

**UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN**

**FACULTAD DE INGENIERIA**

**ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS  
Y COMPUTACIÓN**



**TESIS**

**Sistema de gestión de seguridad de la información para  
mejorar la protección informática de la Comisaria Región**

**Huancavelica**

**Para optar el título profesional de:**

**Ingeniero de Sistemas y Computación**

**Autor: Bach. Williams HUINCHO RAMOS**

**Asesor: Dr. Ángel Claudio NUÑEZ MEZA**

**Cerro de Pasco – Perú – 2019**

**UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN**

**FACULTAD DE INGENIERIA**

**ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS  
Y COMPUTACIÓN**



**Sistema de gestión de seguridad de la información para  
mejorar la protección informática de la Comisaria Región  
Huancavelica**

**Sustentada y aprobada ante los miembros del jurado:**

---

**Mg. Raúl Delfín CONDOR BEDOYA**

**PRESIDENTE**

---

**Ing. Melquiades Arturo TRINIDADMALPARTIDA**

**MIEMBRO**

---

**Dr. Zenón Manuel LOPEZ ROBLES**

**MIEMBRO**

**DEDICATORIA**

Agradezco a Dios, con todo aprecio a mis padres y a mis seres queridos por el apoyo constante y aliento permanente que me dieron en el trayecto de mis estudios en la educación académica; por el sacrificio de ellos, por lograr mis sueños de ser profesional.

## RESUMEN

El presente estudio está enfocado en la apreciación y análisis de un factor riesgos que provienen desde el interior de la institución, asegurar sus datos e información de valor con la ayuda de un Sistema de Gestión de Seguridad de la Información, conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en nuestra empresa.

Es importante diferenciar entre seguridad informática y seguridad de la información.

La primera, la seguridad informática, se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación que soportan nuestro negocio.

Entre los muchos ejemplos de información que podemos encontrar en nuestra empresa están los correos electrónicos, páginas web, imágenes, bases de datos, faxes, contratos, presentaciones, documentos y un largo etcétera.

Además, es necesario considerar el ciclo de vida de la información.

Esta metodología nos va a permitir, en primer lugar, analizar y ordenar la estructura de los sistemas de información.

En segundo lugar, nos facilitará la definición de procedimientos de trabajo para mantener su seguridad.

La gestión de los riesgos a través de un Sistema de Gestión de Seguridad de la Información nos va a permitir preservar la confidencialidad, integridad y disponibilidad de la misma, en el interior de la empresa, ante nuestros clientes y ante las distintas partes interesadas en nuestro negocio.

Con el fin de proporcionar un marco de Gestión de la Seguridad de la Información utilizable por cualquier tipo de organización se ha creado un conjunto de estándares bajo el nombre de ISO/IEC 27000.

Esta implementación de SGSI permitió un gran aumento en la seguridad de los activos de información de la comisaría región Huancavelica., que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

**Palabras clave:** Herramienta tecnológica moderna; seguridad de información.

## SUMMARY

This study is focused on the appreciation and analysis of a risk factor that comes from within the institution, securing its data and valuable information with the help of an Information Security Management System, knowing, managing and minimizing the possible risks that threaten the security of the information in our company.

It is important to differentiate between computer security and information security.

The first, computer security, refers to the protection of the information and communication technology infrastructures that support our business.

Among the many examples of information that we can find in our company are emails, web pages, images, databases, faxes, contracts, presentations, documents and a long etcetera.

In addition, it is necessary to consider the life cycle of the information.

This methodology will allow us, in the first place, to analyze and order the structure of information systems.

Second, it will make it easier for us to define work procedures to keep you safe.

Risk management through an Information Security Management System will allow us to preserve the confidentiality, integrity and availability of the same, within the company, before our clients and before the different parties interested in our deal.

In order to provide an Information Security Management framework usable by any type of organization, a set of standards has been created under the name of ISO / IEC 27000.

This implementation of ISMS allowed a great increase in the security of the information assets of the Huancavelica region commissioner, which guarantees that information security risks are known, assumed, managed and minimized in a documented, systematic, structured and repeatable way. , efficient and adaptable to changes that occur in risks, the environment and technologies.

**Keywords:** Modern technological tool; information security.

## INTRODUCCIÓN

En la presente tesis, se diseña y desarrolla el modelo para implementar un sistema de gestión de seguridad de información para cualquier tipo de organización y se encuentra ubicado dentro del área temática de industrias de la información y del conocimiento. Para la aplicación del presente trabajo, se trabajará con la Comisaria PNP región Huancavelica.

La seguridad de información, en términos generales es entendida como todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma. Un activo de información es un activo que tiene un determinado valor para la organización, sus operaciones y su continuidad.

En la Comisaria PNP región Huancavelica se realizó un proceso de diagnóstico, a partir del cual se determinó que no poseía los mecanismos, ni los procesos idóneos para proteger su información. Con base en esta situación, se decidió realizar un plan piloto para implementar políticas que se ajustaran a la norma de un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001, que ayudara al equipo de stakeholders al levantamiento inicial de información, al análisis de brechas; y que ayudara al auditor del seguimiento y gestión de cada uno de los procesos de la norma.

EL AUTOR



## INDICE

**DEDICATORIA**

**RESUMEN**

**SUMMARY**

**INTRODUCCIÓN**

**INDICE**

### CAPITULO I

#### PROBLEMA DE INVESTIGACIÓN

1.1.	Identificación y determinación del Problema .....	1
1.2.	Delimitación de la investigación. ....	5
1.3.	Formulación del Problema .....	6
	1.3.1 Problema principal.....	6
	1.3.2 Problemas Específicos .....	6
1.4.	Formulación de Objetivos .....	6
	1.4.1. Objetivos Generales .....	6
	1.4.2. Objetivos Específicos .....	6
1.5.	Justificación de la investigación .....	7
1.6.	Limitaciones de la investigación.....	11

### CAPITULO II

#### MARCO TEÓRICO

2.1.	Antecedentes de estudio .....	12
2.2.	Bases teóricas - científicas .....	13
2.3.	Definición de términos básicos .....	45
2.4.	Formulación de Hipótesis .....	48
	2.4.1. Hipótesis General .....	48
	2.4.2. Hipótesis Específicas .....	48
2.5.	Identificación de las Variables.....	49
2.6.	Definición operacional de variables e indicadores. ....	49

**CAPITULO III****METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN**

3.1. Tipo de investigación. ....	51
3.2. Métodos de investigación. ....	51
3.3. Diseño de Investigación.....	51
3.4. Población y muestra. ....	53
3.5. Técnicas e instrumentos de recolección de datos.....	55
3.6. Técnicas de procesamiento y análisis de datos .....	60
3.7. Tratamiento Estadístico .....	60
3.8. Selección, validación y confiabilidad de los instrumentos de investigación.....	61
3.9. Orientación ética.....	70

**CAPITULO IV****RESULTADOS Y DISCUSIÓN**

4.1. Descripción del trabajo de campo .....	71
4.2. Presentación, análisis e interpretación de resultados .....	71
4.3. Prueba de Hipótesis.....	79
4.4. Discusión de Resultados .....	86

**CONCLUSIONES****RECOMENDACIONES****BIBLIOGRAFÍA.****ANEXOS**

## CAPÍTULO I

### PROBLEMA DE INVESTIGACIÓN

#### 1.1. Identificación y determinación del Problema

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. *La confidencialidad, integridad y disponibilidad de información* sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de

denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

La Policía Nacional del Perú, institución del Estado encargada de la seguridad ciudadana, tiene como misión prevenir, investigar y combatir la delincuencia, así como prestar protección y ayuda a las personas y a la comunidad. Las comisarías, dependencias policiales de una determinada jurisdicción a nivel nacional, en muchas ocasiones no logran cumplir la misión presentada por diferentes motivos como error en la toma de

decisiones (distribución de patrullajes, turnos y policías), falta de recursos (policías, infraestructura tecnológica, vehículos) y un indebido manejo de la información, por ejemplo, al no brindar información que pueda ayudar o prevenir a la comunidad o no tener la información centralizada para todas las comisarías y los factores mencionados impiden a las comisarías brindar un buen servicio a la comunidad y no cumplir con salvaguardar la seguridad ciudadana.

Actualmente la comisaria no cuenta con los controles, medidas, procedimientos de seguridad necesarios para resguardar sus activos de información, tales como documentos, software, dispositivos físicos, personas, imagen, reputación y servicios, están expuestos a altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas existentes:

- ☞ Desastres naturales (Tormentas, rayos, terremotos, inundaciones, etc.)
- ☞ Estructurales (Incendios, inundaciones, humedad, cortes de electricidad, agua, refrigeración, comunicaciones, etc.)
- ☞ Hardware (Fallo total o parcial de Servidores, Estaciones PC, portátiles, etc.)
- ☞ Software (Errores en los SO, BD, software base, Web servers, aplicaciones, elementos de seguridad, etc.)
- ☞ Red LAN y WAN (red interna, redes con delegaciones, sistemas de seguridad de las comunicaciones, redes públicas ajenas, etc.)
- ☞ Copias de seguridad (Fallos en elementos de copias, fallos en soportes cintas, discos, etc.)

- ☞ Información (Bases de datos, ficheros, manuales, procedimientos, planes de contingencia, etc.)
- ☞ Personal (Errores y ataques de personal interno, externo, funciones, perfiles, formación, etc.)
- ☞ Riesgos contra el patrimonio (Robo, pérdida no intencionada de activos, etc.)
- ☞ Otros riesgos (Terrorismo, epidemias, confianza de los clientes, imagen de empresa, insolvencia de servicios externos, seguros, outsourcing, etc.)

Las organizaciones públicas y privadas día a día generan conocimientos, datos, reportes, actas y material de diferente índole de suma importancia para ellas, lo cual representa toda la información que requieren para su funcionalidad. Esta información en la mayoría de los casos, es almacenada en diferentes medios tanto físicos como electrónicos, además es puesta a disposición del personal que requiere hacer uso de esta información para toma de decisiones, realización de planes, reportes, inventarios, entre otros.

El acceso no autorizado a la información se ha vuelto más fácil debido a los tantos métodos existentes y nuevos para extraer información, esto ha permitido que sea más difícil salvaguardar la información y sus métodos de transmisión; ya sean estos comunicados verbales, archivos, documentos, base de datos, entre otros.

La probabilidad de que la información sea interceptada, robada y/o modificada por personas inescrupulosas y sin autorización de acceso a

esta, ha aumentado exponencialmente. Lo cual resulta peligroso para los sistemas informáticos de la comisaria, ya que mucha de la información fundamental e importante para la realización de los procesos críticos del negocio puede ser vulnerada y amenazada ocasionando la interrupción de estos procesos; que conllevan, de esta manera, a una pérdida no solo de información, sino también del proceso de seguridad ciudadana.

Por lo anteriormente citado es necesaria la implementación de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos garantizar a que accedan a la información quienes estén designados para su uso, esté disponible cuando se requiera y permanezca tal como fue creada por sus propietarios y asegurar también la actualización de la misma.

## **1.2. Delimitación de la investigación.**

### **1.2.1. Delimitación espacial**

El presente estudio abarca la Comisaria de la Policía Nacional del Perú Región Huancavelica.

### **1.2.2. Delimitación temporal**

El periodo que comprenderá la presente investigación abarca el año 2019.

### **1.2.3. Delimitación social**

El sujeto de análisis que corresponde al presente estudio comprende al personal de la Comisaria de la Policía Nacional del Perú Región Huancavelica.

### **1.3. Formulación del Problema**

#### **1.3.1 Problema principal**

¿El Sistema de Gestión de Seguridad de Información mejorará la protección informática de la Comisaria región Huancavelica?

#### **1.3.2 Problemas Específicos**

1.- ¿El Sistema de Gestión de Seguridad de Información incrementará la confidencialidad de la seguridad en la protección informática de la Comisaria región Huancavelica?

2.- ¿El Sistema de Gestión de Seguridad de Información incrementará la integridad de la seguridad en la protección informática de la Comisaria región Huancavelica?

3.- ¿El Sistema de Gestión de Seguridad de Información incrementará la disponibilidad de la seguridad en la protección informática de la Comisaria región Huancavelica?

### **1.4. Formulación de Objetivos**

#### **1.4.1. Objetivos Generales**

Medir el grado de influencia que ejerce un Sistema de Gestión de Seguridad de Información para la mejora de la protección informática de la Comisaria región Huancavelica.

#### **1.4.2. Objetivos Específicos**

1.- Medir el grado de influencia que ejerce un Sistema de Gestión de Seguridad de Información para la mejora de confidencialidad de la seguridad en la protección informática de la Comisaria región Huancavelica.



2.- Medir el grado de influencia que ejerce un Sistema de Gestión de Seguridad de Información para la mejora de integridad de la seguridad en la protección informática de la Comisaria región Huancavelica.

3.- Medir el grado de influencia que ejerce un Sistema de Gestión de Seguridad de Información para la mejora de disponibilidad de la seguridad en la protección informática de la Comisaria región Huancavelica.

### **1.5. Justificación de la investigación**

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

Debido a los riesgos a los que están expuestos los activos de información, el impacto que la interrupción de estos puede causar, es preponderante la definición de una metodología y el uso de herramientas que nos ayuden reducir y mitigar estos riesgos.

Es por ello que se propone la implementación de un Sistema de gestión de seguridad de información (SGSI), el cual nos brindará los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, las amenazas, las vulnerabilidades de los activos de información, implantar los controles necesarios que ayudarán a salvaguardar los activos de información de los procesos de tecnología, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de Información (SGSI) de la comisaria región Huancavelica, alineándolo de esta manera a los objetivos estratégicos de la organización.

### **Importancia y Alcance de la Investigación**

#### **Importancia de la Investigación**

Un sistema de gestión de la seguridad de la información (SGSI) (en inglés: information security management system, ISMS) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

Un SGSI es para una organización el 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.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización, así como los externos del entorno.

El propósito de este proyecto se centra en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollado.

### **Alcance de la Investigación**

El alcance de una investigación indica el resultado lo que se obtendrá a partir de ella y condiciona el método que se seguirá para obtener dichos resultados, por lo que es muy importante identificar acertadamente dicho alcance antes de empezar a desarrollar la investigación. A continuación se presentan los cuatro tipos de alcance que puede tener una investigación, explicando cuándo es conveniente aplicar cada uno.

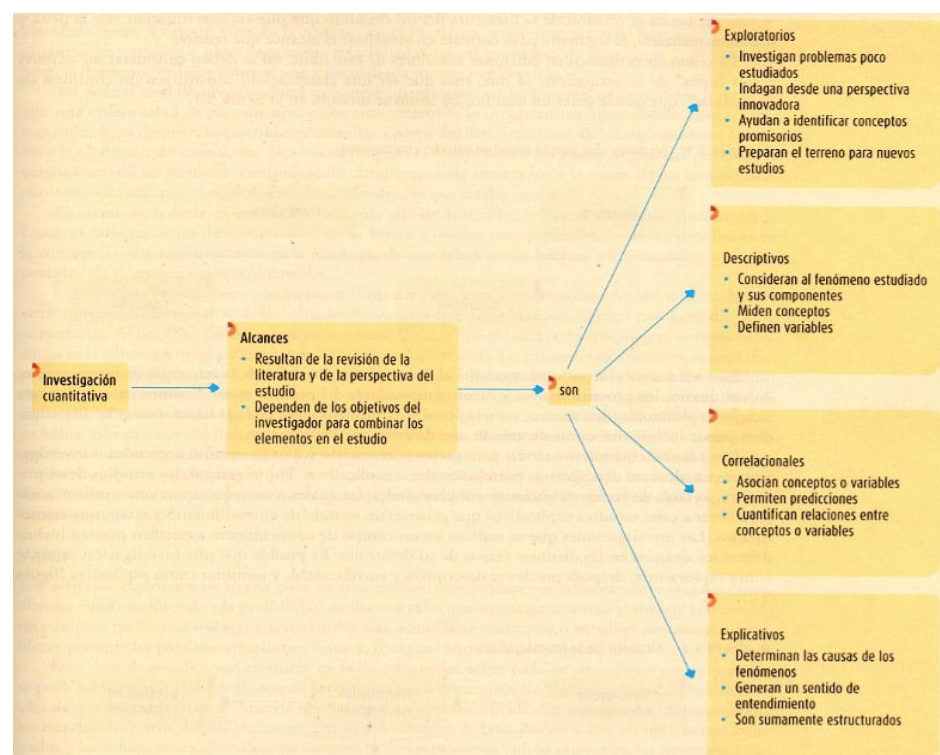
Un proyecto de investigación nace con una idea que tiene el investigador de estudiar un tema de su interés, y que al revisar la literatura disponible encuentra un problema o área de oportunidad a atender. Y cuando se define el problema de investigación, es momento también de establecer el alcance de la misma.

