tr>
<tr>
<td>9) ¿Realizan copias de seguridad de los datos almacenados en tu Tablet y/o celular?</td>
<td>9) ¿Realizarían copias de seguridad de los datos almacenados en tu Tablet y/o celular?</td>
</tr>
<tr>
<td> 

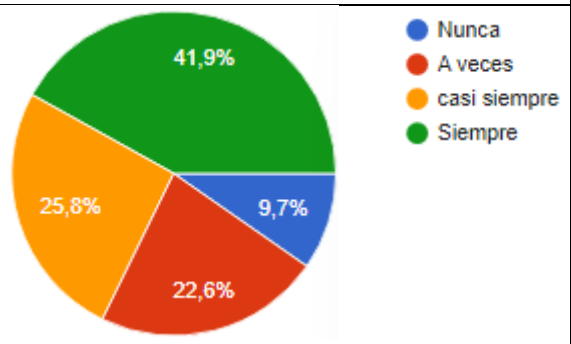
Interpretación: De la figura se puede notar que un 25,8% de los trabajadores realizan copias de seguridad de los datos almacenados en sus tabletas y/o celulares,</td>
<td> 

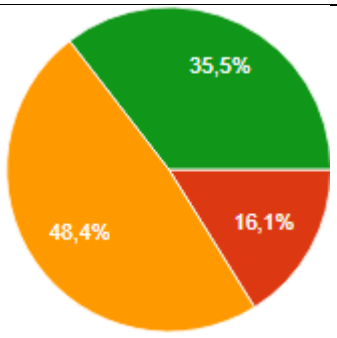
interpretación: De la figura se puede notar que un 25,8% de los trabajadores realizan copias de seguridad de los datos almacenados en sus tabletas y/o</td>
</tr>
</table>

mientras que un 22,6% nunca realizan dicha actividad, también teniendo un 38,7% y 12,9% que dijeron a veces o casi siempre se realizan las copias de seguridad en las tabletas y/o celulares respectivamente.	celulares, mientras que un 22,6% a veces realizan dicha actividad, también teniendo un 51,6% que dijeron casi siempre.
Análisis: Como se aprecia en el pre test los trabajadores opinaron de forma positiva con un 38,7% y en el post test opinaron positivamente en un 77,4% de lo cual podemos concluir que las propuestas de las políticas para un sistema de gestión de seguridad de la información mejoran la opinión de los usuarios en un 38,7%.	
10) ¿La computadora asignada para su labor cuenta con un software antivirus y actualizado?	**10) ¿La computadora asignada para su labor contaría con un software antivirus y actualizado?**
 **Interpretación:** Se observa que un 54,8% de la figura dice que siempre la computadora cuenta con un antivirus y actualizado el cual significa que trabaja en óptimas condiciones, pero un 22,6% dijeron casi siempre y un 19,4% aseguraron a veces.	 **Interpretación:** Observamos que un 58,1% de la figura dice siempre y un 35,5% casi siempre de que la computadora contaría con un antivirus y actualizado, pero un 65,5% dijeron casi siempre.
Análisis: Como se aprecia en el pretest los usuarios opinaron de forma positiva en un 77,4% y en el post test opinan positivamente en un 93,6% de lo cual podemos concluir que las propuestas de las políticas para que el computador contase con un antivirus y esto mejora la opinión de los usuarios en un 16,2%	
11) ¿Usan software original o legal instalado en las computadoras?	**11) ¿Usarían software original o legal instalado en las computadoras?**

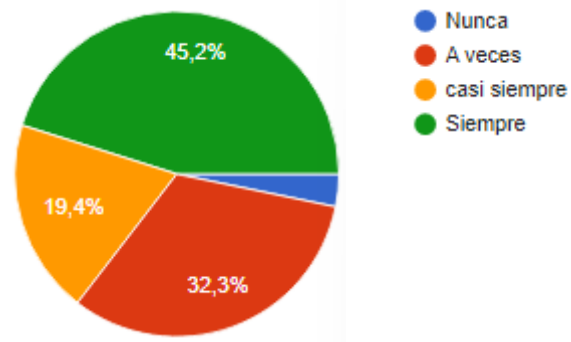
<table>
<tr>
<td> 

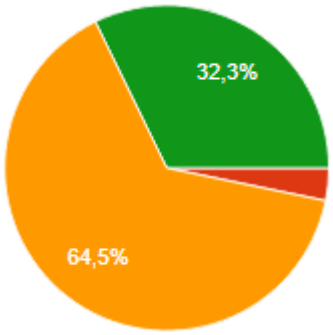
Interpretación: Del gráfico anterior se puede notar que un 58,1% de los encuestados aseguran que siempre en el trabajo se cuenta con software original o legal, también un 35,5% de los encuestados dentro de los cuales se encuentra las opciones de casi siempre y a veces.</td>
<td> 

Interpretación: Del gráfico se puede notar que un 41,9% de los encuestados aseguran que casi siempre en el trabajo se contaría con software original o legal, así mismo un 35,5% dice a veces, un 19,4% siempre y un 3,2% nunca.</td>
</tr>
<tr>
<td colspan="2">Análisis: Como podemos apreciar en el pre test los usuarios opinan de forma positiva en un 80,7% y en el post opinan positivamente en un 77,4% de lo cual podemos concluir que las propuestas de las políticas para el uso de software original instalado en las computadoras mejoran la opinión de los usuarios en un – 3,3%.</td>
</tr>
<tr>
<td>12) ¿Existen zonas restringidas de acceso al personal en determinadas áreas de trabajo?</td>
<td>12) ¿Existirían zonas restringidas de acceso al personal en determinadas áreas de trabajo?</td>
</tr>
<tr>
<td> 

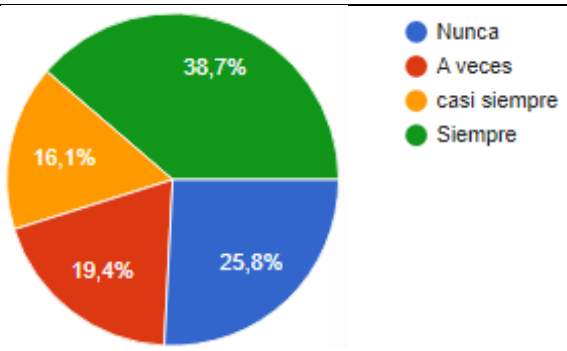
Interpretación: Se observa que un 41,9% de los encuestados dicen que siempre existe zonas restringidas de acceso al personal en determinadas áreas de trabajo coma</td>
<td> 

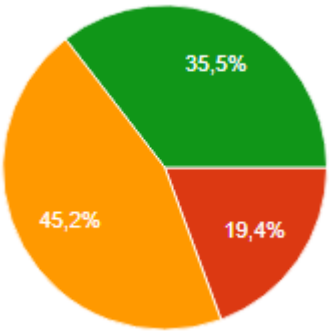
Interpretación: Se observa que un 35,5% de los encuestados dicen que siempre existen zonas restringidas de acceso al personal en determinadas áreas</td>
</tr>
</table>

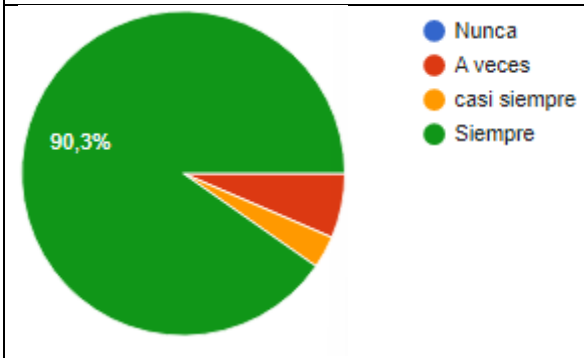
<table>
<tr><td>mientras que los 58,1% de los encuestados aseguran que a veces casi siempre o nunca existen zonas restringidas</td><td>de trabajo coma mientras que los 48,4% de los encuestados aseguran que casi siempre y el 16,1% a veces.</td></tr>
<tr><td colspan="2">Análisis: Como podemos apreciar en el pre test los usuarios opinaron de forma positiva en un 67,7% y en el post test opinan positivamente en un 83,9% de lo cual podemos concluir que las propuestas de las políticas para un sistema de gestión de seguridad la información mejora la opinión de los usuarios en un 16,2%.</td></tr>
<tr><td>13) ¿Se realiza mantenimiento preventivo y correctivo a la red de datos y wifi?</td><td>13) ¿Se realizarían mantenimiento preventivo y correctivo a la red de datos y wifi?</td></tr>
<tr><td> 

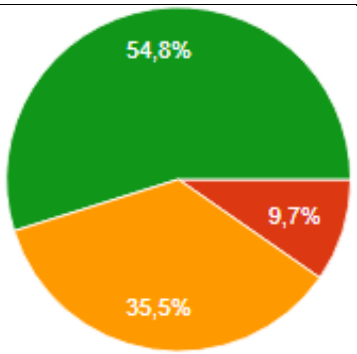
Interpretación: De la información anterior se puede notar que un 45,2% de los trabajadores encuestados seleccionaron siempre se realiza el mantenimiento preventivo y correctivo a la red de datos y wifi, y un 19,4% asegura que así siempre con 32,3% optó por seleccionar a veces.</td><td> 

