UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CALIDAD DE PROCESOS EN LA I.E.P. ALBERT EINSTEIN

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

RIDER SLEITHER ZARBE TORRES

PUCALLPA – PERÚ

2019

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL
ESCUELA PROFESIONAL DE INGENIERÍA CIVIL
COMISIÓN DE GRADOS Y TÍTULOS

ACTA DE EVALUACIÓN DE SUSTENTACIÓN DE TESIS N° 014-2023

GRADUANDO : **Bach. RIDER SLEITHER ZARBE TORRES**

TEMA : **"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CALIDAD DE PROCESOS EN LA I.E.P. ALBERT EINSTEIN".**

ASESOR : **MG. ARTURO YUPANQUI VILLANUEVA**

CRITERIOS	PUNTAJE			
	3	2	1	0
I- PRESENTACION				
* MOTIVACION		X		
* TONO DE VOZ		X		
* CALIDAD DE MATERIAL AUDIOVISUAL			X	
II- DESARROLLO DE CONTENIDO				
* SECUENCIA			X	
* DOMINIO DE VOZ		X		
* USO ADECUADO DEL MATERIAL			X	
* VALIDEZ DE LOS HALLAZGOS			X	
III- ABSOLUCION DE PREGUNTAS				
* RESPONDE A LAS PREGUNTAS FORMULADAS POR EL JURADO		X		
IV- APORTE CIENTIFICO Y TECNOLOGICO				
* AL DESARROLLO DE LA COMUNIDAD		X		
* A LA PROFESION		X		

EVALUACION

- EXCELENCIA — 26 A 30 PUNTOS
- UNANIMIDAD — 21 A 25 PUNTOS
- MAYORIA — 16 A 20 PUNTOS
- DESAPROBADO — 15 A MENOS

CALIFICACION FINAL:
PUNTAJE : 16 / 30

CONCLUSIONES:
APROBADO POR : Mayoría
DESAPROBADO POR :

JURADO EVALUADOR

DR. JORGE LUIS HILARIO RIVAS
PRESIDENTE

M.SC. EUCLIDES PANDURO PADILLA
MIEMBRO

M.SC. RONALD HAROLD ULLOA GÁLVEZ
MIEMBRO

M.SC. CLOTILDE RIOS HIDALGO DE CERNA

PUCALLPA, 04 DE JULIO DEL 2023

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE FACULTAD DE INGENIERIA DE SISTEMAS E INGENIERIA CIVIL
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS
Carretera Federico Basadre Km 6200 - Pucallpa - Ucayali

ACTA DE APROBACION DE INFORME FINAL DE TESIS

En la Ciudad Universitaria, a los 19 días del mes junio del 2023 siendo horas 10: 00 : 00 . Los miembros delJurado, declaran APROBADO POR UNANIMIDAD el PROYECTO DE INVESTIGACIÓN DE TESIS titulado:

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CALIDAD DE PROCESOS EN LA I.E.P. ALBERT EINSTEIN".

Presentado por el(la) Bachiller:

RIDER SLEITHER ZARBE TORRES

De la Escuela Profesional de:

INGENIERIA DE SISTEMAS

Siendo el Jurado Dictaminador, conformado por:

Presidente	: Dr. JORGE LUIS HILARIO RIVAS
Primer Miembro	: Ing. MSC. EUCLIDES PANDURO PADILLA
Segundo Miembro	: Ing. MSC. RONALD HAROLD ULLOA GÁLVEZ
Asesor	: Ing. Mg. ARTURO YUPANQUI VILLANUEVA

Para dar fe de este proceso, se le asigna la presente acta y a partir de la presente fecha queda expedito para continuar con los trámites de sustentación de la TESIS.

Pucallpa, 19 de junio de 2023

Dr. JORGE LUIS HILARIO RIVAS
PRESEIDENTE

Ing. MSC. EUCLIDES PANDURO PADILLA
PRIMER MIEMBRO

Ing. MSC. RONALD HAROLD ULLOA GÁLVEZ
SEGUNDO MIEMBRO

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

Nº V/0524-2023.

La Dirección de Producción Intelectual de la Universidad Nacional de Ucayali, hace constar por la presente, que el trabajo académico de investigación, titulado:

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CALIDAD DE PROCESOS EN LA I.E.P. ALBERT EINSTEIN"

Autor(es)	:	**ZARBE TORRES, RIDER SLEITHER**
Facultad	:	**INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL**
Escuela	:	**Ing. Sistemas**
Asesor(a)	:	**Mg. Yupanqui Villanueva, Arturo**

Presenta un **porcentaje de similitud de 5%**, verificado en el Sistema Antiplagio URKUND/OURIGINAL, De acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO, el cual indica que todo trabajo de investigación no debe superar el 10%. **En tal sentido, se declara, que el presente trabajo de investigación: SI Contiene un porcentaje aceptable de similitud**, procediéndose a emitir la presente Constancia de Originalidad de Trabajo de Investigación (COTI) a solicitud del asesor.

En señal de conformidad se firma y sella el presente documento.

Fecha: 28/08/2023

Mg. JOSÉ MANUEL CÁRDENAS BERNAOLA
Director de Producción Intelectual

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

AUTORIZACIÓN DE PUBLICACIÓN

Repositorio de la Universidad Nacional de Ucayali

Yo, RIDER SLEITHER ZARBE TORRES

Autor de la tesis titulada : SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA CALIDAD DE PROCESOS EN LA I.E.P ALBERTH EINSTEN

Sustentada el año 2023

Asesor(a): Mg. ARTURO YUPANQUI VILLANUEVA

Escuela de Posgrado

Maestría:

Mención:

Autorizo la publicación:

PARCIAL [ ] TOTAL [X]

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali licencia no exclusiva para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 12/09/2023

Email: RIDERZARBE16@gmail.com Firma:

Teléfono: 930550038 DNI: 70938819

DEDICATORIA

A todas las personas que desde un inicio confiaron en mi persona, pero sobre todo a dos personas muy especial, como es mi madre y mi abuela María que me cuida y protege desde el cielo.

AGRADECIMIENTO

Agradecer a todas aquellas personas quienes me apoyaron en el proceso de realización del presente proyecto; familia, novia, amigos, pero sobre todo a mis docentes de la Universidad Nacional de Ucayali.

RESUMEN

La investigación: “Sistema de gestión de seguridad de la información para la calidad de procesos en la I.E.P. Albert Einstein.”, tuvo como objetivo establecer el desarrollo de un sistema de gestión de seguridad de información en la calidad de procesos. Esto para reducir los riesgos, las amenazas y vulneraciones los cuales puedan afectar los activos de información de la Institución, generando garantía en cuanto a confidencialidad, integridad y disponibilidad de la información de la institución. Para la realización adoptaremos el modelo “Plan – Do - Check – Act”, también conocido como PDCA, el cual es aplicado a toda la estructura de los procesos. Los resultados evidenciaron que se plantea mejorar en un 60% la seguridad de la información y los activos de la información en la I.E.P. Albert Einstein, mediante la propuesta de implementación de un Sistema de Gestión de Seguridad de la Información y una capacitación constante de los trabajadores administrativos en los temas de seguridad de la información que permitirá disminuir el índice de pérdida de información en las diferentes áreas administrativas de la Institución.

Palabra clave: gestión de seguridad, información, procesos.

ABSTRACT

The research: “Information security management system for the quality of processes in the I.E.P. Albert Einstein”, Aimed to establish the development of an information security management system in the quality of processes. This is to reduce the risks, threats and violations which may affect the information assets of the Institution, generating a guarantee regarding the confidentiality, integrity and availability of the institution's information. To carry it out, we will adopt the "Plan - Do - Check - Act" model, also known as PDCA, which is applied to the entire structure of the processes. The results showed that it is proposed to improve by 60% the security of information and information assets in the I.E.P. Albert Einstein, by proposing the implementation of an Information Security Management System and constant training of administrative workers in information security issues that will reduce the rate of information loss in the different administrative areas of the Institution.

Keyword: security management, information, processes.

INDICE

DEDICATORIA ..... **VI**
AGRADECIMIENTO ..... **VII**
RESUMEN ..... **VIII**
ABSTRACT ..... **IX**
INTRODUCCIÓN ..... **xii**
1.1. ANTECEDENTES DEL PROBLEMA 14
1.2. FORMULACION DEL PROBLEMA 16
1.2.1. General 16
1.2.2. Específicos 16
1.3. OBJETIVOS DE LA INVESTIGACIÓN 17
1.3.1. Objetivo general 17
1.3.2. Objetivos específicos 17
1.4. JUSTIFICACION E IMPORTANCIA 18
1.4.1. Justificación 18
1.4.2. Importancia 18
1.5. HIPOTESIS 19
1.5.1. Hipótesis general 19
1.5.2. Hipótesis secundarias 19
1.6. DELIMITACIONES DE LA INVESTIGACIÓN 19
1.6.1. Delimitación espacial 19
1.6.2. Delimitación social 20
1.6.3. Delimitación temporal 20
1.6.4. Delimitación conceptual 20
1.7. VARIABLES 20
1.7.1. Definición conceptual 20
1.7.2. Definición operacional 21
CAPÍTULO II MARCO TEÓRICO **24**
2.1. ANTECEDENTES DE LA INVESTIGACION 24
2.1.1. Tesis Internacionales 24
2.1.2. Tesis nacionales 28
2.2. BASES TEÓRICAS 32
2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS 37
CAPÍTULO III METODOLOGIA **41**
3.1. METODO DE INVESTIGACION 41

3.1.1. Tipo de investigación 41
3.1.2. Nivel de investigación 41
3.1.3. Diseño de investigación....41
3.2. POBLACION Y MUESTRA....42
3.3. TECNICAS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS 43
3.3.1. Técnicas....43
3.3.2. Instrumentos....44
3.4. TRATAMIENTO DE DATOS 45
CAPÍTULO IV PLAN DEL SGSI 47
4.1. ANÁLISIS DE LA PROPUESTA....47
4.2. IMPLEMENTACION....50
4.2.2. Do (Implementar y Operar el SGSI) 59
4.2.3. Check (Monitorizar y Revisar el SGSI) 74
4.2.4. Act (Mantener y Mejorar el SGSI)....76
CAPÍTULO V: PRESENTACION, ANALISIS E INTERPRETACION DE RESULTADOS 79
5.1. ANÁLISIS DE TABLAS Y FIGURAS 79
5.2. CONTRASTACIÓN DE HIPÓTESIS 101
5.3. DISCUSIÓN DE RESULTADOS....108
CONCLUSIONES....110
RECOMENDACIONES 111
REFERENCIAS BIBLIOGRAFICAS....112
ANEXOS....119
ANEXO 1: MATRIZ DE CONSISTENCIA SISTÉMICA....120
ANEXO 2: OPERACIONALIZACIÓN DE VARIABLES....121
ANEXO 3: FORMATO DE REUNION SGSI CP – I.E.P. ALBERT EINSTEIN....122
ANEXO 4: INSTRUMENTOS DE RECOLECCIÓN DE DATOS CUESTIONARIO.127
ANEXO 5....129
COMPROMISO DE CONFIDENCIALIDAD DEL PERSONAL INTERNO I.E.P. ALBERT EINSTEIN....129
ANEXO 6....131
COMPROMISO DE CONFIDENCIALIDAD DEL PERSONAL INTERNO....131
I.E.P. ALBERT EINSTEIN 131

INDICE DE TABLAS

Tabla 1: Indicadores de la variable independiente. 22
Tabla 2: Indicadores de la variable dependiente 23
Tabla 3: Organiaciones Certificadas con SGSI....49
Tabla 4: Activos Informáticos....53
Tabla 5: Software Licenciado de la I.E.P. Albert Einstein....60
Tabla 6: Clasificación e Inventario de Hardware....61
Tabla 7: Clasificación de Documentos 62
Tabla 8: Servidores....63
Tabla 9: Sistemas operativos / gestor de base de datos....63
Tabla 10: Clasificacion de servidores....64
Tabla 11: Equipos de Backup....65
Tabla 12: Clasificacion de Backup....65
Tabla 13: Formato de monitoreo. 76
Tabla 14: Numero de elementos analizados. 79
Tabla 15: Validacion de alfa de Cronbach. 79
Tabla 16: Resultados pregunta 1. 80
Tabla 17: Resultados pregunta 2. 81
Tabla 18: Resultados pregunta 3. 82
Tabla 19: Resultados pregunta 4. 83
Tabla 20: Resultados pregunta 5. 84
Tabla 21: Resultados pregunta 6. 85
Tabla 22: Resultados pregunta 7. 86
Tabla 23: Resultados pregunta 8. 87
Tabla 24: Resultados pregunta 9. 88
Tabla 25: Resultados pregunta 10. 89
Tabla 26: Resultados pregunta 11. 90
Tabla 27: Resultados pregunta 12. 91
Tabla 28: Resultados pregunta 13. 92
Tabla 29: Resultados pregunta 14. 93
Tabla 30: Resultados pregunta 15. 94
Tabla 31: Resultados pregunta 16. 95
Tabla 32: Resultados pregunta 17. 96
Tabla 33: Resultados pregunta 18. 97
Tabla 34: Resultados pregunta 19. 98
Tabla 35: Resultados pregunta 20. 99
Tabla 36: Resultados pregunta 21. 100
Tabla 37: Correlación de Hipótesis General....103
Tabla 38: Correlación de hipótesis especifica N° 1. 104
Tabla 39: Correlación de hipótesis especifica N° 2. 105
Tabla 40: Correlación de hipótesis especifica N° 3. 106
Tabla 41: Correlación de hipótesis especifica N° 4. 107

INDICE DE FIGURAS

Figura 1: Resultados pregunta 1. 80
Figura 2: Resultados pregunta 2. 81
Figura 3: Resultados pregunta 3. 82
Figura 4: Resultados pregunta 4. 83
Figura 5: Resultados pregunta 5. 84
Figura 6: Resultado pregunta 6. 85
Figura 7: Resultados pregunta 7. 86
Figura 8: Resultados pregunta 8. 87
Figura 9: Resultados pregunta 9. 88
Figura 10: Resultados pregunta 10 89
Figura 11: Resultados pregunta 11 90
Figura 12: Resultados pregunta 12 91
Figura 13: Resultados pregunta 13 92
Figura 14: Resultados pregunta 14 93
Figura 15: Resultados pregunta 15 94
Figura 16:Resultados pregunta 16 95
Figura 17: Resultado pregunta 17. 96
Figura 18: Resultados pregunta 18 97
Figura 19: Resultados pregunta 19 98
Figura 20: Resultados pregunta 20 99
Figura 21: Resultados pregunta 21 100

INTRODUCCIÓN

Un sistema de gestión de seguridad de la información será en la I.E.P. Albert Einstein; una organización del diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información.

En la actualidad, las empresas se enfrentan a muchos riesgos e inseguridades procedentes de focos diversos. Esto quiere decir que los activos de información de las empresas, uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades. La seguridad de estos activos de información está en función de la correcta gestión de una serie de factores como: la capacidad, la elaboración de un plan de contingencia frente a los incidentes, el análisis de riesgos, las competencias, el grado de involucración de la dirección, las inversiones en seguridad y el grado de implementación de controles.

Los capítulos que abarca la investigación son: En el capítulo I, denominado planteamiento del problema, se expone la descripción de los antecedentes del problema, formulación del problema, objetivos de la investigación, justificación e importancia, hipótesis y las variables, definiendo de manera conceptual y operacional. En el capítulo II, denominado marco teórico, se expone la descripción de los antecedentes de la investigación, que comprenden estudios previos que tengan relación con la investigación y las

bases teóricas de acuerdo a las variables, así mismo la definición de términos básicos. En el capítulo III, denominado metodología, se expone la descripción del método de investigación, como, el tipo, nivel y diseño que presenta el estudio, de igual manera la población y muestra establecidas para realizar el análisis de los resultados, procedimientos de recolección de datos, técnicas e instrumentos para recolección de datos, procesamiento para recolección de datos y el tratamiento de datos realizados. En el capítulo IV, denominado resultados, que se presentan a partir del análisis y el diseño de propuesta planteadas en esta investigación. El capítulo V, denominado presentación, análisis e interpretación de resultados. Muestra el análisis de tablas, figuras y la contratación de la hipótesis. Además, nos muestra las conclusiones, recomendaciones, referencias bibliográficas y anexos.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

La necesidad de gestionar la seguridad de la información nace de un entorno cada vez más globalizado donde las empresas deben tomar decisiones rápidas y eficientes convirtiendo la información en uno de los activos más importantes dentro de las organizaciones llegando a tener una importancia estratégica para muchas de ellas ya que les permite mantener una ventaja competitiva frente a otras empresas (NORMA ISO/IEC 27001).

La seguridad de la información se encarga de la búsqueda de la preservación de la confidencialidad, integridad y disponibilidad de la información, es decir buscar protegerla tanto como el aprovechar vulnerabilidades de los sistemas de información.

En nuestro país, desde hace más de 10 años, las políticas del gobierno están recomendando una adecuada gestión de la seguridad de la información con resoluciones ministeriales tales como la Nº 224.2004-PCM en la que aprueban eso uso obligatorio de la NTP ISO/IEC 17799:2004 en las entidades públicas referentes a las buenas prácticas para gestionar la seguridad de la información.

Adicionalmente, el marco legal de nuestro país obliga a las entidades públicas, pertenecientes al Sistema Nacional de Informática, el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basándose en la norma técnica peruana (NTP) – ISO/IEC 27001: 2008 mediante resolución ministerial Nº 129-2012-PCM emitida en mayo del 2012.

Ambas normas técnicas peruanas, la NTP ISO/IEC 27001 y la NTP ISO/IEC 17799, están basadas en la familia de normas ISO 27000 correspondiente a seguridad de la información. La primera, es el estándar principal de esta familia y menciona a cuáles sin los requerimientos para desarrollar un Sistema de Gestión de Seguridad de la Información basándose en el ciclo de DEMING, o ciclo Plan – Do – Check – act, una metodología cíclica muy usada en las normas ISO relacionadas a normas de gestión (NTP ISO/IEC 27001).

Es fundamental establecer el desarrollo de un sistema de gestión de seguridad de información en la calidad de procesos en la I.E.P. Albert Einstein. Para que el control y manejo de la información que se realizan en los puestos administrativos sean óptimos de acuerdo a las normas

actuales. Mediante la investigación se ha corroborado que el personal administrativo desconoce los lineamientos a cumplir para redactar documentos que contengan información y que carecen de un régimen de creación y manejo de procesos. Esto incide que los padres de familia en ocasiones suelen quejarse que la información sobre el desempeño de sus hijos porque no se encuentran en orden o actualizado

Por eso se requiere la optimización en la calidad de sus procesos que realizan en el manejo, almacenamiento, distribución y obtención de información en la I.E.P. Albert Einstein que ayude en la calidad de procesos que se realiza dentro de la empresa, maximizando así el control y seguridad de su información.

1.2. FORMULACION DEL PROBLEMA

1.2.1. General

¿Cómo desarrollar un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein?

1.2.2. Específicos

- ¿Cómo desarrollar la planificación en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein?
- ¿Cómo desarrollar lo que se debe hacer en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein?

- ¿Cómo desarrollar el control en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein?
- ¿Cómo desarrollar la forma de actuar en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo general

Establecer el desarrollo de un sistema de gestión de seguridad de información en la calidad de procesos para la I.E.P. Albert Einstein.

1.3.2. Objetivos específicos

- Evaluar el desarrollo de la planificación en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein.
- Definir el desarrollo de lo que se debe hacer en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein.
- Precisar el desarrollo del control en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein.
- Especificar el desarrollo de la forma de actuar en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein.

1.4. JUSTIFICACION E IMPORTANCIA

1.4.1. Justificación

Un Sistema de Gestión de Seguridad de la Información (SGSI) mejorará la calidad de los procesos dentro de la I.E.P. Albert Einstein, consiguiendo la disminución del impacto de los riesgos; mayores garantías de continuidad del negocio basadas en la adopción de un plan de contingencia.

El procedimiento de la metodología, consiste en lo siguiente:

- Fase de Planificar
- Fase de Hacer
- Fase de Controlar
- Fase de Actuar.

La calidad de procesos con la que cuenta la I.E.P. Albert Einstein son realizadas sin ningún tipo de parámetro o estándar apropiado, al notar la carencia de estos, se vio la necesidad de analizar y diseñar un Sistema de Gestión de Seguridad de la Información, que genere la calidad en los procesos que se generan dentro de la institución.

Para desarrollar el informe, seguimos los lineamientos del proceso de investigación, la cual contiene formulación del problema, objetivos e hipótesis, para establecer acerca de los factores que influyen en la calidad de procesos en la I.E.P. Albert Einstein.

1.4.2. Importancia

Con un Sistema de Gestión de Seguridad de la Información se obtendrá mayor seguridad y control del activo más fundamental, y

evitando filtraciones hacia la competencia y entre otros riesgos, por todas estas razones, se vuelve una necesidad.

1.5. HIPOTESIS

1.5.1. Hipótesis general

“Existe el desarrollo positivo de un sistema de gestión de seguridad de información en la calidad de procesos para la I.E.P. Albert Einstein”

1.5.2. Hipótesis secundarias

- “La aplicación es positiva entre la aplicación y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein.”
- “La aplicación es positiva entre lo que se debe hacer y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein.”
- “La aplicación es positiva entre el control y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein.”
- “La aplicación es positiva entre la forma de actuar y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein.”

1.6. DELIMITACIONES DE LA INVESTIGACIÓN

1.6.1. Delimitación espacial

La presente investigación se llevará a cabo en las instalaciones de la I.E.P. Albert Einstein, ubicado en Jr. Emancipación # 517, en el distrito de Callería en la provincia de Coronel Portillo, en el departamento de Ucayali.

1.6.2. Delimitación social

El entorno laboral objeto de estudio será el personal que labora en la I.E.P. Albert Einstein, conformado por un total de 8 trabajadores.

1.6.3. Delimitación temporal

La presente investigación se llevará a cabo en un periodo de 4 meses a partir del mes de mayo de presente año 2018.

1.6.4. Delimitación conceptual

Se emplearán términos referentes al giro del proyecto, se darán a conocer les ventajas y desventajas presentes en el análisis para su posterior diseño e implementación.

1.7. VARIABLES

1.7.1. Definición conceptual

Sistema de Gestión de Seguridad de La Información: Es un marco de administración general a través del cual las organizaciones identifican, analizan y direccionan sus riesgos en la seguridad de la información. Su correcta implementación garantiza que los acuerdos de seguridad están afinados para mantenerse al ritmo constante con las amenazas de seguridad, vulnerabilidades e impactos en el negocio, el cual es un aspecto a considerar profundamente teniendo en cuenta la competitividad y cambios a los que enfrentan las organizaciones hoy en día. (TAMAYO, 2001)

Calidad de Procesos: Según la ISO9001, (2014) Un proceso es un conjunto de actividades que están interrelacionadas y que pueden interactuar entre sí. Estas actividades transforman los elementos de entrada en resultados, para ello es esencial la asignación de recursos.