Como explica *Hernández Sampiere, Fernández Collado & Baptista Lucio (2010)*, Autor del libro *Metodología de la Investigación 6<sup>ta</sup> edición*; cuando se habla sobre el alcance de una investigación no

se debe pensar en una tipología, ya que más que una clasificación, lo único que indica dicho alcance es el resultado que se espera obtener del estudio. Según estos autores, de una investigación se pueden obtener cuatro tipos de resultados:

- 1) Estudio exploratorio: Se realizan cuando el objeto consiste en examinar un tema poco estudiado.
- 2) Estudio descriptivo: Busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice. Describe tendencias de un grupo o población.
- 3) Estudio correlacional: Asocia variables mediante un patrón predecible para un grupo o población.
- 4) Estudio explicativo: pretende establecer las causas de los eventos, sucesos o fenómenos que se estudian.

**Figura 1:** Alcances de los procesos de la Investigación Cuantitativa.





El alcance de esta presente investigación es **correlacional** y **explicativo**.

### **1.6. Limitaciones de la investigación**

El diseño de SGSI, estará limitado por los siguientes factores:

**a. Factor Recurso:**

La disponibilidad de los recursos es autofinanciada por el tesista.

**b. Factor Tiempo:**

Diseñar y aplicar un Sistema de Gestión de Seguridad de Información requiere de mucho tiempo de labor por parte del tesista. Es por ello que dentro de los objetivos de este proyecto se encuentra analizar el SGSI.

## **CAPÍTULO II**

### **MARCO TEÓRICO**

#### **2.1. Antecedentes de estudio**

**TESIS:** “IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA COMUNIDAD NUESTRA SEÑORA DE GRACIA, ALINEADO TECNOLÓGICAMENTE CON LA NORMA ISO 27001”.

*Objetivo:* Reducir y mitigar los riesgos de los activos de información de los procesos que se encuentran bajo la gerencia de tecnología.

*Conclusiones:*

Actualmente en la sociedad de la información, es necesario que todas las organizaciones, sin tener en cuenta su tamaño, implementen mecanismos que permitan mantenerla segura, donde se usa la norma internacional ISO/IEC 27001 como un sistema basado en procesos que busca garantizar la seguridad de la información, siguiendo una serie de

pautas y controles que, de aplicarse, minimizan los riesgos a los cuales se ve expuesta.

La implementación del SGSI es beneficioso para la Comunidad en cuanto a seguridad efectiva en los sistemas de información; mejoras continuas en procesos de auditorías internas dentro de la Comunidad; incremento de la confianza en la Comunidad y mejora de su imagen. Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad, entre otros servicios de seguridad.

## **2.2. Bases teóricas - científicas**

### **2.2.1. Seguridad de la información.**

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros.

### **CONCEPCIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.**

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o sabotada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

**Crítica:** Es indispensable para la operación de la empresa.

**Valiosa:** Es un activo de la empresa y muy valioso.

**Sensible:** Debe de ser conocida por las personas autorizadas.



Existen dos palabras muy importantes que son riesgo y seguridad:

**Riesgo:** Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.

**Seguridad:** Es una forma de protección contra los riesgos.

La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

Precisamente la reducción o eliminación de riesgos asociado a una cierta información es el objeto de la seguridad de la información y la seguridad informática. Más concretamente, la seguridad de la información tiene como objeto los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de información. Los términos seguridad de la información, seguridad informática y garantía de la información son usadas frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información. Sin embargo, no son exactamente lo mismo existiendo algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración. Además, la seguridad de la

información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran. La seguridad de la información incumbe a gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas con información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera.

### **Servicios de seguridad**

El objetivo de un servicio de seguridad es mejorar la seguridad de los sistemas de procesamiento de datos y la transferencia de información en las organizaciones. Los servicios de seguridad están diseñados para contrarrestar los ataques a la seguridad y hacen uso de uno o más mecanismos de seguridad para proporcionar el servicio.

### **Protocolos de seguridad de la información.**

Los protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación

de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información. Se componen de:

- Criptografía (Cifrado de datos). Se ocupa de transposicionar u ocultar el mensaje enviado por el emisor hasta que llega a su destino y puede ser descifrado por el receptor.
- Lógica (Estructura y secuencia). Llevar un orden en el cual se agrupan los datos del mensaje el significado del mensaje y saber cuándo se va enviar el mensaje.
- Identificación (Autenticación). Es una validación de identificación técnica mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor.

### **Planificación de la seguridad**

Hoy en día la rápida evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. El propósito del plan de seguridad del sistema es proporcionar una visión general de los requisitos de seguridad del sistema y se describen los controles en el lugar o los previstos para cumplir esos requisitos. El plan de seguridad del sistema también delinea las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema. Debe reflejar las aportaciones de distintos gestores con responsabilidades sobre el sistema,

incluidos los propietarios de la información, el propietario de la red, y el alto funcionario de la agencia de información de seguridad.

Los administradores de programas, los propietarios del sistema, y personal de seguridad en la organización debe entender el sistema de seguridad en el proceso de planificación. Los responsables de la ejecución y gestión de sistemas de información deben participar en el tratamiento de los controles de seguridad que deben aplicarse a sus sistemas.

### **El manejo de riesgos**

Dentro de la seguridad en la información se lleva a cabo la clasificación de las alternativas para manejar los posibles riesgos que un activo o bien puede tener dentro de los procesos de organización. Esta clasificación lleva el nombre de manejo de riesgos. El manejo de riesgos, conlleva una estructura bien definida, con un control adecuado y su manejo, habiéndolos identificado, priorizados y analizados, a través de acciones factibles y efectivas. Para ello se cuenta con las siguientes técnicas de manejo del riesgo:

- **Evitar.** El riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que

ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades. Ejemplo:

No instalar empresas en zonas sísmicas.

- **Reducir.** Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla. Se consigue optimizando los procedimientos, la implementación de controles y su monitoreo constante. Ejemplo:

No fumar en ciertas áreas, instalaciones eléctricas anti flama, planes de contingencia.

- **Retener, Asumir o Aceptar el riesgo.** Es uno de los métodos más comunes del manejo de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las pérdidas involucradas, esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente. Ejemplo de asumir el riesgo:

Con recursos propios se financian las pérdidas.

- **Transferir.** Es buscar un respaldo y compartir el riesgo con otros controles o entidades. Esta técnica se usa ya sea para eliminar un

riesgo de un lugar y transferirlo a otro, o para minimizar el mismo, compartiéndolo con otras entidades. Ejemplo:

Transferir los costos a la compañía aseguradora.

### **2.2.2. Sistema de gestión de la seguridad de la información.** WWW.ISO27000.ES

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

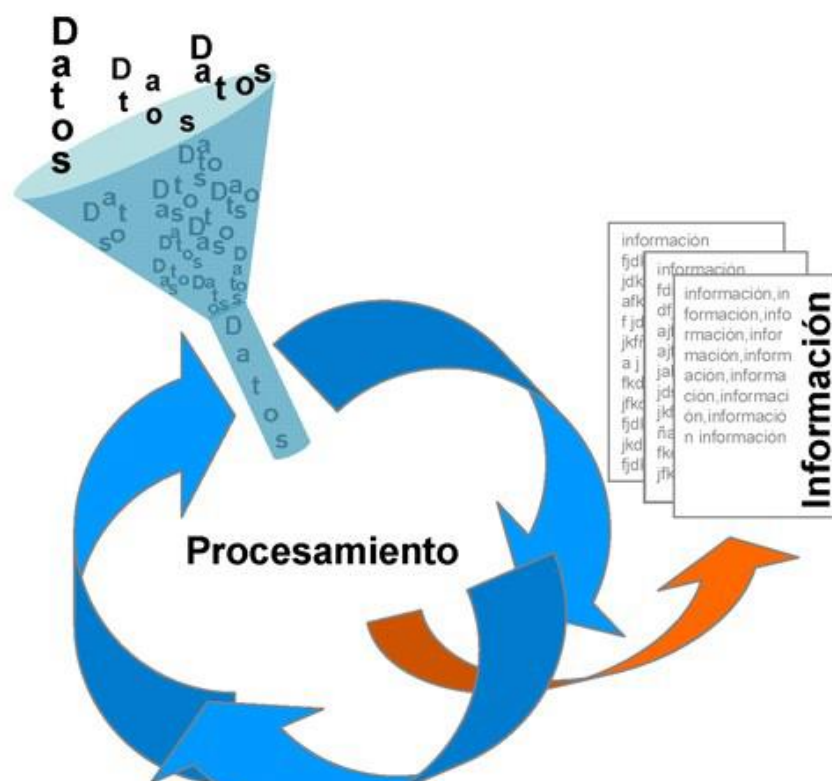
Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En las siguientes secciones, se desarrollarán los conceptos fundamentales de un SGSI según la norma ISO 27001.

## 1. ¿Qué es un SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.



**Figura 2:** Proceso de Datos para obtener Información.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

**2. ¿Para qué sirve un SGSI?**

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen



empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe

contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.



**Figura 3:** Con un SGSI, la organización conoce los riesgos a los que está sometida su información.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

### 3. ¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a

un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:



**Figura 4:** Sistema de Gestión de la Seguridad de la Información basado en ISO 27001.

#### **Documentos de Nivel 1**

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

#### **Documentos de Nivel 2**

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

### **Documentos de Nivel 3**

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

### **Documentos de Nivel 4**

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
- Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- Procedimientos y mecanismos de control que soportan al SGSI:

aquellos procedimientos que regulan el propio funcionamiento del SGSI.

- Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.
- Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

- Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

### **CONTROL DE LA DOCUMENTACIÓN**

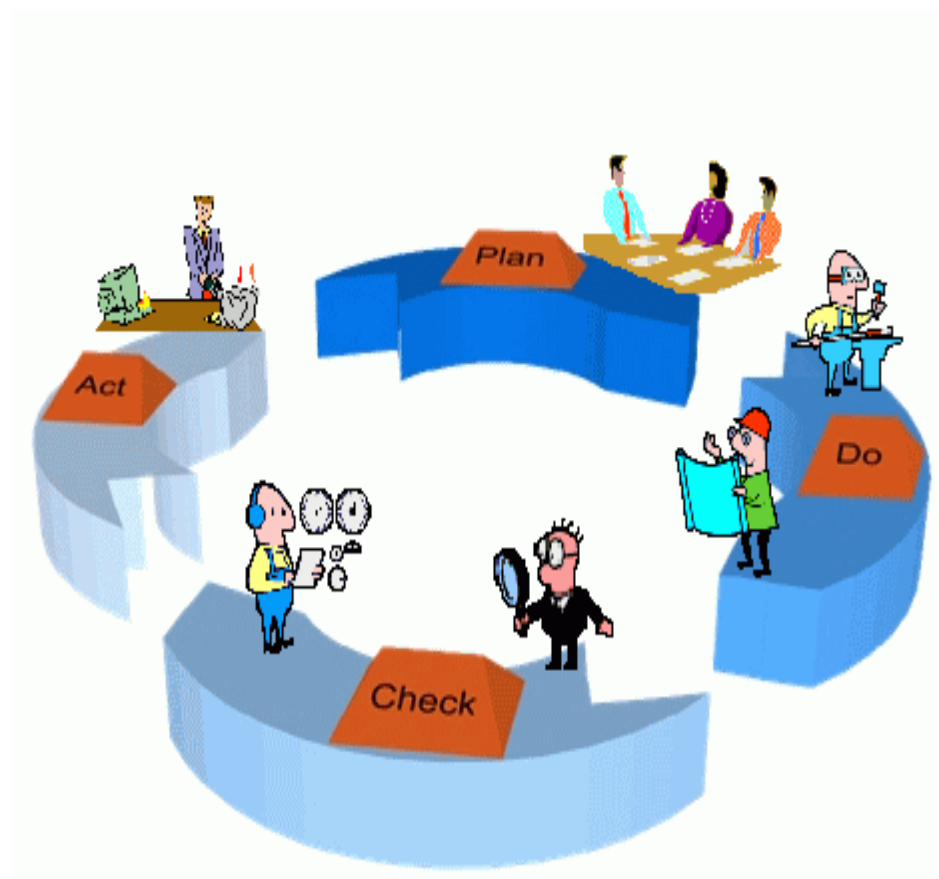
Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.

- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

#### 4. ¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.



**Figura 5:** Ciclo continuo PDCA.

- Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.
- Act (actuar): mantener y mejorar el SGSI.

### **Plan: Establecer el SGSI**

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad que:
  - incluya el marco general y los objetivos de seguridad de la información de la organización;
  - considere requerimientos legales o contractuales relativos a la seguridad de la información;
  - esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
  - establezca los criterios con los que se va a evaluar el riesgo;
  - esté aprobada por la dirección.
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).
- Identificar los riesgos:



- Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios; – identificar las amenazas en relación a los activos;
  - Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
  - Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- Analizar y evaluar los riesgos:
    - Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
    - Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
    - Estimar los niveles de riesgo;
    - Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
  - Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
    - aplicar controles adecuados;

- aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
- evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
- transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.



**Figura 6:** Sistema de Gestión de la Seguridad de la Información.

- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.

- Definir una declaración de aplicabilidad que incluya:
  - los objetivos de control y controles seleccionados y los motivos para su elección;
  - los objetivos de control y controles que actualmente ya están implantados;
  - los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001, en su segunda cláusula, en términos de documento indispensable para la aplicación de este documento” y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

#### **Do: Implementar y utilizar el SGSI**

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

#### **Check: Monitorizar y revisar el SGSI**

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
  - detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
  - identificar brechas e incidentes de seguridad;
  - ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
  - detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
  - determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

**Act: Mantener y mejorar el SGSI**

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

## **5. ¿Qué tareas tiene la Gerencia en un SGSI?**

Uno de los componentes primordiales en la implantación exitosa de un Sistema de Gestión de Seguridad de la Información es la implicación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI

una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (recuérdese que el alcance no tiene por qué ser toda la organización).

Algunas de las tareas fundamentales del SGSI que ISO 27001 asigna a la dirección se detallan en los siguientes puntos:

### **Compromiso de la dirección**

La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Para ello, debe tomar las siguientes iniciativas:

- ☞ Establecer una política de seguridad de la información.
- ☞ Asegurarse de que se establecen objetivos y planes del SGSI.
- ☞ Establecer roles y responsabilidades de seguridad de la información.
- ☞ Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- ☞ Asignar suficientes recursos al SGSI en todas sus fases.

- ☞ Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- ☞ Asegurar que se realizan auditorías internas.
- ☞ Realizar revisiones del SGSI, como se detalla más adelante.

### **Asignación de recursos**

Para el correcto desarrollo de todas las actividades relacionadas con el SGSI, es imprescindible la asignación de recursos. Es responsabilidad de la dirección garantizar que se asignan los suficientes para:

- ☞ Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- ☞ Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
- ☞ Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- ☞ Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- ☞ Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- ☞ Mejorar la eficacia del SGSI donde sea necesario.

### **Formación y concienciación**

La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al



que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado. Se deberá:

- ☞ Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.
- ☞ Satisfacer dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación del personal ya formado.
- ☞ Evaluar la eficacia de las acciones realizadas.
- ☞ Mantener registros de estudios, formación, habilidades, experiencia y cualificación.

Además, la dirección debe asegurar que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

### **Revisión del SGSI**

A la dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.

- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.
- Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a mejora de la eficacia del SGSI.
- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

## **6. ¿Se integra un SGSI con otros sistemas de gestión?**

Un SGSI es, en primera instancia, un sistema de gestión, es decir, una herramienta de la que dispone la gerencia para dirigir y

controlar un determinado ámbito, en este caso, la seguridad de la información.

La gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales: se gestiona la calidad según ISO 9001, el impacto medio-ambiental según ISO 14001. Ahora, se añade ISO 27001 como estándar de gestión de seguridad de la información.

Las empresas tienen la posibilidad de implantar un número variable de estos sistemas de gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

El objetivo último debería ser llegar a un único sistema de gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA de mejora continua común a todos estos estándares. Las facilidades para la integración de las normas ISO son evidentes mediante la consulta de sus anexos.

ISO 27001 detalla en su Anexo C, punto por punto, la correspondencia entre esta norma y la ISO 9001 e ISO 14001. Ahí se observa la alta correlación existente y se puede intuir la posibilidad de integrar el sistema de gestión de seguridad de la información en los sistemas de gestión existentes ya en la organización. Algunos puntos que suponen una novedad en ISO 27001 frente a otros estándares son la evaluación de riesgos y el establecimiento de una declaración de aplicabilidad (SOA), aunque ya se plantea incorporar éstos al resto de normas en un futuro.