Interpretación: De la información brindada se tiene que un 32,3% de los trabajadores encuestados eligieron siempre y un 64,5% aseguraron casi siempre Y teniendo un 3,2% a veces.</td></tr>
<tr><td colspan="2">Análisis: Como se puede notar en el pre test los trabajadores opinaron de manera positiva con un 64,67% y en el post test opinan positivamente con un 96,8% de los cuales podemos concluir que las propuestas de las políticas para el sistema de gestión de la información mejora la opinión de los trabajadores en un 32,2%.</td></tr>
<tr><td>14)¿Se cuenta con sistemas de alarma, detectores de humo y detectores de humedad en las áreas de trabajo?</td><td>14) ¿Se contaría con sistemas de alarma, detectores de humo y detectores de humedad en las áreas de trabajo?</td></tr>
</table>

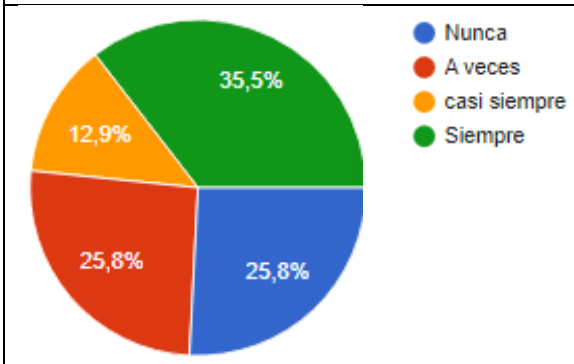
<table>
<tr>
<td> 

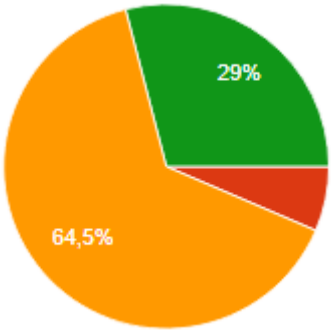
Interpretación: Del gráfico anterior se deduce que el 38,7% eligió la opción siempre ante la interrogante si se cuenta con sistemas de alarma con detectores de humo y humedad, de la misma manera hay un 61,3% de los encuestados que eligieron la opción casi siempre a veces y nunca.</td>
<td> 

Interpretación: Se deduce que el 35,5% eligió a la opción siempre un 45,2% eligió casi siempre y un 19,4% a veces; Esto fue ante la interrogante si se contase con sistemas de alarma como detectores de humo y humedad en las áreas de trabajo</td>
</tr>
<tr>
<td colspan="2">Análisis: como podemos apreciar en el pre test los usuarios opinaron de forma positiva en un 54,8% y en el post opinan positivamente en un 80,7% de la cual podemos concluir que las propuestas de las políticas para el sistema de gestión de seguridad información mejoran la opinión de los usuarios en un 25,9%.</td>
</tr>
<tr>
<td>15) ¿Existe vigilancia al ingreso del local?</td>
<td>15) ¿Existiría vigilancia al ingreso del local?</td>
</tr>
<tr>
<td> 

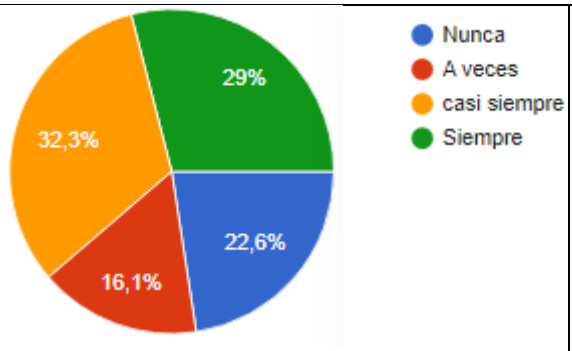
Interpretación: De la figura anterior podemos apreciar que un 90,3% de los encuestados confirman la existencia de vigilancia, el 9,7% seleccionaron otras</td>
<td> 

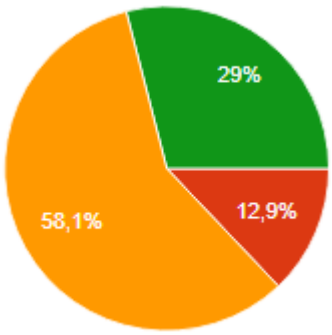
Interpretación: De la figura anterior podemos apreciar que un 100% de los encuestados confirman la existencia de vigilancia en la entrada del edificio.</td>
</tr>
</table>

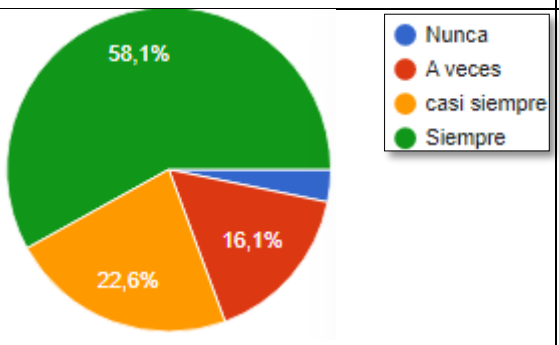
<table>
<tr><td>opciones o alternativas como casi siempre a veces o nunca</td><td></td></tr>
<tr><td colspan="2">Análisis: Como podemos apreciar en el pre test los usuarios opinan de forma positiva en un 90,3% y en el post opinan positivamente un 100% de lo cual podemos concluir que las propuestas de las políticas para el sistema de gestión de seguridad de la información mejoran la opinión de los usuarios en un 9,7%.</td></tr>
<tr><td>16) ¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado y funcionando?</td><td>16) ¿Los lugares donde están los equipos de cómputo contarían con aire acondicionado y funcionando?</td></tr>
<tr><td> 

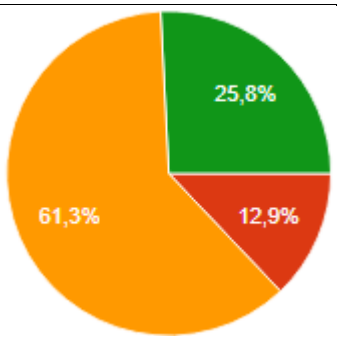
Interpretación: Se observa entre los encuestados que un 35,5% manifestaron siempre un 12,9%, un 25,8% y un 25,8% manifestaron casi siempre a veces y nunca respectivamente.</td><td> 

Interpretación: De la figura se observa entre los encuestados que un 29% son trabajadores que manifiestan que siempre los lugares donde hay equipos de cómputo cuentan con aire acondicionado y funcionando asimismo un 64,5% manifiesta casi siempre.</td></tr>
<tr><td colspan="2">Análisis: Como se puede apreciar en el pretest los usuarios opinaron de forma positiva en un 48,4% y en el posttest opinaron positivamente un 93,5% de lo cual podemos concluir que las propuestas de las políticas para el sistema de gestión de seguridad de la información mejoran la opinión de los trabajadores en un 45,1%.</td></tr>
<tr><td>17) ¿Cuentan con seguro los equipos informáticos de uso diario?</td><td>17) ¿Contarían con seguro los equipos informáticos de uso diario?</td></tr>
</table>

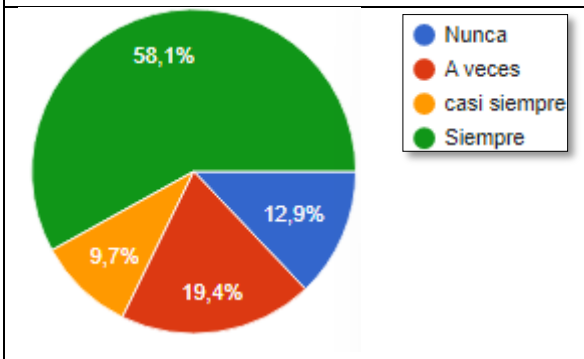
<table>
<tr>
<td> 

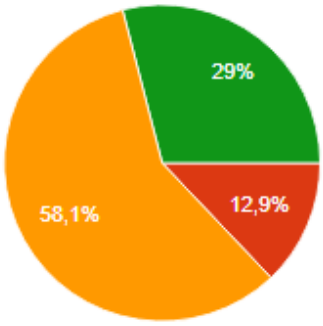
Interpretación: De la figura anterior se puede deducir que un 29% de los trabajadores encuestados afirman que siempre cuentan con seguro los equipos informáticos de uso diario y un 32,3% casi siempre, así como un 16,1% dicen a veces y un 22,6% asegura decir nunca.</td>
<td> 