Los procesos constan de:

- Elementos de entrada y salida, los cuales pueden ser tangibles o intangibles. Los resultados pueden ser también no intencionados como por ejemplo la contaminación ambiental.
- Clientes y partes interesadas que tengan necesidades y expectativas en los procesos, ellos son los que definirán los resultados que requiere un determinado proceso. Sistemas de medición para proporcionar información sobre el desempeño del proceso. Cualquier resultado debería ser analizado para poder determinar si existe necesidad de aplicar algún tipo de acción correctiva o de mejora.

1.7.2. Definición operacional

Variable independiente: Sistema de gestión de seguridad de la información

Variable susceptible de medición a través de las dimensiones Planificar, Hacer, Controlar y Actuar.

Tabla 1:

Indicadores de la variable independiente.

VARIABLE	DIMENSIONES	INDICADORES	ESCALA DE MEDICION
Sistema de gestión de seguridad de la información	PLANIFICAR	▪ Política de administración. ▪ Alcance del ISO 27001. ▪ Análisis de riesgos. ▪ Seleccionar los riesgos. ▪ Definir competencias. ▪ Definir autoridades y responsabilidades	No Poco Si
	HACER	▪ Implantar el plan de administración de riesgos. ▪ Implantar el SGSI. ▪ Implantar controles.	
	CONTROLAR	▪ Revisar internamente el SGSI. ▪ Poner en marcha indicadores y métricas. ▪ Hacer revisión por parte de la Dirección.	
	ACTUAR	▪ Adoptar acciones correctivas. ▪ Adoptar acciones de mejora.	

Variable dependiente: Calidad de procesos

Variable susceptible de medición a través de las dimensiones Sub sistema de auditoría.

Tabla 2:

Indicadores de la variable independiente.

VARIABLE	DIMENSIONES	INDICADORES	ESCALA DE MEDICION
CALIDAD DE PROCESOS	SUBSISTEMA DE AUDITORIA	▪ Trabajo en equipo ▪ Experiencia laboral ▪ Motivación intrínseca ▪ Eventos de socialización ▪ Ética ▪ Responsabilidad	No Poco Si

.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACION

A continuación, se describe los antecedentes encontrados tanto nacionales como internacionales, con referencia al presente trabajo de investigación:

2.1.1. Tesis Internacionales

Yáñez Cáceres, (2017) en su tesis “Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño” concluye que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Subsecretaría de Economía y Empresas de Menor Tamaño utilizando herramientas open source y modelos de desarrollo de mejora continua para dar cumplimiento a un subconjunto de 44 objetivos de control del anexo normativo de la norma ISO27001:2013. La presente tesis no cubre la implementación de los 114 objetivos de control de la norma ISO27001,

pero cierra las principales brechas de seguridad de la información existentes en la organización al cubrir en forma completa el primer ciclo PDCA del SGSI, escogiendo un subconjunto de 44 objetivos de control priorizados por una análisis de brechas, incorporando las recomendaciones de DIPRES y cuya selección se realizó por un comité de seguridad de la Información constituido en el presente trabajo Las políticas y procedimientos son mantenidos en régimen mediante los seis sistemas que forman el SGSI y cuyo objetivo es administrar, monitorear, documentar y mejorar en forma continua la seguridad de la información, la metodología que se utiliza esta tesis, se centra en ciclos de aprobación que permitan establecer consensos y conciliar visiones en torno a un fuerte sentimiento de trabajo en equipo para facilitar la implementación de las políticas y procedimientos de seguridad de la información. Esta tesis propone que la metodología de implementación de SGSI se apoye en la gestión de riesgos, utilizando las guías y buenas prácticas de la norma ISO31000. Con ello los procesos estratégicos de la subsecretaría son clasificados por prioridad según su exposición a los riesgos y su impacto.

De este modo se optimiza la asignación de recursos a los proyectos de seguridad de la información, se favorece el aprendizaje y la creación de equipos de trabajo orientados a los objetivos prioritarios, sin que ellos perdieran la visión de conjunto y objetivo final. Como evaluación de la implementación del SGSI y de las políticas y procedimientos de seguridad de la información se realizaron dos auditorías, una interna y otra realizada por una empresa externa. Ambas auditorias fueron

totalmente independientes al equipo que diseñó e implementó tanto el SGSI como las políticas y procedimientos de seguridad de la información.

Ambas auditorias llegaron a la conclusión que el estado actual de seguridad de la información está en un nivel medio. Esto es un avance sustancial pues al inicio de la presente tesis no había un SGSI ni políticas y procedimientos efectivos para proteger la seguridad de la información. La principal recomendación entregada por las auditorías fue profundizar la difusión de las políticas y procedimientos de seguridad de la información, continuar con la implementación de los restantes 70 objetivos de control de la norma ISO27001:2013 y realizar una nueva evaluación durante el 2017 del funcionamiento del SGSI, es decir se han implementado los restante objetivos de control y evaluar el grado de institucionalización de las políticas y procedimientos de seguridad de la información.

Mayorga Mayorga, (2017) en su tesis “Sistema de Gestión de Seguridad de la información basado en la Norma ISO/IEC 27001 para el Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación” concluye que su objetivo garantizar la seguridad de los procesos organizacionales a través de un modelo estructurado de carácter preventivo (sistema de gestión de seguridad de la información) basado en la norma ISO/IEC 27001. La importancia radica en los dominios de seguridad que lo conforman, entre ellos políticas de seguridad, administración de activos, seguridad de los recursos humanos, sistema de control de accesos, etc. cada uno con sus respectivos controles. Se presentan los resultados de una experiencia aplicando las

fases de análisis y evaluación de riesgos a través de herramientas como entrevistas al personal de sistemas y observación directa mediante visitas programadas. Posteriormente se realiza un análisis de controles basados en la declaración de aplicabilidad donde se justifican aquellos controles aplicables en razón de las necesidades institucionales y a partir de ello se proponen políticas de seguridad coherentes y enmarcadas dentro de los límites de cumplimiento institucional, cuyo objetivo será apoyar y proporcionar la guía para gestionar adecuadamente la seguridad de la información.

Acosta Contreras, (2017) en su tesis “Diseño del sistema de gestión de seguridad de la información (SGSI) en la secretaría de hacienda del municipio de Cucunubá Cundinamarca bajo norma ISO 27001” concluye que la finalidad de su investigacion es identificar las amenazas y riesgos a los que puede estar expuesta la alcaldía municipal de Cucunubá en el área de la Secretaría de Hacienda donde se manejan los recursos y presupuesto del municipio, razón por la cual se deben implementar las medidas para salvaguardar la información y de esta forma evitar que personas mal intencionadas puedan acceder a ella con fines fraudulentos o intereses de terceros, ocasionando inconvenientes para el buen funcionamiento de la entidad, el objetivo es hacer la implementación de controles regidos bajo la Norma ISO 27001 de 2013 y establecer así las políticas de seguridad de la información para mitigar los posibles riesgos que se identifiquen.

2.1.2. Tesis nacionales

Warton Tapia, (2018) en su tesis “Implementación de un sistema de gestión de seguridad y salud ocupacional en la empresa Panoro Apurímac” concluye quesu objetivio de la tesis es de diseñar e Implementar un Sistema de Gestión de Seguridad y Salud Ocupacional basado en normas vigentes, que permita al Proyecto de Exploración Minera Cotabambas, tener bases consolidadas de cómo reducirlas lesiones personales, en función a esto se requiere elaborar el diagnostico situacional en materia de accidentes y problemas conexos a la actividad Otro objetivo es Elaborar los mecanismos existentes para la identificación de peligros y evaluación de los riesgos (matriz de riesgos), a los cuales están expuestos los trabajadores, evaluar el nivel de cumplimiento de la normativa legal vigente y evaluar los mecanismos de cada uno de los elementos requeridos para el seguimiento del sistema de gestión implementado. Se ha utilizado los métodos descriptivos (interpretar) y aplicativos. Estos consisten en describir situaciones, eventos y hechos particulares de la realidad. Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles más importantes de personas, grupo, comunidades o cualquier otro fenómeno que se someta a un análisis. Los estudios aplicativos buscan que todos los temas desarrollados dentro del trabajo sean aplicados en las actividades consideradas. El planteamiento de la hipótesis establecía que si se controlaba los riesgos a los que están expuestos los trabajadores en el Proyecto de Exploración Minera Cotabambas, se permitiría aportar al mejoramiento en el cumplimiento del plan de trabajo vigente en las

actividades de exploración minera, los resultados corroboran esto, ya que al implementar un sistema se gestiona el manejo integral de la seguridad para evitar accidentes que infieren en horas hombre trabajadas, tiempos por descansos médicos, investigaciones, re- instrucciones, gastos por atenciones médicas, entre otros. Para la empresa Panoro, el implementar el sistema de gestión resulto un cambio total en la estructura de la empresa en material de seguridad, de tal manera que se cuenta con un diagnóstico inicial de la situación de la empresa en materia de seguridad y salud ocupacional, mediante la matriz de riesgos ocupacionales se conoce cuáles son los peligros y el nivel de riesgo de exposición que tienen los trabajadores, se analizó con criterios de la norma (D.S.024-2016-EM) cuales serían las actividades y controles a implementar para eliminar y/o reducir la consecuencia de estas mismas en las personas, equipos, materiales, infraestructura y/o proceso, y como efecto de todos estos pasos, contar ahora con un sistema de Gestión que integra los principios de seguridad para evitar accidentes, se ha obtenido contar con una estructura de manejo adecuada, de manera que todos los procesos y actividades están alineados a seguir los criterios de seguridad, establecer controles y su respectivo seguimiento. Ya que toda la implementación se encuentra dentro de un marco de mejora continua, si hubiera cambios, o implementación de nuevos procesos este sistema al ser cíclico llamara a realizar un análisis previo para de nuevo establecer los nuevos controles.

Agurto Huanca, (2018) en su tesis “Sistema de gestión de seguridad y salud en el trabajo para reducir los accidentes laborales en

una empresa de servicios generales, Lurín, 2017” concluye que en la actualidad todas las empresas deben de contar un con un Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST), puesto que este sistema ayudará a la organización mantenerse constantemente actualizado con las legislaciones vigentes, además que permitirá una participación activa entre los trabajadores y el empleador, reducirá el índice de accidentabilidad y lo más importante es que generará una Cultura de Seguridad en el Trabajador. La presente tesis sugiere la implementación de un SGSST en una empresa de servicios generales, ya que tiene como objetivo la disminución de frecuencia de accidentes como la gravedad de los mismos. Además cabe mencionar que este estudio podrá ser replicado en empresas que estén en el mismo rubro. En el primer capítulo se muestra las generalidades de la investigación, la realidad problemática de la empresa, la formulación del problema. También se desarrolla los objetivos tanto general como específico de la investigación, marco teórico como también las hipótesis. En la segunda parte del capítulo se desarrolla la metodología de investigación, la situación actual de la empresa, aquí se determinará qué tipo de investigación será, que método, herramientas y técnicas de recolección se utilizará. En la tercera parte del capítulo se muestra los resultados obtenidos luego de la implementación del SGSST, se conoce el análisis descriptivo como también el análisis inferencial. En el cuarto capítulo se da a conocer la difusión de presente tesis, el cual nos da información de cómo disminuyo los índices de frecuencia como gravedad de los accidentes ocupacionales. En el quinto capítulo da las conclusiones a las

que se llegó luego de la implementación del SGSST. En el sexto capítulo se da a conocer las referencias bibliográficas que aportaron para poder realizar la presente tesis. En el último capítulo se adjuntan los anexos, los cuales ayudan a entender con más detalle la tesis, los cuales son necesarios para implementar el SGSST.

Cruz Diaz, (2017) en su tesis “Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la Clínica MEDCAM Perú SAC” concluye que su objetivo diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) con el fin de proteger los activos de información que influyan directamente en el cumplimiento de los objetivos de la empresa. Como metodología para el diseño del SGSI, se utilizó el método Deming o PDCA (Plan-Do-Check-Act), sugerida por la norma ISO/IEC 27001, la cual parte de la identificación de los activos de información y, es a base de la clasificación de los mismos, que se determina el posible impacto ante un evento de pérdida, y se establecen acciones de respuesta para la mitigación de los riesgos a los que están expuestos los activos. Los controles en respuesta se obtuvieron de la norma ISO/IEC 27002. Como resultado, se consiguió implementar un SGSI con lo que se logró minimizar los riesgos de amenazas y vulnerabilidades sobre los activos de información de MEDCAM Perú S.A.C. y así, lograr la confidencialidad, disponibilidad e integridad de la información. Concluimos que el beneficio más importante es asegurar los activos de información y así el cumplimiento de los objetivos de la empresa; así como, que cada SGSI

debe estar acorde con el tamaño y madurez de los procesos de la empresa.

2.2. BASES TEÓRICAS

2.2.1 Seguridad Informática y la vulnerabilidad en los sistemas

La seguridad informática es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

La seguridad informática es en realidad una rama de un término más genérico que es seguridad de la información, aunque en la práctica se suelen utilizar de distintas formas la aplicación de sus términos. La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls y otras medidas que dependen del usuario. La figura II.E.1 muestra algunas amenazas en la red que existen o se pueden presentar en las organizaciones.

Cuando se almacenan grandes cantidades de datos en forma electrónica, estos son vulnerables a muchos más tipos de amenazas de los que existen en forma física. Los sistemas de información se interconectan en diversas ubicaciones a través de la red de la empresa. El potencial de acceso sin autorización, abuso o fraude no se limita a una sola ubicación, sino que puede ocurrir en cualquier punto de la red de la empresa, para ello todo el personal debe contar con un plan de capacitación en Cyberseguridad puesto que pueden provocar daños al

introducir errores o acceder a los sistemas sin autorización como también abrir aplicativos o programas sin tener el conocimiento sobre su funcionamiento.

2.2.2 Identificación de activos

El activo es todo lo que le da valor a la organización y puede considerarse como activos a las impresoras, dispositivos de almacenamiento (discos duros externos, etc.) aplicaciones, inclusive los mismos colaboradores de una empresa por poseer información en formato digital o físico, para identificarlos es necesario dimensionarlos en los 3 pilares de la seguridad que es la confidencialidad, disponibilidad e integridad Por otro lado, existen elementos que no son considerados activos puesto que no cuentan con información pero se relacionan directamente con los activos cercanos a él, por ejemplo, un sistema de aire acondicionado, no tiene información pero su función es mantener a los servidores a una temperatura adecuada para que no se sobrecalienten ni presenten fallas en su funcionamiento puesto que cuentan con información para la organización.

2.2.3 Identificación de amenazas y vulnerabilidades

Como en toda organización, sus activos están expuestos a amenazas y que aprovechan de las vulnerabilidades para causar un impacto negativo adulterando su información y generar riesgos. Por tanto, es recomendable que se identifiquen qué amenazas y vulnerabilidades son las que están presentes en la organización por cada tipo de activo y

realizar el análisis para posteriormente calcular el nivel de riesgo existente.

2.2.4 Gestión de Riesgo

INSTITUTE, (2013), Define que es una combinación entre las actitudes de los interesados frente al riesgo y la exposición al riesgo estratégico de un determinado proceso, realizando un análisis del perfil de riesgo de los interesados a fin de clasificar y calificar el apetito y la tolerancia al riesgo de los interesados del proyecto. La gestión de riesgo es un enfoque estructurado para estudiar la posibilidad de que ocurra o no un riesgo, por tanto, para evitar que ocurra el riesgo, se lleva a cabo actividades para evaluar, mitigar el riesgo y estrategias para manejar el riesgo, reducirlos o aceptarlos, de tal forma que las posibles pérdidas y la posibilidad que se haga presente el riesgo se minimicen. En resumen, la gestión de riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

2.2.5 Cálculo del nivel de riesgo.

Para calcular el nivel del riesgo se tienen metodologías como Margerit, ISO27001, Cramm, Octave, etc., cada una de ellas se diferencian por su fórmula de calcular el nivel del riesgo, en otros casos se considera la valorización del activo basado en su confidencialidad, disponibilidad e integridad tal cual lo indica la norma ISO 27001

2.2.6 Medición del riesgo de seguridad de información

IRAM, (2010) Menciona que la ISO 27001 requiere que los controles sean medibles, por tanto la ISO 27004 aporta la forma de llevar a cabo dichas mediciones, entonces, la operación de medición de la seguridad de la información comprende de actividades que son esenciales para asegurar que los resultados de las mediciones proporcionan información de un Sistema de Gestión de Seguridad de la Información, controles o políticas implementadas y la necesidad de acciones apropiadas de mejora, lo cual incluye la integración de los procedimientos de medición dentro de la operatividad del SGSI, así como también recolectar, almacenar y verificar los datos.

2.2.7 Origen e historia de las normas ISO/IEC 27001

La Organización Internacional de estándares conocida como la ISO y la Comisión Electrotécnica Internacional por sus siglas IEC, son actualmente las principales organizaciones a nivel mundial para la estandarización de aspectos técnicos, de seguridad, entre otros. Dichas organizaciones, junto con otros organismos internacionales públicos o privados, participan en la realización de comités técnicos para establecer acuerdos y estándares en áreas específicas del conocimiento. Las normas conocidas como ISO/IEC 27001 y 27002, el cual su evolución se muestra en la figura II.B.1, que proporcionan un marco de gestión para la seguridad de la información aplicable por cualquier tipo de organización sin importar su naturaleza o tamaño, surgieron como resultado del Comité Técnico conjunto ISO/IEC JTC 1, llamado de las Tecnologías de la Información, subcomité 27 (SC 27), asociado con Técnicas de seguridad.

2.2.8 Modelo Deming

NTP-ISO 27001, (2005) El modelo conocido como “Planear-Hacer-Verificar- Actuar” - PDCA (Plan-Do-Check-Act), por sus siglas en inglés, puede aplicarse a todos los procesos del SGSI. La Figura II.C.3 ilustra cómo un ISMS toma como entrada los requisitos y expectativas de seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios genera productos de seguridad de la información (es decir: gestión de la seguridad de la información) que cumple estos requisitos y expectativas.

La adopción del modelo PDCA también reflejará los principios como se establecieron en la pautas de OECD (Guía para la Seguridad de los Sistemas de Información) para la gobernabilidad de los sistemas y redes de la seguridad de información. El ISO 27001:2005 provee un modelo para implementar los principios en las pautas que gobiernan la evaluación del riesgo, el diseño e implementación de la seguridad, la gestión de seguridad y la reevaluación.

1. Fase I: Plan - Establecer el SGSI

   Establecer las políticas, objetivos, procesos y procedimientos de seguridad relevantes para administrar el riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos de la organización.

2. Fase II: Do - Implementar y utilizar el SGSI

   Implementar y operar las políticas, controles, procesos y procedimientos de seguridad.

3. Fase III Check - Monitorizar y revisar el SGSI

Monitorear y evaluar el funcionamiento de los procesos con respecto a las políticas, objetivos y experiencia práctica de seguridad, informando sobre los resultados obtenidos a la gerencia para su revisión.

4. Fase IV Act - Mantenimiento y auditoría del SGSI

Tomar acciones correctivas y preventivas basándose en los resultados de la revisión gerencial para alcanzar la mejora continua del SGSI.

2.2.9 Política de Seguridad

LAUDON & LAUDON, (2012), Menciona que consiste de procedimientos, actividades o enunciados que clasifican los riesgos de información, identifican los objetivos de seguridad que están implementados y que van acorde con la organización y sobre todo las herramientas a utilizar para lograr estos objetivos. La política de seguridad controla las políticas que determinan el uso eficiente de los recursos de información para que los usuarios o colaboradores lo usen de manera adecuada bajo la conformidad en el acceso por la gerencia.

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

- **Sistema de Información,** Soto, (2007) Define Sistema de Información como: El sistema de personas, registros de datos y

actividades que procesa los datos y la información en cierta organización, incluyendo manuales de procesos o procesos automatizados.

- **Seguridad de la Información**, TARRILLO CLAVO & CORREA CUBAS, (2015) La Organización Internacional para la Estandarización (ISO) define Seguridad de la Información (SI) como: La preservación de la confiabilidad, integridad y disponibilidad de la información; así como de los sistemas implicados en su tratamiento, dentro de una organización.

- **Computación**, ciencia que estudia el tratamiento automático de la información, mediante máquinas diseñadas para ese propósito, (Elizondo, 2016).

- **Análisis y Evaluación de Riesgos**, Daltabuit & otros, (2007) es la selección de mecanismos para proteger, permitiendo estimular las pérdidas importantes en su información; ayudando a seleccionar los mismos.

- **Amenazas,** Alexander & otros, (2007) en conjunto con la ISO/IEC 27001, amenaza es una causa potencial de los incidentes no deseados, que pueda causar daños al sistema o una empresa**.**

- **Vulnerabilidad,** TARRILLO CLAVO & CORREA CUBAS, (2015) lo considera a las acciones vinculadas a debilidades de los activos que contengan información.

- **Informática,** Ciencia al cual estudia los métodos automáticos y racionales de la información mediante la obtención, conversión, uso y transmisión de información a través de activos de información computacionales, (Elizondo, 2016).

- **Investigación**, determinada por la indagación de datos-información o la búsqueda de soluciones a inconvenientes, (Pérez Porto & Gardey, 2012).

- **Activos de Información,** denominado a todo aquello que tiene valor para la entidad y por ende deba protegerse, puesto que contiene información valiosa**.**

- **Plan de Concientización en Seguridad de la Información,** TARRILLO CLAVO & CORREA CUBAS, (2015) comprende las actividades necesarias para establecer las estrategias de sensibilidades y divulgación de políticas y procedimientos para la Gestión de la Seguridad de la Información, con el propósito de establecer al interior de la organización un grado de compromiso y concientización con respeto al SGSI.

- **Monitoreo y Control al SGSI,** Del Carpio, (2006) involucra la realización de procesos administrativos de los riesgos que responden a los eventos que comprometen la seguridad de los activos de información.
- **Beneficios de un SGSI,** Kwell, (2008) define los beneficios de implantar un SGSI, los cuales son: (a)Establecimiento de una metodología de gestión de la seguridad clara y estructurada,

(b)Reducción del riesgo de pérdida, robo o corrupción de información, (c)Los clientes tienen acceso a la información a través medidas de seguridad, (d)Los riesgos y sus controles son continuamente revisados, (e)Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial, (f)Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar, (g)Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad, (i)Reducción de costos y mejora de los procesos y servicio, (j)Aumento de la motivación y satisfacción del personal, (k)Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

- **Magerit,** TARRILLO CLAVO & CORREA CUBAS, (2015) define la metodología promovida por CSAE (consejo superior de administración electrónica) que persigue una aproximación metódica al análisis de riesgos. Se trata por tanto de una metodología para auxiliar en tarea de toma de decisiones en entornos críticos.