### 2.2.3. Desarrollo de la propuesta

#### MODELO DE CASOS DE USO DEL NEGOCIO

**Diagrama 2.1:** Caso de uso del Negocio de SGSI de la Comisaria de la PNP región Huancavelica.

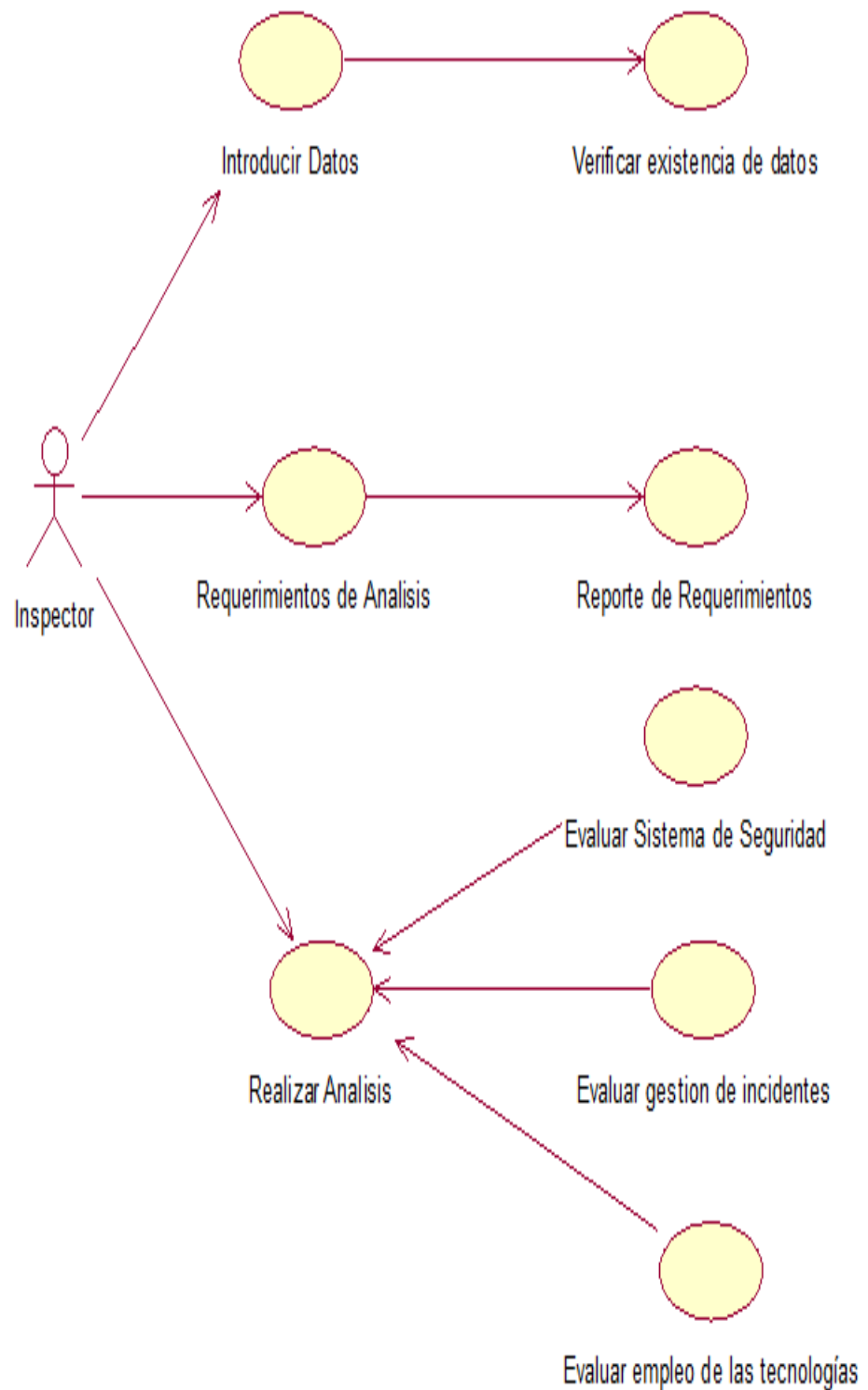


Diagrama 2.2: DIAGRAMA DE CLASES

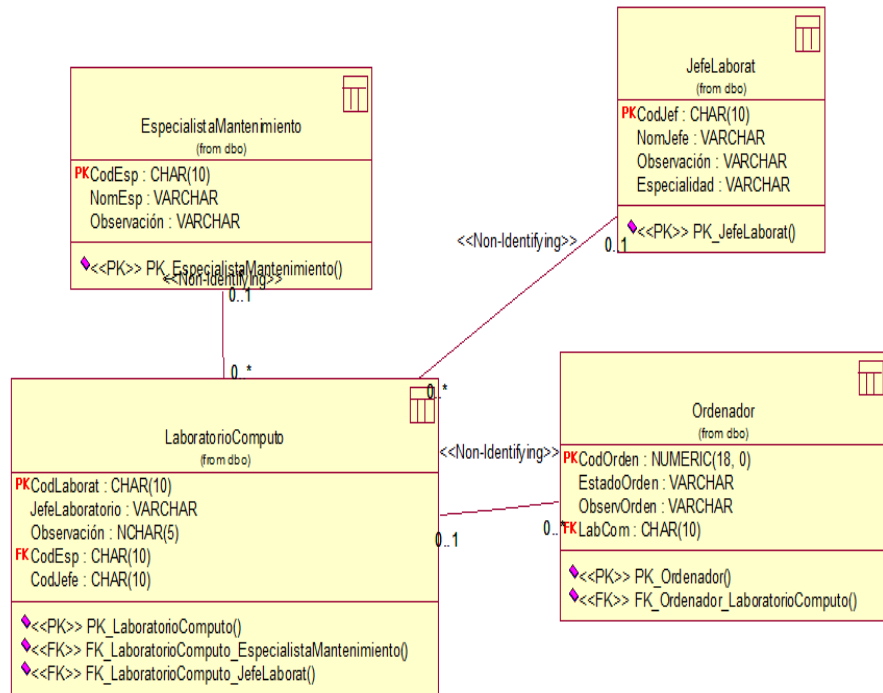
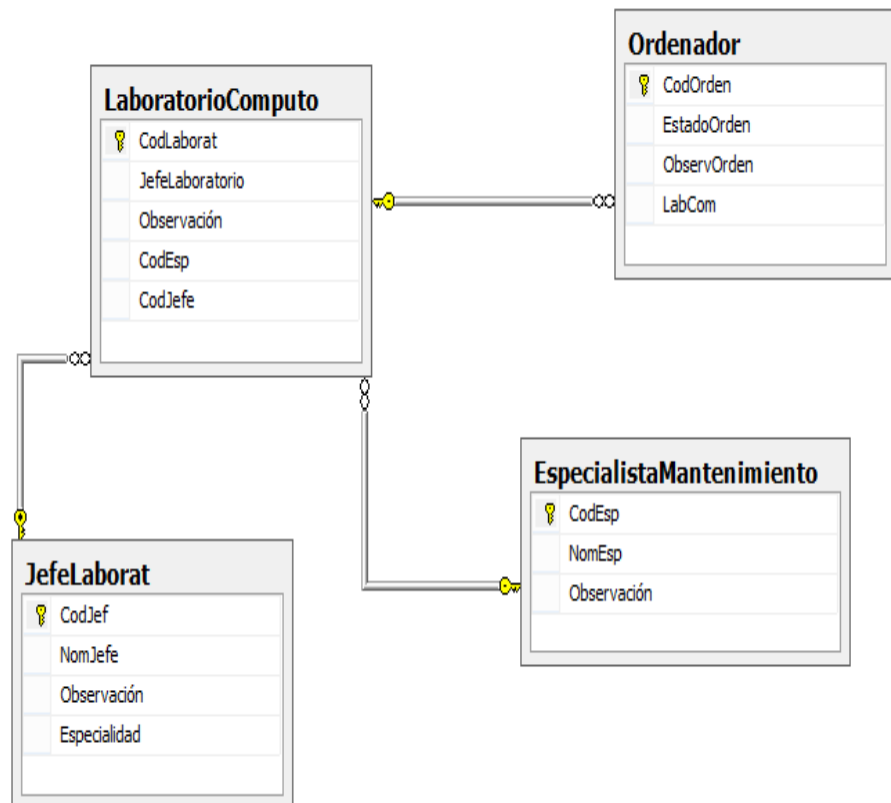
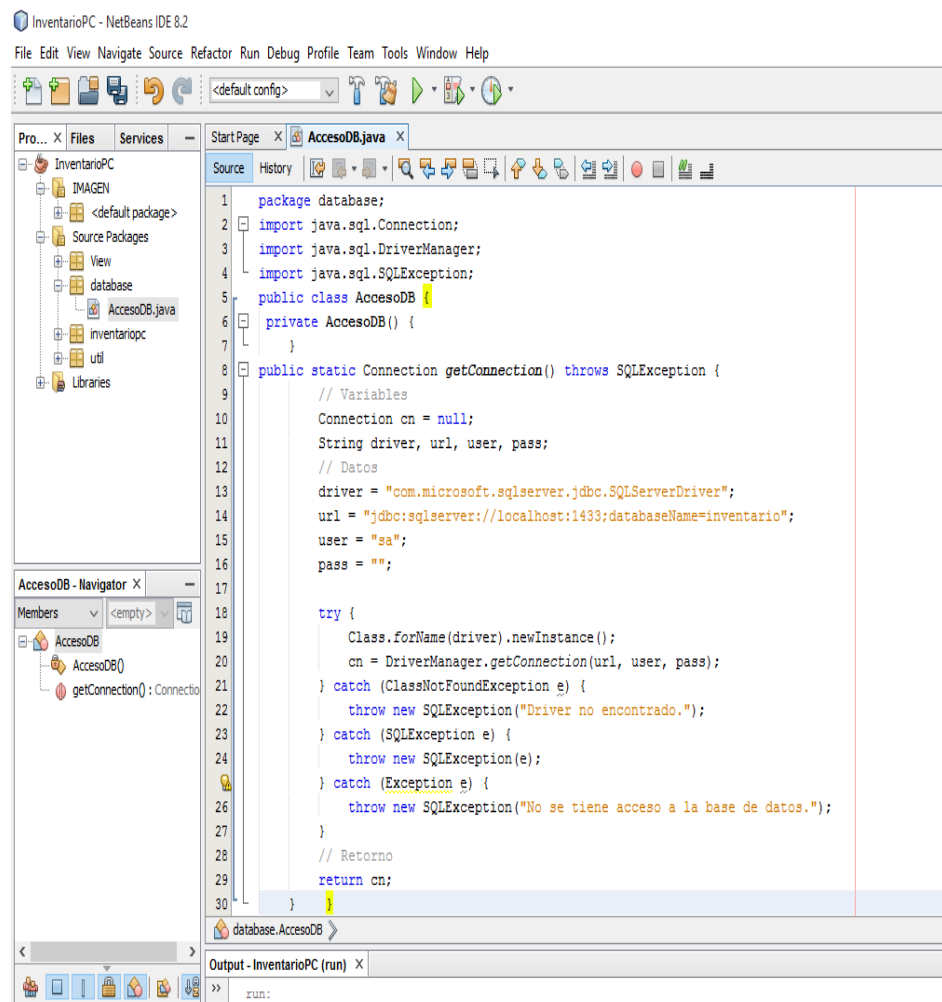


Diagrama 2.3: DISEÑO FISICO DE LA BASE DE DATOS.



**Diagrama 2.4:** Conexión de Base de Datos SQL a NetBeans.



**Diagrama 2.5:** Interfaz Usuario a NetBeans.



**Diagrama 2.6:** Interfaz Ingresar Datos de HARDWARE.

PROYECTO DE TESIS - UNDAC

Insertar Datos Consulta Reporte Ventana

**Características de HARDWARE**

Código de Equipo: 30

Tipo de HARDWARE: Monitor

Serie de HARDWARE: 564646464645

Marca de HARDWARE: LG

Color de HARDWARE: NEGRO

Característica de HARDWARE: 17"

Estado: ACTIVO

Fecha de Ingreso: 2018-12-01

Fecha de baja: 2017-02-03

Área o Lugar: AREA01

Nuevo

Grabar

Modificar

Eliminar

**Diagrama 2.7:** Reporte Inventario de Hardware.

Reporte General

REPORTE DE HARDWARE

**INVENTARIO DE HARDWARE**

Nº	Tipo	Serie	Marca	Color	Característica	Estado	Fecha Entrada	Fecha Salida	codArea
1	Monitor	564646464645	LG	NEGRO	17"	ACTIVO	1/12/18 0:00	3/02/17 0:00	AREA01
2	TECLADO	564646464646	GENIUS	BLANCO	ESPAÑOL	ACTIVO	11/05/08 0:00	4/02/10 0:00	AREA01
5	DISCO DURO	3133656454	TOSHIBA	NEGRO	1 G	ACTIVO	13/08/14 0:00	25/04/17 0:00	AREA01
6	DISCO DURO	9798956562	SAMSUNG	PLATEADO	3 G	ACTIVO	13/08/15 0:00	25/04/18 0:00	AREA01
7	IMPRESORA	8756235485	HP	PLOMO	CON CARTUCHO	ACTIVO	7/09/13 0:00	4/05/15 0:00	AREA01

Página 1 de 1

## 2.3. Definición de términos básicos

### 2.3.1. Sistema de información (SI).

Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos formarán parte de alguna de las siguientes categorías:

Personas;

Actividades o técnicas de trabajo;

Datos;

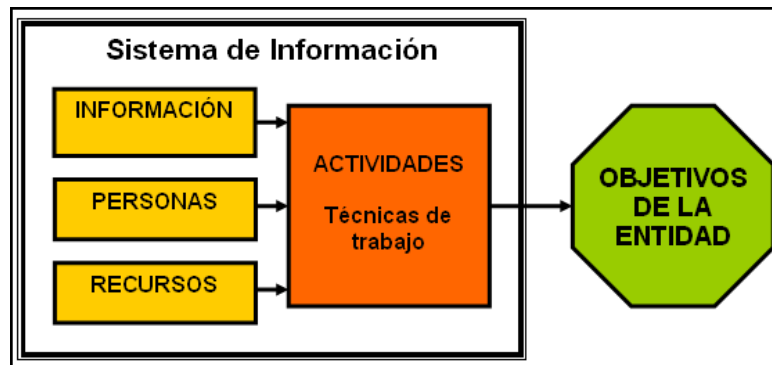
Recursos materiales en general [(Papel, lápices, libros, carpetas, etc. Estas actividades de recolección y procesamiento de información, eran actividades manuales y solo con la llegada de la tecnología, (computadoras, Internet, etc, se han convertido en sistemas con recursos informáticos y de comunicación).

Todos estos elementos interactúan para procesar los datos (incluidos los procesos manuales y automáticos) y dan lugar a información más elaborada, que se distribuye de la manera más adecuada posible en una determinada organización, en función de sus objetivos. Si bien la existencia de la mayor parte de sistemas de información es de conocimiento público, recientemente se ha revelado que desde finales del siglo XX diversos gobiernos han instaurado sistemas de información para el espionaje de carácter secreto.

Habitualmente el término "sistema de información" se usa de manera errónea como sinónimo de sistema de información informático, en parte porque en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos. Estrictamente hablando, un sistema de información no tiene por qué disponer de dichos recursos (aunque en la práctica esto no suele ocurrir). Se podría decir entonces que los sistemas de



información informáticos son una subclase o un subconjunto de los sistemas de información en general.



**Figura 7:** Elementos de un sistema de información.

### 2.3.2. Información

La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Existen diversos enfoques para el estudio de la información:

En biología, la información se considera como estímulo sensorial que afecta al comportamiento de los individuos.

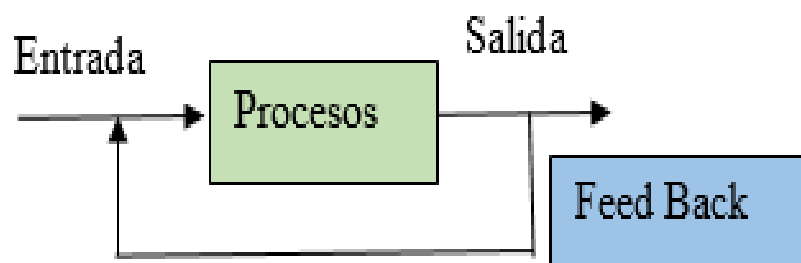
En computación y teoría de la información, como una medida de la complejidad de un conjunto de datos.