Interpretación: Se observa que un 29% de los trabajadores encuestados afirman siempre contarían con seguro los equipos informáticos de uso diario, un 58,1% afirma que casi siempre y un 12,9% dice a veces.</td>
</tr>
<tr>
<td colspan="2">Análisis: Como podemos apreciar en el pretest los usuarios opinan de forma positiva en un 61,3% y en el posttest opinan positivamente en un 87,1% de lo cual podemos concluir que las propuestas de las políticas para el sistema de gestión de la información mejoran la opinión de los usuarios en un 25,8%.</td>
</tr>
<tr>
<td>18) ¿Existe algún control para navegar en internet?</td>
<td>18) ¿Existiría algún control para navegar en internet?</td>
</tr>
<tr>
<td> 

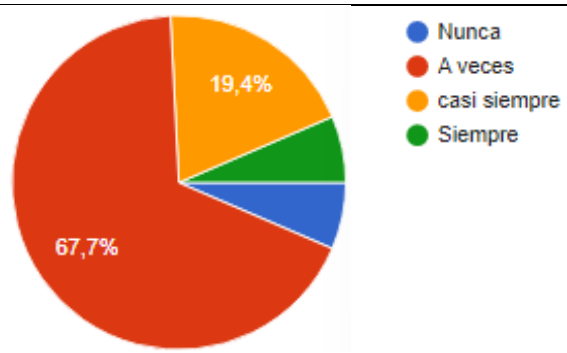
Interpretación: En la medición del ítem 18 se observa que un 58,1% dicen que siempre y 22,6% casi siempre teniendo un porcentaje menor equivalente a 16,1%, a</td>
<td> 

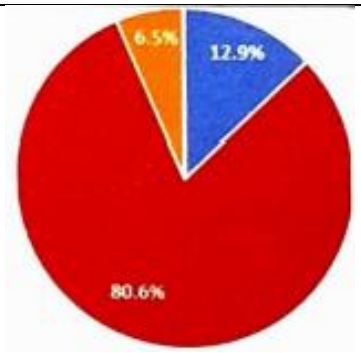
Interpretación: Se observa que un 25,8% de los encuestados dice que siempre existiría algún control para navegar en internet, 61,3% dice casi siempre y 12,9% respondieron a veces.</td>
</tr>
</table>

<table>
<tr><td>veces, pero 3,2% aseguran que nunca hay un control para navegar en internet.</td><td></td></tr>
<tr><td colspan="2">Análisis: Como podemos apreciar en el pre test los usuarios opinaron de forma positiva en un 80,7% y en el post opinan positivamente un 87,1% de lo cual podemos concluir que las propuestas de las políticas para el sistema de gestión de seguridad de la información mejoran la opinión de los usuarios en un 6,4%.</td></tr>
<tr><td>19) ¿Existe control sobre el uso del correo electrónico?</td><td>19) ¿Existiría control sobre el uso del correo electrónico?</td></tr>
<tr><td> 

Interpretación: De la figura se puede notar que un 58,1% de los trabajadores encuestados afirman que siempre existe un control sobre el uso del correo electrónico, 9,7% dicen que casi siempre, 19,4% a veces y 12,9% afirman que nunca se realiza dicha acción.</td><td> 

Interpretación: Como se observa 29% de los trabajadores encuestados afirman que siempre existe un control sobre el uso del correo electrónico, 58,1% dicen que casi siempre y 12,9% a veces.</td></tr>
<tr><td colspan="2">Análisis: Como podemos apreciar en el pretest los usuarios opinaron de forma positiva en un 67,8% y en el posttest opinan positivamente en un 87,1% de lo cual podemos concluir que las propuestas de las políticas para el sistema de gestión de seguridad de la información mejoran la opinión de los usuarios en un 19,3%.</td></tr>
<tr><td>20) ¿El SITC presenta problemas cuando se trabaja en campo?</td><td>20) ¿El SITC presentaría problemas cuando se trabaja en campo?</td></tr>
</table>

<table>
<tr>
<td> 

Interpretación: Se observa entre los encuestados que un 67,7% manifiestan que a veces presenta problemas con el SITC así como 19,4% afirma que le sucede casi siempre pero tenemos que un 6,5% siempre.</td>
<td> 

Interpretación: Del gráfico se puede deducir que entre los encuestados 80,6% a veces presenta problemas con el SITC cuándo trabaja en campo, 12,9% afirma que nunca le sucede y un 6,5% casi siempre.</td>
</tr>
<tr>
<td colspan="2">análisis: Como podemos apreciar en el pretest los usuarios opinaron de forma positiva en un 74,2% y en el postest opina positivamente en un 93,5% de lo cual podemos concluir que las propuestas de las políticas para el sistema de gestión de seguridad de la información mejoran la opinión de los usuarios en un 19,3%.</td>
</tr>
</table>

5.2. Análisis inferencial y/o contrastación

a. Análisis inferencial de la hipótesis general.

Como el nivel de significancia según Wilcoxon como se muestra líneas abajo, tenemos un valor de 0.033, que es un valor menor a 0.05 (0.000 < 0.05) entonces se rechaza la hipótesis nula y aceptamos la alterna, afirmando que el diseño propuesto de un SGSI basado en el estándar ISO/IEC 27001:2013 mejorará el sistema de gestión de seguridad de la información en el programa JUNTOS – Huánuco.

Tabla 9: Estadísticos descriptivos

	N	Media	Desviación típica	Mínimo	Máximo
Pre	31	2,94	,772	2	4
Pos	31	3,29	,461	3	4

Tabla 10: Prueba de los rangos con signo Wilcoxon.

Rangos

		N	Rango promedio	Suma de rangos
Pos - Pre	Rangos negativos	5[a]	8,00	40,00
	Rangos positivos	13[b]	10,08	131,00
	Empates	13[c]		
	Total	31		

b. Pos < Pre

c. Pos > Pre

d. Pos = Pre

Tabla 11: Estadísticos de contraste[a]

	Pos - Pre
Z	**-2.129[b]**
Sig.asintót (bilateral)	**,033**

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos

Análisis inferencial de la hipótesis específica.

H_1i: Mediante la descripción del Sistema de Seguridad de la Información se logró conocer la situación real en el PNDAP – JUNTOS en el Departamento de Huánuco.

H_2i: Se logró diagnosticar el sistema de Seguridad de la Información en el PNDAP – JUNTOS mediante el ISO/IEC 27001:2013.

H_3i: La propuesta de políticas de seguridad de la información de un SGSI se desarrolló mediante el estándar ISO/IEC 27001:2013 en el PNDAP – JUNTOS en el Departamento de Huánuco.

H_4i: Mediante las políticas propuestas de la seguridad de la información de un SGSI se logrará mejorar mediante el estándar ISO/IEC 27001:2013 en el PNDAP – JUNTOS en el Departamento de Huánuco.

5.3. Discusión de resultados

Resultados del diagnóstico del estado situacional del programa JUNTOS, para realizar el diagnóstico se ha elaborado un cuestionario teniendo en cuenta los puntos básicos de la información para determinar el estado situacional. El cuestionario consta de 20 preguntas que ha sido usado para encuestar a 31 trabajadores o colaboradores del programa JUNTOS.

Se pudo determinar que el Diseño propuesto de un SGSI basado en el estándar ISO/IEC 27001:2013 mejorará el sistema de gestión de seguridad de la información en el programa JUNTOS – Huánuco.

5.4. Aporte científico de la investigación

La investigación tuvo como propósito determinar si el uso del estándar ISO/IEC 27001:2013 afectaría o influiría en la mejora de la seguridad de la información en el programa JUNTOS – Huánuco; y definitivamente la aplicación e implementación de las políticas va a mejorar el sistema de gestión de seguridad en el programa. Ya que la búsqueda y protección de la

confidencialidad, la integridad y disponibilidad de la información en diversas formas deben ser la razón de ser de toda organización que cumpla criterios de funcionalidad.

Es importante mencionar que, al desarrollar la presente investigación esta puede ser empleada como material de consulta para futuras investigaciones que tengan el fin de estudiar las políticas de seguridad de la información mediante el estándar ISO/IEC 27001:2013 en entidades públicas y privadas.

CONCLUSIONES

En cuanto al primer objetivo específico, se describió haciendo uso de material bibliográfico, visita a las instalaciones, conversaciones con los trabajadores y equipo jerárquico del Programa - Huánuco.

En cuanto al segundo objetivo específico, para tal fin se hizo uso de una encuesta que consistía en 20 preguntas a 31 trabajadores permitiéndonos saber la situación actual del Programa JUNTOS sobre el sistema de seguridad de la información, por ejemplo ante la interrogante de si existe un manual de funciones de la seguridad de la información tuvimos como resultado que un 48.4% de los trabajadores respondieron que no existe un manual de funciones o desconocen, así mismo un grupo representado por 35.5% que casi siempre y un 16.1% señalaron a veces. Después de aplicar el uso de las políticas las repuestas fueron muy significativas y más contundentes y ante la misma interrogante respondieron de manera positiva en un 90.3% y mejorando un 6.4% su opinión.

En cuanto al tercer objetivo específico, se elaboró políticas del sistema de gestión de seguridad de la información basada en el estándar ISO/IEC 27001:2013. Las políticas se dieron a conocer a los encuestados y se volvió a interrogar mediante una encuesta que consistía en 20 preguntas a los 31 trabajadores.