CAPÍTULO III

METODOLOGIA

3.1. METODO DE INVESTIGACION

3.1.1. Tipo de investigación

Aplicada: De acuerdo con BARRANTES, (2008), la implementación de un Sistema de Gestión de Seguridad de la Información, realiza una solución para el problema de la I.E.P. ALBERT EINSTEIN.

3.1.2. Nivel de investigación

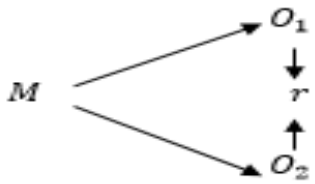
Descriptivo: De acuerdo con BARRANTES, (2008), se describe los estándares sobre la calidad de procesos, y los aportes para la propuesta de solución.

3.1.3. Diseño de investigación

Se aplicará el método “correlacional” en la medición de la variable dependiente ante la aplicación de la variable independiente.

Se puede representar mediante la siguiente simbología:

Diseño de la Investigación



Donde:

M: muestra.

O_1: Observación de la V1

r: Correlación entre dichas variables

O_2: Observación de la V2

3.2. POBLACION Y MUESTRA

a) Población

Estará conformada por el personal de la I.E.P. ALBERT EINSTEIN, que se encargan de las labores administrativas, que en total son 8.

b) Muestra

Se estimará siguiendo los criterios que ofrece la estadística, teniendo en cuenta el muestreo no probabilístico, por conveniente. El tamaño de la muestra es de 08.

3.3. TECNICAS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS

3.3.1. Técnicas

La técnica de recolección de datos es la parte operativa del diseño investigativo. Hace relación al procedimiento, condiciones y lugar de la recolección de datos. Tamayo y Tamayo, El proceso de la investigación científica, (2015)

Para realizar el presente trabajo de investigación se utilizaron las siguientes técnicas de recolección de datos: la observación directa, la encuesta y el análisis documental.

Encuesta

Consiste en un documento formado por un conjunto de preguntas que están redactadas de forma coherente, a través de la organización y secuencia (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014).

La encuesta es un cuestionario que se lee al responder, continua una serie de ítems empadronados a quien responde Tamayo y Tamayo, El proceso de la investigación científica, (2015).

Con relación a esto, la encuesta permitió obtener información relevante con respecto la investigación, y permitió conocer las opiniones de los colaboradores de la I.E.P. ALBERT EINSTEIN.

Análisis documental

Es la relación de documentos sea libros, informes o páginas webs que los investigadores deben leer para realizar su

marco teórico (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014).

Esto permitió recolectar información fundamental para el marco teórico de la investigación.

Observación de campo

La observación es un proceso intelectual e intencional que el investigador realiza sobre hechos, acontecimientos, datos y relaciones que señalan la existencia de fenómenos que pueden explicarse en el marco de la ciencia sobre la que realiza (Méndez Álvarez, 2011).

La aplicación de la observación directa en esta investigación, es similar a la que menciona el autor anterior porque se estuvo en las oficinas de la institución, observando la forma de trabajo que allí se realiza e incluso copiando en la guía de observación aquellos detalles resaltantes, que permitieron al autor conocer más de cerca las características de la estructura y funcionamiento

3.3.2. Instrumentos

Instrumento de recolección de datos es cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información (Arias, El Proyecto de Investigación - Introducción a la metodología científica, 2012).

Cuestionario

Preguntas en formato digital o papel auto respondidas, (Arias, EL PROYECTO DE INVESTIGACION, 2012).

Guía de Observación

Es un instrumento diseñado para registrar una conducta y sus repeticiones siendo estas medibles, (Arias, EL PROYECTO DE INVESTIGACION, 2012)

3.4. TRATAMIENTO DE DATOS

Validación del instrumento

Para el caso de la presente investigación, la validación del instrumento estuvo a cargo del juicio expertos, luego de conocer la problemática existente, los objetivos y las variables que se deseaban medir, procedieron a evaluar el cuestionario, constatando que con su aplicación se podrían cubrir los objetivos planteados y elaborar la propuesta.

Plan de recolección y procesamiento de datos.

- **Técnica:** Generada por la observación de campo y la encuesta.
- **Instrumento:** Elaborado por la guía de observación y cuestionario.
- **Ubicación:** La encuesta será realizada en las instalaciones de la I.E.P. ALBERT EINSTEIN, Jr. Emancipación Nº 517 – Distrito de Callería – Provincia de Coronel Portillo – Departamento de Ucayali

- **Recursos:** Para la recolección de datos se hará uso del cuestionario, la guía de observación, tablero de apuntes y lapiceros.
- **Tiempo:** La Observación de campo se llevará a cabo durante 2 semanas, de lunes a viernes, se dará inicio a las 09:00 a.m. hasta la 01:00 p.m.

Al finalizar la observación de campo se procederá a formular el cuestionario de preguntas de acuerdo a los datos obtenidos, el cual se llevará a cabo en un solo día posterior a la observación de campo, se dará inicio a las 09:00 a.m. hasta las 11:00 a.m., para comenzar luego con el procesamiento de datos.

Los softwares utilizados para nuestra investigación son los siguientes:

- **IBM SPSS Statistics Base,** plataforma de software que ofrece análisis estadísticos avanzados, de fácil uso, flexibilidad y escalabilidad hace que sea accesible a todo usuario, siendo útil en el proyecto de inicio a fin (IBM, 2014).
- **Excel 2016,** Es un programa de hojas de cálculo que permite crear y aplicar formato a libros, para analizar datos y tomar decisiones fundadas sobre aspectos de su negocio, Microsoft (2017).

Los datos obtenidos y su posterior procesamiento serán interpretados en:

- Tablas.
- Figuras elaboradas en diagrama de barras y curvas de frecuencia.
- Prueba de hipótesis.
- Correlación de datos.
- Alfa de Cronbach

CAPÍTULO IV
PLAN DEL SGSI

4.1. ANÁLISIS DE LA PROPUESTA

a) Importancia de un Sistema de Gestión de Seguridad de la Información para la I.E.P. Albert Einstein

- ✓ Reducir los riesgos, las amenazas y vulneraciones los cuales puedan afectar los activos de información de la Institución.
- ✓ Generar garantía en cuanto a confidencialidad, integridad y disponibilidad de la información de la institución.
- ✓ Lograr la total confiabilidad de la información en la I.E.P. Albert Einstein.

- ✓ Prevenir los riesgos y gestionar acciones de seguridad en cuanto a la información.
- ✓ Fomentar la costumbre de cuidar la información utilizando las normas de seguridad.
- ✓ Proteger la información contra los riesgos de destrucción, pérdida, divulgación, malversación y no disponibilidad.

b) Beneficios de implantar un Sistema de Gestión de Seguridad de la Información.

- ✓ Reducir el riesgo de que se produzcan pérdidas de información en las organizaciones, por perdidas también se entiende a robos y corrupciones en la manipulación.
- ✓ Se realiza revisión consecutiva de los riesgos a los que se pueden exponer la empresa y la información de los clientes, adicionalmente si tiene control.
- ✓ Establecer una metodología con la cual se puede gestionar la seguridad de la información.
- ✓ Implantar medidas de seguridad para los propios clientes.
- ✓ Implementar un SGSI otorga a la institución la garantía que los clientes y socios requieren, ya que ofrece un servicio con total confidencialidad y seguridad.

c) Implementaciones Certificadas

En todo el mundo existen cantidad de empresas que actualmente implementaron un Sistema de Gestión de Seguridad de la

Información y que están en plena operación, pero de todo este universo de empresas, solo algunas de estas cuentan con la certificación que acredita que su operación es la adecuada.

Se mostrarán algunas de las empresas conocidas en el mundo que cuentan con esta certificación, tanto en el ámbito nacional como internacional.

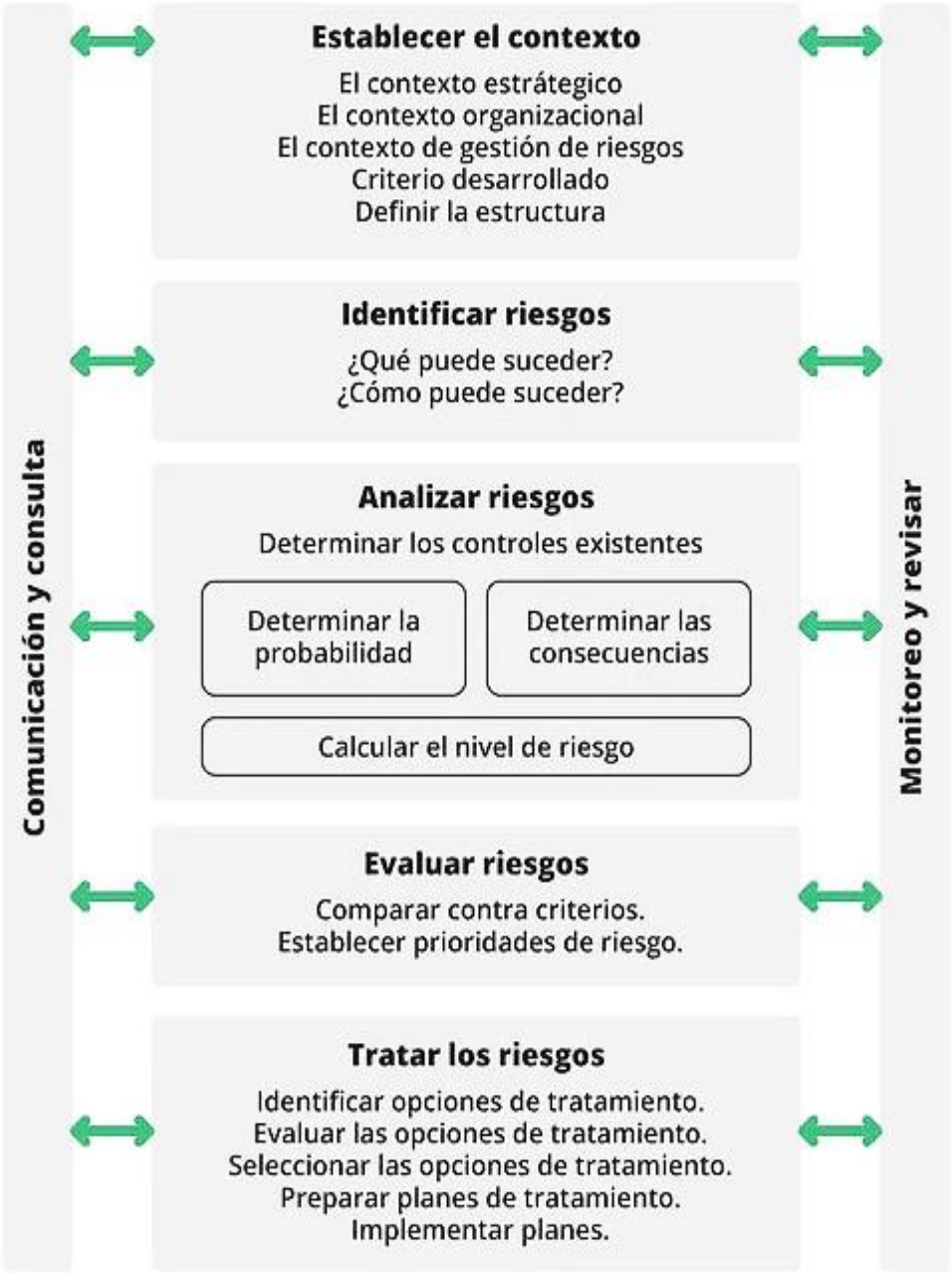
Tabla 3:

Organizaciones Certificadas con SGSI.

ÁMBITO	ORGANIZACIÓN CERTIFICADA
SGSI Internacionales	Microsoft Global Foundation Services (GFS), Google Apps, Amazon Web Services (AWS), IFX Networks Colombia, EQUIFAX Chile.
SGSI Nacionales Sector Público	Oficina de Normalización Previsional (ONP), Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN), Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), Banco Central de Reserva del Perú (BCRP), Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI),
SGSI Nacionales Sector Privado	Bolsa de Valores de Lima (BVL), Grupo Graña y Montero (GMD), RIMAC Seguros, Hermes, Compañía Minera Hochscild, Terra (Media Network), Atento Perú, T-Gestiona, Telefónica Empresas, Telefónica del Perú,

.

d) Proceso de gestión de riesgo



4.2. IMPLEMENTACION

a) Desarrollo Del Sistema de Gestión de Seguridad de la Información

En el desarrollo del SGSI se tomará como referente a la norma ISO 27001 e SIO/IEC 17799, con estos estándares fueron creados para proveer de un modelo para establecer, implementar, operar, monitorear y mejorar un SGSI.

Para la realización del SGSI adoptaremos el modelo “Plan – Do - Check – Act ”, también conocido como PDCA, el cual es aplicado a toda la estructura de los procesos del SGSI.

- ✓ **Plan (Establecer el SGSI):** Implica establecer la política del SGSI, sus objetivos, procesos y procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, con resultados acordes a las políticas y objetivos de toda la organización.

- ✓ **DO (Implementar y Operar el SGSI):** Representa la forma en que se debe operar e implementar las políticas, controles, procesos y procedimientos que se vayan a definir en la planificación del SGSI.

- ✓ **Check (Monitorizar y revisar el SGSI):** analizar a medida donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- ✓ **Act (Mantener y Mejorar el SGSI):** Realizar las acciones preventivas y correctivas, basados en las auditorías internas y

externas, revisiones del SGSI p cualquier otra información relevante para permitir la continua mejora del sistema.

4.2.1 Plan (Establecer el SGSI)

Martínez Ramos, (2014) El sistema de Gestión de Seguridad de la Información a proponer está conformado por procesos, los cuales son: clasificación y control de activos, Seguridad ligado al personal, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de accesos y gestión de continuidad del negocio.

Para el conocimiento de la situación actual en la que se encuentran estos procesos se realizará una auditoría a cada proceso, para obtener resultados. Para ello se realizar una evaluación de cuál es la realidad de la institución según los procedimientos a desarrollar, según los datos obtenidos se plasmará cual o cuales son las actividades, equipos tecnológicos a implementar para fortalecer la debilidad encontrada y estructurar la implementación del sistema de Gestión de Seguridad de la Información.

Para el seguimiento de la secuencia de implementación del SGSI, se establecerán reuniones al inicio y fin de cada proceso, el cual ayudará a identificar quienes serán los actores principales y/o el equipo de trabajo, así como realizar seguimiento el avance de cada proceso, el cual se plasmarán las reuniones en el **FORMATO DE REUNION** (Anexo 3).

a) Clasificación y Control de Activos

Tabla 4:

Activos Informáticos.

Nº	Activo	Descripción
01	Software	Se cuenta con Software de ofimática, desarrollo.
02	Hardware	Se cuenta con equipos de cómputo, impresión, fotocopiado, etc.
03	Documentación	Se cuenta con documentación con conteniendo información, soporte, etc.
04	Servidores	No se cuenta con servidores de información, programas, archivos, etc
05	Backup	No se cuenta con copia de respaldo de información física ni virtual

Para el desarrollo de este proceso, se desarrolla el trabajo de campo, a la par de realizar consultas al Director de la institución como autoridad máxima para obtener información de los activos informáticos, obteniendo la siguiente información:

- El Software con el que cuenta la Institución educativa no se encuentran clasificados de acuerdo a importancia y uso por oficina, considerando que los software no cuentan con licencia original
- El Hardware con el que cuenta la Institución educativa no está inventariado desde el 2015, generando esto la no actualización de los nuevos equipos.

- La documentación Institución Educativa se encuentra archivada es estands dentro de cada oficina, sin clasificación alguna como memos, informes, resoluciones, formatos, etc; no contando con un ambiente de archivo general.
- La Institución Educativa no cuenta con un cuarto de servidores (DATA CENTER).
- La Institución Educativa no cuenta con ningún tipo de backup (copia de respaldo) de su información física ni virtual.

b) Seguridad Ligada al Personal

Para el desarrollo de este proceso, se desarrolla el trabajo de campo, a la par de realizar consultas al Director de la institución como autoridad máxima para obtener información de los activos informáticos, obteniendo la siguiente información:

- El personal administrativo al ingresar a laborar a la Institución no se le hace firmar ningún acuerdo de confidencialidad.
- El personal administrativo al ingresar a laborar en la Institución y según sus funciones tendrá acceso a los servicios informáticos, en la actualidad el personal administrativo no cuenta con capacitación sobre la seguridad de la información.
- Cuando se contrata personal para realizar trabajos en calidad de tercero (outsorcing) dentro de la institución educativa, no se le hace firmar ningún compromiso de confidencialidad.

c) Seguridad Física y del Entorno

Para el desarrollo de este proceso, se desarrolla el trabajo de campo, a la par de realizar consultas al Director de la institución como autoridad máxima para obtener información de los activos informáticos, obteniendo la siguiente información:

- El acceso al área administrativo de la Institución es utilizado tanto por el personal interno como por los clientes, en los casos en que los clientes vienen a solicitar información sobre el desempeño de sus hijos. Actualmente el área administrativa de la Institución con 02 puertas de acceso, pero solo se utiliza la principal.
- El área administrativa de la Institución cuenta 2 cámaras de seguridad (1 en la parte externa y 1 en la parte interna), la cual registra el ingreso y salida tanto de trabajadores como de clientes.
- El control del ingreso a las áreas administrativas es realizado solo por la secretaria, quien toma nota de la hora de llegada de cada colaborador, este registro solo es realizado para trabajadores, mas no para el fluido de ingreso y salida de clientes.

d) Gestión de Comunicaciones y Operaciones

Para el desarrollo de este proceso, se desarrolla el trabajo de campo, a la par de realizar consultas al Director de la institución como autoridad máxima para obtener información de los activos informáticos, obteniendo la siguiente información:

- En la Institución no existen procedimientos documentados para actividades del sistema asociados con la manipulación de información, tales como el encendido y apagado de las computadoras, los correos corporativos y la seguridad de la misma, los cuales brindan la información corporativa a los diferentes usuarios.
- La Institución cuenta en la actualidad con 7 formas de control.
  - ✓ Control Logístico
  - ✓ Control Tesorería
  - ✓ Control de Contabilidad General
  - ✓ Control de Contabilidad de Costos
  - ✓ Control Patrimonial
  - ✓ Control de Personal
  - ✓ Control de Requerimiento de Oficina
- Cada control es asignado de acuerdo al área y al cumplimiento de sus funciones a cada usuario. Actualmente no se cuenta con un procedimiento para consignar los incidentes que se producen cuando se hace uso de los controles.
- Los cambios que cada control sufre es realizado por la propuesta del usuario administrativo. Generalmente estos cambios son realizados, pero en la mitad de los casos no son comunicados o plasmados en documentos, los cuales ha provocado perdida de información.
- Los softwares ofimáticos que se utilizan para las tareas administrativas no cuentan con su versione actualizada, el manejo

y guardado de la información son en las bases de datos propios de estos, generando una vulnerabilidad de la perdida de información.

- Actualmente las computadoras, laptops y otros equipos de cómputo, no cuentan con un antivirus con licencia activa y original, que garantice la protección del equipo.
- Se encontraron otros riesgos considerables que afectan el manejo y distribución de la información.

e) Control de Accesos

Para el desarrollo de este proceso, se desarrolla el trabajo de campo, a la par de realizar consultas al Director de la institución como autoridad máxima para obtener información de los activos informáticos, obteniendo la siguiente información:

- Actualmente al despedir a un usuario (acceso a un equipo informático, correo, etc.) este deja la clave de acceso que utilizo al nuevo usuario, el cual tiene posibilidad de cambiarlo o no, corriendo el riesgo de que en un intento de robo de información este pueda realizarse.

- Actualmente la Institución no maneja un registro de altas y bajas de usuarios de los equipos informáticos para los accesos a estos y a la información que contienen.

- Actualmente la Institución no realiza auditorias para poder constatar que tan protegido o expuestos se encuentra en el caso de algún intento de robo o acceso a la información por parte de personas inescrupulosas.

- Actualmente la Institución, no tiene una definición de claves de acceso por nivel de usuario o por la importancia de equipo según información almacene.

- Actualmente para la creación de una contraseña de acceso para los equipos informáticos o la codificación de la documentación en físico, no cuenta con una estructura que prevea parámetros de seguridad.

f) Gestión de Continuidad del Negocio

Para el desarrollo de este proceso, se desarrolla el trabajo de campo, a la par de realizar consultas al Director de la institución como autoridad máxima para obtener información de los activos informáticos, obteniendo la siguiente información:

Actualmente la Institución no cuenta con planes de contingencias antes distintos desastres, como pueden ser:

- ✓ No se identifican los riesgos a los que está expuesto la Institución en caso de producirse algún desastre natural o artificial.

- ✓ No se especifica la frecuencia y probabilidad de ocurrencia por cada riesgo identificado.
- ✓ No se especifica las acciones que se están realizando para mitigar los riesgos potenciales a los cuales se está expuesto cada día.

- ✓ El personal no tiene claro conocimiento de las acciones que tiene que realizar durante un desastre, situación que provocaría mayores daños con respeto a los activos informáticos y el personal del área.

4.2.2. Do (Implementar y Operar el SGSI)

Una vez que se ha identificado los problemas en la etapa anterior y en cada uno de los procesos, ahora definiremos las acciones y actividades necesarias para la implementación de SGSI por proceso.

Para el seguimiento de la secuencia de implementación del SGSI, se establecerán reuniones al inicio y fin de cada proceso, el cual ayudará a identificar quienes serán los actores principales y/o el equipo de trabajo, así como realizar seguimiento el avance de cada proceso, el cual se plasmarán las reuniones en el **FORMATO DE REUNION** (Anexo 3).

a) Clasificación y Control de Activos

- **Clasificación de Software**

  La clasificación del software se realizará en base al uso e importancia, donde el total estará representado por el producto de ambos criterios.

  - ❖ Software usado frecuentemente, poca importancia “1”
  - ❖ Software usado regularmente, mediana importancia “2”
  - ❖ Software usado siempre, gran importancia “3”

Tabla 5:

Software Licenciado de la I.E.P. Albert Einstein.

SOFTWARE DE LA I.E.P. ALBERT EINSTEIN					
Sistemas Operativos	**Versión**	**Cantidad**	**Uso**	**Importancia**	**Total**
WINDOWS					
Windows 8	2012	3	3	3	6
Windows 8.1	2013	3	3	3	6
OFIMATICA					
OFFICE WORD	2016	6	3	3	6
OFFICE EXCEL	2016	6	3	3	6
OFFICE POWER POINT	2016	6	3	3	6
OFFICE ACCESS	2016	6	3	3	6
OFFICESS PUBLISHER	2016	6	3	3	6
OFFICE ONENOTE	2016	6	3	3	6
SOFTWARE ANTIVIRUS					

AVAS SEGURITY	2018	2	1	3		4
ESET SEGURITY	2018	4	1	3		4

- **Clasificación de hardware**

  Para tener una mejor clasificación e inventario del hardware se utilizará la siguiente estructura:

Tabla 6:

Clasificación e Inventario de Hardware.