En comunicación social y periodismo, como un conjunto de mensajes intercambiados por individuos de una sociedad con fines organizativos concretos.

Los datos sensoriales una vez percibidos y procesados constituyen una información que cambia el estado de conocimiento, eso permite a los individuos o sistemas que poseen dicho estado nuevo

de conocimiento tomar decisiones pertinentes acordes a dicho conocimiento.

Desde el punto de vista de la ciencia de la computación, la información es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del que posee dicha información con su entorno.



**Figura 8:** Datos procesados se obtiene la información.

## 2.4. Formulación de Hipótesis

### 2.4.1. Hipótesis General

**Hi:** El Sistema de Gestión de Seguridad de Información mejorará la protección informática de la Comisaria región Huancavelica.

### 2.4.2. Hipótesis Específicas

**H1:** El Sistema de Gestión de Seguridad de Información incrementará la confidencialidad de la seguridad en la protección informática de la Comisaria región Huancavelica.

**H2:** El sistema de gestión de seguridad de información incrementará la integridad de la seguridad en la protección informática de la Comisaria región Huancavelica.

**H3:** El sistema de gestión de seguridad de información incrementará la disponibilidad de la seguridad en la protección informática de la Comisaria región Huancavelica.

## 2.5. Identificación de las Variables

### 2.5.1. Variable Independiente

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

### 2.5.2. Variable Dependiente

LA PROTECCIÓN INFORMÁTICA.

## 2.6. Definición operacional de variables e indicadores.

VARIABLES	INDICADORES
<p><b>Variable Independiente</b></p> <p>SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</p>	<ul style="list-style-type: none"> <li>➤ Gestión del riesgo</li> <li>➤ Control de la seguridad</li> <li>➤ Ciclo de vida de los sistemas</li> <li>➤ Planes de seguridad</li> <li>➤ Seguridad en Recursos Humanos</li> <li>➤ Protección física de las oficinas de trabajo</li> <li>➤ Seguridad en el puesto de trabajo</li> <li>➤ Control de la información saliente/entrante</li> </ul>

	<ul style="list-style-type: none"> <li>➤ Mantenimiento y actualización del hardware y software</li> <li>➤ Documentación de las políticas, procesos, guías e instrucciones técnicas</li> <li>➤ Concienciación de los usuarios</li> <li>➤ Respuesta ante incidentes</li> </ul>
<p><b>Variable Dependiente</b></p> <p>LA PROTECCIÓN INFORMÁTICA.</p>	<ul style="list-style-type: none"> <li>➤ Nivel de confidencialidad de la seguridad de información.</li> <li>➤ Nivel de integridad de la seguridad de información.</li> <li>➤ Nivel de disponibilidad de la seguridad de información.</li> <li>➤ Nivel de Autenticación. de la seguridad de información</li> </ul>

## CAPÍTULO III

### METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN

#### 3.1. Tipo de investigación.

- Según la finalidad: Investigación **Aplicada**, porque se está utilizando conocimientos pre existente.

Investigaciones teóricas o experimentales que aplican los conocimientos de la ciencia básica para resolver problemas prácticos. Estudia problemas de posible interés social.

- Según naturaleza de las Variables: Investigación **cuantitativa**.

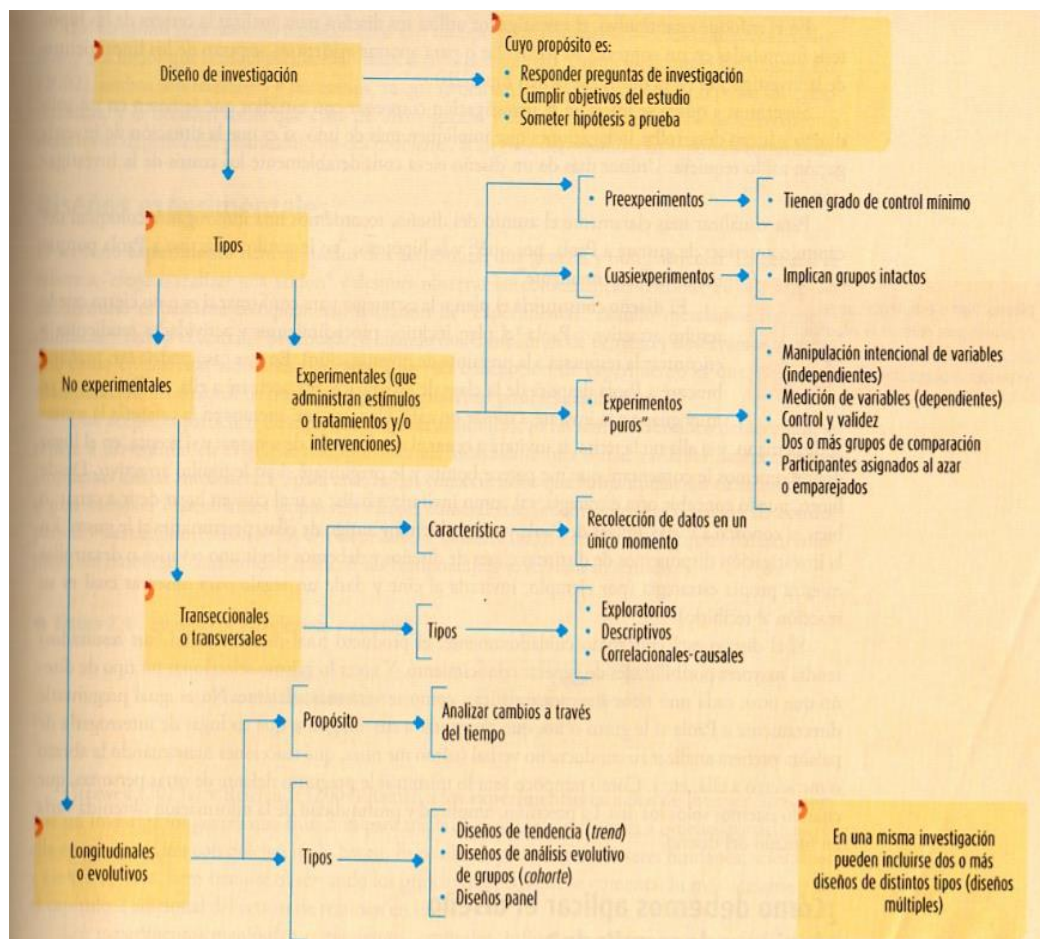
#### 3.2. Métodos de investigación.

Para el presente trabajo de investigación se empleará el método **Hipotético deductivo**.

#### 3.3. Diseño de Investigación

- **Experimental.**

Según el libro Metodología de Investigación 6ta Edición Pag. 127 de Hernández Sampiere, Fernández Collado & Baptista Lucio (2010), los Tipos de Diseño de investigación son No experimentales y experimentales. Este proyecto de tesis es de tipo experimental y a su vez es de tipo experimentos “Puros” porque se administra estímulos o se manipula intencionalmente la variable independiente y se mide la variable dependiente. Tenemos dos grupos de comparación uno es el grupo de control y el otro es el grupo experimental.



**Figura 9:** Tipos de Diseño de investigación.

### 3.4. Población y muestra.

- ☞ **Universo:** La población de la presente investigación lo constituirá los policías especialistas en área informática de la Comisaria de la PNP de la región de Huancavelica.
- ☞ **Muestra:** Esta muestra se considera del tipo probabilística de la presente investigación; lo constituirá los 30 policías especialista en área informática de la Comisaria de la PNP de la región de Huancavelica.

$$n = \frac{N * Z_{\infty}^2 * p * q}{d^2 * (N - 1) + Z_{\infty}^2 * p * q^2}$$

Dónde:

n = Tamaño de la muestra

N = Tamaño de la población o universo.

Z = Valor de Z crítico, calculado en las tablas del área de la curva normal.

Llamado también nivel de confianza.

$s^2$  = Varianza de la población en estudio (Que es el cuadrado de la desviación estándar y puede obtenerse de estudios similares o pruebas piloto).

d = nivel de precisión absoluta. Referido a la amplitud del intervalo de confianza deseado en la determinación del valor promedio de la variable en estudio.

$q = 1 - p$  (en este caso  $1 - 0.05 = 0.95$ ) si no se tiene  $P=50\%$  (Probabilidad de éxito)  $Q=50\%$  (Probabilidad de fracaso).

$d = 5\%$ (Error muestral)

Entonces:

☞  $N = 32$

☞  $Z\alpha = 1.96$  al cuadrado (si la seguridad es del 95%)

☞  $p =$  proporción esperada (en este caso  $50\% = 0.5$ )

☞  $q = 1 - p$  (en este caso  $1 - 0.5 = 0.5$ )

☞  $d =$  precisión (en su investigación use un 5%) o error muestral.

$$n = \frac{32 * 1.96^2 * 0.5 * 0.5}{0.05^2 * (32 - 1) + 1.96^2 * 0.5 * 0.5}$$

$$n = \frac{32 * 3.84 * 0.25}{0.0025 * (31) + 3.84 * 0.25}$$

$$n = \frac{32 * 0.96}{0.0025 * (31) + 0.96}$$

$$n = \frac{30.72}{0.08 + 0.96}$$

$$n = \frac{30.72}{1.04}$$

$$n = 29.54$$

$$n = 30$$



La muestra es n=30.

**Calculadora del tamaño de la muestra**

Traducida y adaptada por Manuel Lobos González  
2005  
© 2004 by Raosoft, Inc

**¿Cuál es el tamaño de la Población?**  Corresponde al total de unidades de las cuales se puede seleccionar su muestra aleatoria.  
Si usted no conoce el tamaño de la Población, use 150000. Si no conoce el tamaño de la población, digite 150000.

**¿Cuál es el margen de error que acepta?**  % El margen de error es la cantidad de error que usted puede tolerar. Significa elegir la probabilidad de rechazar una hipótesis nula verdadera. Por ejemplo, un margen de error de 1% significa que las observaciones o resultados derivados de la investigación en curso, pueden deberse al azar en hasta un 1% de los casos. Para un margen inferior de error, se requiere un tamaño de muestra mayor.

**¿Cuál es el nivel de confianza que usted necesita?**  % El nivel de confianza indica el porcentaje de seguridad que existe para generalizar los resultados obtenidos. Esto quiere decir que un porcentaje del 100% equivale a decir que no existe ninguna duda para generalizar tales resultados, pero también implica estudiar a la totalidad de los casos de la población. Para evitar un costo muy alto para el estudio o debido a que en ocasiones llega a ser prácticamente imposible el estudio de todos los casos, entonces se busca un porcentaje de confianza menor. Comúnmente en las investigaciones sociales se busca un 95%. Un alto nivel de confianza requiere un tamaño de muestra mayor.

**¿Cuál es la variabilidad conocida?**  % La variabilidad es la probabilidad (o porcentaje) con el que se aceptó y se rechazó la hipótesis que se quiere investigar en alguna investigación anterior o en un ensayo previo a la investigación actual. El porcentaje con que se aceptó tal hipótesis se denomina variabilidad positiva y se denota por p, y el porcentaje con el que se rechazó se la hipótesis es la variabilidad negativa, denotada por q. Cuando se habla de la máxima variabilidad, en el caso de no existir antecedentes sobre la investigación (no hay otras o no se pudo aplicar una prueba previa), entonces los valores de variabilidad es p=q=0.5 o 50%.

---

**El tamaño recomendado para su muestra es de**  **unidades** Éste es el tamaño mínimo recomendado para la muestra de su estudio.  
Con este mínimo de unidades, usted podrá realizar la investigación sin más costo del necesario, pero con la seguridad de que las condiciones aceptadas para la generalización (confiabilidad, variabilidad y error) se mantienen.

**Escenarios Alternativos**

Con un tamaño de muestra de	<input style="width: 40px;" type="text" value="100"/>	<input style="width: 40px;" type="text" value="200"/>	<input style="width: 40px;" type="text" value="300"/>	Para un nivel de confianza de	<input style="width: 40px;" type="text" value="90"/>	<input style="width: 40px;" type="text" value="95"/>	<input style="width: 40px;" type="text" value="99"/>
Su margen de error sería	0.00%	0.00%	0.00%	El tamaño de su muestra debe ser de	29	30	31

**Figura 10:** Calculadora para hallar la muestra de investigación científica en página WEB.

### 3.5. Técnicas e instrumentos de recolección de datos.

#### 3.5.1. Técnicas:

- ✓ Encuestas.- La encuesta es una técnica de adquisición de información de interés sociológico, mediante un cuestionario

previamente elaborado, a través del cual se puede conocer la opinión o valoración del sujeto seleccionado en una muestra sobre un asunto dado.

- ✓ La observación.- La observación es una técnica que consiste en la utilización de los sentidos para captar cualquier hecho, fenómeno o situación relativa a la investigación en progreso. Esta técnica puede tomar dos modalidades: Estructurada y no estructurada o libre, según el investigador previamente establezca o no, un plan de trabajo e incorpore o no los dispositivos o herramientas apropiadas para la elección y registro de los aspectos a observar.

La observación como técnica de recolección de datos se materializa mediante siete instrumentos: Guía de observación, lista de frecuencia, lista de cotejo o de chequeo, escala de estimación, registro anecdótico, cuaderno de protocolo y diario de campo, (para observación estructurada, para observación no estructurada).

- ✓ Entrevistas.- La entrevista es una técnica de recopilación de información mediante una conversación profesional, con la que además de adquirirse información acerca de lo que se investiga, tiene importancia desde el punto de vista educativo; los resultados a lograr en la misión dependen en gran medida del nivel de comunicación entre el investigador y los participantes en la misma.

Si la entrevista persigue el objetivo de adquirir información acerca de las variables de estudio, el entrevistador debe tener clara la hipótesis de trabajo, las variables y relaciones que se quieren demostrar; de

forma tal que se pueda elaborar un cuestionario adecuado con preguntas que tengan un determinado fin y que son imprescindibles para esclarecer la tarea de investigación, así como las preguntas de apoyo que ayudan a desenvolver la entrevista.

### 3.5.2. Instrumentos:

- ✓ Cuestionarios. El cuestionario es un instrumento básico de la observación en la encuesta y en la entrevista. En el cuestionario se formula una serie de preguntas que permiten medir una o más variables. Posibilita observar los hechos a través de la valoración que hace de los mismos el encuestado o entrevistado, limitándose la investigación a las valoraciones subjetivas de éste.

Ejemplo:

Considera usted que la motivación es esencial en el rendimiento laboral. Si\_\_\_\_ No\_\_\_\_\_.

Marque con una equis (x) el último nivel de estudios culminado Básico completo\_\_\_\_ Media Diversificada\_\_\_\_ Técnico Superior\_\_\_\_\_.

Licenciatura o equivalente \_\_\_\_ Especialización \_\_\_\_ Maestría\_\_\_\_  
 Doctorado\_\_\_\_\_ En referencia a la intervención de fuerzas militares extranjeras en otro país, usted está:

A favor\_\_\_\_ En contra\_\_\_\_\_. El otorgamiento de incentivos económicos incrementa la productividad de los empleados.

Siempre \_\_\_\_ Casi siempre \_\_\_\_ Algunas veces \_\_\_\_ Nunca \_\_\_\_.

✓ Guías de Observación.

Consiste en listar la serie de eventos, procesos, hechos o situaciones a ser observados, su ocurrencia y características (ello es factible con base a un ejercicio de visión previo con miras a establecer los aspectos a observar). Se asocia generalmente con las interrogantes u objetivos específicos del estudio.

Ejemplo:

Objetivo específico: Identificar los mecanismos de acceso a las instalaciones de la Empresa					
Hechos o eventos	Registro de identificación	Control informático de entrada	Autorización de entrada	Ingreso a Las instalaciones	Registro de presencia en las instalaciones
Lista De empleados					

✓ Lista de Cotejo o Chequeo.

Es un tipo de instrumento en el que se indica o no la presencia de un aspecto, rasgo, conducta o situación a ser observada. Su estructura debe especificar los aspectos, conductas, hechos, etc que se pretendan observar y la presencia o no de estas. Es conveniente vincularla a algún objetivo específico.

Ejemplo:

Objetivo específico: caracterizar la situación actual de la Planta Física del Cuam, Div. Caracas		
Aspectos	Si	No
Los salones de clase son amplios		
La iluminación es apropiada		
La ventilación es adecuada		
Los baños están en buen estado		
Las salidas de emergencia funcionan		

✓ Escala de Estimación.