En cuanto al cuarto objetivo específico, habiendo elaborado las políticas del SGSI se volvió a entrevistar y encuestar con 20 preguntas y a los 31 trabajadores. Teniendo resultados ahora de un pre y un pos; después de aplicado las políticas se tendría mejoras en el sistema de gestión de la seguridad de la información.

SUGERENCIAS

- ✓ Implementar las políticas de seguridad de la información basado en el estándar ISO/IEC 27001:2013. Para lo cual se debe de solicitar a la Unidad Central la asignación de presupuesto y personal calificado con la finalidad de preservar la información en sus diversas formas en el Programa Nacional de Apoyo Directo de los más Pobres JUNTOS – Huánuco.

- ✓ Supervisar el uso y la aplicabilidad de las políticas de seguridad de la información en los trabajadores que laboran en el PNADP JUNTOS – Huánuco con el fin de velar la confidencialidad, integridad y disponibilidad de la información. Lo cual debe de partir desde Jefatura hasta el último trabajador, y solo de esa manera se lograría el éxito en la implementación.

REFERENCIAS

AENOR. (2014). UNE-ISO/IEC 27001. Madrid, Madrid, España: Aenor**.**

Agudelo, L., (2012). Evolución de la Gestión por procesos, Colombia: Icontec.

Aguirre Mollehuanca, D. (15 de Agosto de 2014). Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A. Lima, Lima, Perú.

Bertalanffy, L., (2003). General System Theory, United States:G. Braziller.

Brunner, J., (1990). Educación Superior en América Latina, Chile: Fondo de Cultura Económica.

Bueñano Quintana, J. L., & Granda Luces, M. (12 de Abril de 2009). Planeación y diseño de un Sistema de Gestión de Seguridad de la Información basado en las normas ISO / IEC 27001 – 27002. Guayaquil, Guayaquil, Ecuador.

Carletti Estrada, A. (2017). *Ciberseguridad "Una estrategia militar"*. Madrid: Darfe.

Castrejón, J., (1982). El concepto de Universidad, México: Océano.

Cegarra, J., (2014). Gestión por procesos de negocios, Colombia: Ecobook.

Centro de Encuentro BPM (2011). Tecnologías, conceptos, Enfoques Metodológicos y Estándares, España: Print Marketing.

Chang, J., (2005). Business Process Management Systems, United States: Auerbach Publications.

Cordova Rodriguez, N. E. (3 de Mayo de 2003). Plan de seguridad informática para una entidad financiera. Lima, Lima, Perú.

Garimella, K., Lees, M., Williams, B (2008). Introducción a BPM para Dummies, United States: Wiley Publishing, Inc.

Giraldo Cepeda, L. E. (13 de Febrero de 2016). Análisis para la Implementación de un Sistema de Gestión de la Seguridad de la Información Según la Norma ISO 27001 en la Empresa SERVIDOC S.A. Santiago de Cali, Santiago de Cali, Colombia.

Kendall, K. y Kendall, J., (1998). Análisis y Diseño de Sistemas, México:Prentice-Hall Hispanoamericana

Howard S., Peter F., (2006). Business Process Management the third wave, United States: Meghan Kiffer Pr.

Kosutic, D. (2012). *Cibersguridad en 9 pasos "El manual sobre la seguridad de la información para el gerente".* Zagreb, Croacia: EPPS Services Ltd.

Mark Ryan, T. M., & Jason L., M. (2013). *Information Security Risk Assessment Tolkit.* USA: Syngress.

Pallas Megas, G. (15 de Octubre de 2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Montevideo, Uruguay, Uruguay.

RAE. (14 de Febrero de 2018). www.rae.es. Madrid, Madrid, España.

Torres Suarez, E. E. (12 de Junio de 2015). La Norma Técnica Peruana ISO/IEC 27001:2014 y las Políticas de Seguridad de la Información en la Dirección de Administración del Proyecto Especial CORAH. Aguaytía, Padre Abad, Perú.

ANEXOS

ANEXO 01

MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	MÉTODO
PROBLEMA GENERAL ¿El diseño propuesto de un SGSI basado en ISO/IEC 27001:2013 mejorará la seguridad de la información en el PNADP JUNTOS – Huánuco? **PROBLEMAS ESPECÍFICOS** ✓ ¿Cuál es el estado actual del Sistema de Seguridad de la Información en PNADP JUNTOS – Huánuco? ✓ ¿Cuál es el análisis del SGSI basado en el estándar ISO/IEC 27001:2013 en el PNADP JUNTOS – Huánuco? ✓ ¿Cuál es el tipo adecuado del SGSI basado en el estándar ISO/IEC 27001:2013 para la seguridad de la información en el PNADP JUNTOS – Huánuco?	**OBJETIVO GENERAL** Determinar en qué medida el diseño propuesto de un SGSI basado en el estándar ISO/IEC 27001:2013 mejorará la seguridad de la información en el PNADP JUNTOS - Huánuco. **OBJETIVOS ESPECÍFICOS** ✓ Describir el Sistema de Seguridad de la Información en PNADP JUNTOS – Huánuco. ✓ Diagnosticar el Sistema de Seguridad de la Información en el PNADP JUNTOS – Huánuco. ✓ Elaborar las políticas del basado en el estándar ISO/IEC 27001:2013 en el PNADP – JUNTOS en el Departamento de Huánuco. ✓ Desarrollar el tipo de SGSI basado en el estándar ISO/IEC 27001:2013 para la seguridad de la información en el PNADP JUNTOS – Huánuco.	**HIPÓTESIS GENERAL:** El Diseño propuesto de un SGSI basado en el estándar ISO/IEC 27001:2013 mejorará el sistema de gestión de seguridad de la información en el PNADP JUNTOS – Huánuco. **HIPÓTESIS ESPECÍFICA** $H_1 1$: Mediante la descripción del Sistema de Seguridad de la Información se logró conocer la situación real en el PNADP – JUNTOS en el Departamento de Huánuco. $H_2 1$: Se logró diagnosticar el sistema de Seguridad de la Información en el PNADP – JUNTOS mediante el ISO/IEC 27001:2013. $H_3 1$: La propuesta de políticas de la seguridad de la información de un SGSI se desarrolló mediante el ISO/IEC 27001:2013 en el PNADP – JUNTOS. $H_4 i$: Mediante las políticas propuestas de la seguridad de la información de un SGSI se logrará mejorar mediante el ISO/IEC 27001:2013 en el PNADP – JUNTOS.	**VARIABLE DE INVESTIGACIÓN** "Sistema de gestión de la seguridad de la información basado en el estándar ISO/IEC 27001:2013, en el PNADP de JUNTOS - Huánuco". VI: Diseño de SGSI mediante estándar ISO/IEC 27001:2013. VD: La Seguridad de la Información en el PNADP de JUNTOS – Huánuco.	**TIPO DE INVESTIGACIÓN** ✓ Investigación cuantitativa. **DISEÑO Y ESQUEMA DE LA INVESTIGACIÓN** ✓ Transaccional **POBLACIÓN Y MUESTRA** **Población**: Trabajadores del PNADP JUNTOS – Huánuco. N = 120 **Muestra:** n = 31 **TECNICAS DE RECOJO, PROCESAMIENTO Y PRESENTACIÓN DE DATOS** ✓ Observación, Cuestionario, entrevistas, encuestas, registros y Software de apoyo.

ANEXO 02

CONSENTIMIENTO INFORMADO

.

ID: _____ **FECHA: _____**

TÍTULO: "SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN UN ESTÁNDAR DE SEGURIDAD EN EL PROGRAMA JUNTOS, HUÁNUCO"

OBJETIVO: Determinar en qué medida el diseño propuesto de un SGSI basado en el estándar ISO/IEC 27001:2013 mejorará la seguridad de la información en el PNADP – JUNTOS en el Departamento de Huánuco..

INVESTIGADOR: POZO MEZA DALI RAFAEL

Consentimiento / Participación voluntaria

Acepto participar en el estudio: He leído la información proporcionada, o me ha sido leída. He tenido la oportunidad de preguntar dudas sobre ello y se me ha respondido satisfactoriamente. Consiento voluntariamente participar en este estudio y entiendo que tengo el derecho de retirarme en cualquier momento de la intervención (tratamiento) sin que me afecte de ninguna manera.

- **Firmas del participante o responsable legal**

Huella digital si el caso lo amerita

Firma del participante:_____

Firma del investigador responsable:_____

ANEXO 03

INSTRUMENTO

CUESTIONARIO

Estimados colaboradores del programa JUNTOS, la presente encuesta tiene la finalidad de conocer el sistema de gestión de seguridad de la información en el Programa Nacional de Apoyo Directo a los más Pobres JUNTOS en el departamento de Huánuco. La encuesta es anónima por lo cual invitamos a contestar con sinceridad, los datos serán usados con fines de investigación - académicos.