		EQUIPO OCUPACIONAL		**MONITOR**		**OPERADOR USUARIO**	
C.H.	**USUARIO**	C.ACTUAL	DESCRIPCION	C.ACTUAL	MARCA	CARGO	NOMBRE

Donde:

C.H, costo de Hardware

USUARIO, descripción del usuario

C.ACTUAL, código actual del equipo

DESCRIPCION, características del Hardware

MARCA, marca del equipo

CARGO, cargo del usuario

NOMBRE, nombre del usuario

Con este formato se va a realizar el inventario de todo el Hardware de la Institución y de todas sus áreas.

- **Clasificación de Documentos**

  Se clasificará todos los documentos archivados en la Institución se realizará de la siguiente manera.

  ❖ Usado frecuentemente, poca importancia “1”

  ❖ Usado regularmente, mediana importancia “2”

  ❖ Usado siempre, gran importancia “3”

Tabla 7:

Clasificación de Documentos.

DOCUMENTACION	USO	IMPORTANCIA	TOTAL
Memorándum de accesos	1	3	4
Formatos de Usuarios	2	3	5
Documentación de Sistemas	3	3	6
Documentación de Software	2	2	4
Memorándum Internos	2	1	3

- **Clasificación de Servidores**

  Actualmente la Institución no cuenta con ningún tipo de equipamiento tecnológico de servidor (Data Center), por lo

que para la implementación del Sistema de Seguridad de Gestión de la Información se recomienda la adquisición de 2 equipos para uso de servidores: 1 como el servidor de uso cotidiano y 1 para el servidor de respaldo.

A continuación, se describirán las características que deben cumplir como servidor:

Tabla 8:

Servidores

EQUIPO	CARACTERISTICAS	CANTIDAD
SERVIDOR 1	DELL POWEREDGE T150 XEON E-2336 16 GB RAM 2TB T 150anq 3v1	1
SERVIDOR 2 RESPALDO	TORRES HP MI350 G10 XEON 4210 RAM 128 3TB – DDR4	1

Tabla 9:

Sistemas Operativos / Gestor de Base de Datos.

SISTEMA OPERATIVO	GESTOR BASE DE DATOS
WINDOWS SERVER 2012 R2	SQL SERVER 2012

Se clasificará todos los servidores en la Institución de la siguiente manera:

- ❖ Usado frecuentemente, poca importancia “1”
- ❖ Usado regularmente, mediana importancia “2”
- ❖ Usado siempre, gran importancia “3”

Tabla 10:

Clasificación de Servidores.

DESCRIPCION	USO	IMPORTANCIA	TOTAL
Contingencias	1	3	4
Base de Datos	2	3	5
Archivos	3	3	6
Correo	2	2	4
Memorándum Internos	2	1	3

- **Clasificación de Backup**

Actualmente la Institución no realiza un Backup diario, semanal y menos mensual, a lo que la única información que tienen dentro de la institución en caso ocurra algún desastre natural son los archivadores físicos, por lo que para la implementación del Sistema de Seguridad de Gestión de la Información se recomienda a la Institución lo siguiente: a) Realizar un Cronograma de Backup diario, semanal y mensual de toda la información, la información física debe ser escaneada y así mismo la información guardadas en el servidor y equipos de cómputo.

Para el Backup se debe contar con:

Tabla 11:

Equipos de Backup.

EQUIPO	CARACTERISTICAS	CANTIDAD
DISCO DURO EXTERNO	2TB	2
MEMORIA EXTRAIBLE USB	128 GB	7

Se clasificará todos los servidores en la Institución de la siguiente manera:

- ❖ Usado frecuentemente, poca importancia “1”
- ❖ Usado regularmente, mediana importancia “2”
- ❖ Usado siempre, gran importancia “3”

Tabla 12:

Clasificación de Backup.

DOCUMENTACION	USO	IMPORTANCIA	TOTAL
Base de Datos	3	3	6
Software	3	3	6
Correo	3	3	6
Archivos – Usuarios	3	3	6
Sistemas	3	3	6

b) Seguridad Ligada al Personal

- ❖ **Acuerdo de Confidencialidad (Interno)**

Considerando la necesidad de tener con un documento en el cual todo el personal de la Institución, responsable de manipular información confidencial se comprometa en todo momento a mantener en secreto toda información “confidencial” perteneciente a la Institución, por tal motivo como parte del proceso de implementación se ha

estructurado el **Compromiso De Confidencialidad (Anexo 5).**

- **Acuerdo de Confidencialidad (Externo)**

Debido a que la Institución trabaja con personal externo es necesario contar con el compromiso que no se divulgue/manipule ningún tipo de información sin autorización y conocimiento de un personal administrativo, por tal motivo como parte del proceso de implementación se ha estructurado el **Compromiso De Confidencialidad (Anexo 6).**

- **Capacitación al Personal Nuevo**

Se logrará coordinar con la oficina de Administración para que todo personal sea enviado antes de empezar sus labores a la Institución, donde el Director del colegio en conjunto con el encargado del área informática le brindarán capacitaciones que se basan en seguridad de la información en base a los servicios informáticos que manipulará para el desarrollo de sus funciones en su área respectiva, por tal motivo se ha elaborado el **Formato de Capacitación (Anexo 7)**. Adicionalmente se programará constantemente capacitaciones a todas las áreas para mantener a los trabajadores actualizados en temas de seguridad de la información.

c) Seguridad Física y del Entorno

❖ Ingreso de Personal Externo a la Institución

En la Institución se dispondrá que todo colaborador externo deba ingresar por la 2da puerta y no por la principal. Podrá ingresar a los ambientes administrativos siempre y cuando esté un trabajador presente en los ambientes, hasta que termine de realizar su actividad programada, por tal motivo se ha elaborado el **Registro de Ingreso de personal Externo (Anexo 8).**

❖ Seguridad Física de la I.E.P. Albert Einstein

Frente a la presente situación se ha propuesto al Director de la Institución, considerar en el presupuesto la adquisición de un guardia de seguridad y un Libro de Incidencias, donde el guardia de seguridad anotará todas las actividades que se consideren inusuales dentro de la institución, con la finalidad de establecer una seguridad más física.

❖ Vigilancia de la I.E.P. Albert Einstein

Se coordinará con la Oficina de Dirección de la institución la adquisición de nuevas cámaras de video vigilancia, la adquisición de un equipo DVR de mayo capacidad de almacenamiento tales como:

EQUIPO	CARACTERISTICAS
Cámaras De Vigilancia	Full Hd Con Sensor De Movimiento Y Visión Nocturna
DVR (Digital Video Recorder)	Capacidad De Almacenamiento De 2 Tb

Se capacitará al guardia de seguridad para que en todo momento se tenga resguardado las instalaciones de la Institución, sobre todo en los meses Enero – Agosto – Diciembre, que es donde están vigentes las matrículas y traslados de alumnado.

d) Gestión de Comunicaciones y Operaciones

❖ **Documentación de Procesos Informáticos Operativos**

Con el fin de facilitar a los usuarios realizar sus actividades, se documentarán y publicarán los siguientes procesos a cargo del Director

- Correo Electrónico
- Backup
- Acceso a Internet
- Uso de Equipos de Cómputo

Como parte del Sistema de Gestión de Seguridad de la Información, la institución generará un cronograma de capacitación por Oficina sobre el uso de los Procesos Administrativos, para esto se implementará el **Registro de Capacitación de Procesos Informáticos (Anexo 9).**

Así mismo se identificó que la Institución no tiene actualizado la documentación sobre el MOF (Manual de Organización Funcional) y el ROF (Reglamento de Organización y Funciones), documentación la cual, al no estar actualizado y no contar con las políticas de seguridad que se plantea, puede generar, vacíos reglamentarios. Por tal motivo se sugiere a la Institución la pronta actualización de estos documentos, que, al no contar con el personal y la logística necesaria, se puede generar la contratación de un especialista externo.

- **Gestión de comunicación**

La Institución, establecerá acciones a realizar ante cualquier incidente sea de origen natural o artificial, como las siguientes acciones:

- El usuario avisará el acontecimiento al Director, enviando copias de su informe también a todos los administradores vía correo electrónico.
- Una vez prevenido a los colaboradores del incidente, se pasará a buscar la solución y proveer que se repita el acontecimiento.
- El director comunicará vía correo electrónico la solución del problema y lo pondrá como antecedente y dando las instrucciones para que tomen las precauciones.

- El encargado del Área de Informática, registrará el incidente en el **Registro de Incidentes de Seguridad de la Información (Anexo 10)**, en conjunto con el Director evaluaran el incidente para prevenirlo para futuros casos.

❖ **Gestión de Cambios**

La Institución establecerá comunicación vía correo electrónica a todos los usuarios informáticos, las siguientes actividades:

- Cambios y mantenimientos de los equipos de cómputo.
- Mantenimiento de los Servidores
- Actualización de los softwares ofimáticos
- Obtención de sistemas de Información

❖ **Gestión de Respaldo y Recuperación**

El respaldo y recuperación de la información es un proceso de gran importancia para la Institución, porque se establecieron las siguientes acciones:

- El personal de informática realizar una copia de respaldo de los servidores diario, así como de la información dentro de los equipos de cómputo de las oficinas.
- El personal administrativo realizará copias de seguridad de los archivos, formando así una base de datos de toda la información.

- El director de la Institución recaudará la copia de seguridad de cada personal, para así poder crear una copia semanal y guardar.
- Toda la información almacenada será guardada en dos discos duros, los cuales estarán a cargo de la alta gerencia, es este caso de la Dirección de la Institución y el Área de Informática.
- Toda copia de seguridad que se realice de forma semanal se deberá plasmar en el **Registro de Backup Semanal (Anexo 11).**

❖ **Gestión de Medios de Almacenamiento**

La Institución utilizará diferentes estrategias para el almacenamiento y desplazamiento de la información entre el personal administrativo.

Todo personal administrativo deberá contar con un dispositivo de almacenamiento (USB, disco duro, etc.) solo de uso en el trabajo, el cual se usará únicamente para obtener y brindar información en el área laboral. Los dispositivos de almacenamiento utilizados por el personal interno y que contenga información de importancia, deberán ser almacenados en lugares seguros, en el que solo el usuario pueda acceder o tenga conocimiento.

Para el uso de los dispositivos de almacenamiento (USB, disco duro, etc.), personal deberá realizar los siguientes pasos:

- Analizar el dispositivo de almacenamiento en modo avanzado utilizando el antivirus instalado en el equipo, asegurándose de completar todas las fases de revisiones y análisis.

e) Control de Accesos

❖ **Gestión de Acceso a Usuarios**

Para poder brindar seguridad adecuada en el acceso de usuarios a los servicios informáticos, se ha complemento la seguridad de la siguiente manera:

- El Director enviará un memorándum a la oficina de la administración oficializando la salida de un usuario y el ingreso del nuevo, para hacer los cambios respectivos.

La baja de un usuario por renuencia o despido se complementará con la siguiente acción:

- El usuario comunicará vía correo electrónico la fecha hasta la cual se quedará y hará uso de los activos de información que están bajo su poder, de esta manera la administración tendrá en cuenta el cese de un usuario y la creación de uno nuevo para el colaborador que ingrese.
- El área de secretaría utilizará el **REGISTRO DE ACTIVACION/DESACTIVACION DE USUARIOS**

(Anexo 12), formato que será supervisado de manera mensual por el área de Informática y la Oficina de Dirección.

f) Gestión de Continuidad del Negocio

La Institución tendrá en cuenta los siguientes aspectos para implementar una adecuada Gestión de Continuidad del Negocio.

❖ **Seguridad de la Información en la Continuidad del Negocio**

- Entender los riesgos a los que la Institución está expuesto, desde un punto de vista vulnerable y el impacto, incluyendo la identificación y priorización de los procesos críticos del negocio.
- Concientizar el impacto que se tendrá las interrupciones en los procesos de la Institución y su repercusión en la economía de la entidad.
- Considerar un plan de seguridad del personal y protección de las instalaciones de procesamiento de información.
- Documentar y actualizar el plan de continuidad del negocio, agregando los requisitos de seguridad mencionados líneas arriba y retroalimentar cada proceso.

PRESENTACION, ANALISIS E INTERPRETACION DE RESULTADOS

- **Continuidad del Negocio y Evaluación de Riesgos**
  - Evaluar los riesgos por parte de los administrativos encargados de la dirección de la Institución, incluyendo los recursos críticos, impacto de interrupciones y tiempo de recuperación.
  - Elaborar el plan de estrategia, con la finalidad de determinar un enfoque global de la continuidad de los procesos de la Institución.

4.2.3. Check (Monitorizar y Revisar el SGSI)

Después de englobar todos los indicadores en los 06 procesos del SGSI, se realizará una auditoría de cada proceso del SGSI, con la intención de constatar que todo lo planteado ha brindado resultados positivos con la seguridad de la información en la I.E.P. Albert Einstein. La continuidad de la auditoria será cada 04 meses, teniendo la participación de los administrativos, el director y un especialista en seguridad de la información.

Se contratará los servicios de un especialista en seguridad de la información, el mismo que identificará los resultados positivos y negativos de cada uno, con la información recabada se hará lo siguiente:

- **LOS RESULTADOS POSITIVOS:** Se estructurará un cronograma de retroalimentación de los procesos, a fin de continuar con la mejor y el buen proceso.
- **LOS RESULTADOS NEGATIVOS:** Identificara cual es el riesgo, enumerando las debilidades tanto del proceso detallado, como de los procesos que realiza la parte administrativa, la parte informática.
- **ALTERNATIVAS A REALIZAR:** Se detallarán las actividades a realizar para la mejoría del proceso, en conjunto con las oficinas implicadas.

- **OBSERVACIONES ADICIONALES:** Son aquellas que el especialista y/o personal administrativo observan como parte de una debilidad o traba para el cumplimiento del proceso evaluado.

Tabla 13:

Formato de Monitoreo

PROCESO	
RESULTADOS POSITIVOS	RESULTADOS NEGATIVOS

ALTERNATIVAS A REALIZAR

OBSERVACIONES ADICIONALES

VºBº Director IEP Albert Einstein	VºBº Jefe de SI

4.2.4. Act (Mantener y Mejorar el SGSI)

Para poder mantener y guiar a mejorar el SGSI se ha acordado responsabilidades a todos los miembros de la Institución, con el fin de contribuir al mejoramiento de la seguridad de la información. Tales responsabilidades se plasman en la siguiente tabla:

RESPONSABILIDADES PARA EL MANTENIMIENTO DEL SGSI
Jefe de la Oficina Estratégica
- Liderar el equipo de trabajo - Proponer al Jefe de la Institución la asignación de los recursos necesarios para el mejoramiento de la seguridad de la información. - Proponer mejorar al equipo de trabajo en los aspectos de seguridad de la información.
Director de la Institución
- Supervisar el cumplimiento de las acciones establecidas por el SGSI - Proponer procesos de mejoras en el aspecto de seguridad de la información - Coordinar equipos de trabajo para la implementación de alternativas de seguridad. - Asignar responsabilidades para mantener y mejorar el SGSI. - Aprobar las alternativas de seguridad propuestas por el personal de la IEP Albert Einstein
Jefe Administrativo
- Implementar los procesos del SGSI en el desarrollo y mantenimiento de los sistemas de información. - Coordinar con el Analistas de Seguridad de la Información la implementación de procedimientos de seguridad. - Proponer nuevas técnicas y procedimientos que permitan mejorar la seguridad de la información de los sistemas en funcionamiento. - Implementar metodologías de desarrollo que involucren aspectos de seguridad de la información.
Especialista de Seguridad de la Información
- Liderar el equipo frente a aspectos de seguridad de la información.

- Proponer al feje de la Institución nuevas metodologías, técnicas o procedimientos de seguridad de la información.
- Sustentar alternativas de mejora de los procesos de seguridad de la información.
- Investigar e implementar todo lo relacionado a seguridad de la información.
- Supervisar y coordinar las acciones propuestas por el personal de la Institución relacionados a seguridad de la información.

CAPÍTULO V:

PRESENTACION, ANALISIS E INTERPRETACION DE RESULTADOS

5.1. ANÁLISIS DE TABLAS Y FIGURAS

5.1.1. LA encuesta se realizó en las instalaciones de la I.E.P. ALBERT EINSTEIN, donde los encuestados respondieron las siguientes preguntas:

Tabla 14:

Número de elementos analizados

		N	%
	Válido	8	100,0
	Excluidos	0	,0
	Total	8	100,0

Tabla 15:

Validación de alfa de Cronbach

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,784	,745	21

Pregunta 1: ¿Conoce usted alguna política de administración en la I.E.P. ALBERT EINSTEIN?

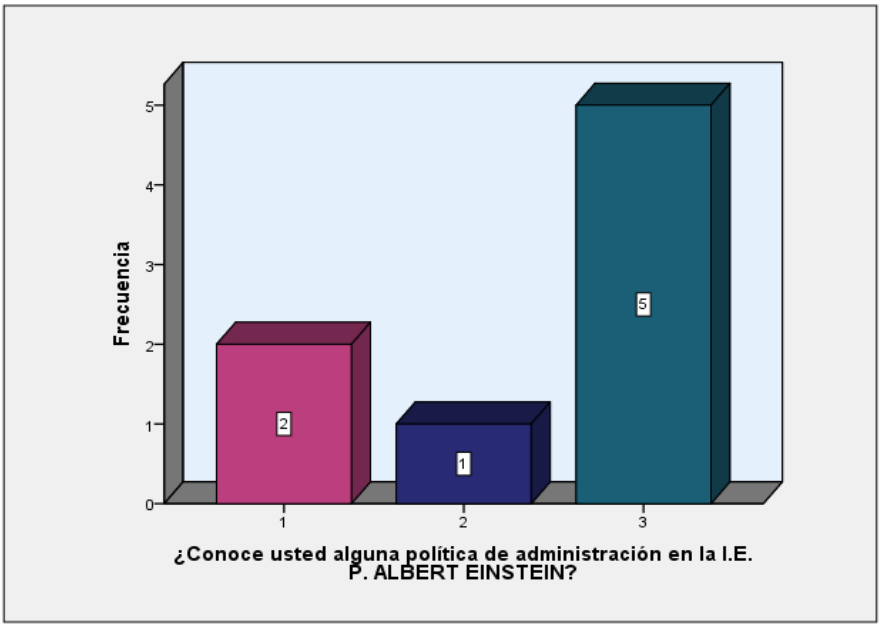
Tabla 16:

Resultado pregunta 1

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	2	25,0	25,0	25,0
	POCO	1	12,5	12,5	37,5
	SI	5	62,5	62,5	100,0
	Total	8	100,0	100,0	

Figura 1:

Resultados pregunta 1.



Interpretación: En la Figura 1 nos demuestra que 5 de los 8 entrevistados conocen alguna política de administración dentro de la I.E.P. Albert Einstein.

Pregunta 2: ¿Conoce usted el alcance del ISO 27001 en la I.E.P. ALBERT EINSTEIN?

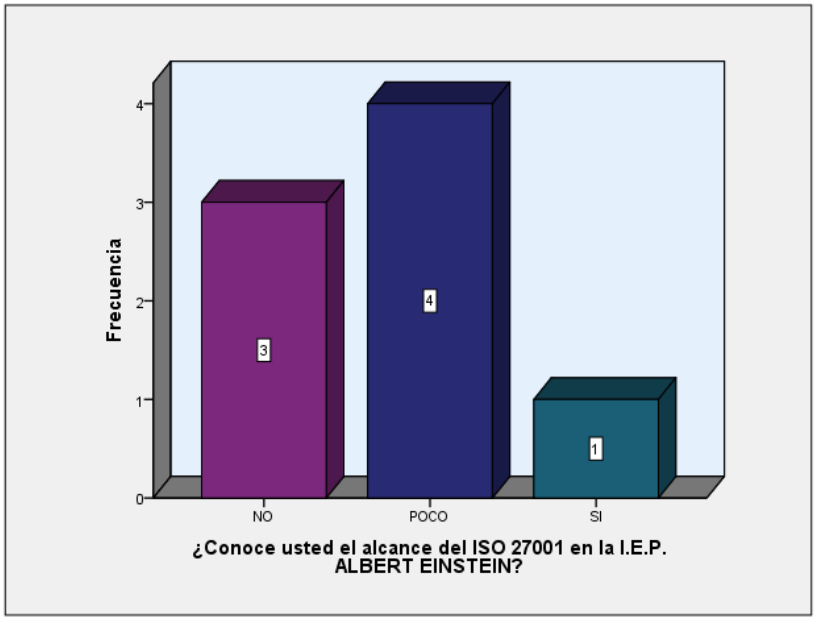
Tabla 17:

Resultados pregunta 2.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	3	37,5	37,5	37,5
	POCO	4	50,0	50,0	87,5
	SI	1	12,5	12,5	100,0
	Total	8	100,0	100,0	

Figura 2:

Resultados pregunta 2.



Interpretación: En la Figura 2 nos demuestra que 4 de los 8 entrevistados conocen poco sobre el alcance de un ISO 27001 en la I.E.P. Albert Einstein.

Pregunta 3: ¿Conoce usted el análisis de riesgo 27001 en la I.E.P. ALBERT EINSTEIN?

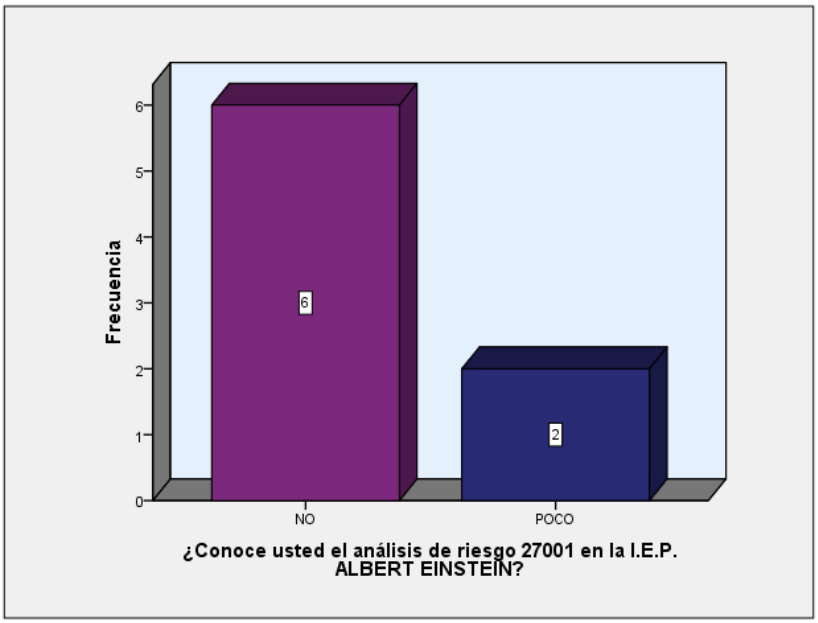
Tabla 18:

Resultados pregunta 3

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	6	75,0	75,0	75,0
	POCO	2	25,0	25,0	100,0
	Total	8	100,0	100,0	

Figura 3:

Resultados pregunta 3.