Esta modalidad de instrumento no solo considera la presencia o ausencia de los aspectos a observar, sino que incluye una escala que estima o valora, con algún criterio, como se manifiesta la situación, conducta o hecho objeto de la observación, vale decir presentan gradaciones para jerarquizarlas o calificarlas.

Ejemplo:

\* El trato que se ofrece a los clientes es:

Bueno\_\_\_\_\_, Regular \_\_\_\_\_, Malo\_\_\_\_\_, Muy malo\_\_\_\_\_.

\* El profesor promueve la participación en clase

Siempre\_\_\_\_\_, Casi siempre\_\_\_\_\_, Algunas veces\_\_\_\_\_,  
Nunca\_\_\_\_\_.

Técnica	Tipo	Instrumento
Observación	Participante	Registro anecdótico, cuaderno de protocolo, diario de campo
	No participante	Guía de observación, lista de frecuencia, lista de chequeo o cotejo, escala de estimación, matriz de análisis
Encuesta	Oral	Grabadora, video
	Escrita	Cuestionario, prueba, test, escala
Entrevista	Estructurada	Guión o guía de entrevista
	No estructurada	Libreta de notas, grabador/ cámara de video
Sociométrica		Test sociométrico
De organización y métodos		Flujogramas de procesos, diagrama de análisis y recorrido de formas y gráfico de Gantt.

### 3.6. Técnicas de procesamiento y análisis de datos

Una vez recogido los datos, es necesario realizar su procesamiento, lo que incluye:

- La codificación
- La Tabulación
- El análisis y la interpretación

### 3.7. Tratamiento Estadístico

La estrategia para probar las hipótesis, se iniciará primero con la formulación de la encuesta., se determinará el estadístico de prueba seleccionado y corresponde al investigador la interpretación del resultado. El estadístico a emplear será el chi-cuadrado, porque permite determinar la relación entre las dos variables determinadas, como es en el caso de la presente investigación, que se presentan en una tabla de contingencia, asimismo la prueba de independencia del Chi-cuadrado, partirá de la hipótesis de que las variables son independientes; es decir,

que no existe ninguna relación entre ellas y que por lo tanto ninguna ejerce influencia sobre la otra. El objetivo de la prueba de Chi-cuadrado, es comprobar la hipótesis mediante el nivel de significación, por lo que si el valor de significación es mayor o igual que el alfa predeterminado (0.05 ó 5%) se aceptara la hipótesis, pero si esta es menor, será rechazada.

Con la finalidad de lograr medir la influencia de la variable independiente (causa) *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN* para la obtención de resultados de la variable dependiente (efecto) *PROTECCIÓN DE INFORMACIÓN* de la Comisaria de la PNP de la región de Huancavelica se ejecuta y presenta los resultados de la encuesta y el análisis e interpretación correspondiente: **RESULTADO DE LA ENCUESTA PARA LOGRAR MEDIR LA INFLUENCIA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA PROTECCIÓN INFORMÁTICA DE LA COMISARIA REGIÓN HUANCAVELICA.**

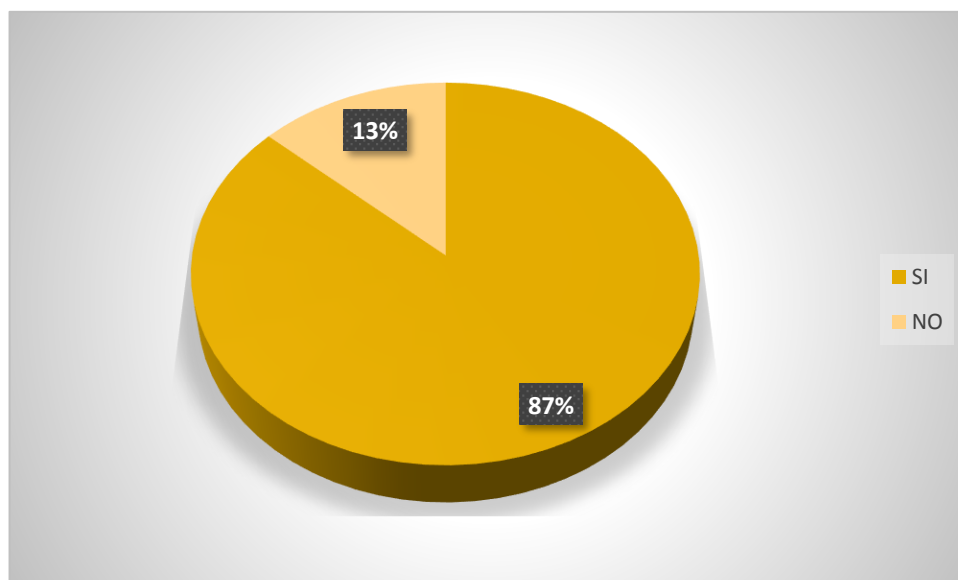
### 3.8. Selección, validación y confiabilidad de los instrumentos de investigación.

1. ¿La organización reduce y mitiga los riesgos de los activos de información?

**Tabla 4.1:** Reducirá y mitigará los riesgos de los activos de la información.

<b>SI</b>	26	86.67
<b>NO</b>	4	13.33
<b>Total</b>	30	100

Gráfico 4.1



#### a) Análisis

Tomando como referencia el porcentaje del gráfico 4.1, se analiza la pregunta Nro. 1 que al 87% Reducirá y mitigará los riesgos de los activos de la información.

#### b) Interpretación

Minimizará los riesgos de los activos de la información al 87%.

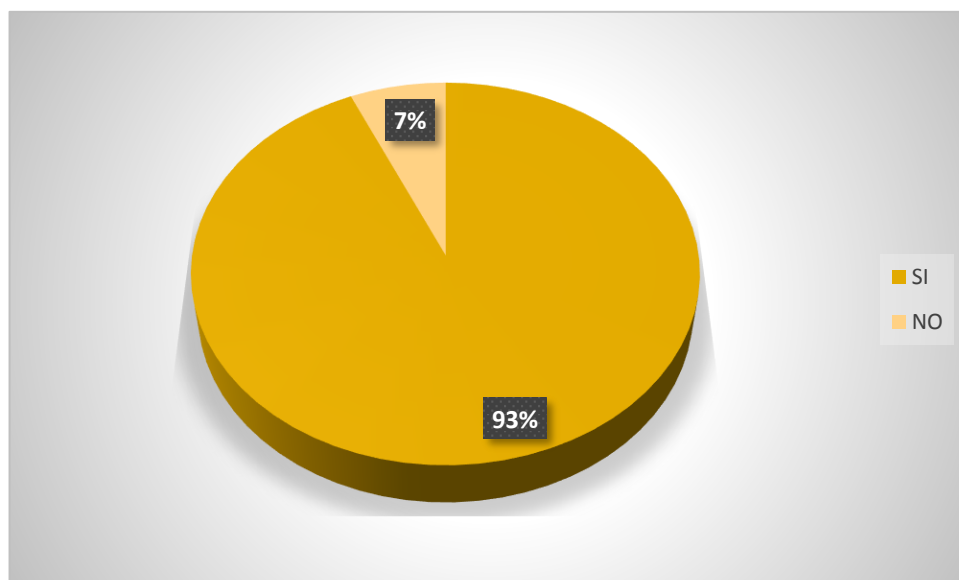
1. ¿La organización logra gestionar, monitorear, de manera eficiente los incidentes y vulnerabilidades de seguridad de la información?

**Tabla 4.2:** La organización gestiona, monitorea, de manera eficiente los incidentes y vulnerabilidades de seguridad de la información.

<b>SI</b>	28	93.33
<b>NO</b>	2	6.67
<b>Total</b>	30	100



Gráfico 4.2



#### a) Análisis

Tomando como referencia el porcentaje del gráfico 4.2, se ha logrado al 93% para gestionar, monitorear, de manera eficiente los incidentes y vulnerabilidades de seguridad de la información y el 7% no se ha logrado.

#### b) Interpretación

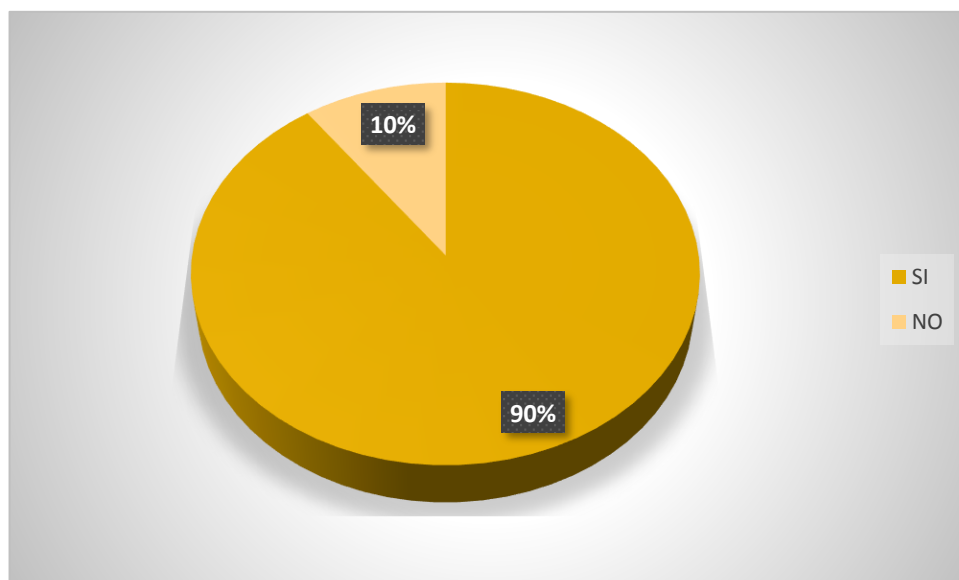
Al 93% la organización gestiona, monitorea, de manera eficiente los incidentes y vulnerabilidades de seguridad de la información.

2. ¿Los especialistas desarrolla medidas de seguridad para reducir los riesgos?

**Tabla 4.3:** Los especialistas desarrollan las medidas de seguridad para gestionar los riesgos.

<b>SI</b>	27	90.00
<b>NO</b>	3	10.00
<b>Total</b>	30	100

Gráfico 4.3



#### a) Análisis

Tomando como referencia el porcentaje del gráfico 4.3, al 90% los especialistas desarrollan las medidas de seguridad para gestionar los riesgos.

#### b) Interpretación

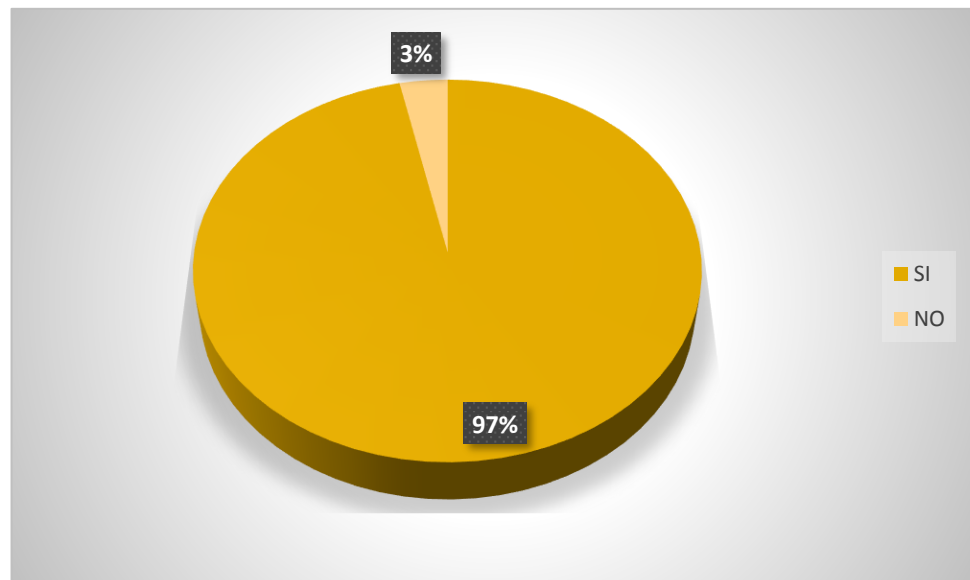
Los encuestados responden que al 90% los especialistas desarrollan las medidas de seguridad para gestionar los riesgos.

- ¿Seleccionan y capacitan especialistas involucrados en los procesos de Tecnología, en temas de seguridad de información?

**Tabla 4.4:** Seleccionan y capacitan especialistas involucrados en los procesos de Tecnología, en temas de seguridad de información.

<b>SI</b>	29	96.67
<b>NO</b>	1	3.33
<b>Total</b>	30	100

Gráfico 4.4

**a) Análisis**

Tomando como referencia el porcentaje del gráfico 4.4, de la pregunta Nro. 4 Seleccionan y capacitan especialistas involucrados en los procesos de Tecnología, en temas de seguridad de información al 97%.

**b) Interpretación**

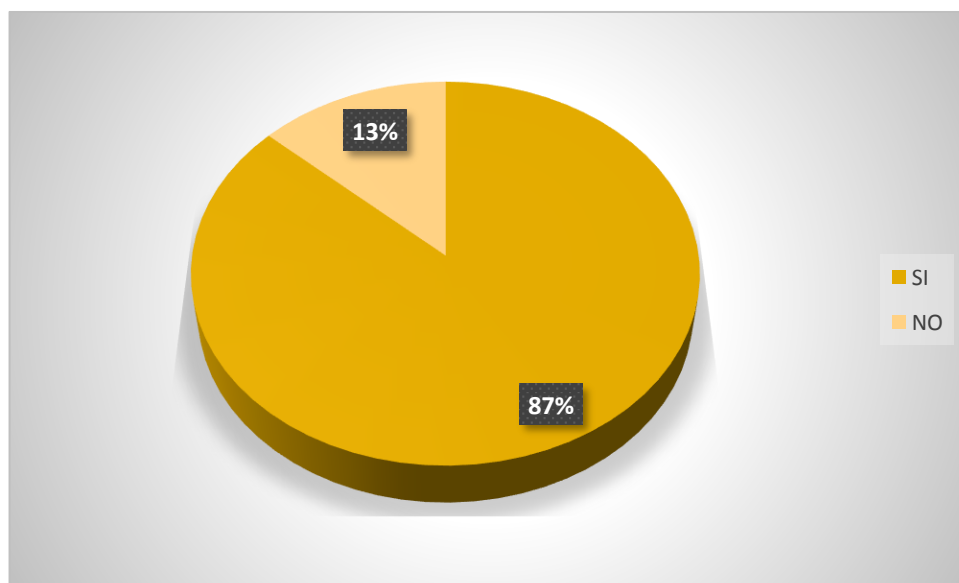
La organización selecciona y capacita especialistas involucrados en los procesos de Tecnología, en temas de seguridad de información al 97%.

4. ¿Cree usted que las medidas de seguridad utilizadas son suficientes para proteger la información y prevenir posibles incidentes?

**Tabla 4.5:** Las medidas de seguridad utilizadas son suficientes para proteger la información y prevenir posibles incidentes.

<b>SI</b>	26	86.67
<b>NO</b>	4	13.33
<b>Total</b>	30	100

**Gráfico 4.5**



**a) Análisis**

Tomando como referencia el porcentaje del gráfico 4.5, al 87% las medidas de seguridad utilizadas son suficientes para proteger la información y prevenir posibles incidentes.

**b) Interpretación**

Las medidas de seguridad utilizadas son suficientes al 87% para proteger la información y prevenir posibles incidentes.

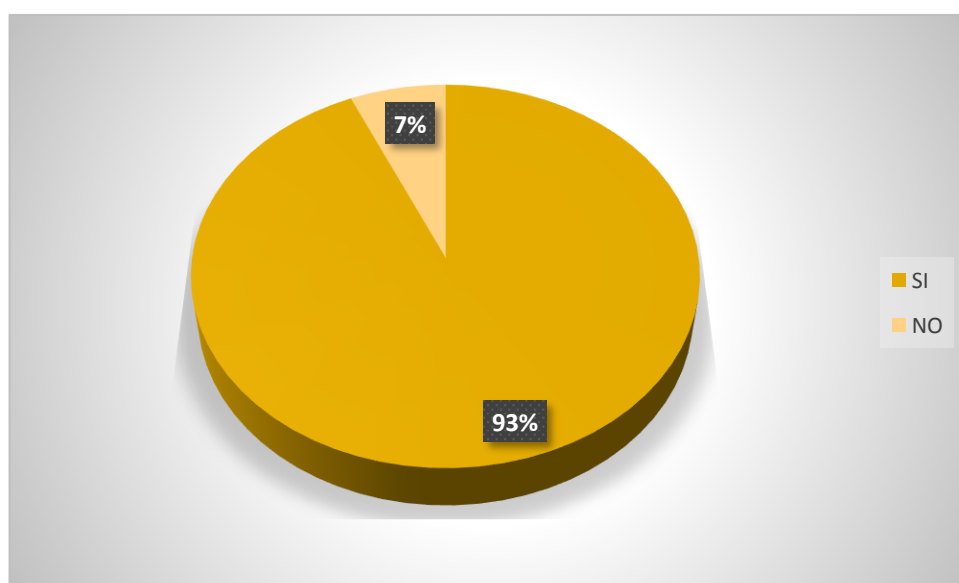
5. ¿Recomendaría usted adoptar políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la información?