INSTRUCCIONES: para seleccionar la respuesta correcta hacer un clic en una de las opciones (Checklist)

1) ¿El computador asignado para el desarrollo de sus actividades recibe mantenimiento?
   o Nunca o A veces o Casi siempre o Siempre

2) ¿La Tablet y/o celular asignado para el desarrollo de sus actividades recibe mantenimiento?
   o Nunca o A veces o Casi siempre o Siempre

3) ¿Existe un manual de funciones de la Seguridad de la información?
   o Nunca o A veces o Casi siempre o Siempre

4) ¿Se capacita al personal en temas de seguridad información?
   o Nunca o A veces o Casi siempre o Siempre

5) ¿Existen políticas para el cambio frecuente de las contraseñas del email y el acceso a dispositivos electrónicos asignados?
   o Nunca o A veces o Casi siempre o Siempre

6) ¿TI está monitoreando tu computador asignado?
   o Nunca o A veces o Casi siempre o Siempre

7) ¿Cuándo ocurre un evento relacionado con seguridad de la información sabes a quién reportarlo?
   o Nunca o A veces o Casi siempre o Siempre

8) ¿Realizan copias de seguridad de los datos almacenados en tu computadora?
   o Nunca o A veces o Casi siempre o Siempre

9) ¿Realizan copias de seguridad de los datos almacenados en tu Tablet y/o celular?
   o Nunca o A veces o Casi siempre o Siempre

10) ¿La computadora asignada para su labor cuenta con antivirus y actualizado?
    o Nunca o A veces o Casi siempre o Siempre

11) ¿En el trabajo usan software original o legal?
    o Nunca o A veces o Casi siempre o Siempre

ANEXO 04

VALIDACIÓN DE LOS INSTRUMENTOS POR JUECES

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO

ANEXO 10

VALIDACIÓN POR JUECES

Hoja de instrucciones para la evaluación

CATEGORÍA	CALIFICACIÓN	INDICADOR
RELEVANCIA El ítem es esencial o importante, es decir, debe ser incluido	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo nivel	El ítem tiene una alguna relevancia, pero otro ítem puede estar incluyendo lo que mide este
	3. Moderado nivel	El ítem es relativamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que están midiendo	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo nivel	El ítem tiene una relación tangencial con la dimensión
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo
	4. Alto nivel	El ítem tiene relación lógica con la dimensión
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de esta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión
	2. Bajo nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente
	4. Alto nivel	Los ítems son suficientes
CLARIDAD El ítem se comprende fácilmente, es decir, sus sintácticas y semánticas son adecuadas	1. No cumple con el criterio	El ítem no es claro
	2. Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras que utilizan de acuerdo a su significado o por la ordenación de los mismos
	3. Moderado nivel	Se requiere una modificación muy específica de algunos términos de ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Título de la Investigación: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.**

Nombre del Tesista: **Dalí Rafael Pozo Meza**

Nombre del experto: Mg. Jorge Luis Pozo Malpartida. Asesor: **Mg. Yessica Raquel Reyes Ayala**

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIA
A5. Políticas de la seguridad de la información.	¿Existe un manual de funciones de la Seguridad de la información?	4	3	4	4	15	3.75
A6. Organización de la seguridad de la información.	¿TI está monitoreando tu computador asignado?	3	4	3	4	14	3.5
	¿La computadora asignada para su labor cuenta con antivirus y actualizado?	4	4	3	3	14	3.5
	¿En el trabajo usan software original o legal?	4	3	4	3	14	3.5
A7. Seguridad de los Recursos Humanos.	¿Se capacita al personal en temas de seguridad información?	3	4	4	3	14	3.5
	¿Se cuenta con sistemas de alarma como detectores de humo y humedad?	4	4	4	4	16	4
A8. Gestión de Activos.	¿El computador asignado para el desarrollo de sus actividades recibe	4	4	3	3	14	3.5
	¿La Tablet y/o celular asignado para el desarrollo de sus actividades recibe mantenimiento?	3	4	3	3	13	3.25
	¿Se realiza mantenimiento preventivo y correctivo a la red de datos y wifi?	4	4	3	4	15	3.75
A9. Control de Acceso.	¿Existen zonas restringidas de acceso al personal en determinadas áreas	4	4	4	3	15	3.75
	¿Existe vigilancia en la entrada del edificio?	3	4	4	4	15	3.75
A10. Criptografía.	¿Existen políticas para el cambio frecuente de las contraseñas del email y el acceso a dispositivos electrónicos asignados?	3	3	3	4	13	3.25
	¿Existe control sobre el uso del correo electrónico?	4	4	4	3	15	3.75
	PROM	3.61	3.76	3.53	3.46	14.38	3.59

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO (X) En caso de Sí, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO: El instrumento debe ser aplicado: SI (X) NO ( )

020.

Firma y Sello del juez

UNIVERSIDAD NACIONAL HERMILIO VALDIZAN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Título de la Investigación: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.**

Nombre del Tesista: **Dalí Rafael Pozo Meza**

Nombre del experto: Mg. Jorge Luis Pozo Malpartida

Asesor: **Mg. Yessica Raquel Reyes Ayala**

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIAL
A11. Seguridad física y del entorno.	¿Realizan copias de seguridad de los datos almacenados en tu computadora?	4	3	4	4	15	3.75
	¿Realizan copias de seguridad de los datos almacenados en tu Tablet y/o celular?	4	4	4	4	16	4
	¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado y funcionando?	3	3	4	3	13	3.25
A12. Seguridad de las Operaciones.	¿Existe algún control para navegar en internet?	4	4	3	4	15	3.75
A13. Seguridad de las comunicaciones.	¿El SITC presenta problemas cuando se trabaja en campo?	4	3	3	4	14	3.5
A16. Gestión de incidentes de seguridad de la información.	¿Cuándo ocurre un evento relacionado con seguridad de la información sabes a quién reportarlo?	4	4	3	3	14	3.5
A18. Cumplimiento.	¿Cuentan con seguro los equipos informáticos de uso diario?	4	4	4	3	15	3.75
	PROM	3.86	3.57	3.57	3.57	14.57	3.64

CALIFICACIÓN: **1=No Cumple; 2=Nivel Bajo; 3=Nivel Moderado; 4=Nivel Alto**

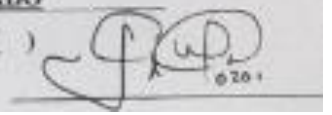
CALIFICACIÓN DEL INSTRUMENTO 3.64 **Redondeo** 4

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO (X) En caso de SI, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO:

CALIFICACIÓN: **MODERADO**

El instrumento debe ser aplicado: SI (X) NO ( )



UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Título de la Investigación: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.**

Nombre del Tesista: **Dalí Rafael Pozo Meza**

Nombre del experto: Mg. Liesel Adriana Barrueta Rojas Asesor: **Mg. Yessica Raquel Reyes Ayala**

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIAL
A5. Políticas de la seguridad de la información.	¿Existe un manual de funciones de la Seguridad de la información?	4	4	4	4	16	4
A6. Organización de la seguridad de la información.	¿TI está monitoreando tu computador asignado?	4	3	4	3	14	3.5
	¿La computadora asignada para su labor cuenta con antivirus y actualizado?	3	4	4	4	15	3.75
	¿En el trabajo usan software original o legal?	4	4	3	3	14	3.5
A7. Seguridad de los Recursos Humanos.	¿Se capacita al personal en temas de seguridad información?	4	4	3	4	15	3.75
	¿Se cuenta con sistemas de alarma como detectores de humo y humedad?	4	3	4	4	15	3.75
A8. Gestión de Activos.	¿El computador asignado para el desarrollo de sus actividades recibe	3	4	3	4	14	3.5
	¿La Tablet y/o celular asignado para el desarrollo de sus actividades recibe mantenimiento?	4	4	4	4	16	4
	¿Se realiza mantenimiento preventivo y correctivo a la red de datos y wifi?	4	4	3	3	14	3.5
A9. Control de Acceso.	¿Existen zonas restringidas de acceso al personal en determinadas áreas	4	4	4	3	15	3.75
	¿Existe vigilancia en la entrada del edificio?	4	4	4	4	16	4
A10. Criptografía.	¿Existen políticas para el cambio frecuente de las contraseñas del email y el acceso a dispositivos electrónicos asignados?	4	3	4	4	15	3.75
	¿Existe control sobre el uso del correo electrónico?	3	4	4	3	14	3.5
	PROM	3.77	3.77	3.69	3.69	14.85	3.71

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO (X) En caso de Si, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO: El instrumento debe ser aplicado: SI (X) NO ( )

Firma y Sello del juez

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Titulo de la Investigación: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.**

Nombre del Tesista: **Dali Rafael Pozo Meza**

Nombre del experto: Mg. Lisset Adriana Barrueta Rojas Asesor: **Mg. Yessica Raquel Reyes Ayala**