Interpretación: En la Figura 3 nos demuestra que 6 de los 8 entrevistados no conocen sobre el análisis de riesgos 27001 en la I.E.P. Albert Einstein.

Pregunta 4: ¿Conoce usted como seleccionar controles 27001 en la I.E.P. ALBERT EINSTEIN?

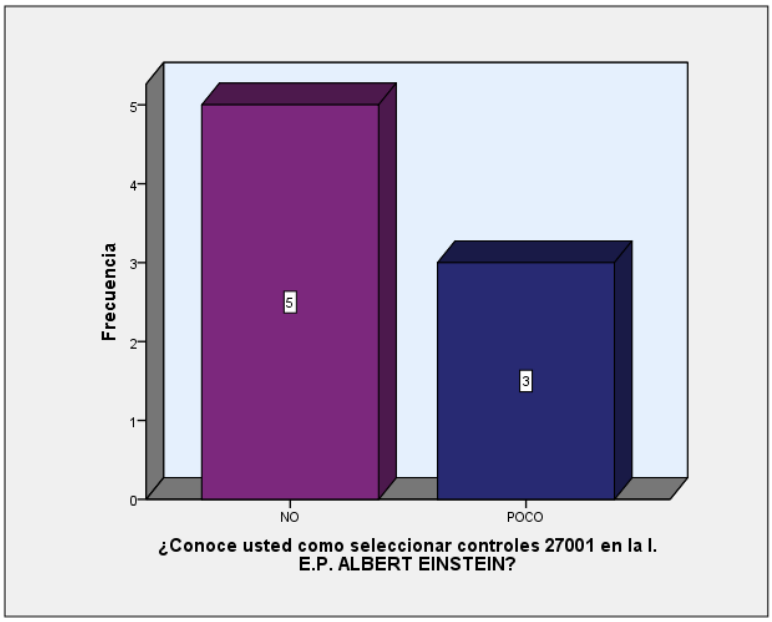
Tabla 19:

Resultados pregunta 4.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	5	62,5	62,5	62,5
	POCO	3	37,5	37,5	100,0
	Total	8	100,0	100,0	

Figura 4:

Resultados pregunta 4.



Interpretación: En la Figura 4 nos demuestra que 5 de los 8 entrevistados n conocen sobre como seleccionar controles 27001 en la I.E.P. Albert Einstein.

Pregunta 5: ¿Conoce usted sobre la definición 27001 en la I.E.P. ALBERT EINSTEIN?

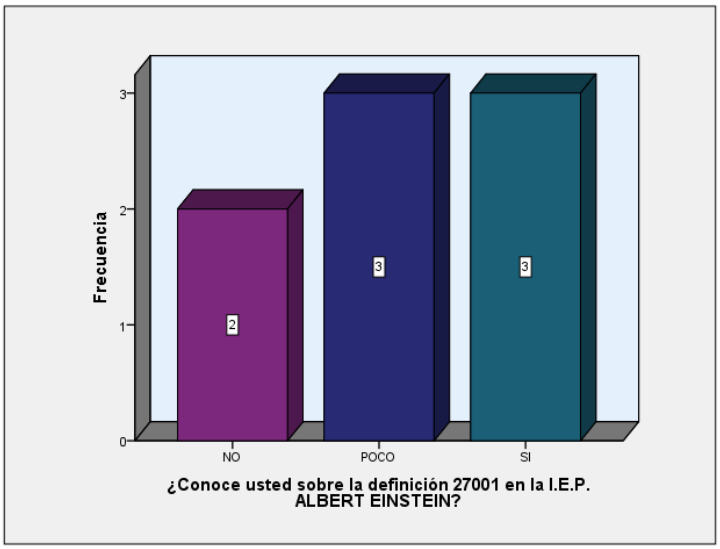
Tabla 20:

Resultados pregunta 5***.***

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	2	25,0	25,0	25,0
	POCO	3	37,5	37,5	62,5
	SI	3	37,5	37,5	100,0
	Total	8	100,0	100,0	

Figura 5:

Resultados pregunta 5.



Interpretación: En la Figura 5 nos demuestra que 6 de los 8 entrevistados conocen sobre la definición del iso 27001 en la I.E.P. Albert Einstein.

Pregunta 6: ¿Conoce usted sobre la definición de autoridades y responsabilidades 27001 en la I.E.P. ALBERT EINSTEIN?

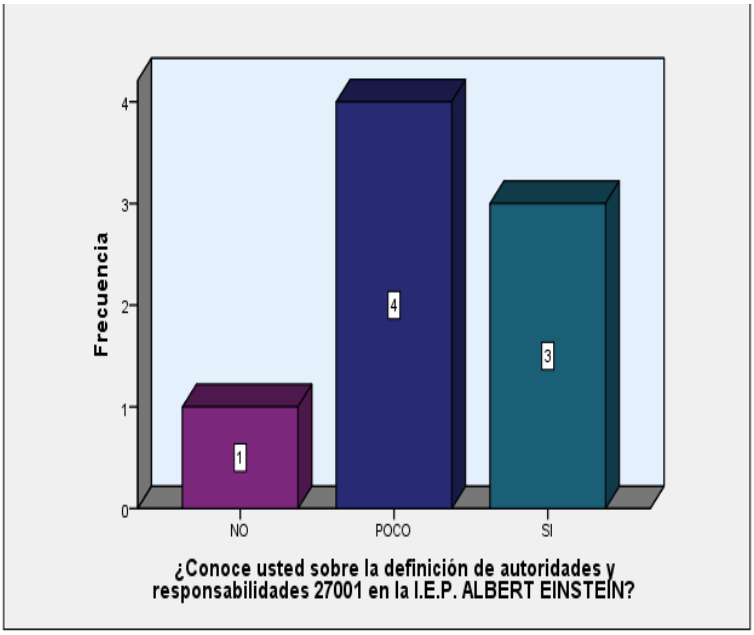
Tabla 21:

*Resultados pregunta 6***.**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	1	12,5	12,5	12,5
	POCO	4	50,0	50,0	62,5
	SI	3	37,5	37,5	100,0
	Total	8	100,0	100,0	

Figura 6:

Resultados pregunta 6.



Interpretación: En la Figura 6 nos demuestra que 4 de los 8 entrevistados conocen poco sobre la definición de autoridades y responsabilidades 27001 en la I.E.P. Albert Einstein.

Pregunta 7: ¿Conoce usted como implantar el plan de riesgo 27001 en la I.E.P. ALBERT EINSTEIN?

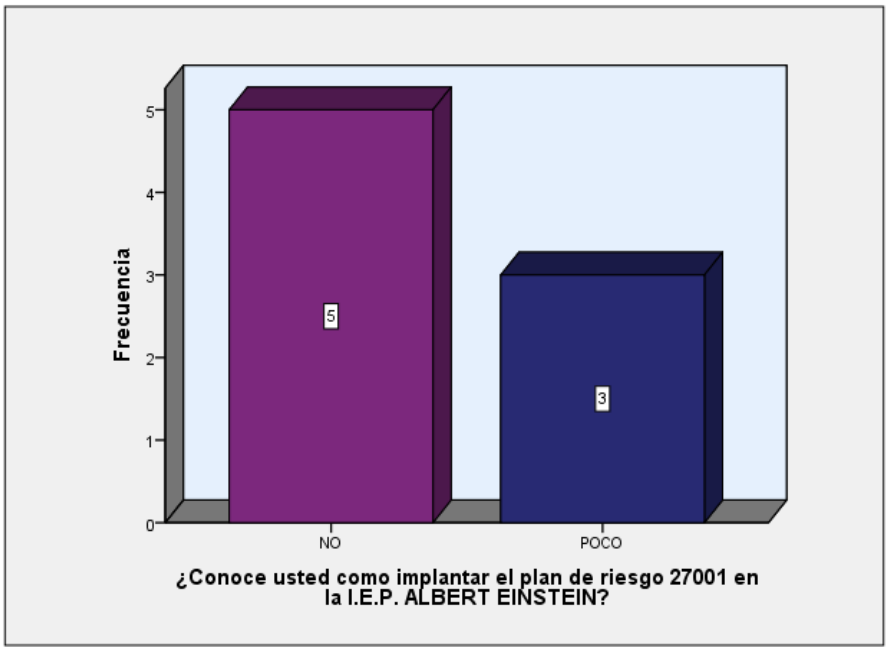
Tabla 22:

*Resultados pregunta 7***.**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	5	62,5	62,5	62,5
	POCO	3	37,5	37,5	100,0
	Total	8	100,0	100,0	

Figura 7:

Resultados pregunta 7.



Interpretación: En la Figura 7 nos demuestra que 5 de los 8 entrevistados no conocen sobre como implantar el plan de riesgo 27001 en la I.E.P. Albert Einstein.

Pregunta 8: ¿Conoce usted como implantar un SGSI (Sistema de Gestión de Seguridad de la Información) 27001 en la I.E.P. ALBERT EINSTEIN?

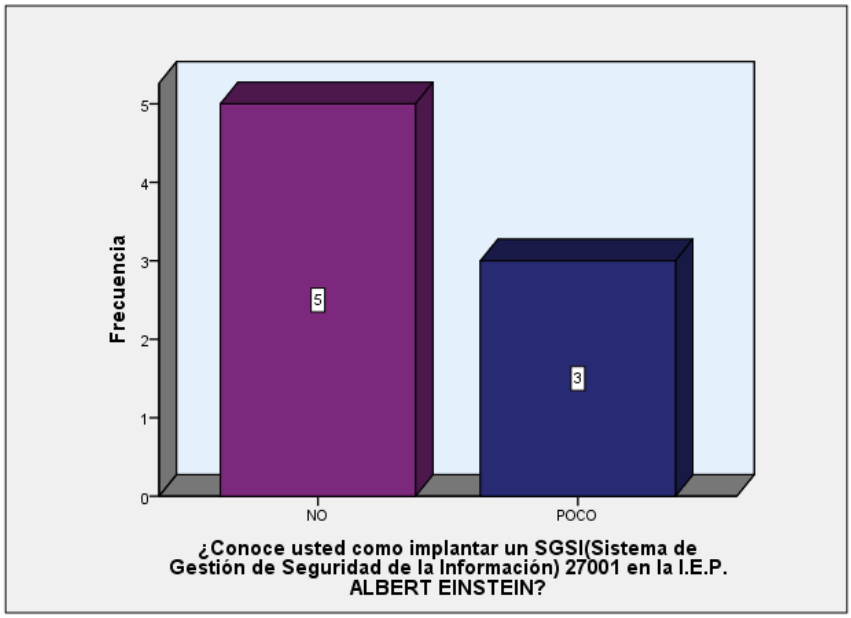
Tabla 23:

*Resultados pregunta 8***.**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	5	62,5	62,5	62,5
	POCO	3	37,5	37,5	100,0
	Total	8	100,0	100,0	

Figura 8:

Resultados pregunta 8.



Interpretación: En la Figura 8 nos demuestra que 5 de los 8 entrevistados no conocen sobre como implantar un SGSI 27001 en la I.E.P. Albert Einstein.

Pregunta 9: ¿Conoce usted como implantar controles 27001 en la I.E.P. ALBERT EINSTEIN?

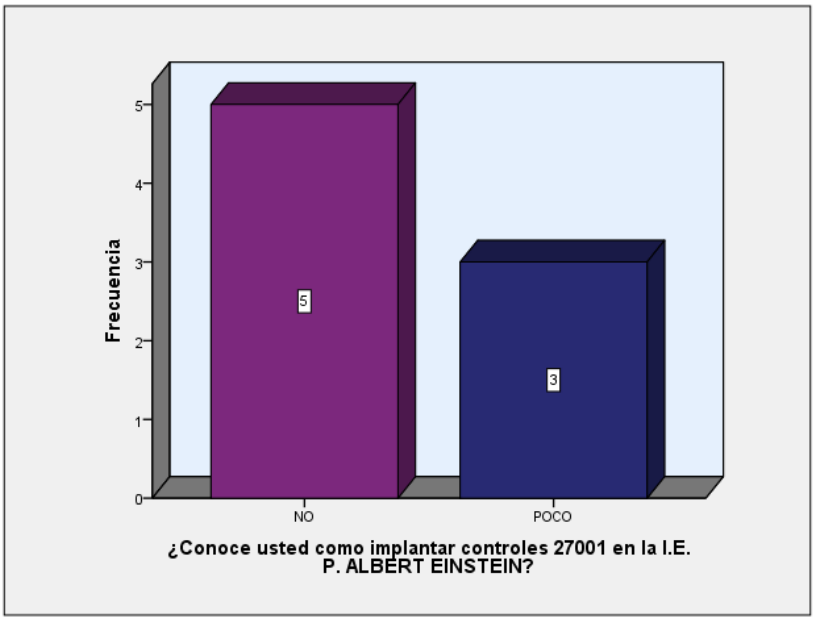
Tabla 24:

*Resultados pregunta 9***.**

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	5	62,5	62,5	62,5
	POCO	3	37,5	37,5	100,0
	Total	8	100,0	100,0	

Figura 9:

Resultados pregunta 9.



Interpretación: En la Figura 9 nos demuestra que 5 de los 8 entrevistados no conocen sobre como implantar controles 27001 en la I.E.P. Albert Einstein.

Pregunta 10: ¿Conoce usted como revisar internamente un SGSI (Sistema de Gestión de Seguridad de la Información) en la I.E.P. ALBERT EINSTEIN?

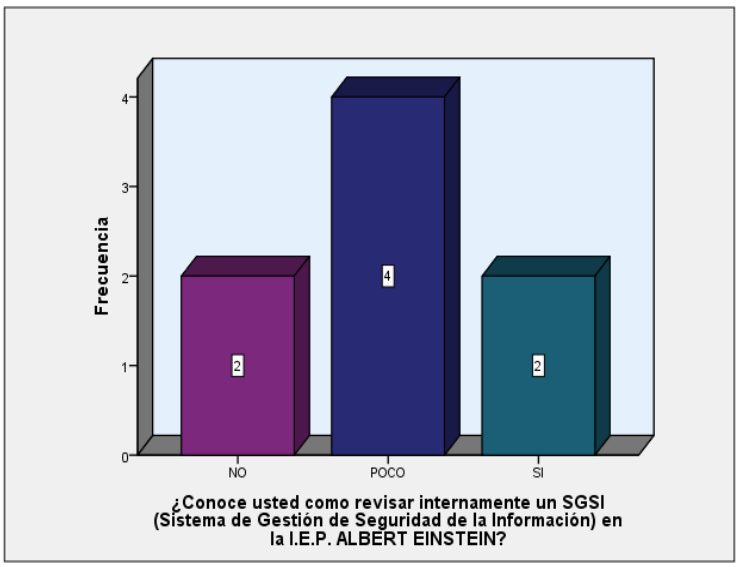
Tabla 25:

Resultados pregunta 10.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO	2	25,0	25,0	25,0
	POCO	4	50,0	50,0	75,0
	SI	2	25,0	25,0	100,0
	Total	8	100,0	100,0	

Figura 10:

Resultados pregunta 10.



Interpretación: En la Figura 10 nos demuestra que 6 de los 8 entrevistados conocen sobre como revisar internamente un SGSI en la I.E.P. Albert Einstein.

Pregunta 11: ¿Conoce usted como poner en marcha indicadores y métricas en la I.E.P. ALBERT EINSTEIN?

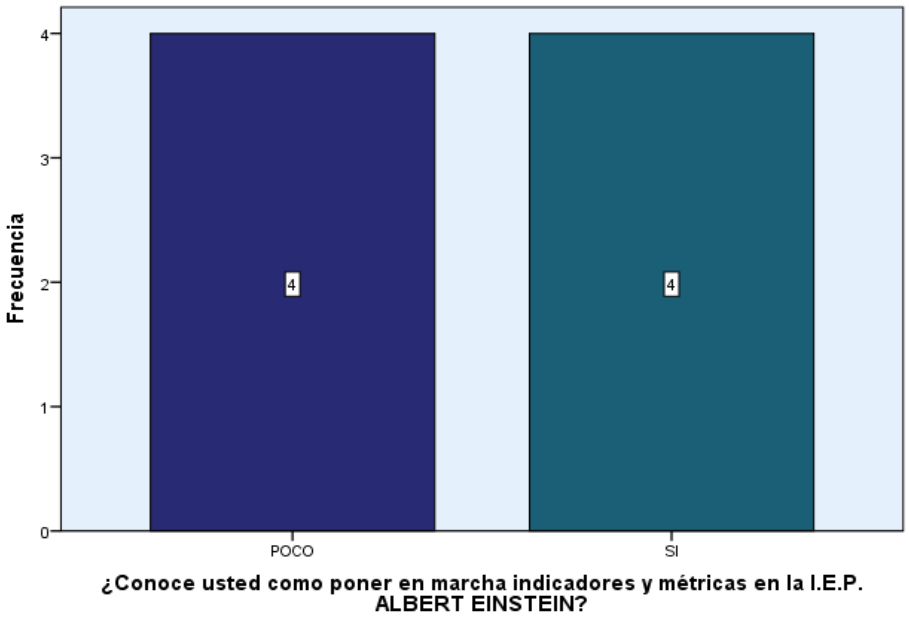
Tabla 26:

Resultados pregunta 11.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	4	50,0	50,0	50,0
	SI	4	50,0	50,0	100,0
	Total	8	100,0	100,0	

Figura 11:

Resultados pregunta 11.



Interpretación: En la Figura 11 nos demuestra que el total de entrevistados conocen sobre cómo poner en marcha indicadores y métricas en la I.E.P. Albert Einstein.

Pregunta 12: ¿Conoce usted como debe hacerse una revisión por parte de la dirección en la I.E.P. ALBERT EINSTEIN?

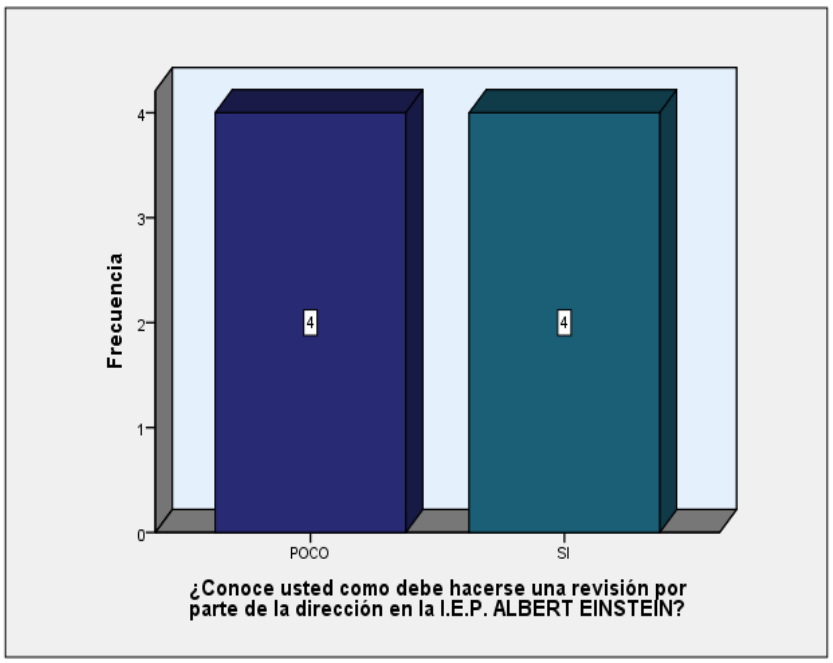
Tabla 27:

Resultados pregunta 12.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	4	50,0	50,0	50,0
	SI	4	50,0	50,0	100,0
	Total	8	100,0	100,0	

Figura 12:

Resultados pregunta 12.



Interpretación: En la Figura 12 nos demuestra que el total de entrevistados conocen sobre cómo debe hacerse una revisión por parte de la dirección en la I.E.P. Albert Einstein.

Pregunta 13: ¿Conoce usted como adoptar acciones correctivas en la I.E.P. ALBERT EINSTEIN?

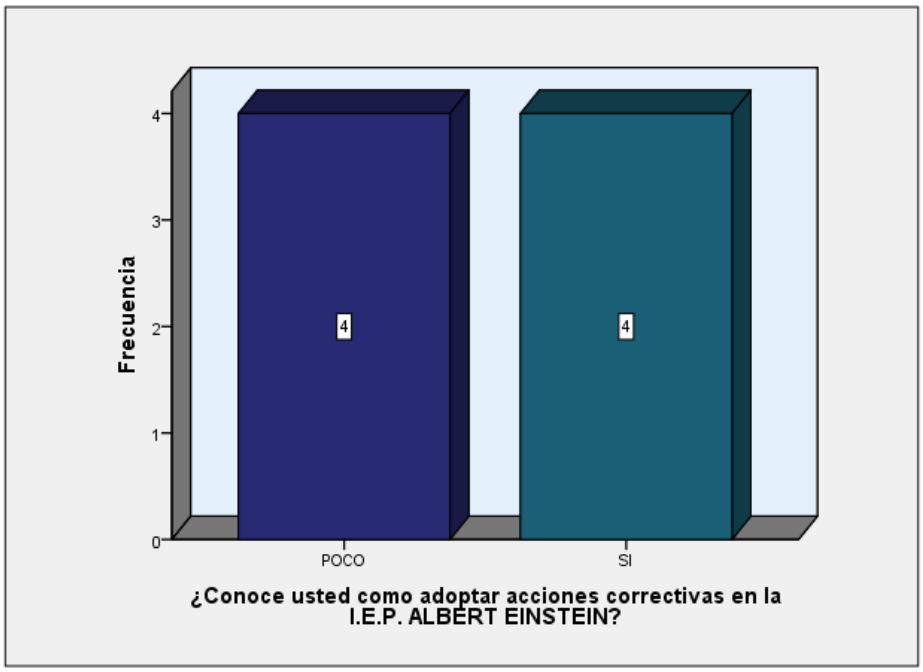
Tabla 28:

Resultados pregunta 13.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	4	50,0	50,0	50,0
	SI	4	50,0	50,0	100,0
	Total	8	100,0	100,0	

Figura 13:

Resultados pregunta 13.



Interpretación: En la Figura 13 nos demuestra que el total de entrevistados conocen sobre cómo adoptar acciones correctivas en la I.E.P. Albert Einstein.

Pregunta 14: ¿Conoce usted como adoptar acciones de mejora en la I.E.P. ALBERT EINSTEIN?