**Tabla 4.6:** Recomendaría usted adoptar políticas de seguridad

encaminadas a proteger la información y evitar posibles daños de la información.

<b>SI</b>	28	93.33
<b>NO</b>	2	6.67
<b>Total</b>	30	100

**Gráfico 4.6**



#### **a) Análisis**

Tomando como referencia el porcentaje del gráfico 4.6, Según la encuesta en la pregunta Nro. 6 recomienda adoptar los encuestados al 93% política de seguridad encaminada a proteger la información y evitar posibles daños de la información

#### **b) Interpretación**

Al 93% de los encuestados recomiendan políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la

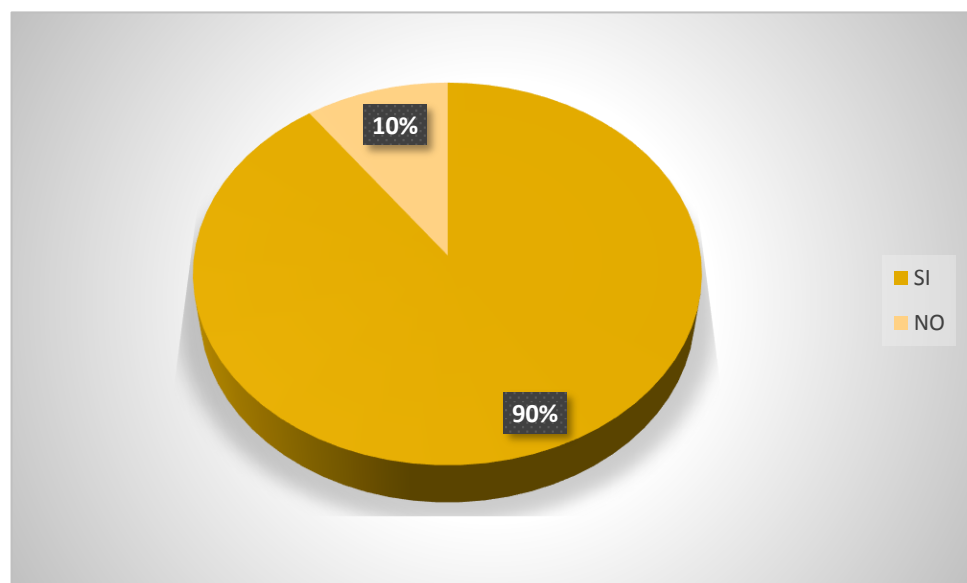
información.

6. ¿La organización elabora el plan de tratamiento de riesgos?

**Tabla 4.7:** La organización elabora el plan de tratamiento de riesgos.

<b>SI</b>	27	90.00
<b>NO</b>	3	10.00
<b>Total</b>	30	100

**Gráfico 4.7**



#### a) Análisis

Tomando como referencia el porcentaje del gráfico 4.7, se analiza la pregunta Nro. 7 que al 90% la organización tiene interés de elaborar el plan de tratamiento de riesgos.

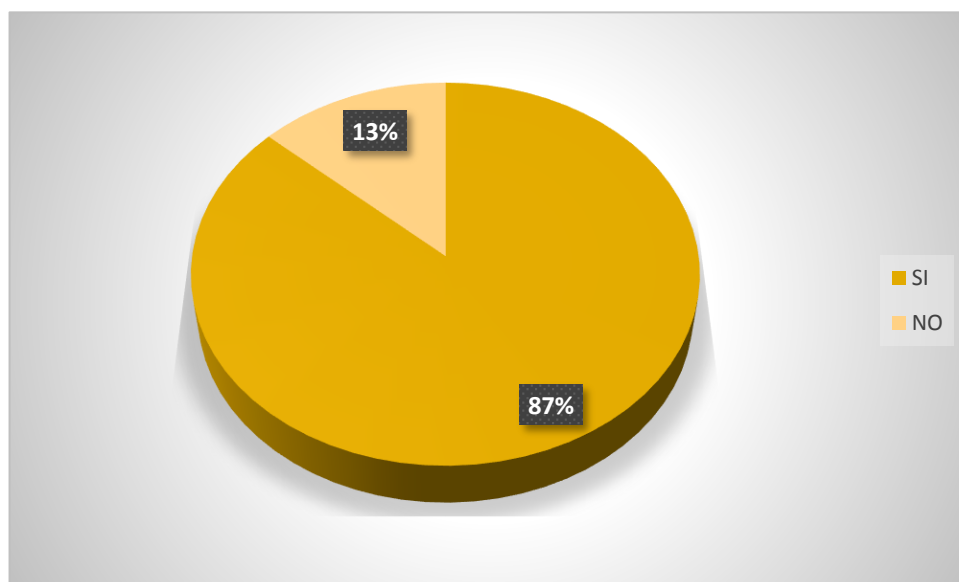
#### b) Interpretación

La organización tiene interés de elaborar el plan de tratamiento de riesgos al 90%.

7. ¿Cumplen la legislación vigente de seguridad de información?

**Tabla 4.8:** Cumplen la legislación vigente de seguridad de información.

<b>SI</b>	26	86.67
<b>NO</b>	4	13.33
<b>Total</b>	30	100

**Gráfico 4.8****a) Análisis**

Tomando como referencia el porcentaje del gráfico 4.8, se analiza la pregunta Nro. 8 que al 87% la organización cumple la legislación vigente de seguridad de información.

**b) Interpretación**

La organización cumple la legislación vigente de seguridad de información al 87%.

### **3.9. Orientación ética.**

El objetivo principal de la realización del estudio, fue la de establecer la relación que existe entre las variables: Sistema de gestión de seguridad de la información para mejorar la protección informática de la Comisaria región Huancavelica, dicho en otros términos se trató de verificar si la optimización de la capacidad de la protección de la Comisaria región Huancavelica, está vinculado a la necesidad del Sistema de gestión de seguridad de la información.



## **CAPÍTULO IV**

### **RESULTADOS Y DISCUSIÓN**

#### **4.1. Descripción del trabajo de campo**

Se trabajó con las unidades de análisis en base a una muestra representativa de 30 personas integrantes de la muestra en estudio. En cuanto a la recopilación de los datos, se emplearon como instrumento las encuestas, en base a un cuestionario de preguntas como técnica, el mismo que fue aplicado a las unidades de análisis anteriormente señalado, de otro lado para la comprobación de las hipótesis de investigación, se utilizó el estadístico de prueba de la Ji (Chi) Cuadrada ( $X^2$ ), por tratarse de variables cuanti-cualitativas, dando como resultado que tanto la hipótesis principal, como las específicas nulas fueran rechazadas, aceptándose las respectivas hipótesis planteadas

#### **4.2. Presentación, análisis e interpretación de resultados**

Una vez que se precisó el planteamiento del problema, se definió el alcance inicial de investigación y se formularon las hipótesis (o no se establecieron debido a la naturaleza de estudio), el término diseño se

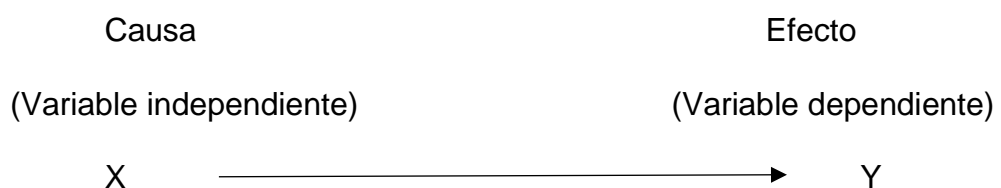
refiere al plan o estrategia concebida para obtener la información que se desea.

En el enfoque cuantitativo, el investigador utiliza su o sus diseños para analizar la certeza de las hipótesis formuladas en un contexto particular o para aportar evidencia respecto de los lineamientos de la investigación (si es que no tiene hipótesis).

Sugerimos a quien se inicia dentro de la investigación comenzar con estudios que se basen en un solo diseño. Utilizar más de un diseño eleva considerablemente los costos de la investigación.

El diseño de investigación es de tipo experimental donde tiene dos acepciones, una general y otra particular. *La general se refiere a “elegir o realizar una acción” y después observar las consecuencias. La esencia de esta concepción de experimento es que se requiere la manipulación intencional de una acción para analizar sus posibles resultados.*

*La que vamos a usar en nuestro proyecto es la acepción particular de experimento se refiere a un estudio en el que se manipula intencionalmente una y más variables independientes (supuestas causas-antecedentes), para analizar las consecuencias que la manipulación tiene sobre una o más variables dependientes (supuestos efectos-consecuentes), dentro de una situación de control para el investigador.*



**Figura 11.** Esquema de experimento y variable.

Los experimentos manipulan tratamientos, estímulos, influencias o intervenciones (denominadas variables independientes) para observar sus efectos sobre otras variables (las dependientes) en una situación de control.

El primer requisito de un experimento es la manipulación intencional de una o más variables independientes. La variable independiente es la que se considera como supuesta causa en una relación entre variables, es la condición antecedente, y al efecto provocado por dicha causa se le denomina variable dependiente (consecuente).

**VARIABLE INDEPENDIENTE:** Es el variable en el experimento, esta variable recibe el tratamiento o estímulo experimental.

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN.

**VARIABLE DEPENDIENTE:** Es la variable que mide el efecto LA PROTECCIÓN INFORMÁTICA

**INDICADORES DE LA VARIABLE DEPENDIENTE:**

- ☞ Nivel de confidencialidad de la seguridad de información.
- ☞ Nivel de integridad de la seguridad de información.
- ☞ Nivel de disponibilidad de la seguridad de información.
- ☞ Nivel de Autenticación de la seguridad de información.

**Eficacia** es la capacidad de lograr un efecto deseado, esperado o anhelado. En cambio, **Eficiencia** es la capacidad de lograr ese efecto en cuestión con el mínimo de recursos posibles o en el menor tiempo posible.

**La Efectividad** es la unión de Eficiencia y Eficacia, es decir busca lograr un efecto deseado, en el menor tiempo posible y con la menor cantidad de recursos.

Esta observación se realizó entre los días lunes 23 y martes 24 de julio del 2019; se utilizó los instrumentos como guía de observación y ficha técnica para la encuesta a 30 trabajadores y lograr obtener resultados de evaluación para la seguridad de información.

Se ha tomado esta cantidad de personas aleatoriamente porque es la muestra de la población que son los trabajadores de la Comisaria de la PNP de la región de Huancavelica para poder llevar a cabo el experimento.

Según Hernández Sampieri Roberto el grado de manipulación de la variable independiente en esta investigación es el nivel mínimo de manipulación es de presencia-ausencia de la variable independiente. Cada nivel o grado de manipulación involucra un grupo en el experimento. Este nivel o grado implica que un grupo se expone a la presencia de la variable independiente y el otro no. Posteriormente, los dos grupos se comparan para saber si el grupo expuesto a la variable independiente difiere del grupo que no fue expuesto. Al primero se le conoce como **grupo experimental** y al otro en el que está ausente la variable independiente, se le denomina **grupo de control**. Pero en realidad ambos grupos participan en el experimento.

A la presencia de la variable independiente con frecuencia se le llama "tratamiento experimental", "intervención experimental" o "estímulo experimental". Es decir, el grupo experimental recibe el tratamiento o estímulo experimental o lo que es lo mismo se le expone a la variable independiente; el grupo de control no recibe el tratamiento experimental. Ahora bien, el hecho de que uno de los grupos no se exponga al

tratamiento experimental no significa que su participación en el experimento sea pasiva. Por el contrario, implica que realiza las mismas actividades que el grupo experimental, excepto someterse al estímulo. Con los 30 especialistas en informática, se ha procedido a hacer las pruebas para el proceso del Sistema Tradicional de Seguridad de la Información y los resultados que se han obtenido se presentan en la siguiente tabla, TABLA N° 4.9.

- **Sistema Tradicional de Seguridad de la Información (Grupo de Control).**

En este grupo no se somete al estímulo experimental a la variable independiente es decir que el experimento realizado es con el Sistema tradicional o acostumbrado el proceso ES DE FORMA TRADICIONAL O NO SE MANIPULA.

El puntaje de la encuesta que se ha obtenido de los trabajadores encuestados para la seguridad de información tradicional de la comisaria es aceptado con 158 puntos y no es aceptada con 82 puntos.

<b>Encuesta a los 30 especialistas de Informática, trabajadores de la Comisaria de la PNP de la región de Huancavelica</b>	<b>SI</b>	<b>NO</b>
1. ¿La organización reduce y mitiga los riesgos de los activos de información?	20	10

2. ¿La organización logra gestionar, monitorear, de manera eficiente los incidentes y vulnerabilidades de seguridad de la información?	22	8
3. ¿Los especialistas desarrolla medidas de seguridad para reducir los riesgos?	18	12
4. ¿Seleccionan y capacitan especialistas involucrados en los procesos de Tecnología, en temas de seguridad de información?	19	11
5. ¿Cree usted que las medidas de seguridad utilizadas son suficientes para proteger la información y prevenir posibles incidentes?	23	7
6. ¿Recomendaría usted adoptar políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la información?	24	6
7. ¿La organización elabora el plan de tratamiento de riesgos?	10	20
8. ¿Cumplen la legislación vigente de seguridad de información?	22	8
<b>Puntaje de resultado de encuesta a los especialistas:</b>	<b>158</b>	<b>82</b>

<b>La MEDIA de puntaje obtenido en la encuesta de las muestras es:</b>	<b>18.42</b>
<b>La DESVIACIÓN ESTÁNDAR de puntaje obtenido en la encuesta de las muestras es:</b>	<b>4.432</b>

**TABLA N° 4.9: Sistema tradicional de Seguridad de la Información (Grupo de Control).**

Para este proceso se realizó un seguimiento de cada uno de los 30 encuestados para calcular el promedio de aceptación y para calcular el promedio de negación.

Como podemos observar la Media de aceptación es 18.42 y La Desviación Estándar es de 4.432.

- **Sistema de Gestión de Seguridad de la Información SGSI (Grupo experimental).**

En este grupo se somete al estímulo experimental a la variable independiente que es el SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN como podemos observar se obtuvo de la encuesta el puntaje de aceptación es 217 y el promedio de negación es 23.

Los resultados que se han obtenido se presentan en la TABLA N° 4.10.

**TABLA N° 4.10: Sistema de Gestión de Seguridad de la Información SGSI (Grupo experimental).**

Encuesta a los 30 especialista de Informática, trabajadores de la Comisaria de la PNP de la región de Huancavelica	SI	NO
1. ¿La organización reduce y mitiga los riesgos de los activos de información?	26	4

2. ¿La organización logra gestionar, monitorear, de manera eficiente los incidentes y vulnerabilidades de seguridad de la información?	28	2
3. ¿Los especialistas desarrolla medidas de seguridad para reducir los riesgos?	27	3
4. ¿Seleccionan y capacitan especialistas involucrados en los procesos de Tecnología, en temas de seguridad de información?	29	1
5. ¿Cree usted que las medidas de seguridad utilizadas son suficientes para proteger la información y prevenir posibles incidentes?	26	4
6. ¿Recomendaría usted adoptar políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la información?	28	2
7. ¿La organización elabora el plan de tratamiento de riesgos?	27	3
8. ¿Cumplen la legislación vigente de seguridad de información?	26	4
<b>Puntaje de resultado de encuesta a los especialistas:</b>	<b>217</b>	<b>23</b>

<b>La MEDIA de puntaje obtenido en la encuesta de las muestras es:</b>	27.08
<b>La DESVIACIÓN ESTÁNDAR de puntaje obtenido en la encuesta de las muestras es:</b>	1.126



Como podemos observar la Media de aceptación es 27.08 y La Desviación Estándar es de 1.126. Entonces se muestra en las tablas los resultados que el Sistema tradicional es menos aceptada por los especialistas encuestados que con el Sistema de Gestión de Seguridad de Información.