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIAL
A11. Seguridad física y del entorno.	¿Realizan copias de seguridad de los datos almacenados en tu computadora?	4	4	3	4	15	3.75
	¿Realizan copias de seguridad de los datos almacenados en tu Tablet y/o celular?	4	4	4	4	16	4
	¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado y funcionando?	4	3	3	4	14	3.5
A12. Seguridad de las Operaciones.	¿Existe algún control para navegar en internet?	4	3	4	4	15	3.75
A13. Seguridad de las comunicaciones.	¿El SITC presenta problemas cuando se trabaja en campo?	4	4	4	4	16	4
A16. Gestión de incidentes de seguridad de la información.	¿Cuándo ocurre un evento relacionado con seguridad de la información sabes a quién reportarlo?	3	4	4	3	14	3.5
A18. Cumplimiento.	¿Cuentan con seguro los equipos informáticos de uso diario?	4	3	4	4	15	3.75
	PROM	3.86	3.57	3.71	3.86	15	3.96

***CALIFICACIÓN:* 1=No Cumple; 2=Nivel Bajo; 3=Nivel Moderado; 4=Nivel Alto**

CALIFICACIÓN DEL INSTRUMENTO 3.73 **Redondeo** 4

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO ( ) En caso de Si, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO:

CALIFICACIÓN: Nivel Alto

El instrumento debe ser aplicado: SI (X) NO ( )

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Título de la Investigación: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.**

Nombre del Tesista: **Dalí Rafael Pozo Meza**

Nombre del experto: Mg. Ricardo Carlos Inquilla Quispe Asesor: **Mg. Yessica Raquel Reyes Ayala**

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIAL
A5. Políticas de la seguridad de la información.	¿Existe un manual de funciones de la Seguridad de la información?	4	4	4	4	16	4
A6. Organización de la seguridad de la información.	¿TI está monitoreando tu computador asignado?	4	3	4	4	15	3.75
	¿La computadora asignada para su labor cuenta con antivirus y actualizado?	3	4	4	4	15	3.75
	¿En el trabajo usan software original o legal?	4	3	4	4	15	3.75
A7. Seguridad de los Recursos Humanos.	¿Se capacita al personal en temas de seguridad información?	4	4	3	4	15	3.75
	¿Se cuenta con sistemas de alarma como detectores de humo y humedad?	3	4	4	3	14	3.5
A8. Gestión de Activos.	¿El computador asignado para el desarrollo de sus actividades recibe	3	4	4	4	15	3.75
	¿La Tablet y/o celular asignado para el desarrollo de sus actividades recibe mantenimiento?	4	4	4	4	15	3.75
	¿Se realiza mantenimiento preventivo y correctivo a la red de datos y wifi?	3	3	3	4	13	3.25
A9. Control de Acceso.	¿Existen zonas restringidas de acceso al personal en determinadas áreas	4	4	4	3	15	3.75
	¿Existe vigilancia en la entrada del edificio?	3	4	4	4	15	3.75
A10. Criptografía.	¿Existen políticas para el cambio frecuente de las contraseñas del email y el acceso a dispositivos electrónicos asignados?	4	4	4	3	15	3.75
	¿Existe control sobre el uso del correo electrónico?	3	4	4	4	15	3.75
	PROM	4	4	4	4	15	3.75

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO (X) En caso de Sí, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO: El instrumento debe ser aplicado: SI (X) NO ( )

Firma y Sello del juez

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Título de la Investigación: SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.

Nombre del Tesista: Dall Rafael Pozo Meza

Nombre del experto: Mg. Ricardo Carlos Ingunza Quispe Asesor: Mg. Yessica Raquel Reyes Ayala

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIAL
A11. Seguridad física y del entorno.	¿Realizan copias de seguridad de los datos almacenados en tu computadora?	3	4	4	4	15	3.75
	¿Realizan copias de seguridad de los datos almacenados en tu Tablet y/o celular?	4	4	4	4	16	4
	¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado y funcionando?	4	4	4	4	16	4
A12. Seguridad de las Operaciones.	¿Existe algún control para navegar en internet?	4	4	4	3	15	3.75
A13. Seguridad de las comunicaciones.	¿El SITC presenta problemas cuando se trabaja en campo?	3	3	4	4	14	3.5
A16. Gestión de incidentes de seguridad de la información.	¿Cuándo ocurre un evento relacionado con seguridad de la información sabes a quién reportarlo?	4	4	4	3	15	3.75
A18. Cumplimiento.	¿Cuentan con seguro los equipos informáticos de uso diario?	4	3	4	4	15	3.75
	PROM	3.71	3.71	4	3.71	15.14	3.78

CALIFICACIÓN: 1=No Cumple; 2=Nivel Bajo; 3=Nivel Moderado; 4=Nivel Alto

CALIFICACIÓN DEL INSTRUMENTO: 3.76 Redondeo: 3.80

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO (X) En caso de SI, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO:

CALIFICACIÓN: Alto

El instrumento debe ser aplicado: SI (X) NO ( )

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Título de la Investigación: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.**

Nombre del Tesista: **Dali Rafael Pozo Meza**

Nombre del experto: Mg. Carlos Alberto León Moreno

Asesor: **Mg. Yessica Raquel Reyes Ayala**

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIAL
A5. Políticas de la seguridad de la información.	¿Existe un manual de funciones de la Seguridad de la información?	4	3	4	4	15	3.75
A6. Organización de la seguridad de la información.	¿TI está monitoreando tu computador asignado?	4	4	4	4	16	4
	¿La computadora asignada para su labor cuenta con antivirus y actualizado?	4	3	4	4	15	3.75
	¿En el trabajo usan software original o legal?	4	4	4	4	16	4
A7. Seguridad de los Recursos Humanos.	¿Se capacita al personal en temas de seguridad información?	4	4	4	4	16	4
	¿Se cuenta con sistemas de alarma como detectores de humo y humedad?	3	4	3	4	14	3.5
A8. Gestión de Activos.	¿El computador asignado para el desarrollo de sus actividades recibe	4	4	4	3	15	3.75
	¿La Tablet y/o celular asignado para el desarrollo de sus actividades recibe mantenimiento?	4	3	4	4	15	3.75
	¿Se realiza mantenimiento preventivo y correctivo a la red de datos y wifi?	4	4	4	4	16	4
A9. Control de Acceso.	¿Existen zonas restringidas de acceso al personal en determinadas áreas	4	4	4	4	16	4
	¿Existe vigilancia en la entrada del edificio?	4	4	4	4	16	4
A10. Criptografía.	¿Existen políticas para el cambio frecuente de las contraseñas del email y el acceso a dispositivos electrónicos asignados?	4	4	4	4	16	4
	¿Existe control sobre el uso del correo electrónico?	3	4	4	4	15	3.75
	PROM	3.84	3.77	3.92	3.92	15.46	3.86

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO (×) En caso de Si, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO: El instrumento debe ser aplicado: SI (×) NO ( )

Firma y Sello del juez

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Título de la Investigación: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.**

Nombre del Tesista: **Dalí Rafael Pozo Meza**

Nombre del experto: Mg. Carlos Alberto León Moreno

Asesor: **Mg. Yessica Raquel Reyes Ayala**

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIAL
A11. Seguridad física y del entorno.	¿Realizan copias de seguridad de los datos almacenados en tu computadora?	4	4	4	4	16	4
	¿Realizan copias de seguridad de los datos almacenados en tu Tablet y/o celular?	4	3	4	4	15	3.75
	¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado y funcionando?	4	4	4	4	16	4
A12. Seguridad de las Operaciones.	¿Existe algún control para navegar en internet?	4	4	4	4	16	4
A13. Seguridad de las comunicaciones.	¿El SITC presenta problemas cuando se trabaja en campo?	4	4	4	4	16	4
A16. Gestión de incidentes de seguridad de la información.	¿Cuándo ocurre un evento relacionado con seguridad de la información sabes a quién reportarlo?	4	3	4	4	15	3.75
A18. Cumplimiento.	¿Cuentan con seguro los equipos informáticos de uso diario?	4	4	4	4	16	4
	PROM	4	3.71	4	4	15.71	3.93

***CALIFICACIÓN:* 1=No Cumple; 2=Nivel Bajo; 3=Nivel Moderado; 4=Nivel Alto**

CALIFICACIÓN DEL INSTRUMENTO 3.89 **Redondeo** 3.90

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO (X) En caso de SI, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO:

CALIFICACIÓN: ALTO

El instrumento debe ser aplicado: SI (X) NO ( )

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Título de la Investigación: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.**

Nombre del Tesista: **Dalí Rafael Pozo Meza**

Nombre del experto: Dr. Freddy Ronald Huapaya Condori Asesor: **Mg. Yessica Raquel Reyes Ayala**