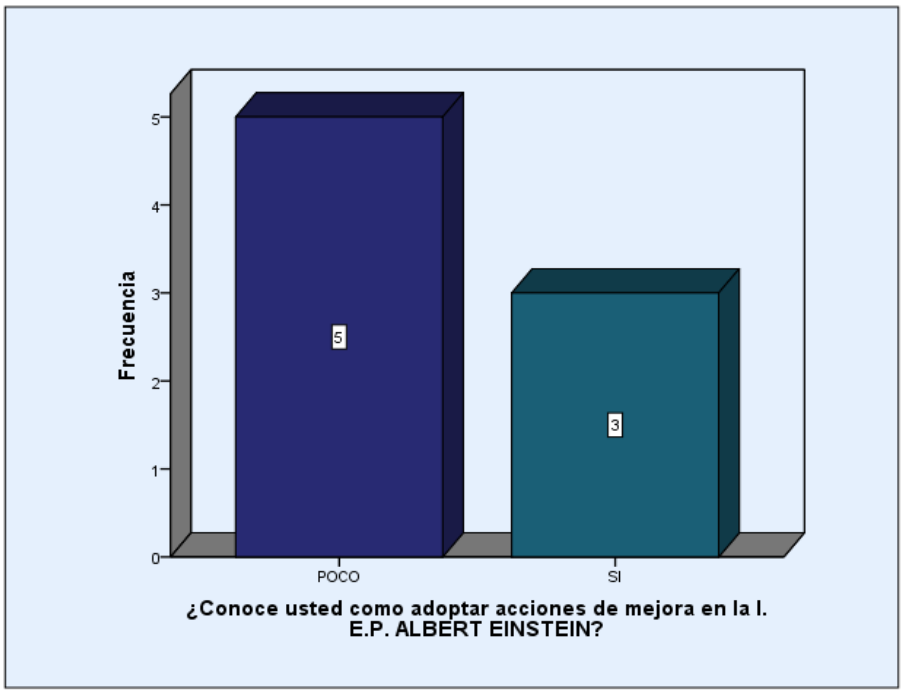
Tabla 29:

Resultados pregunta 14.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	5	62,5	62,5	62,5
	SI	3	37,5	37,5	100,0
	Total	8	100,0	100,0	

Figura 14:

Resultados pregunta 14



Interpretación: En la Figura 14 nos demuestra que el total de entrevistados conocen sobre cómo adoptar acciones de mejora en la I.E.P. Albert Einstein.

Pregunta 15: ¿Conoce usted sobre el trabajo en equipo en la I.E.P. ALBERT EINSTEIN?

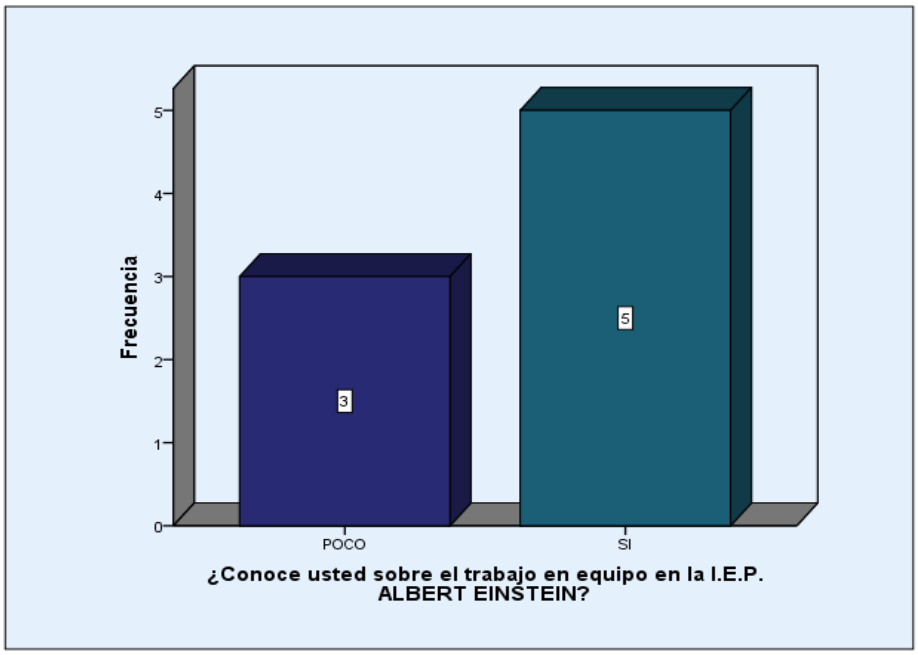
Tabla 30:

Resultados pregunta 15.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	3	37,5	37,5	37,5
	SI	5	62,5	62,5	100,0
	Total	8	100,0	100,0	

Figura 15:

Resultados pregunta 15



Interpretación: En la Figura 15 nos demuestra que 5 de los 8 entrevistados conocen sobre el trabajo en equipo en la I.E.P. Albert Einstein.

Pregunta 16: ¿Conoce usted sobre la experiencia laboral en la I.E.P. ALBERT EINSTEIN?

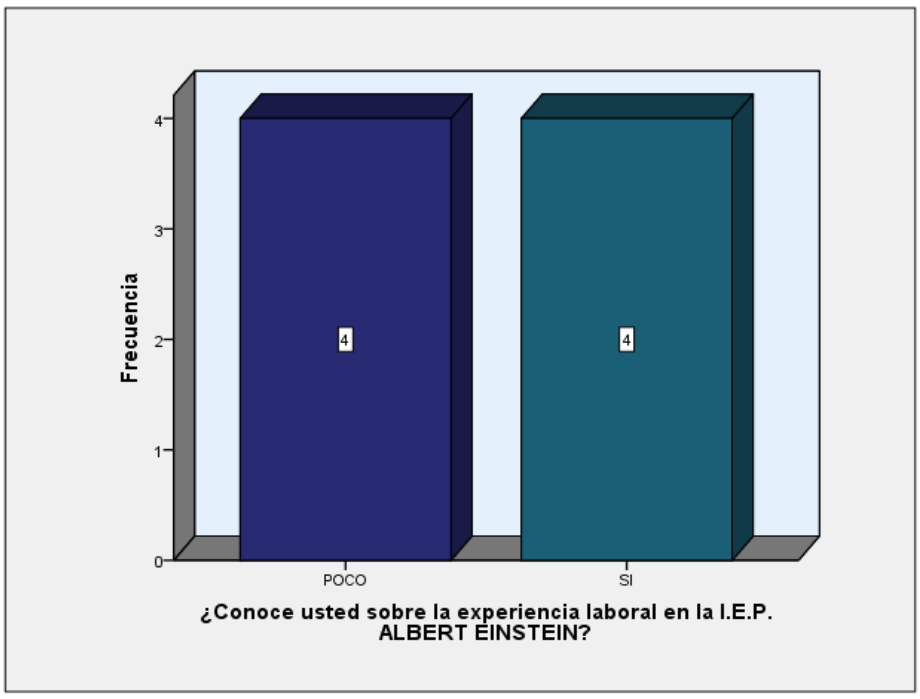
Tabla 31:

Resultados pregunta 16.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	4	50,0	50,0	50,0
	SI	4	50,0	50,0	100,0
	Total	8	100,0	100,0	

Figura 16:

Resultados pregunta 16



Interpretación: En la Figura 16 nos demuestra que el total de entrevistados tienen experiencia laboral en la I.E.P. Albert Einstein.

Pregunta 17: ¿Conoce usted sobre si existe la motivación en la I.E.P. ALBERT EINSTEIN?

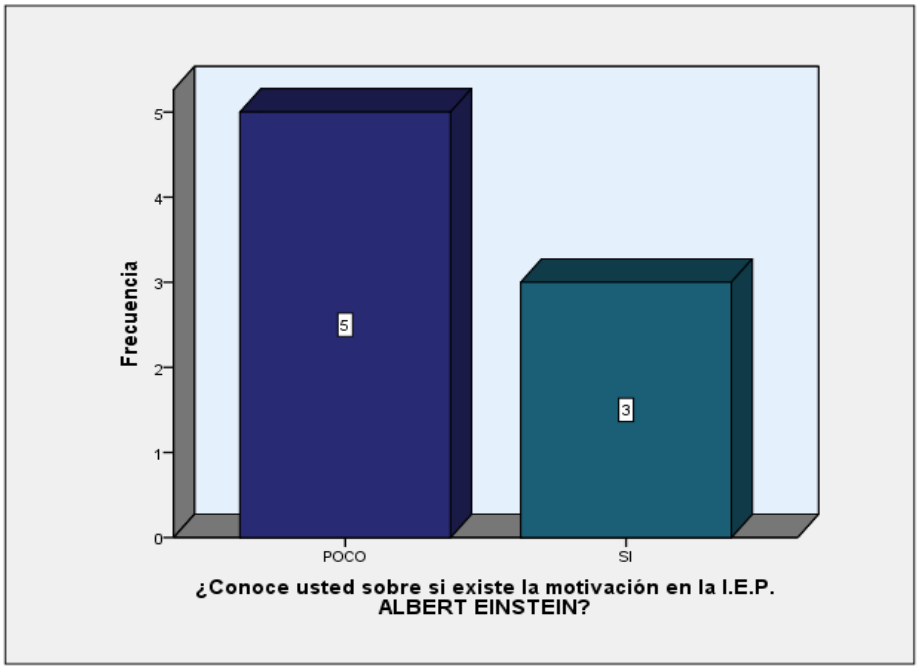
Tabla 32:

Resultados pregunta 17.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	5	62,5	62,5	62,5
	SI	3	37,5	37,5	100,0
	Total	8	100,0	100,0	

Figura 17:

Resultados pregunta 17



Interpretación: En la Figura 17 nos demuestra que el total de entrevistados conocen sobre la existencia de motivación laboral en la I.E.P. Albert Einstein.

Pregunta 18: ¿Conoce usted sobre eventos de socialización en la I.E.P. ALBERT EINSTEIN?

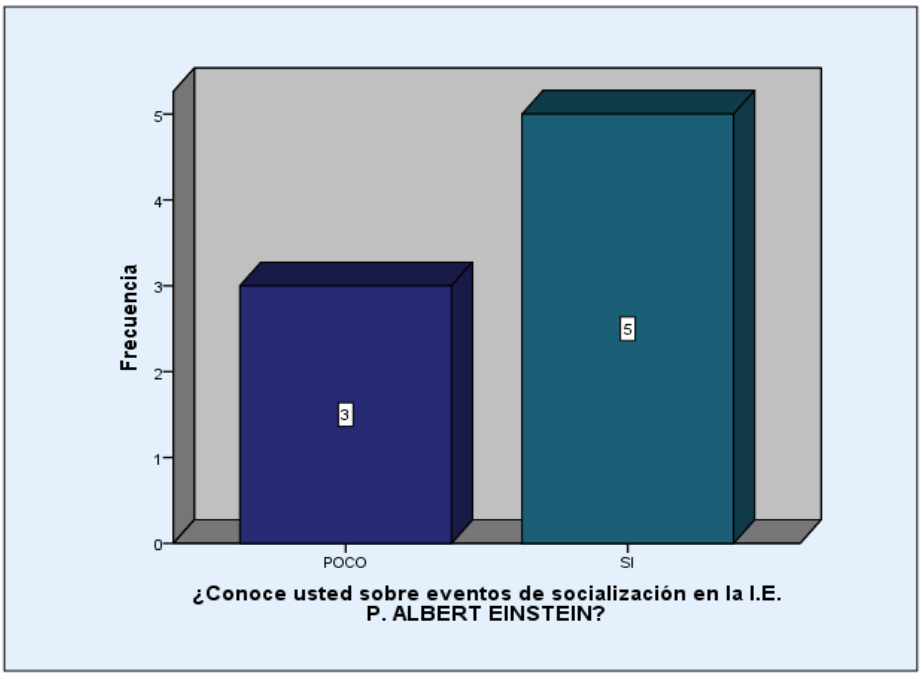
Tabla 33:

Resultados pregunta 18.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	3	37,5	37,5	37,5
	SI	5	62,5	62,5	100,0
	Total	8	100,0	100,0	

Figura 18:

Resultados pregunta 18



Interpretación: En la Figura 18 nos demuestra que el total de entrevistados conocen sobre eventos de socialización en la I.E.P. Albert Einstein.

Pregunta 19: ¿Conoce usted sobre la motivación en la I.E.P. ALBERT EINSTEIN?

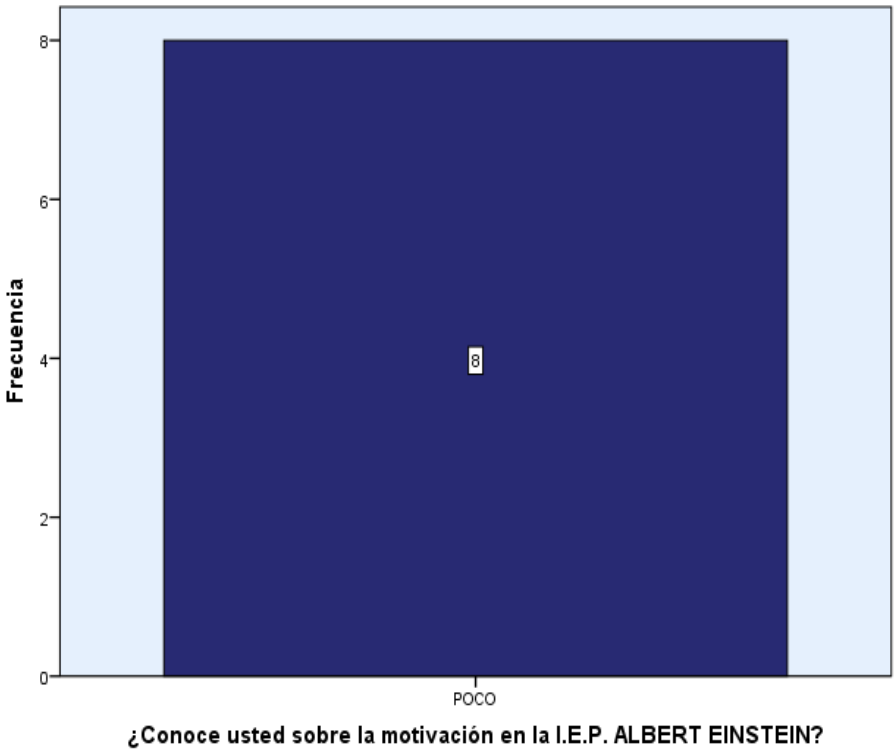
Tabla 34:

Resultados pregunta 19.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	8	100,0	100,0	100,0

Figura 19:

Resultados pregunta 19



Interpretación: En la Figura 19 nos demuestra que el total de entrevistados conocen sobre la motivación en la I.E.P. Albert Einstein.

Pregunta 20: ¿Conoce usted sobre la ética en la I.E.P. ALBERT EINSTEIN?

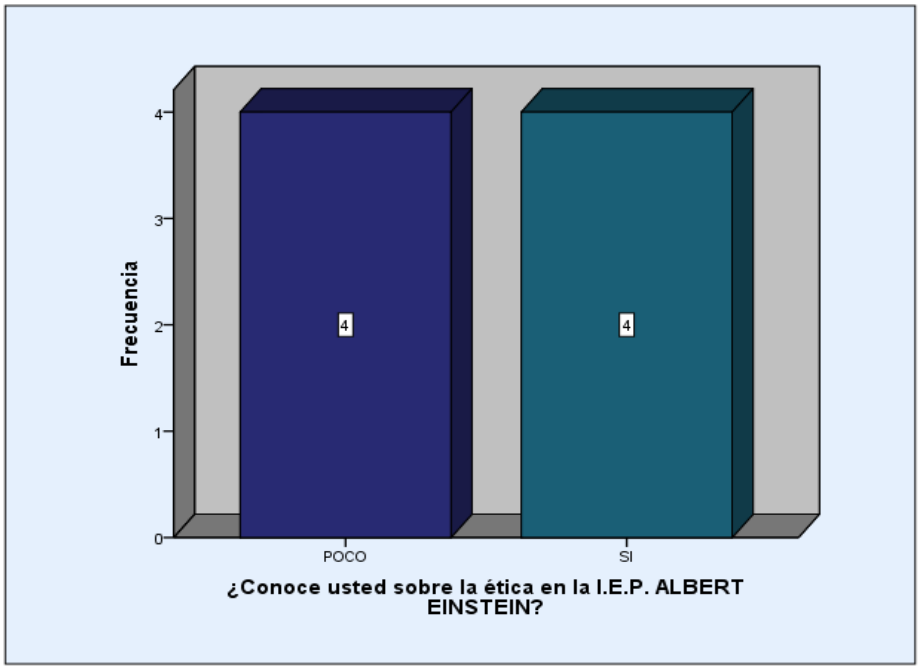
Tabla 35:

Resultados pregunta 20.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	4	50,0	50,0	50,0
	SI	4	50,0	50,0	100,0
	Total	8	100,0	100,0	

Figura 20:

Resultados pregunta 20



Interpretación: En la Figura 20 nos demuestra que el total de entrevistados conocen sobre la ética laboral en la I.E.P. Albert Einstein.

Pregunta 21: ¿Conoce usted sobre la práctica de la responsabilidad en la I.E.P. ALBERT EINSTEIN?

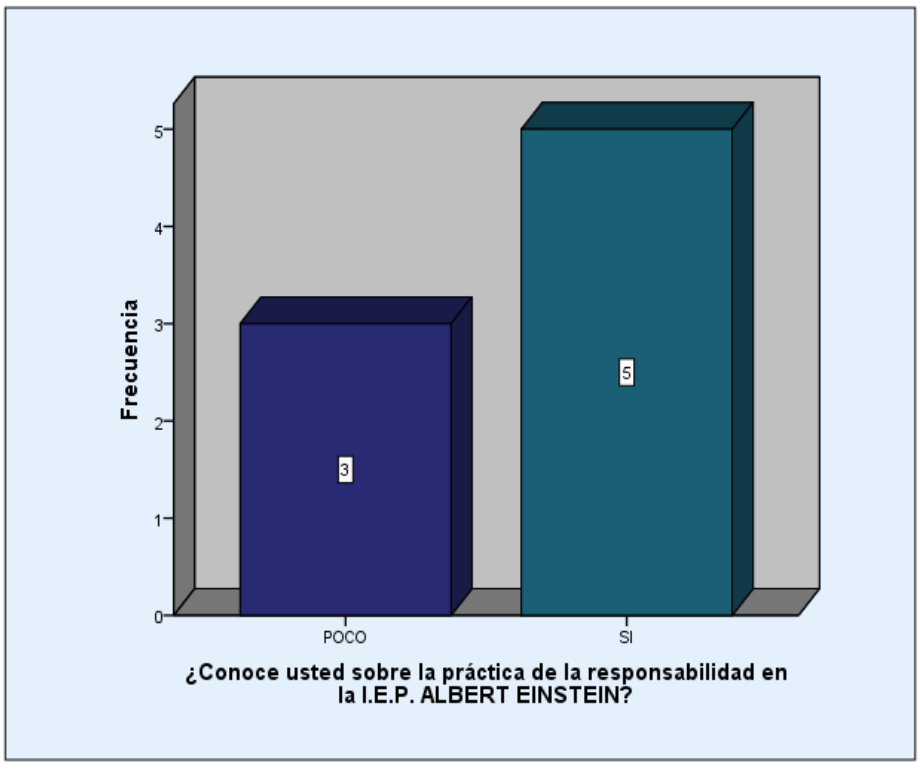
Tabla 36:

Resultados pregunta 21.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	POCO	3	37,5	37,5	37,5
	SI	5	62,5	62,5	100,0
	Total	8	100,0	100,0	

Figura 21:

Resultados pregunta 21



Interpretación: En la Figura 21 nos demuestra que el total de entrevistados conocen sobre la práctica de responsabilidad en la I.E.P. Albert Einstein.

5.2. CONTRASTACIÓN DE HIPÓTESIS

5.2.1. Enfoque de la hipótesis

General

"Desarrollo positivo de un sistema de gestión de seguridad de información en la calidad de procesos en la I.E.P. Albert Einstein."

Secundarias

1. "Aplicación es positiva entre la aplicación y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein."
2. "Aplicación es positiva entre lo que se debe hacer y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein."
3. "Aplicación es positiva entre el control y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein."
4. "Aplicación es positiva entre la forma de actuar y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein

5.2.2. Suposición de la prueba de hipótesis

- La existencia de una variable dependiente en el presente proyecto es "Calidad de Procesos" en la I.E.P. Albert Einstein.
- La existencia de una variable independiente que es el "Sistema de Gestión de Seguridad de la Información"

- Se utilizó un 95% de nivel de confiabilidad y un 5% de nivel de significancia.
- La hipótesis nula Ho es una negación de la relación que existe entre la variable independiente y la variable dependiente.
- La hipótesis Ha es la afirmación de la relación que existe entre la variable independiente y dependiente.

5.2.3. Cálculo del valor crítico e función de prueba

Hipótesis General:

Ho: No existe el desarrollo positivo de un sistema de gestión de seguridad de la información en la calidad de procesos en la I.E.P. Albert Einstein.

Ha: Existe el desarrollo positivo de un sistema de gestión de seguridad de la información en la calidad de procesos en la I.E.P. Albert Einstein.

Para esta prueba de hipótesis se tomó como base los indicadores para obtener el coeficiente de relación por el método de Pearson.

Tabla 37:

Correlación de Hipótesis General.

		VARDEP	VARIND
Correlación de	VARDEP	1,000	,409
Pearson	VARIND	,409	1,000
Sig. (unilateral)	VARDEP	.	,310
	VARIND	,310	.
N	VARDEP	8	8
	VARIND	8	8

De la tabla N° 32 después de aplicar la estadística de correlación de Pearson se pudo obtener un coeficiente de correlación positiva y moderada de 0.409, entre la Calidad de Procesos y Sistema de Gestión de Seguridad de la Información, con un nivel de significancia p<0.001, así: (p=0.409; p< 0.001). lo que indica que conforme aumenta la utilización de un Sistema de Gestión de Seguridad de la Información, la Calidad de Procesos también aumenta de forma moderada, y con un nivel de significancia inferior a 0.05 se descarta la **Ho** y se concluye que es posible medir el grado de correlación entre el Sistema de Gestión de Seguridad de la Información y la Calidad de Procesos de I.E.P. Albert Einstein.

Hipótesis especifica N° 1

Ho: La aplicación no es positiva entre la aplicación y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein.

Ha: La aplicación es positiva entre la aplicación y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein.

Tabla 38:

Correlación de hipótesis especifica N° 1.

		VARDEP	VARDEPDIM1
Correlación de Pearson	VARDEP	1,000	,958
	VARDEPDIM1	,958	1,000
Sig. (unilateral)	VARDEP	.	,000
	VARDEPDIM1	,000	.
N	VARDEP	8	8
	VARDEPDIM1	8	8

Del análisis de la tabla N° 33, se concluye que el conocimiento generado por un SGSI influye significativamente en la calidad de procesos en la empresa.

Hipótesis especifica N° 2

Ho: La aplicación no es positiva entre lo que se debe hacer y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein.

Ha: La aplicación es positiva entre lo que se debe hacer y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein.

Tabla 39:

Correlación de hipótesis especifica N° 2.