#### 4.3. Prueba de Hipótesis

De la población se toma una muestra de 30 personas especialista en seguridad de información para cuantificar la diferencia de nivel de aceptación entre el SISTEMA TRADICIONAL DE SEGURIDAD DE INFORMACIÓN y el que se quiere implementar el SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN, para lograr calcular el resultado la prueba de hipótesis se usará la comprobación Z.

Se calcula la media y la desviación estándar, datos obtenidos sobre la encuesta realizada a las personas encuestadas para la mejora de seguridad de información; cuando se utiliza el SISTEMA TRADICIONAL DE LA SEGURIDAD DE INFORMACIÓN y cuando se utiliza el SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN aplicando para mejorar de la protección informática de la comisaria de la PNP de la región de Huancavelica.

UTILIZANDO SISTEMA TRADICIONAL DE LA SEGURIDAD DE INFORMACIÓN.	UTILIZANDO SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN
$\bar{x}_1 = 18.42$	$\bar{x}_2 = 27.08$
Dsv. Estándar $s_1 = 4.432$	Dsv. Estándar $s_2 = 1.126$

Para complementar el estudio estadístico Z valor de z crítico, calculados en las tablas de área de curva normal llamado también nivel de confianza, se ha calculado de la siguiente manera:

Para trabajar con tablas normalizadas:

$$z = \frac{(\bar{x}_1 - \bar{x}_2)}{\sqrt{\frac{(s_1)^2}{n_1} + \frac{(s_2)^2}{n_2}}}$$

$$z = \frac{(18.42 - 27.08)}{\sqrt{\frac{(4.432)^2}{30} + \frac{(1.126)^2}{30}}}$$

$$z = \frac{(-8.66)}{\sqrt{\frac{19.643}{30} + \frac{1.268}{30}}}$$

$$z = \frac{-8.66}{\sqrt{\frac{20.911}{30}}}$$

$$z = \frac{-8.66}{\sqrt{0.697}}$$

$$z = \frac{-8.66}{0.84}$$

$$z = -10.31$$

**Figura 12:** Usando Microsoft Excel (hoja de cálculo) devuelve la función de distribución normal estándar acumulativa, se usa esta función en lugar de una tabla estándar de áreas de curvas normales como se muestra en esta imagen.

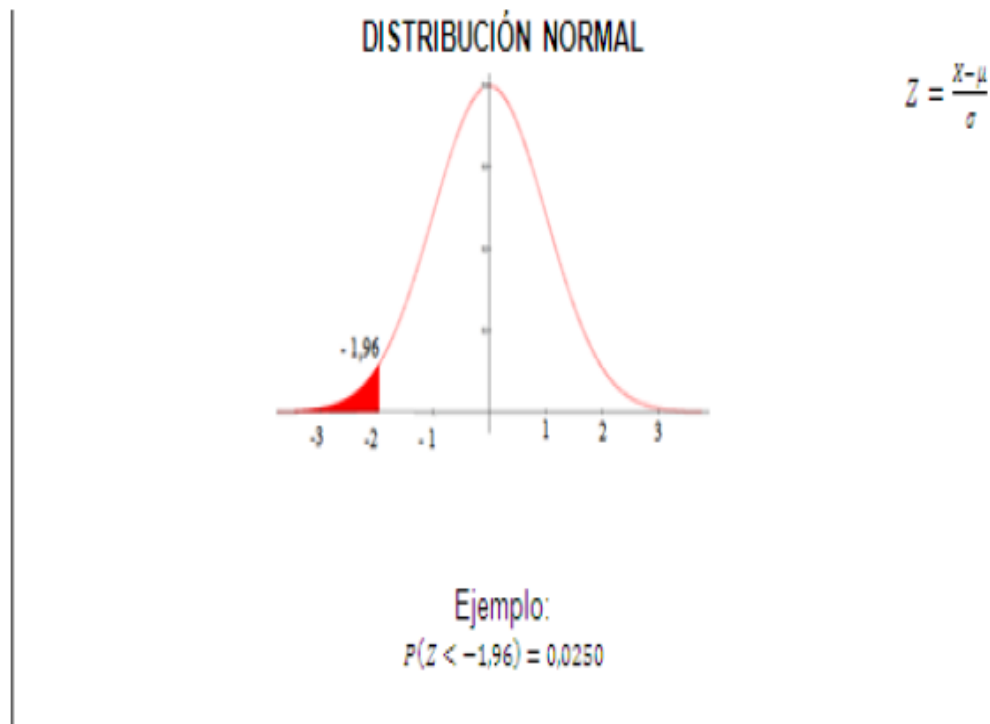
Z = valor de Z crítico, calculado en las tablas del Área bajo la curva normal o tabla de Probabilidades de la Distribución Normal Estandar.  
 $\alpha$  = Nivel de significancia o nivel alfa  
 $1-\alpha$  = Nivel de confianza

Z	$\alpha$	
-1.644	0.050088101	Error tolerable máximo o margen de error
-10.31	3.17507E-25	


0.95	1.64485363	1.64485363	0.95
0.96	1.75068607	1.75068607	0.96
0.97	1.88079361	1.88079361	0.97
0.98	2.05374891	2.05374891	0.98
0.99	2.32634787	2.32634787	0.99
0.01	-2.32634787	-2.32634787	0.01
0.02	-2.05374891	-2.05374891	0.02
0.03	-1.88079361	-1.88079361	0.03
0.04	-1.75068607	-1.75068607	0.04
0.05	-1.64485363	-1.64485363	0.05

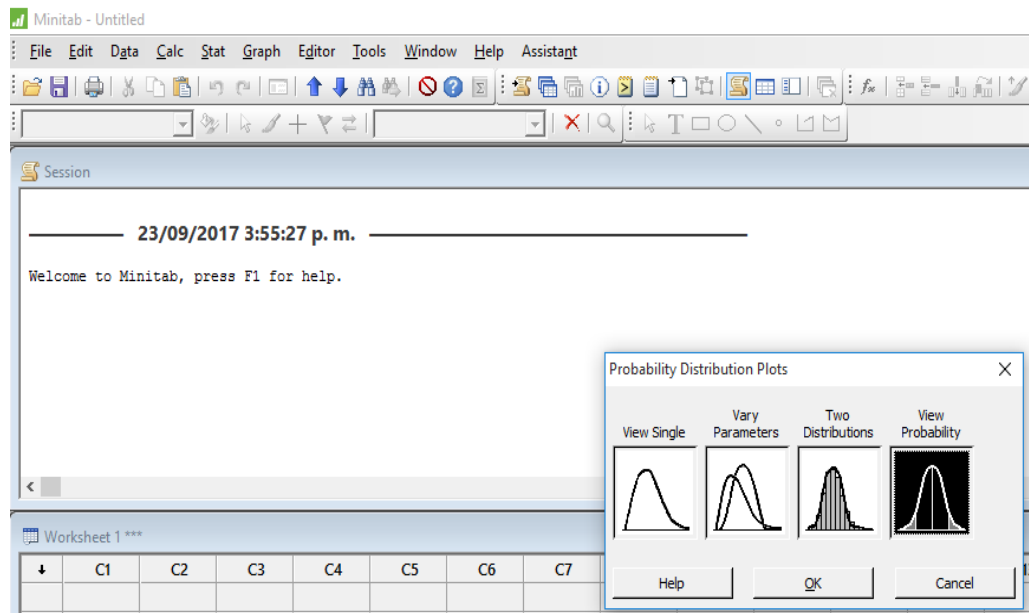
**Figura 13.** Tabla de Distribución Normal



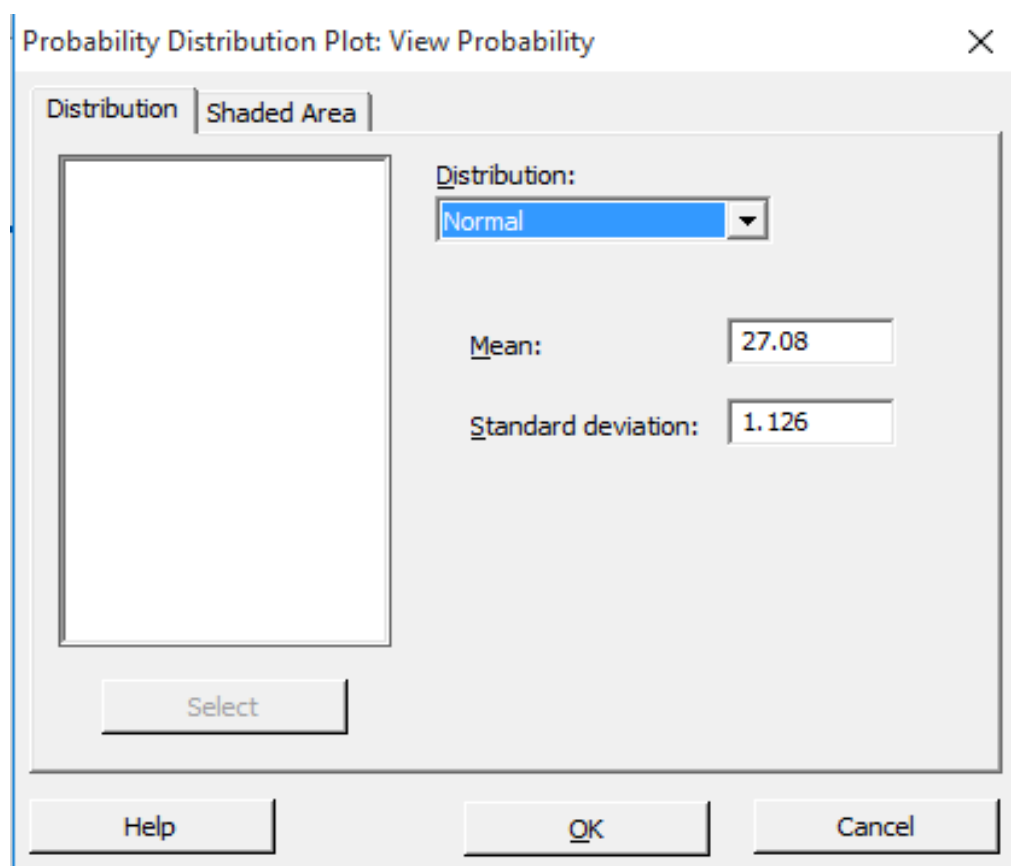
Z	0,00	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09
	∴		∴							
0,8	0,7881	0,7910	0,7939	0,7967	0,7995	0,8023	0,8051	0,8078	0,8106	0,8133
0,9	0,8159	0,8186	0,8212	0,8238	0,8264	0,8289	0,8315	0,8340	0,8365	0,8389
1	0,8413	0,8438	0,8461	0,8485	0,8508	0,8531	0,8554	0,8577	0,8599	0,8621
1,1	0,8643	0,8665	0,8686	0,8708	0,8729	0,8749	0,8770	0,8790	0,8810	0,8830
1,2	0,8849	0,8869	0,8888	0,8907	0,8925	0,8944	0,8962	0,8980	0,8997	0,9015
1,3	0,9032	0,9049	0,9066	0,9082	0,9099	0,9115	0,9131	0,9147	0,9162	0,9177
1,4	0,9192	0,9207	0,9222	0,9236	0,9251	0,9265	0,9279	0,9292	0,9306	0,9319
1,5	0,9332	0,9345	0,9357	0,9370	0,9382	0,9394	0,9406	0,9418	0,9429	0,9441
1,6	0,9452	0,9463	0,9474	0,9484	0,9495	0,9505	0,9515	0,9525	0,9535	0,9545
1,7	0,9554	0,9564	0,9573	0,9582	0,9591	0,9599	0,9608	0,9616	0,9625	0,9633
1,8	0,9641	0,9649	0,9656	0,9664	0,9671	0,9678	0,9686	0,9693	0,9699	0,9706
1,9	0,9713	0,9719	0,9726	0,9732	0,9738	0,9744	0,9750	0,9756	0,9761	0,9767
2	0,9772	0,9778	0,9783	0,9788	0,9793	0,9798	0,9803	0,9808	0,9812	0,9817
2,1	0,9821	0,9826	0,9830	0,9834	0,9838	0,9842	0,9846	0,9850	0,9854	0,9857

Utilizando el software Minitab se obtiene el resultado en el gráfico.

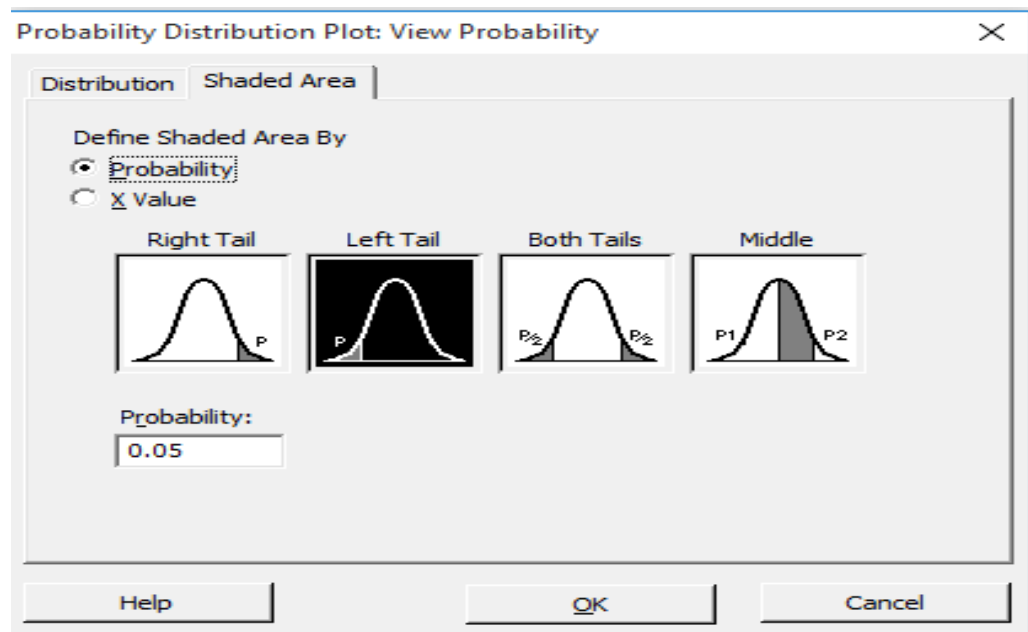
Gráfico N° 4.9. Se selecciona en el menú gráfico  Probability Distribution Plot...



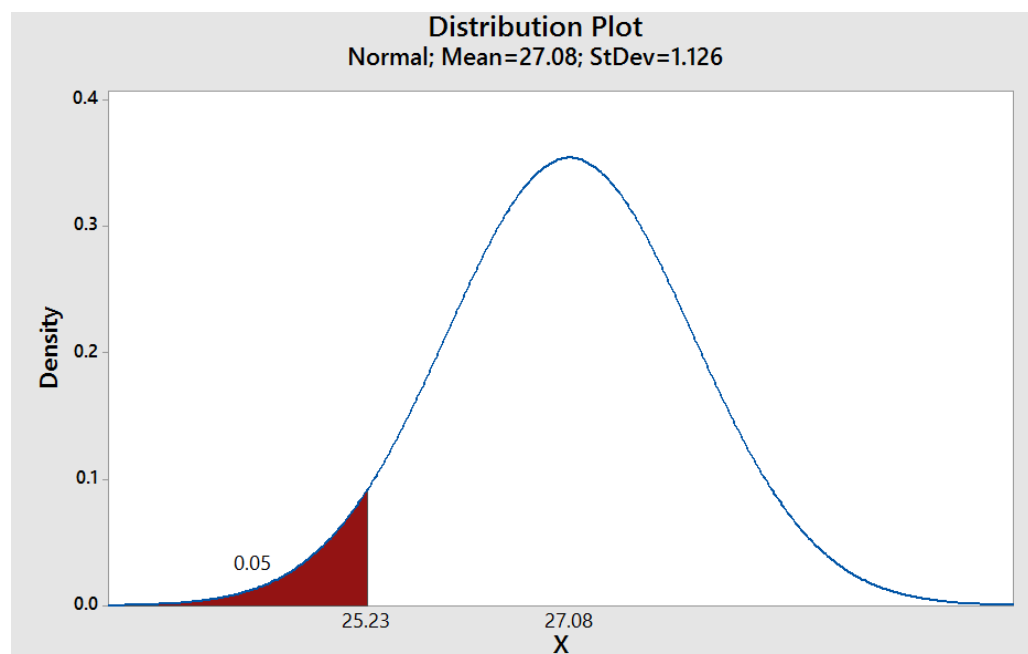
**Gráfico N° 4.10:** Distribución normal.