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIAL
A5. Políticas de la seguridad de la información.	¿Existe un manual de funciones de la Seguridad de la información?	3	3	4	4	14	3.5
A6. Organización de la seguridad de la información.	¿TI está monitoreando tu computador asignado?	4	4	4	3	15	3.75
	¿La computadora asignada para su labor cuenta con antivirus y actualizado?	3	4	3	4	14	3.5
	¿En el trabajo usan software original o legal?	4	4	4	3	15	3.75
A7. Seguridad de los Recursos Humanos.	¿Se capacita al personal en temas de seguridad información?	3	4	4	4	15	3.75
	¿Se cuenta con sistemas de alarma como detectores de humo y humedad?	4	4	3	4	15	3.75
A8. Gestión de Activos.	¿El computador asignado para el desarrollo de sus actividades recibe	4	4	4	4	16	4
	¿La Tablet y/o celular asignado para el desarrollo de sus actividades recibe mantenimiento?	4	4	4	4	16	4
	¿Se realiza mantenimiento preventivo y correctivo a la red de datos y wifi?	4	3	4	4	15	3.75
A9. Control de Acceso.	¿Existen zonas restringidas de acceso al personal en determinadas áreas	4	4	4	4	16	4
	¿Existe vigilancia en la entrada del edificio?	3	4	4	3	14	3.5
A10. Criptografía.	¿Existen políticas para el cambio frecuente de las contraseñas del email y el acceso a dispositivos electrónicos asignados?	4	4	4	4	16	4
	¿Existe control sobre el uso del correo electrónico?	4	3	4	4	15	3.75
	PROM	3.69	3.77	3.94	3.77	15.07	3.77

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO (×) En caso de Si, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO: El instrumento debe ser aplicado: SI (×) NO ( )

Firma y Sello del juez

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
HUÁNUCO – PERÚ

ESCUELA DE POSGRADO
VALIDACIÓN DEL INSTRUMENTO

Título de la Investigación: **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO/IEC 27001:2013 EN EL PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES JUNTOS – HUÁNUCO.**

Nombre del Tesista: **Dali Rafael Pozo Meza**

Nombre del experto: Dr. Freddy Ronald Huapaya Condori

Asesor: **Mg. Yessica Raquel Reyes Ayala**

"Calificar con 1, 2, 3 ó 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad"

DIMENSIÓN	ÍTEM	RELEVANCIA	COHERENCIA	SUFICIENCIA	CLARIDAD	TOTAL	C.PARCIAL
A11. Seguridad física y del entorno.	¿Realizan copias de seguridad de los datos almacenados en tu computadora?	4	4	4	4	16	4
	¿Realizan copias de seguridad de los datos almacenados en tu Tablet y/o celular?	3	4	4	4	15	3.75
	¿Los lugares donde están los equipos de cómputo cuentan con aire acondicionado y funcionando?	4	3	3	4	14	3.5
A12. Seguridad de las Operaciones.	¿Existe algún control para navegar en internet?	4	4	4	3	15	3.75
A13. Seguridad de las comunicaciones.	¿El SITC presenta problemas cuando se trabaja en campo?	4	4	3	3	14	3.5
A16. Gestión de incidentes de seguridad de la información.	¿Cuándo ocurre un evento relacionado con seguridad de la información sabes a quién reportarlo?	4	3	4	4	15	3.75
A18. Cumplimiento.	¿Cuentan con seguro los equipos informáticos de uso diario?	4	4	4	4	16	4
	PROM	3.86	3.71	3.71	3.71	15	3.75

CALIFICACIÓN: **1=No Cumple; 2=Nivel Bajo; 3=Nivel Moderado; 4=Nivel Alto**

CALIFICACIÓN DEL INSTRUMENTO 3.75 **Redondeo** 4

¿Hay alguna dimensión o ítem que no fue evaluada? SI ( ) NO (X) En caso de Si, ¿Qué dimensión o ítem falta? _____

DECISIÓN DEL EXPERTO:

CALIFICACIÓN: ALTO

El instrumento debe ser aplicado: SI (X) NO ( )

NOTA BIOGRÁFICA

Nacido en el departamento de Huánuco – Perú, vivió con sus padres Héctor y Belia. Realizó sus estudios primarios en la IE René Guardián Ramírez y los secundarios en el colegio La Aplicación UNHEVAL. Ingreso en el año de 1994 a la Universidad de Huánuco a la Facultad de Ingeniería de Sistemas e Informática egresando el año 1999. Su primera experiencia laboral como bachiller fue para el grupo Telefónica en las ciudades de Huánuco, Huancayo y Ayacucho hasta el año 2002.

Seguidamente asumió labores de docencia en los Institutos y Universidades de nuestra región como la UNHEVAL, UDH y la UNAS; laborando por un período largo en la ciudad de Tingo María en la UNAS.

Habiendo laborado también en instituciones públicas y privadas como Municipios y empresas del rubro tecnológico y de la construcción.

Actualmente se desempeño como instructor en el SENATI.

Le apasiona hoy el mundo del Blockchain y el metaverso, proyectos de los cuales forma parte con amigos de Perú, México, España y Colombia. Así como el MLM.

Su deporte favorito definitivamente es el fútbol.

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN
LICENCIADA CON RESOLUCIÓN DEL CONSEJO DIRECTIVO N° 099-2019-SUNEDU/CD
Huánuco – Perú
ESCUELA DE POSGRADO
Campus Universitario, Pabellón V "A" 2do. Piso – Cayhuayna
Teléfono 514760 -Pág. Web. www.posgrado.unheval.edu.pe

ACTA DE DEFENSA DE TESIS DE MAESTRO

En la Plataforma Microsoft Teams de la Escuela de Posgrado, siendo las **19:00h,** del día miércoles **22 MARZO DE 2023** ante los Jurados de Tesis constituido por los siguientes docentes:

Dr. Abimael Adam FRANCISCO PAREDES	Presidente
Dra. Ines Eusebia JESUS TOLENTINO	Secretaria
Mg. Heidy Velsy RIVERA VIDAL DE SANCHEZ	Vocal

Asesor (a) de tesis: Mg. Yessica Raquel REYES AYALA (Resolución N° 04211-2022-UNHEVAL/EPG-D)

El aspirante al Grado de Maestro en Ingeniería de Sistemas, mención en Tecnología de Información y Comunicación, Don Dali Rafael POZO MEZA.

Procedió al acto de Defensa:

Con la exposición de la Tesis titulado: **"SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN UN ESTÁNDAR DE SEGURIDAD EN EL PROGRAMA JUNTOS, HUÁNUCO".**

Respondiendo las preguntas formuladas por los miembros del Jurado y público asistente.

Concluido el acto de defensa, cada miembro del Jurado procedió a la evaluación del aspirante al Grado de Maestro, teniendo presente los criterios siguientes:

a) Presentación personal.
b) Exposición: el problema a resolver, hipótesis, objetivos, resultados, conclusiones, los aportes, contribución a la ciencia y/o solución a un problema social y recomendaciones.
c) Grado de convicción y sustento bibliográfico utilizados para las respuestas a las interrogantes del Jurado y público asistente.
d) Dicción y dominio de escenario.

Así mismo, el Jurado plantea a la tesis **las observaciones** siguientes:

.....
.....

Obteniendo en consecuencia el Maestrista la Nota de...Diecisiete..... (17)
Equivalente a ...Muy...bueno....., por lo que se declara .....Aprobada.....
(Aprobado o desaprobado)

Los miembros del Jurado firman el presente **ACTA** en señal de conformidad, en Huánuco, siendo las..20:15.. horas de 22 de marzo de 2023.

.....
PRESIDENTE
DNI N° .....22498088.....

.....
SECRETARIO
DNI N° .....40246404.....

.....
VOCAL
DNI N° .....41048834.....

Leyenda:
19 a 20: ExcelenteS
17 a 18: Muy Bueno
14 a 16: Bueno

(Resolución N° 0816-2023-UNHEVAL/EPG)

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

ESCUELA DE POSGRADO

CONSTANCIA DE ORIGINALIDAD

El que suscribe:

Dr. Amancio Ricardo Rojas Cotrina

HACE CONSTAR:

Que, la tesis titulada: ***"SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN UN ESTÁNDAR DE SEGURIDAD EN EL PROGRAMA JUNTOS, HUÁNUCO",*** *realizado por el Maestrista en Ingeniería de Sistemas, mención en Tecnología de Información y Comunicación,* ***Dali Rafael POZO MEZA,*** *cuenta con un* ***índice de similitud del 20%****, verificable en el Reporte de Originalidad del software Turnitin. Luego del análisis se concluye que cada una de las coincidencias detectadas no constituyen plagio; por lo expuesto, la Tesis cumple con las normas para el uso de citas y referencias, además de no superar el 20,0% establecido en el Art. 233° del Reglamento General de la Escuela de Posgrado Modificado de la UNHEVAL (Resolución Consejo Universitario N° 0720-2021-UNHEVAL, del 29.NOV.2021).*

Cayhuayna, 13 de marzo de 2023.

UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN" ESCUELA DE POSGRADO DIRECTOR HUÁNUCO

Dr. Amancio Ricardo Rojas Cotrina

DIRECTOR DE LA ESCUELA DE POSGRADO

SECC

Reporte de similitud

NOMBRE DEL TRABAJO
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN UN ES TÁNDAR DE SEGURIDAD EN EL PROGRA

AUTOR
DALI RAFAEL POZO MEZA

RECUENTO DE PALABRAS
11479 Words

RECUENTO DE CARACTERES
60844 Characters

RECUENTO DE PÁGINAS
53 Pages

TAMAÑO DEL ARCHIVO
1.4MB

FECHA DE ENTREGA
Mar 6, 2023 1:35 PM GMT-5

FECHA DEL INFORME
Mar 6, 2023 1:36 PM GMT-5

20% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base c

- 19% Base de datos de Internet
- Base de datos de Crossref
- 16% Base de datos de trabajos entregados
- 6% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 12 palabras)

AUTORIZACIÓN DE PUBLICACIÓN DIGITAL Y DECLARACIÓN JURADA DEL TRABAJO DE INVESTIGACIÓN PARA OPTAR UN GRADO ACADÉMICO O TÍTULO PROFESIONAL

1. Autorización de Publicación: *(Marque con una "X")*

Pregrado		Segunda Especialidad		Posgrado:	Maestría	X	Doctorado	

Pregrado (*tal y como está registrado en **SUNEDU)***

Facultad	
Escuela Profesional	
Carrera Profesional	
Grado que otorga	
Título que otorga	

Segunda especialidad (*tal y como está registrado en **SUNEDU)***

Facultad	
Nombre del programa	
Título que Otorga	

Posgrado (*tal y como está registrado en **SUNEDU)***

Nombre del Programa de estudio	Ingeniería de Sistemas, mención en Tecnología de Información y Comunicación
Grado que otorga	Maestro en Ingeniería de Sistemas, mención en Tecnología de Información y Comunicación

2. Datos del Autor(es): *(Ingrese todos los **datos** requeridos **completos**)*

Apellidos y Nombres:	Pozo Meza Dali Rafael							
Tipo de Documento:	**DNI**	**X**	**Pasaporte**		**C.E.**		**Nro. de Celular:**	944560745
Nro. de Documento:	40109229						**Correo Electrónico:**	rafaxn49@gmail.com

Apellidos y Nombres:								
Tipo de Documento:	**DNI**		**Pasaporte**		**C.E.**		**Nro. de Celular:**	
Nro. de Documento:							**Correo Electrónico:**	

Apellidos y Nombres:								
Tipo de Documento:	**DNI**		**Pasaporte**		**C.E.**		**Nro. de Celular:**	
Nro. de Documento:							**Correo Electrónico:**	

3. Datos del Asesor: *(Ingrese todos los **datos** requeridos **completos según DNI**, no es necesario indicar el Grado Académico del Asesor)*

¿El Trabajo de Investigación cuenta con un Asesor?: (*marque con una "**X**" en el recuadro del costado, según corresponda*)							**SI**	**X**	**NO**	
Apellidos y Nombres:	Reyes Ayala Yessica Raquel					**ORCID ID:**	0000-0002-4520-7617			
Tipo de Documento:	**DNI**	**X**	**Pasaporte**		**C.E.**		**Nro. de documento:**	18226800		

4. Datos del Jurado calificador: *(Ingrese solamente los **Apellidos y Nombres completos según DNI**, no es necesario indicar el Grado Académico del Jurado)*

Presidente:	FRANCISCO PAREDES Adam
Secretario:	JESUS TOLENTINO Ines
Vocal:	RIVERA VIDAL Velsy
Vocal:	
Vocal:	
Accesitario	

5. Declaración Jurada: *(Ingrese todos los **datos** requeridos **completos**)*

a) **Soy Autor (a) (es) del Trabajo de Investigación Titulado:** *(Ingrese el título tal y como está registrado en el **Acta de Sustentación**)*
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN UN ESTÁNDAR DE SEGURIDAD EN EL PROGRAMA JUNTOS, HUÁNUCO
b) **El Trabajo de Investigación fue sustentado para optar el Grado Académico ó Título Profesional de:** *(tal y como está registrado en **SUNEDU**)*
Maestro en Ingeniería de Sistemas, mención en Tecnología de información y Comunicación
c) El Trabajo de investigación no contiene plagio (ninguna frase completa o párrafo del documento corresponde a otro autor sin haber sido citado previamente), ni total ni parcial, para lo cual se han respetado las normas internacionales de citas y referencias.
d) El trabajo de investigación presentado no atenta contra derechos de terceros.
e) El trabajo de investigación no ha sido publicado, ni presentado anteriormente para obtener algún Grado Académico o Título profesional.
f) Los datos presentados en los resultados (tablas, gráficos, textos) no han sido falsificados, ni presentados sin citar la fuente.
g) Los archivos digitales que entrego contienen la versión final del documento sustentado y aprobado por el jurado.
h) Por lo expuesto, mediante la presente asumo frente a la Universidad Nacional Hermilio Valdizan (en adelante LA UNIVERSIDAD), cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad del contenido del Trabajo de Investigación, así como por los derechos de la obra y/o invención presentada. En consecuencia, me hago responsable frente a LA UNIVERSIDAD y frente a terceros de cualquier daño que pudiera ocasionar a LA UNIVERSIDAD o a terceros, por el incumplimiento de lo declarado o que pudiera encontrar causas en la tesis presentada, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello. Asimismo, por la presente me comprometo a asumir además todas las cargas pecuniarias que pudieran derivarse para LA UNIVERSIDAD en favor de terceros con motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las que encontraren causa en el contenido del trabajo de investigación. De identificarse fraude, piratería, plagio, falsificación o que el trabajo haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad Nacional Hermilio Valdizan.

6. Datos del Documento Digital a Publicar: *(Ingrese todos los **datos** requeridos **completos**)*

Ingrese solo el año en el que sustentó su Trabajo de Investigación: *(Verifique la Información en el **Acta de Sustentación**)*						2023
Modalidad de obtención del Grado Académico o Título Profesional: *(Marque con **X** según Ley Universitaria con la que inició sus estudios)*	**Tesis**	**X**	**Tesis Formato Artículo**		**Tesis Formato Patente de Invención**	
	Trabajo de Investigación		**Trabajo de Suficiencia Profesional**		**Tesis Formato Libro, revisado por Pares Externos**	
	Trabajo Académico		**Otros** *(especifique modalidad)*			

Palabras Clave: *(solo se requieren 3 palabras)*	Sistemas	Programa JUNTOS	Diseño

Tipo de Acceso: *(Marque con **X** según corresponda)*	**Acceso Abierto**	**x**	**Condición Cerrada** (*)		
	Con Periodo de Embargo (*)		**Fecha de Fin de Embargo:**		

¿El Trabajo de Investigación, fue realizado en el marco de una Agencia Patrocinadora? *(ya sea por financiamientos de proyectos, esquema financiero, beca, subvención u otras; marcar con una "**X**" en el recuadro del costado según corresponda):*	**SI**		**NO**	**X**
Información de la Agencia Patrocinadora:				

El trabajo de investigación en digital y físico tienen los mismos registros del presente documento como son: Denominación del programa Académico, Denominación del Grado Académico o Título profesional, Nombres y Apellidos del autor, Asesor y Jurado calificador tal y como figura en el Documento de Identidad, Titulo completo del Trabajo de Investigación y Modalidad de Obtención del Grado Académico o Título Profesional según la Ley Universitaria con la que se inició los estudios.

7. **Autorización de Publicación Digital:**

A través de la presente. Autorizo de manera gratuita a la Universidad Nacional Hermilio Valdizán a publicar la versión electrónica de este Trabajo de Investigación en su Biblioteca Virtual, Portal Web, Repositorio Institucional y Base de Datos académica, por plazo indefinido, consintiendo que con dicha autorización cualquier tercero podrá acceder a dichas páginas de manera gratuita pudiendo revisarla, imprimirla o grabarla siempre y cuando se respete la autoría y sea citada correctamente. Se autoriza cambiar el contenido de forma, más no de fondo, para propósitos de estandarización de formatos, como también establecer los metadatos correspondientes.

Firma: 		
Apellidos y Nombres:	POZO MEZA DALI RAFAEL	**Huella Digital**
DNI:	40109229	
Firma:		
Apellidos y Nombres:		**Huella Digital**
DNI:		
Firma:		
Apellidos y Nombres:		**Huella Digital**
DNI:		
Fecha: 12/06/2023		

Nota:

- ✓ No modificar los textos preestablecidos, conservar la estructura del documento.
- ✓ Marque con una **X** en el recuadro que corresponde.
- ✓ Llenar este formato de forma digital, con tipo de letra **calibri, tamaño de fuente 09**, manteniendo la alineación del texto que observa en el modelo, sin errores gramaticales *(recuerde las mayúsculas también se tildan si corresponde).*
- ✓ La información que escriba en este formato debe coincidir con la información registrada en los demás archivos y/o formatos que presente, tales como: DNI, Acta de Sustentación, Trabajo de Investigación (PDF) y Declaración Jurada.
- ✓ Cada uno de los datos requeridos en este formato, es de carácter obligatorio según corresponda.