		VARDEP	VARDEPDIM2
Correlación de Pearson	VARDEP	1,000	,951
	VARDEPDIM2	,951	1,000
Sig. (unilateral)	VARDEP	.	,000
	VARDEPDIM2	,000	.
N	VARDEP	8	8
	VARDEPDIM2	8	8

Con lo plasmado en la tabla N°34 presentada en la prueba de hipótesis, se obtiene que la Ha donde se afirma que el valor del conocimiento de un Sistema de Gestión de Seguridad de la Información define significativamente en la Calidad de Procesos en la I.E.P. Albert Einstein.

Hipótesis especifica N° 3

Ho: La aplicación no es positiva entre el control y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein.

Ha: La aplicación es positiva entre el control y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein.

Tabla 40:

Correlación de hipótesis especifica N° 3.

		VARDEP	VARDEPDIM3
Correlación de Pearson	VARDEP	1,000	,639
	VARDEPDIM3	,639	1,000
Sig. (unilateral)	VARDEP	.	,044
	VARDEPDIM3	,044	.
N	VARDEP	8	8
	VARDEPDIM3	8	8

La tabla Nº 35 plasma lo realizado en la presente investigación la cual identifica como positiva la gestión del conocimiento que se deriva de un Sistema de Gestión de Seguridad de la Información en la Calidad de Procesos en la I.E.P. Albert Einstein.

Hipótesis especifica N° 4

Ho: La aplicación no es positiva entre la forma de actuar y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein.

Ha: La aplicación es positiva entre la forma de actuar y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos en la I.E.P. Albert Einstein.

Tabla 41:

Correlación de hipótesis especifica N° 4.

		VARDEP	VARDEPDIM4
Correlación de Pearson	VARDEP	1,000	,456
	VARDEPDIM4	,456	1,000
Sig. (unilateral)	VARDEP	.	,128
	VARDEPDIM4	,128	.
N	VARDEP	8	8
	VARDEPDIM4	8	8

De la tabla N° 36 determina que el modelo de gestión, determina significativamente en la toma de Calidad de Procesos, por lo tanto, se rechaza la hipótesis Ho y se acepta la Ha.

5.3. DISCUSIÓN DE RESULTADOS

Como menciona Mayorga, Franklin la importancia radica en los dominios de seguridad que lo conforman, entre ellos políticas de seguridad, administración de activos, seguridad de los recursos humanos, sistema de control de accesos. En la investigación se pudo obtener un coeficiente de correlación positiva y moderada de 0.409, entre la Calidad de Procesos y Sistema de Gestión de Seguridad de la Información, con un nivel de significancia p<0.001, así: (p=0.409; p< 0.001). lo que indica que conforme aumenta la utilización de un sistema de gestión de seguridad de la información, la calidad de procesos.

También **(Agurto Huanca, 2018)** aporta que en la actualidad todas las empresas deben de contar un con un Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST), puesto que este sistema ayudará a la organización mantenerse constantemente actualizado con las legislaciones vigentes, además que permitirá una participación activa entre los trabajadores y el empleador, reducirá el índice de accidentabilidad y lo más importante es que generará una Cultura de Seguridad en el Trabajador. En la presente investigación se pudo obtener un coeficiente de correlación positiva y moderada de 0.409, entre la Calidad de Procesos y Sistema de Gestión de Seguridad de la Información, con un nivel de significancia p<0.001, así: (p=0.409; p< 0.001). lo que indica que conforme aumenta la utilización de un Sistema de Gestión de Seguridad de la Información, la Calidad de Procesos también aumenta de forma moderada, y con un nivel de significancia inferior a 0.05.

Por otra parte Warton Tapia refiereque toda la implementación se encuentra dentro de un marco de mejora continua, si hubiera cambios, o implementación de nuevos procesos este sistema al ser cíclico llamara a realizar un análisis previo para de nuevo establecer los nuevos controles y es lo que recomendamos periódicamente la asesoría de consultores de seguridad de la información, con el fin de mejorar continuamente los procesos de la I.E.P. Albert Einstein.

CONCLUSIONES

- Se mejora en un 60% la seguridad de la información y los activos de la información en la I.E.P. Albert Einstein, mediante la propuesta de desarrollo de un Sistema de Gestión de Seguridad de la Información.

- Para evaluar el desarrollo de la planificación se utilizó la unión de la Metodología PDCA y Magerit, lo cual permite desarrollar la propuesta de un Sistema de Gestión de Seguridad de la Información.

- La calidad de los procesos en un Sistema de Gestión de Seguridad de la Información se desarrolla por la capacitación constante de los trabajadores administrativos en los temas de seguridad, logrando esto disminuir el índice de pérdida de información en las diferentes áreas administrativas de la Institución.

- Para el desarrollo del control en un Sistema de Gestión de Seguridad de la Información se establece y supervisa los niveles de accesibilidad, logrando la implementación de niveles de seguridad.

- La forma de actuar del Sistema de Gestión de Seguridad de la Información emplea normas relacionados a la seguridad para lograr una adecuada implementación en los procesos de la I.E.P. Albert Einstein.

RECOMENDACIONES

- Planificar reuniones constantes entre el equipo de administrativo y la alta gerencia para analizar el desempeño del SGSI.

- Contratación de periódica de asesoría de consultores de seguridad de la información, con el fin de mejorar continuamente los procesos de la I.E.P. Albert Einstein.

- Investigar e implantar nuevos controles de seguridad en los diferentes procesos de seguridad de la información.

- Mantener simulacros internos, lo cual servirá para brindar una mejor capacitación y entrenamiento personal.

REFERENCIAS BIBLIOGRAFICAS

27001, N.-I. (2005). *NORMA TECNICA PERUANA.*

Acosta Contreras, L. (2017). *Diseño del sistema de gestión de seguridad de la información (SGSI) en la secretaría de hacienda del municipio de Cucunubá Cundinamarca bajo norma ISO 27001.* Colombia: Universidad Piloto de Colombia.

AGUIRRE MOLLEHUANCA, D. A. (2014). *DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA SERVICIOS POSTALES DEL PERU S.A.* LIMA: PONTIFICA UNIVERSIDAD CATOLICA DEL PERU.

Agurto Huanca, J. (2018). *Sistema de gestión de seguridad y salud en el trabajo para reducir los accidentes laborales en una empresa de servicios generales, Lurín, 2017.* Lima: Universidad Cesar Vallejo.

ALCÁNTARA FLORES, J. C. (2015). *GUÍA DE IMPLEMENTACIÓN DE LA SEGURIDAD BASADO EN LANORMA ISO/IEC 27001, PARA APOYAR LA SEGURIDAD EN LOS .* CHICLAYO: UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO.

Aldana de la Vega, L. Á., & RamÍrez Cuéllar, C. (2011). *DISEÑO DE UN MODELO DE GESTION DE CALIDAD PARA LOS PROCESOS ADMINISTRATIVOS - FINANCIEROS DE EL JARDIN INFANTIL TALLER DE ARTE ARCO IRIS.* Chía: Universidad de La Sabana.

Alexander, & otros. (2007).

ARÉVALO ARELLANO, P. J. (2017). *GESTIÓN ADMINISTRATIVA Y CALIDAD DE PROCESOS DEL ÁREA DE INFRAESTRUCTURA DE LA MUNICIPALIDAD DISTRITAL DE MORALES, 2017.* TARAPOTO: UNIVERSIDAD CESAR VALLEJO.

Arias, F. G. (2012). *EL PROYECTO DE INVESTIGACION.* CARACAS: EPISTEME, C.A.

Arias, F. G. (2012). *El Proyecto de Investigación - Introducción a la metodología científica.* Caracas - Venezuela: Editorial EPISTEME, C.A.

BARRANTES. (2008). *metodo aplicativo.* barrantes: barrantes.

CALDERÓN POZO, F. G. (2014). *DIAGNOSTICO Y PROPUESAT DE MEJORA DEL PROCESO DE CONTROL DE LA CALIDAD EN UNA EMPRESA QUE ELABORA ACEITES LUBRICANTES AUTOMOTRICES E INDUSTRIALES UTILIZANDO HERRAMIENTAS Y TECNICASS DE LA CALIDAD.* LIMA: PONTIFICA UNIVERSIDAD CATOLICA DEL PERU.

Cruz Diaz, M. (2017). *Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la Clínica MEDCAM Perú SAC.* Lima: Universidad San Martin de Porras.

CRUZ DIAZ, M. A., & FUKUSAKI INFANTAS, S. (2017). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM PERÚ SAC .* LIMA: UNIVERSIDA SAN MARTIN DE PORRES.

Daltabuit, E., & otros. (2007).

DAZA GÓMEZ, J. E., & FÉRNANDEZ VACA, C. (2013). *IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE CALIDAD PARA LOS PROCESOS PRODUCTIVOS EN LA COMPAÑIA INDUSTRIAS CRUZ HNOS. S.A.* COLOMBIA - BOGOTA: UNIVERSIDAD LIBRE.

Del Carpio. (2006).

DORIA, A. (2014). *RIESGOS Y CONTROL.*

DORIA, A. (2015). *DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION MEDIANTE LA APLICACION DE LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN LA*

OFICINA DE SISTEMAS DE INFORMACION Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE CÓRDOBA. CÓRDOBA: UNIVERSIDAD DE CÓRDOBA.

Elizondo, R. (2016). *Informatica 1 - Serie integral por competencias.* Mexico: Grupo Editorial Patria, S.A de C.V. Obtenido de https://books.google.com.pe/books?id=2BQhDgAAQBAJ&printsec=frontcover#v=onepage&q&f=false

GARCIA GUEVARA, C. A. (2012). *ESTABLECIMIENTO DEL SISTEMA DE SEGURIDAD DE INFORMACION EN SFG BAJO LOS ESTANDARES DE LA NORMA ISO 27001:2005.* BOGOTA: UNIVERSIDAD EAN.

GONZALEZ GARCIA, F. A., & TORRES ROMERO, O. (2016). *ESTANDARIZACIÓN DE PROCESOS EN EL COLEGIO AMERICANO MENNO LA MESA.* BOGOTÁ: UNIVERSIDAD LIBRE.

GUAMAN SEIS, J. A. (2017). *DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA EL DEPARTAMENTO DE INFORMATICA DE LA DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES DEL COMANDO CONJUNTO DE LAS FF.AA. UTILIZANDO LA NORMA ISO 27001.* ECUADOR - GUAYAQUIL: ESCUELA SUPERIOR POLITECNICA DEL LITORAL.

GUARNIZO ARIAS, J. E., & PRIETO SARMIENTO, E. J. (2016). *DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) PARA LA EMPRESA AGILITY S.A.S.* BOGOTA: UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS.

GUEVARA SUAREZ, V. H. (2014). *ESTANDARIZACIÓN DE LOS PROCESOS, PROCEDIMIENTOS Y DISEÑO DEL MANUAL DE DESCRIPCIÓN DE CARGOS - PROCEOS DE APOYO DE LA EMPRESA JCT EMPRESARIAL.* COLOMBIA - SANTIAGO DE CALI: UNIVERSIDAD DEL VALLE.

GUZMAN VILLENA, A. (2006). *MÉTODO INDUCTIVO.*

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodologia de la Investigacion.* México D.F: McGRAW - HILL.

IBM. (2014).

INSTITUTE, P. M. (2013). *Guía de los fundamentos para la dirección de proyectos.* Pensilvania: 5ta. ed. Pensilvania 2013.

IRAM. (2010). *Instituto Argentino de Normalización y Certificación*. Obtenido de Instituto Argentino de Normalización y Certificación: https://www.iram.org.ar/

ISO9001. (2014). *ENTENDIENDO EL ENFOQUE BASADO EN PROCESOS.* ESPAÑA: NORMAS ISO 9001.

JUSTINO SALINAS, Z. I. (2015). *DISEÑO DE UN SISTEMA DE GESTION DE INFORMACION PARA UNA EMPRESA INMOBILIARIA ALINEDO A LA NORMA ISO/IEC 27001.* LIMA: PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU.

Kwell. (2008).

Laudon , K. C., & Laudon , J. P. (2012). *Sistemas de informacion gerencial* (Decimo segunda ed.). Mexico: PEARSON EDUCACIÓN. Obtenido de https://juanantonioleonlopez.files.wordpress.com/2017/08/sistemas-de-informacic3b3n-gerencial-12va-edicic3b3n-kenneth-c-laudon.pdf

LAUDON, K. C., & LAUDON, J. P. (2012). *Sistemas de Información Gerencial.* Mexico: PEARSON EDUCACIÓN.

López Crespo, F., Amutio Gómez, A. M., Candau, J., & Mañas , J. A. (2006). *MAGERIT - VERSION2 METODOLOGIA DE ANALISIS Y GESTION DE RIESGOS DE LOS SISTEMAS DE INFORMACION - METODO I.* MADRID-ESPAÑA: MINISTERIO DE ADMINISTRACION PUBLICA.

LOZA MOLINA, C. A. (2017). *PROPUESTA DE MEJORA EN LOS PROCESOS DE ABASTECIMIENTO, ALMACEN Y PRODUCCION EN UNA EMPRESA METALMECANICA.* LIMA: UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS.

Márquez Cordeiro, J. V., & Galvis Galantini, W. K. (2011). *PROPUESTA DE UN PLAN DE LA CALIDAD PARA LA IMPLEMENTACION DEL SISTEMA DE GESTION DE LA CALIDAD DEL PROCESO "TRANSMITIR ENERGIA ELECTRICA" DE ELECTRIFICACION DEL CARONÍ, C.A.* Puerto Ordaz: Universidad Católica Andrés Bello.

Martínez Ramos, J. (2014). *SISTEMA DE GESTION PARA MEJORAR LA SEGURIDAD DE LA INFORMACION EN LA INSTITUCION SERVICIOS INDUSTRIALES DE LA MARINA.* CHIMBOTE-PERU: UNIVERSIDAD NACIONAL DEL SANTA.

Mayorga Mayorga, F. (2017). *Sistema de Gestión de Seguridad de la información basado en la Norma ISO/IEC 27001 para el Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación.* Ecuador: Universidad Tecnica de Ambato.

Méndez Álvarez, C. E. (2011). *Metodología.* Mexico D.F. - Mexico: Limusa.

Microsoft. (2017).

Moguel. (2005).

MORA CACHO, C. N. (2013). *PROPUESTA DE MEJORA DE PROCESOS DE CONTROL DE CALIDAD EN LA FABRICACIÓN DE TUBOS DE ACERO ESTRUCTURALES EN UNA EMPRESA METALMECÁNICA.* LIMA: UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS.

Muñoz. (2014).

NTP-ISO 27001. (2005). *NORMA TECNICA PERUANA.*

ORTIZ REINOSO, D. Y. (2015). *IMPLEMENTACION DE UN SISTEMA DE GESTION DE CALIDAD DE ISO 27001:2005, PARA APLICAR CONTROLES A LOS ACTIVOS DE UNA ORGANIZACION.* ECUADOR - GUAYAQUIL: ESCUELA SUPERIOR POLITECNICA DEL LITORAL.

Pérez Porto, J., & Gardey, A. (2012). *Definicion de Eficiencia.*

Serrano, G. P. (2000). *Modelos de la Investigacion cualitativa.* Narcea ediciones.

Soto, L. (2007).

Tamayo y Tamayo, M. (2015). *El proceso de la investigación científica.* Mexico D.F. - Mexico: Limusa, Editorial.

Tamayo y Tamayo, M. (2015). *El proceso de la investigación científica.* Mexico D.F. - Mexico: Limusa, Editorial.

Tamayo, & tamayo. (2015).

TAMAYO, A. (2001). *AUDITORIA EN SISTEMAS: UNA VISION PRACTICA.*

TARRILLO CLAVO, E. A., & CORREA CUBAS, J. C. (2015). *METODOLOGIA PARA UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA TECNICA PERUANA NTP - 17799 EN LA ADMINISTRACION DE LA MUNICIPALIDAD DISTRITAL DE LAMBAYEQUE SETIEMBRE 2013 - FERBRERO 2014.* LAMBAYEQUE: UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO.

TOLA FRANCO, D. E. (2015). *IMPLEMENTACION DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA EMPRESA DE CONSULTORIA Y AUDITORIA, APLICANDO LA NORMA ISO 27001.* ECUADOR - GUAYAQUIL: ESCUELA SUPERIOR POLITECNICA DEL LITORAL.

VÍLCHEZ ESPINAL, J. L. (2016). *PROPUESTA DE MEJORA DE CALIDAD EN LOS PROCESOS PARA LA FABRICACIÓN DE CALDERAS A VAPO EN UNA EMPRESA DEL SECTOR METALMECÁNICA.* LIMA: UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS.

Warton Tapia, O. (2018). *Implementación de un sistema de gestión de seguridad y salud ocupacional en la empresa Panoro Apurímac.* Apurimac.

Yáñez Cáceres, N. (2017). *Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño.* Universidad de Chile.

ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA SISTÉMICA

FORMULACION DEL PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES, DIMENSIONES E INDICADORES	METODOLOGIA DE LA INVESTIGACIÓN
¿Cómo desarrollar un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein? a) ¿Cómo desarrollar la planificación en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein? b) ¿Cómo desarrollar lo que se debe hacer en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein? c) ¿Cómo desarrollar el control en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein? d) ¿Cómo desarrollar la forma de actuar en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein?	Establecer el desarrollo de un sistema de gestión de seguridad de información en la calidad de procesos para la I.E.P. Albert Einstein. a) Evaluar el desarrollo de la planificación en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein. b) Definir el desarrollo de lo que se debe hacer Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein. c) Precisar el desarrollo del control en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein. d) Especificar el desarrollo de la forma de actuar en un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein.	Existe el desarrollo positivo de un sistema de gestión de seguridad de información en la calidad de procesos para la I.E.P. Albert Einstein. a) La aplicación es positiva entre la aplicación y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein. b) La aplicación es positiva entre lo que se debe hacer y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein. c) La aplicación es positiva entre el control y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein. e) La aplicación es positiva entre la forma de actuar y un Sistema de Gestión de Seguridad de la Información en la calidad de procesos para la I.E.P. Albert Einstein	VARIABLE 1: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DIMENSIÓN: PLANIFICAR ➢ Política de administración. ➢ Alcance del ISO 27001. ➢ Análisis de riesgos. ➢ Seleccionar los riesgos. ➢ Definir competencias. ➢ Definir autoridades y Responsabilidades. DIMENSIÓN: HACER ➢ Implantar el plan de administración de riesgos. ➢ Implantar el SGSI. ➢ Implantar los controles. DIMENSIÓN: CONTROL ➢ Revisar internamente el SGSI. ➢ Poner en marcha indicadores y métricas. ➢ Hacer una revisión por parte de la Dirección. DIMENSIÓN: ACTUAR ➢ Adoptar acciones correctivas. ➢ Adoptar acciones de mejora. VARIABLE 2: CALIDAD DE PROCESOS DIMENSION SUBSISTEMA DE AUDITORIA ➢ Trabajo en Equipo ➢ Experiencia laboral ➢ Motivación intrínseca ➢ Eventos sociales ➢ Motivación por áreas ➢ Ética ➢ Responsabilidad	**TIPO DE APLICACIÓN** APLICADA **NIVEL DE INVESTIGACIÓN** DESCRIPTIVA **POBLACIÓN** Estará conformado por el personal administrativo de la I.E.P. ALBERT EINSTEIN que en total existe 08 trabajadores. **MUESTRA** Se encuentra conformado por el personal administrativo de la I.E.P. ALBERT EINSTEIN, siendo necesaria para la investigación 08 personas, considerando que la población es menor de 30 personas, aplicaremos la muestra no probabilística. **DISEÑO DE LA INVESTIGACIÓN** Pre Test – Post Test M: **O_(1) → x → O_(2)** **TÉCNICAS** • Encuesta • Análisis Documental **INSTRUMENTOS** **SOFTWARE PARA PROCESAR DATOS:** SPSS FUENTES / TÉCNICAS / HERRAMIENTAS PRIMARIA / ENCUESTA / CUESTIONARIO SECUNDARIA / ANALISIS DOCUMENTAL / RESUMEN DE AUTORES

ANEXO 2: OPERACIONALIZACIÓN DE VARIABLES

VARIABLES	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTOS
SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN	Es una solución de mejora continua basada a la cual puede desarrollarse un Sistema de Gestión de Seguridad de Información (SGSI) y la administración de la seguridad del sistema de información (ASSI) que permite evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros. (la norma ISO 27001 en la implantación de un SGSI: aspectos claves de su diseño e implantación)	Está comprendida por los pasos planteados en el ciclo PDCA del ISO 27001: (P) PLANIFICAR (D) HACER (C) CONTROLAR (A) ACTUAR	PLANIFICAR	➢ Política de administración. ➢ Alcance del ISO 27001. ➢ Análisis de riesgos. ➢ Seleccionar los riesgos. ➢ Definir competencias. ➢ Definir autoridades y responsabilidades.	**CUESTIONARIO**
			HACER	➢ Implantar el plan de administración de riesgos. ➢ Implantar el SGSI. ➢ Implantar los controles.	
			CONTROLAR	➢ Revisar internamente el SGSI. ➢ Poner en marcha indicadores y métricas. ➢ Hacer una revisión por parte de la Dirección.	**GUIA DE OBSERVACION**
			ACTUAR	➢ Adoptar acciones correctivas. ➢ Adoptar acciones de mejora.	
CALIDAD DE PROCESOS	La Calidad puede tener varios significados, dos de los cuales son muy importantes para la empresa, ya que estos sirven para planificar la calidad y la estrategia empresarial. Por calidad se entiende como la ausencia de deficiencias que pueden presentarse como: retraso en la entrega, fallos durante los servicios, facturas incorrectas, cancelación de contratos de ventas, etc. Calidad es adecuarse al uso.("control de calidad "Joseph Juran)	La calidad de procesos comprende de una solución: (a) Subsistema de auditoria.	SUBSISTEMA DE AUDITORIA	➢ Trabajo en Equipo. ➢ Experiencia laboral. ➢ Motivación intrínseca. ➢ Eventos de socialización ➢ Ética ➢ Responsabilidad	**ANALISIS DOCUMENTAL**

ANEXO 3: FORMATO DE REUNION SGSI CP – I.E.P. ALBERT EINSTEIN

	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN LA CALIDAD DE PROCESOS	
	CODIGO	**FT – SGSI CP - 001**
	SGSI CP	
FORMATO DE REUNION	**FECHA : / /**	
	VERSION : 1	

LUGAR: I.E.P. ALBERT EINSTEIN	**HORA DE INICIO**	**HORA DE TERMINO**

PROPOSITO / JUSTIFICACION		
PARTICPANTES		
NOMBRE	**CARGO**	**FIRMA**

_____ Director I.E.P. Albert Einstein	_____ Implementador SGSI CP

ANEXO 3.1: FORMATO DE REUNION 1 SGSI CP – I.E.P. ALBERT EINSTEIN

	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN LA CALIDAD DE PROCESOS	
	CODIGO	FT – SGSI CP - 001
	■ SGSI CP	
FORMATO DE REUNION	FECHA	: 01/02/2021
	VERSION	: 1

LUGAR: I.E.P. ALBERT EINSTEIN	HORA DE INICIO	HORA DE TERMINO
	09:10	10:20

PROPOSITO / JUSTIFICACION

En los ambientes de la **I.E.P. ALBERT EINSTEN** se reúnen el Bach. Ing. Rider Sleither Zarbe Torres y la parte administrativa de la institución educativa para realizar una reunión de trabajo para definir los participantes y roles que representaran en la implementación de un Sistema De Gestión De Seguridad De La Información Para La Calidad De Procesos, llegando a un acuerdo unánime que el representante de la institución de la parte administrativa será el Director, en adelante mencionado como Director y el Bach. Ing. Rider Zarbe, en adelante mencionado como implementador.

definidos e identificados los actores se procede a explicar cuáles son los procesos requeridos que se llevara a cabo para la implementación como son: **Plan (Establecer), Do (Implementar Y Operar), Check (Monitorizar Y Revisar) Y Act (Mantener Y Mejorar).** estableciéndose el inicio del primer paso "plan", el cual implica establecer la política del SGSI, sus objetivos, procesos y procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, con resultados acordes a las políticas y objetivos de toda la organización.

para finalizar se acuerda brindar todas las facilidades para que el implementador realice todo el proceso dentro de la institución y trabajar en conjunto con el director, así mismo al finalizar el análisis del primero proceso se realizará una reunión para dar a conocer lo analizado.