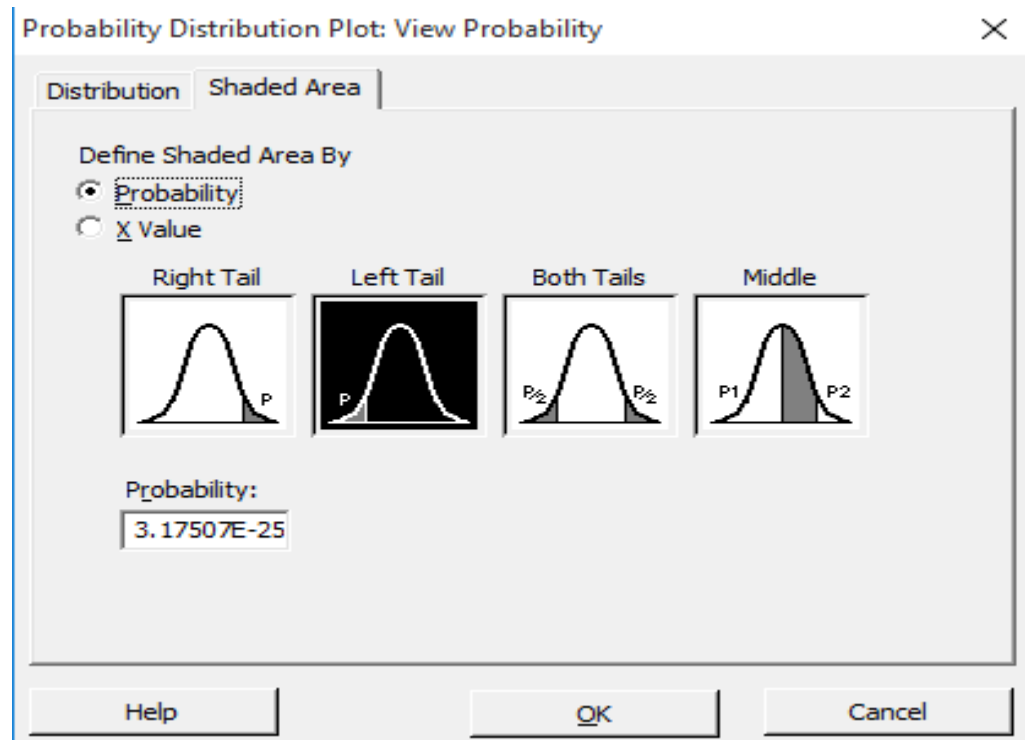
**Gráfico N° 4.11:** Distribución de Probabilidad con el coeficiente significativo de aceptación al nivel de 0.05.



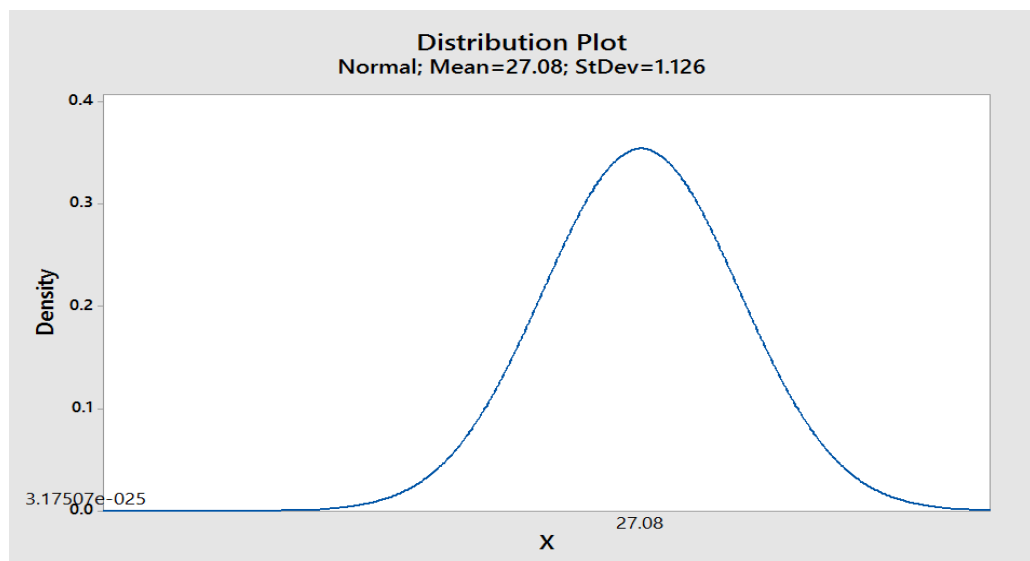
**Gráfico N° 4.12:** Gráfico de distribución probabilidad se dice que el coeficiente es significativo en el nivel de 0.05 (95% de confianza es que la correlación es verdadera y 5% de probabilidad de error).



**Gráfico 4.13:** Distribución de Probabilidad con el coeficiente significativo al nivel de  $3.17507E-25$ .



**Gráfico 4.14:** Distribución probabilidad como resultado de la prueba de hipótesis el coeficiente es significativo al nivel de  $3.17507E-25$ . (99.99% de confianza es que la correlación es verdadera y  $3.17507E-23\%$  de probabilidad de error).



#### 4.4. Discusión de Resultados

☞ Hipótesis Nula  $\mu_1 - \mu_2 = 0$  , no hay diferencia entre aplicación de un SISTEMA TRADICIONAL DE SEGURIDAD DE INFORMACIÓN con un SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN de la Comisaria de la PNP de la región de Huancavelica

☞ Hipótesis Alternativa  $\mu_1 - \mu_2 > 0$  (unilateral), la aplicación de un SISTEMA TRADICIONAL DE SEGURIDAD DE INFORMACIÓN es significativamente mayor que la aplicación de un SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN.

Nivel de significancia:  $\alpha = 0.05$   $Z_{\alpha} = -1.644$ .

☞ Hipótesis Alternativa2  $\mu_1 - \mu_2 < 0$ ; pero el resultado es  $-10.31 < z_{0.05}$  Vale decir, que  $-10.31 < -1.644$  por tanto la aplicación de un SISTEMA TRADICIONAL DE SEGURIDAD DE INFORMACIÓN es menos aceptada por los especialistas encuestados que con la aplicación de un SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA MEJORAR LA PROTECCIÓN INFORMÁTICA DE LA COMISARIA DE LA PNP DE LA REGIÓN DE HUANCVELICA.



## CONCLUSIONES

1. Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido, cobra especial importancia el hecho de que puedan contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas.
2. Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad, entre otros servicios de seguridad.
3. La sociedad de la información y nuevas tecnologías de comunicación plantean la necesidad de mantener la usabilidad y confidencialidad de la información que soportan los sistemas en las organizaciones; para ello, es especialmente importante elegir e implantar los sistemas y métodos de seguridad más idóneos, que protejan las redes y sistemas ante eventuales amenazas, ya sean presentes o futuras.
4. Se puede concluir que actualmente se vive en una época en la que la información y los datos poseen una importancia decisiva en la gran mayoría de organizaciones, convirtiéndose así en su activo más importante. Por ejemplo, en caso de una emergencia, una catástrofe natural y se llegara a caer la instalación de la organización; se puede volver a reconstruir. En cambio, si llegamos a perder la información

de la organización, es muy probable que no podamos volver a recuperarla si no se tienen las consideraciones debidas, con lo que es probable que la empresa deje de operar.

5. Se puede concluir que el Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de la comisaria PNP de la región de Huancavelica, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.
6. Como conclusión final, se debe tener en cuenta que hay que recalcar que de nada sirve contar con un SGSI, que consideren todos los posibles riesgos y controles para mitigarlos o contar con toda la tecnología posible para asegurar la información si no se da una debida importancia a la seguridad de la información por parte de las autoridades dirigentes de la organización y no se cumplen las políticas y procedimientos establecidos por parte del personal de la comisaria de la PNP de la región de Huancavelica.
7. Los usuarios potenciales de la comisaria PNP de la región de Huancavelica y de una manera general de nuestra institución, deberán ser capaces de superar el problema cultural, de sobreponerse al temor natural y apreciar el horizonte de utilidades, aplicaciones, así como del ahorro de tiempo y dinero, que nos ofrecen la seguridad de la información, lo cual será posible a partir de una adecuada implementación y capacitación.

## RECOMENDACIONES

- ☞ Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- ☞ Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- ☞ Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- ☞ Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
- ☞ Ejecutar procedimientos de monitorización y revisión para:
  - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
  - Identificar brechas e incidentes de seguridad;
  - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
- ☞ Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
  - Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- ☞ Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en

cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior requerimientos legales, obligaciones contractuales, etc.

- ☞ Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- ☞ Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- ☞ Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.
- ☞ Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- ☞ Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- ☞ Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

## BIBLIOGRAFÍA

1. Alexander, Alberto G. (2007) *DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION Primera edición.* Colombia: Alfaomega.
2. ISO/IEC 27001:2005. (2005a) International Organization of Standardization and International Electrotechnical Commission. Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Primera edición.
3. ISO/IEC 17799:2005. (2005b) International Organization of Standardization and International Electrotechnical Commission. Tecnologías de la Información – Técnicas de Seguridad – Código para la práctica de la gestión de la seguridad de la información. Segunda Edición.
4. ISO/IEC 27004:2009. (2009) International Organization of Standardization and International Electrotechnical Commission. Tecnología de la Información – Técnicas de seguridad – Gestión de la seguridad de la información – Medición.
5. Project Management Institute. (2008) *Guía de los Fundamentos para la Dirección de Proyectos Cuarta edición.*
6. Granados Rodríguez, Arturo Fernando. (2012) *Auditoria del Desarrollo de Sistemas de Información en el Gobierno Regional de Cajamarca.* de la Universidad Privada del Norte.

7. Martín Méndez, Enrique & Ángel Aguilar, Miguel. (2006) Proyecto Sanitas: Sistema de Gestión de Seguridad de la Información y certificación UNE 71502 e ISO 27001. del Grupo Sanitas.
8. Alfaro Paredes, Emigdio Antoni. (2008) Metodología para la Auditoria Integral de la Gestión de la Tecnología de Información. de la Pontificia Universidad Católica del Perú.
9. Maco Chonate, Ana Pilar de Jesús. (2008) Formulación de un Plan de Seguridad de Información Aplicando las Normas ISO 27001 y 27002, para mejorar la seguridad de la información en la gestión financiera de la caja Sipán: un caso de aplicación de la metodología Magerit. Universidad Católica Santo Toribio de Mogrovejo.
10. Hernández Sampieri, Roberto. (2014) Metodología de la Investigación 6<sup>ta</sup>. Edición. México: McGraw- Hill.
11. Marcombo, Alexander. (2007) Diseño de un Sistema de Seguridad Informática. México: Alfaomega.
12. Chi-Hsiang, Wang. (2010) Integrated Installing ISO 9000 and ISO 27000 Management Systems on an Organization IEEE.
13. La ISO 27000 establece un Sistema de Gestión de Seguridad de la Información, cuyo elemento más importante es la Gestión de los Riesgos. Página en Internet: [WWW.ISO27000.ES](http://WWW.ISO27000.ES).

## **ANEXOS**

## ANEXOS 1: MATRIZ DE CONSISTENCIA.

MATRIZ DE CONSISTENCIA						
TÍTULO						
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LA PROTECCIÓN INFORMÁTICA DE LA COMISARIA REGIÓN HUANCVELICA.						
PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	MÉTODO	TÉCNICAS	INSTRUMENTOS
PRICIPAL	GENERAL	GENERAL	V. Independiente: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. V. Dependiente: LA PROTECCIÓN INFORMÁTICA.	*Tipo de investigación:	* Grupos (de control - experimental) y validez (interna - externa).	* Procesamiento y Análisis de datos.
¿El Sistema de Gestión de Seguridad de Información mejorará la protección informática de la Comisaria Región Huancavelica?	Medir el grado de influencia que ejerce un Sistema de Gestión de Seguridad de Información para la mejora de la protección informática de la Comisaria Región Huancavelica.	Hi: El Sistema de Gestión de Seguridad de Información mejorará la protección informática de la Comisaria Región Huancavelica.		<ul style="list-style-type: none"> <li>• Según la finalidad: Investigación Aplicada, porque se está utilizando conocimientos pre existente.</li> <li>• Según naturaleza de las Variables: Investigación cuantitativa.</li> </ul>	<ul style="list-style-type: none"> <li>☞ Encuestas</li> <li>☞ La observación</li> <li>☞ El Análisis Bibliográfico</li> <li>☞ Entrevistas</li> <li>☞ Cuestionarios</li> </ul>	<ul style="list-style-type: none"> <li>• Una vez recogido los datos, es necesario realizar su procesamiento, lo que incluye:</li> <li>• La codificación</li> <li>• La Tabulación</li> <li>• El análisis y la interpretación</li> </ul>
ESPECIFICO	ESPECIFICO	ESPECIFICO	INDICADORES	*Nivel de investigación (Alcance).		
1.- ¿El Sistema de Gestión de Seguridad de Información incrementará la <b>confidencialidad de la seguridad</b> en la protección	1.- Medir el grado de influencia que ejerce un Sistema de Gestión de Seguridad de Información para la mejora de <b>confidencialidad de la seguridad</b> en la protección informática de	H1: El Sistema de Gestión de Seguridad de Información incrementará <b>la confidencialidad de la seguridad</b> en la protección	<ul style="list-style-type: none"> <li>➤ Nivel de confidencialidad de la seguridad de información.</li> <li>➤ Nivel de integridad de la seguridad de información.</li> </ul>	<ul style="list-style-type: none"> <li>• Explicativa (causal) y correlacional.</li> </ul>		<ul style="list-style-type: none"> <li>• El análisis y la interpretación</li> <li>Para tales casos, hay en el mercado software que cumple esta función.</li> </ul>



informática de la Comisaria Región Huancavelica?	la Comisaria Región Huancavelica.	informática de la Comisaria Región Huancavelica.	<p>➤ Nivel de disponibilidad de la seguridad de información.</p> <p>➤ Nivel de Autenticación de la seguridad de información.</p>	<p><b>*Diseño de Investigación:</b> Experimental.</p>	<p>☞ Guías de Observación</p> <p>☞ Test de evaluación.</p>
2.- ¿El Sistema de Gestión de Seguridad de Información incrementará la integridad de la seguridad en la protección informática de la Comisaria Región Huancavelica?	2.- Medir el grado de influencia que ejerce un Sistema de Gestión de Seguridad de Información para la mejora de integridad de la seguridad en la protección informática de la Comisaria Región Huancavelica.	H2: El sistema de gestión de seguridad de información incrementará la integridad de la seguridad en la protección informática de la Comisaria Región Huancavelica.		<p><b>*Universo:</b> La población de la presente investigación lo constituirá los trabajadores de la Comisaria de la PNP de la región de Huancavelica.</p> <p><b>*Muestra:</b> Esta muestra se considera del tipo probabilística de la presente investigación; lo constituirá los 30 trabajadores de la Comisaria de la PNP de la región de Huancavelica, que además son efectivos policiales.</p>	<p>☞ Lista de Cotejo</p> <p>☞ Ficha técnica</p>
3.- ¿El Sistema de Gestión de Seguridad de Información incrementará la disponibilidad de la seguridad en la protección informática de la Comisaria Región Huancavelica?	3.- Medir el grado de influencia que ejerce un Sistema de Gestión de Seguridad de Información para la mejora de disponibilidad de la seguridad en la protección informática de la Comisaria Región Huancavelica.	H3: El sistema de gestión de seguridad de información incrementará la disponibilidad de la seguridad en la protección informática de la Comisaria Región Huancavelica.			

**ANEXO 2: ENCUESTA PARA LOGRAR OBTENER RESULTADOS DE  
EVALUACIÓN PARA LA SEGURIDAD DE INFORMACIÓN.**

<b>Nº</b>	<b>ITEM</b>	<b>SI</b>	<b>NO</b>	<b>NS/NC</b>
1	¿La organización reduce y mitiga los riesgos de los activos de información?			
2	¿La organización logra gestionar, monitorear, de manera eficiente los incidentes y vulnerabilidades de seguridad de la información?			
3	¿Los especialistas desarrolla medidas de seguridad para reducir los riesgos?			
4	¿Seleccionan y capacitan especialistas involucrados en los procesos de Tecnología, en temas de seguridad de información?			
5	¿Cree usted que las medidas de seguridad utilizadas son suficientes para proteger la información y prevenir posibles incidentes?			
6	¿Recomendaría usted adoptar políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la información?			
7	¿La organización elabora el plan de tratamiento de riesgos?			
8	¿Cumplen la legislación vigente de seguridad de información?			