PARTICPANTES

NOMBRE	CARGO	FIRMA
Hugo Joel Mozombite Arbildo	Director	
RIDER SLEITHER ZARBE TORRES	IMPLEMENTADOR SGSI CP	

Director I.E.P. Albert Einstein

Implementador SGSI CP

ANEXO 3.2: FORMATO DE REUNION 2 SGSI CP – I.E.P. ALBERT EINSTEIN

	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN LA CALIDAD DE PROCESOS	
	CODIGO	FT – SGSI CP - 001
	■ SGSI CP	
FORMATO DE REUNION	FECHA	: 26 / 02 / 2021
	VERSION	: 1

LUGAR: I.E.P. ALBERT EINSTEIN	HORA DE INICIO	HORA DE TERMINO
	10 : 00	11 : 50

PROPOSITO / JUSTIFICACION

En los ambientes de la **I.E.P. ALBERT EINSTEN** se reúnen el Director y el Implementador, para dar a conocer todos los pasos realizados para la elaboración del primero proceso "PLAN (Establecer)", en el cual pudo identificar los siguientes sub procesos como son: Clasificación y Control de Activos, Seguridad ligado al personal, Seguridad Física y del Entorno, Gestión de Comunicaciones y Operaciones, Control de Accesos y Gestión de Continuidad del Negocio.

Exponiendo que se realizó una evaluación de cuál es la realidad de la institución según los procedimientos a desarrollar, según los datos obtenidos se plasmará cual o cuales son las actividades, equipos tecnológicos a implementar para fortalecer la debilidad encontrada y estructurar la implementación del sistema de Gestión de Seguridad de la Información, al finalizar la exposición se hace entrega de una copia del proceso.

Para finalizar el Director establece su conformidad con el trabajo realizado y reafirma su disposición para continuar trabajando en el Proceso de Implementación de SGSI CP dentro de la Institución Educativa.

PARTICPANTES

NOMBRE	CARGO	FIRMA
Hugo Joel Mogombite Arbildo	Director	
RIDER SLEITHER ZARBE TORRES	IMPLEMENTADOR SGSI CP	

Director I.E.P. Albert Einstein

Implementador SGSI CP

ANEXO 3.3: FORMATO DE REUNION 3 SGSI CP – I.E.P. ALBERT EINSTEIN

	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN LA CALIDAD DE PROCESOS	
	CODIGO	FT – SGSI CP - 001
	■ SGSI CP	
FORMATO DE REUNION	FECHA	: 01 / 03 / 2021
	VERSION	: 1

LUGAR: I.E.P. ALBERT EINSTEIN	HORA DE INICIO	HORA DE TERMINO
	8:40	10:10

PROPOSITO / JUSTIFICACION

En los ambientes de la **I.E.P. ALBERT EINSTEN** se reúnen el Director y el implementador, para establecerse el inicio del segundo proceso "**DO (IMPLEMENTAR Y OPERAR)**", en el cual se representará la forma en que se debe operar e implementar las políticas, controles, procesos y procedimientos que se vayan a definir en la planificación del SGSI.

Reiterando que, realizado el primer proceso, el segundo proceso se especificará como debe operar cada sub proceso mencionado con anterioridad, para cumplir con las políticas y controles exigidos en la Norma ISO 27001, también de ser necesario se identificará activos, bienes o servicios que deberán adquirirse para el cumplimiento del segundo proceso.

para finalizar se acuerda brindar todas las facilidades para que el implementador realice todo el proceso dentro de la institución y trabajar en conjunto con el director, así mismo al finalizar el análisis del segundo proceso se realizará una reunión para dar a conocer lo analizado.

PARTICPANTES

NOMBRE	CARGO	FIRMA
Hugo Joel Mogambite Arbildo	Director	
RIDER SLEITHER ZARGE TORRES	IMPLEMENTADOR SGSI	

Director I.E.P. Albert Einstein

Implementador SGSI CP

ANEXO 3.4: FORMATO DE REUNION 4 SGSI CP – I.E.P. ALBERT EINSTEIN

	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION EN LA CALIDAD DE PROCESOS	
	CODIGO	FT – SGSI CP - 001
	■ SGSI CP	
FORMATO DE REUNION	FECHA	: 31 / 03 / 2021
	VERSION	: 1

LUGAR: I.E.P. ALBERT EINSTEIN	HORA DE INICIO	HORA DE TERMINO
	11:20	12:50

PROPOSITO / JUSTIFICACION

En los ambientes de la **I.E.P. ALBERT EINSTEN** se reúnen el Director y implementador, para dar a conocer los pasos realizados para la elaboración del segundo proceso "**Do (Implementar Y Operar)**", en el cual se identificó que varios de estos carecían de: Clasificación según importancia y uso de sus activos, seguridad en el manejo de ingreso de personal, seguridad de la información dentro y fuera de la institución, seguridad del entorno en la institución, falta de capacitaciones sobre el manejo de los activos informáticos, falta de capacitación al personal, falta del equipamiento del DATA CENTER, falta de cronograma de Backus de información, entre otras problemáticas.

Por todo lo detallado el Implementador dentro de la elaboración del segundo proceso, identificó esta problemática y plantea la adquisición de estos bienes y servicios, con las especificaciones técnicas ideales, los cuales representa una inversión por parte de la Institución su compra o adquisición temporal, así como también brinda formatos para realizar labores internas según proceso.

El Director expone que la compra de los bienes y servicios que se plantea para el cumplimiento del segundo proceso tendrá que quedar en espera, puesto que no se cuenta con la estabilidad financiera, considerando la actual emergencia sanitaria en el país a causa del Coronavirus (Covid-19), para finalizar se acuerda continuar con la elaboración de los dos últimos procesos en cuanto a la documentación, reiterando que no se cuenta con la estabilidad financiera para la implementación al 100% del SGSI, pero comprometiéndose como institución interesada realizarlo a futuro contando con todo la documentación de evaluación de los 4 procesos.

Para finalizar el Director establece conformidad con el trabajo realizado y reafirma su disposición para continuar trabajando en el proceso de Implementación del SGSI CP dentro de la Institución Educativa

PARTICPANTES

NOMBRE	CARGO	FIRMA
Hugo Joel Mogombite Arbildo	Director	
RIDER SLEITHER ZARGE TORRES	IMPLEMENTADOR SGSI CP	

Director I.E.P. Albert Einstein

Implementador SGSI CP

ANEXO 4: INSTRUMENTOS DE RECOLECCIÓN DE DATOS
CUESTIONARIO

CUESTIONARIO DE PREGUNTAS DE RECOLECCION DE DATOS

Cuestionario sobre la investigación: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA CALIDAD DE PROCESOS EN LA I.E.P. ALBERT EINSTEIN

N° DE CUESTIONARIO: _____
FECHA: _____

Estimado Señor:
El siguiente formulario tiene como objetivo obtener información, la que tendrá como único fin, aportar datos que contribuyan a la realización del trabajo de tesis final. Se agradece de antemano su colaboración, garantizándole que la información que Ud. brinde es anónima y en estricta reserva.

Por favor marque con una X la opción elegida.

NO	1
POCO	2
SI	3

PREG N°	PREGUNTAS	NO	POCO	SI
VARIABLE 1: SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN				
DIMENSION: PLANIFICAR				
01	¿Conoce usted alguna política de administración en la I.E.P. ALBERT EINSTEIN?			
02	¿Conoce usted el alcance del ISO 27001 en la I.E.P. ALBERT EINSTEIN?			
03	¿Conoce usted el análisis de riesgo 27001 en la I.E.P. ALBERT EINSTEIN?			
04	¿Conoce usted como seleccionar controles 27001 en la I.E.P. ALBERT EINSTEIN?			
05	¿Conoce usted sobre la definición 27001 en la I.E.P. ALBERT EINSTEIN?			
06	¿Conoce usted sobre la definición de autoridades y responsabilidades 27001 en la I.E.P. ALBERT EINSTEIN?			
DIMENSION: HACER				

07	¿Conoce usted como implantar el plan de riesgo 27001 en la I.E.P. ALBERT EINSTEIN?			
08	¿Conoce usted como implantar un SGSI(Sistema de Gestión de Seguridad de la Información) 27001 en la I.E.P. ALBERT EINSTEIN?			
09	¿Conoce usted como implantar controles 27001 en la I.E.P. ALBERT EINSTEIN?			
DIMENSION : CONTROLAR				
10	¿Conoce usted como revisar internamente un SGSI (Sistema de Gestión de Seguridad de la Información) en la I.E.P. ALBERT EINSTEIN?			
11	¿Conoce usted como poner en marcha indicadores y métricas en la I.E.P. ALBERT EINSTEIN?			
12	¿Conoce usted como debe hacerse una revisión por parte de la dirección en la I.E.P. ALBERT EINSTEIN?			
DIMENSION: ACTUAR				
13	¿Conoce usted como adoptar acciones correctivas en la I.E.P. ALBERT EINSTEIN?			
14	¿Conoce usted como adoptar acciones de mejora en la I.E.P. ALBERT EINSTEIN?			
VARIABLE 2: CALIDAD DE PROCESOS				
15	¿Conoce usted sobre el trabajo en equipo en la I.E.P. ALBERT EINSTEIN?			
16	¿Conoce usted sobre la experiencia laboral en la I.E.P. ALBERT EINSTEIN?			
17	¿Conoce usted sobre si existe la motivación en la I.E.P. ALBERT EINSTEIN?			
18	¿Conoce usted sobre eventos de socialización en la I.E.P. ALBERT EINSTEIN?			
19	¿Conoce usted sobre la motivación en la I.E.P. ALBERT EINSTEIN?			
20	¿Conoce usted sobre la ética en la I.E.P. ALBERT EINSTEIN?			
21	¿Conoce usted sobre la práctica de la responsabilidad en la I.E.P. ALBERT EINSTEIN?			

ANEXO 5

COMPROMISO DE CONFIDENCIALIDAD DEL PERSONAL INTERNO I.E.P. ALBERT EINSTEIN

En la ciudad de Pucallpa, con fecha ____ de _____ del año 20___, en las instalaciones de la Institución Educativa Particular Albert Einstein, ubicado en Jr. Emancipación #517, se encuentra el señor(a) _____ Director(a) de la Institución identificado con numero de DNI _____ y el señor(a)_____, identificado con DNI _____ que desempeña el cargo de _____, se ha acordado firmar el presente compromiso de confidencialidad están de acuerdo ambas partes y se regirá por las siguientes clausulas:

IMPORTANTE

Debido a la naturaleza del cargo a desempeñar en la institución, se considera necesario que por el manejo de información propio de la institución y/o información de clientes, se utilice la información con discreción antes, durante y la etapa posterior.

OBJETIVO

El presente es para determinar los acuerdos, términos y condiciones a la cual ambas partes mantendrán la confidencialidad de la información de la institución y clientes, incluye información física (documentación), información digital (guardado en USB, data center, disco duro externos, CD, DVD, equipos tecnológicos, etc.) y cualquier tipo de información sobre la institución y clientes.

CONDICION

Ambas partes acuerdan que la información de la institución y los clientes, será mantenida en estricta confidencialidad. La parte receptora (personal entrante) solo podrá revelar información a quienes lo necesiten y estén autorizados según el nivel de acceso a la información y la oficina solicitante, entiéndase como información confidencial: a) Aquella información que, por su naturaleza, no sea conocida por el resto del personal, b) La que no es de fácil acceso, c) Aquella que se considere protección y resguardo.

EXCEPCIONES

La información no tendrá de carácter confidencial en los siguientes casos: a) cuando la parte receptora tenga conocimiento de la información recibida, b) cuando la información recibida sea de dominio público.

DURACION

El presente compromiso tendrá duración durante todo el tiempo que la parte receptora labore en la institución.

DERECHOS DE PROPIEDAD

Toda información que se adquiera, distribuya y se obtenga durante el tiempo laborado dentro y fuera de la institución, no será utilizada por ninguna de las partes para uso y/o beneficio propio.

MODIFICACION

El presente compromiso solo podrá ser modificado por el Director de la Institución Educativa, y este se responsabilizará de hacer de conocimiento al personal responsable para notificación a ambas partes.

Pucallpa, Ucayali – Perú

_____	_____
Director(a)	Trabajador

ANEXO 6

COMPROMISO DE CONFIDENCIALIDAD DEL PERSONAL INTERNO I.E.P. ALBERT EINSTEIN

En la ciudad de Pucallpa, con fecha ____ de _____ del año 20___, en las instalaciones de la Institución Educativa Particular Albert Einstein, ubicado en Jr. Emancipación #517, se encuentra el señor(a) _____ Director(a) de la Institución identificado con número de DNI _____ y el señor(a)_____, identificado con DNI _____ RUC Nª _____que desempeña el cargo de _____, se ha acordado firmar el presente compromiso de confidencialidad están de acuerdo ambas partes y se regirá por las siguientes clausulas:

IMPORTANTE

Debido a la naturaleza del cargo a desempeñar en la institución, se considera necesario que por el manejo de información propio de la institución y/o información de clientes, se utilice la información con discreción antes, durante y la etapa posterior.

OBJETIVO

El presente es para determinar los acuerdos, términos y condiciones a la cual ambas partes mantendrán la confidencialidad de la información de la institución y clientes, incluye información física (documentación), información digital (guardado en USB, data center, disco duro externos, CD, DVD, equipos tecnológicos, etc.) y cualquier tipo de información sobre la institución y clientes.

CONDICION

Ambas partes acuerdan que la información de la institución y los clientes, será mantenida en estricta confidencialidad. La parte receptora (personal entrante) solo podrá revelar información a quienes lo necesiten y estén autorizados según el nivel de acceso a la información y la oficina solicitante, entiéndase como información confidencial: a) Aquella información que, por su naturaleza, no sea conocida por el resto del personal, b) La que no es de fácil acceso, c) Aquella que se considere protección y resguardo.

EXCEPCIONES

La información no tendrá de carácter confidencial en los siguientes casos: a) cuando la parte receptora tenga conocimiento de la información recibida, b) cuando la información recibida sea de dominio público.

DURACION

El presente compromiso tendrá duración durante todo el tiempo que la parte receptora labore en la institución.

DERECHOS DE PROPIEDAD

Toda información que se adquiera, distribuya y se obtenga durante el tiempo laborado dentro y fuera de la institución, no será utilizada por ninguna de las partes para uso y/o beneficio propio.

MODIFICACION

El presente compromiso solo podrá ser modificado por el Director de la Institución Educativa, y este se responsabilizará de hacer de conocimiento al personal responsable para notificación a ambas partes.

Pucallpa, Ucayali – Perú

_____	_____
Director(a)	Personal Tercero

ANEXO 7

	FORMATO	**Versión**	**01**
	CAPACITACION EN SEGURIDAD DE LA INFROMACION	**Fecha**	
		Página	**1 - 1**

1. DATOS DE LA CAPACITACION

USUARIO : _____

AREA CARGO : _____

FECHA : _____

CAPACITADOR CARGO : _____

2. SERVICIOS INFORMATICOS A CAPACITAR (MARCAR X)

A. SISTEMA INFORMATICO	
B. CORREO ELECTRONICO	
C. INTERNET	
D. ANTIVIRUS	
E. CONDIFENCIALIDAD	

3. CONFORMIDAD DE CAPACITACION

_____ _____

Director(a) Trabajador

ANEXO 8

	INGRESO DE PERSONAL EXTERNO A LA I.E.P. ALBERT EINSTEIN

Nº	NOMBRE / RAZON SOCIA	FECHA	INGRESO	SALIDA	MOTIVO

ANEXO 9

	REGISTRO
	CAPACITACION DE PROCESOS INFORMATICOS

OFICINA : _____

JEFE : _____

CAPACITADOR: _____

FECHA : _____

PROCESO : _____

Nº	APELLIDOS Y NOMBRES	CARGO	FIRMA

ANEXO 10

	REGISTRO DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Nº	FECHA	HORA	INCIDENTE

ANEXO 11

	REGISTRO DE BACKUP SEMANAL

Nº	FECHA	HORA	OFICINA	USUARIO	OBSERVACION

ANEXO 12

	REGISTRO DE ACTIVACION/DESACTIVACION

Nº	FECHA	OFICINA	USUARIO	SERVICIOS ACTIVADOS / DESACTIVADOS

ANEXO 13 : GUIA DE ENTREVISTA

sobre la investigación: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA CALIDAD DE PROCESOS EN LA I.E.P. ALBERT EINSTEIN

Fecha de entrevista: **Nº**

DATOS PERSONALES

DNI: Apellidos: Nombres:

Edad: Cargo: Celular:

INFORMACION

PREGUNTAS DE GUIA PARA ENTREVISTA

- Que es política de administración en la I.E.P. Albert Einstein ----------
- Como se aplica el ISO 27001 en la I.E.P. Albert Einstein ----------
- Como se implanta el plan de riesgo 27001 en la I.E.P. Albert Einstein ----------
- Como se implanta el SGSI 27001 en la I.E.P. Albert Einstein ----------
- Como se pone en marcha indicadores y métricas en la I.E.P. Albert Einstein ----------
- Como son las acciones correctivas en la I.E.P. Albert Einstein ----------
- Como se realiza el trabajo en equipo en la I.E.P. Albert Einstein ----------
- Como es la práctica de la responsabilidad en la I.E.P. Albert Einstein ----------

DATOS DEL ENTREVISTADOR

DNI: Apellidos y Nombres Firma:

ANEXO 14: VALIDACIÓN POR ALFA DE CRONBACH

Para medir la confiabilidad de los datos se utilizó el Alfa de Cronbach, es un modelo de consistencia interna, basado en el promedio de las correlaciones entre los ítems. Entre las ventajas de esta medida se encuentra la posibilidad de evaluar cuánto mejoraría (o empeoraría) la fiabilidad de la prueba si se excluyera un determinado ítem. Como criterio general, se sugiere evaluar los coeficientes de Alfa de Cronbach:

- Coeficiente alfa > 0.9 es excelente.
- Coeficiente alfa > 0.8 es bueno.
- Coeficiente alfa > 0.7 es aceptable.
- Coeficiente alfa > 0.6 es cuestionable.
- Coeficiente alfa > 0.5 es pobre.
- Coeficiente alfa < 0.5 es inaceptable.

Fiabilidad

Resumen de procesamiento de casos

		N	%
Casos	Válido	8	100,0
	Excluido	0	,0
	Total	8	100,0

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

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,784	21

Como se define para la validación de instrumentos de recolección de datos que una correlación total de elementos menor o igual a 0.60 es estadísticamente poco significativa más allá del nivel del 1%.

Así pues, la investigación de fiabilidad del proyecto con un coeficiente de alfa de Cronbach de 0.70 se consideró el proyecto aceptable.

Estadísticas de total de elemento

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
¿Conoce usted alguna política de administración en la I.E.P. ALBERT EINSTEIN?	42,00	20,286	,866	,725
¿Conoce usted el alcance del ISO 27001 en la I.E.P. ALBERT EINSTEIN?	42,63	22,554	,776	,742
¿Conoce usted el análisis de riesgo 27001 en la I.E.P. ALBERT EINSTEIN?	43,13	25,839	,471	,770
¿Conoce usted como seleccionar controles 27001 en la I.E.P. ALBERT EINSTEIN?	43,00	24,571	,668	,757
¿Conoce usted sobre la definición 27001 en la I.E.P. ALBERT EINSTEIN?	42,25	20,786	,892	,725

¿Conoce usted sobre la definición de autoridades y responsabilidades 27001 en la I.E.P. ALBERT EINSTEIN?	42,13	24,982	,394	,772
¿Conoce usted como implantar el plan de riesgo 27001 en la I.E.P. ALBERT EINSTEIN?	43,00	24,571	,668	,757
¿Conoce usted como implantar un SGSI(Sistema de Gestión de Seguridad de la Información) 27001 en la I.E.P. ALBERT EINSTEIN?	43,00	26,286	,323	,777
¿Conoce usted como implantar controles 27001 en la I.E.P. ALBERT EINSTEIN?	43,00	25,143	,550	,764
¿Conoce usted como revisar internamente un SGSI (Sistema de Gestión de Seguridad de la Información) en la I.E.P. ALBERT EINSTEIN?	42,38	23,411	,586	,756
¿Conoce usted como poner en marcha indicadores y métricas en la I.E.P. ALBERT EINSTEIN?	41,88	26,982	,180	,784

¿Conoce usted como debe hacerse una revisión por parte de la dirección en la I.E.P. ALBERT EINSTEIN?	41,88	26,125	,340	,776
¿Conoce usted como adoptar acciones correctivas en la I.E.P. ALBERT EINSTEIN?	41,88	26,982	,180	,784
¿Conoce usted como adoptar acciones de mejora en la I.E.P. ALBERT EINSTEIN?	42,00	26,286	,323	,777
¿Conoce usted sobre el trabajo en equipo en la I.E.P. ALBERT EINSTEIN?	41,75	29,071	-,192	,803
¿Conoce usted sobre la experiencia laboral en la I.E.P. ALBERT EINSTEIN?	41,88	23,554	,854	,745
¿Conoce usted sobre si existe la motivación en la I.E.P. ALBERT EINSTEIN?	42,00	33,143	-,863	,834
¿Conoce usted sobre eventos de socialización en la I.E.P. ALBERT EINSTEIN?	41,75	31,929	-,672	,825
¿Conoce usted sobre la motivación en la I.E.P. ALBERT EINSTEIN?	42,38	28,268	,000	,786
¿Conoce usted sobre la ética en la I.E.P. ALBERT EINSTEIN?	41,88	26,982	,180	,784

¿Conoce usted sobre la práctica de la responsabilidad en la I.E.P. ALBERT EINSTEIN?	41,75	26,500	,282	,779