UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

GUÍA DE IMPLEMENTACIÓN DE LA SEGURIDAD BASADO EN LA NORMA ISO/IEC 27001, PARA APOYAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS DE LA COMISARIA DEL NORTE P.N.P EN LA CIUDAD DE CHICLAYO

TESIS PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS Y COMPUTACIÓN

JULIO CESAR ALCÁNTARA FLORES

Chiclayo 28 de Mayo de 2015

"GUÍA DE IMPLEMENTACIÓN DE LA SEGURIDAD BASADO EN LA NORMA ISO/IEC 27001, PARA APOYAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS DE LA COMISARIA DEL NORTE P.N.P EN LA CIUDAD DE CHICLAYO"

POR:

JULIO CESAR ALCÁNTARA FLORES

Presentada a la Facultad de Ingeniería de la
Universidad Católica Santo Toribio de Mogrovejo
Para optar el título de
INGENIERO DE SISTEMAS Y COMPUTACIÓN

APROBADA POR EL JURADO INTEGRADO POR

_____
Mgtr. Luis Augusto Zuñe Bispo
PRESIDENTE

_____	_____
Ing. Hugo Enrique Saavedra Sánchez	Ing. Juan Rafael Galán Santisteban
SECRETARIO	ASESOR

Dedicatoria

- Este trabajo está dedicado a mi Madre por creer siempre en mí y apoyarme En todo momento, todos mis esfuerzos son para ella.
- A mí Padre y Hermanos porque siempre los tengo presente en todos los momentos de mi vida y por inculcarme los buenos valores

ÍNDICE

I. INTRODUCCIÓN. 8
II. MARCO TEÓRICO. 12
2.1 ANTECEDENTES 12
2.2 BASES TEÓRICAS CIENTÍFICAS. 15
2.2.1 Gestión de la Seguridad de la Información. 15
2.2.2 Aspectos Fundamentales en la Seguridad de la Información. 16
2.2.3 Gestión de Riesgos en la Seguridad Informática. 17
2.2.4 Sistema de Gestión de la Seguridad de la Información (SGSI). 18
2.2.5 Que se entiende por un SGSI. 18
2.2.6 Que Incluye un SGSI. 19
2.2.7 Gestión de la Seguridad de la Información. 21
2.2.8 Fases del Sistema de Gestión de Seguridad de Información. 21
2.2.9 Lista de Verificación de la Norma ISO 27001. 23
2.2.10 Como Implementar la ISO 27001. 24
III. MATERIALES Y MÉTODOS. 26
3.1 DISEÑO DE INVESTIGACIÓN 26
3.1.1 Tipo de Investigación. 26
3.1.2 Hipótesis 26
3.1.3 Diseño de Contrastación. 26
3.1.4 Variables e Indicadores. 26
3.1.5 Población y Muestra. 28
3.1.6 Técnicas de Procesamiento de Datos. 28
3.2 METODOLOGÍA 29
3.2.1 Metodología Norma ISO/IEC 27001. 29
3.2.2 Metodología Magerit. 33
IV. RESULTADOS. 35
4.1 ENTREGABLES REALIZADOS. 35
4.1.1 Procedimiento para control de documentos y registros.36
4.1.2 Plan del proyecto para la implementación del sistema de gestión de seguridad de la información 47
4.1.4 Documento sobre el alcance del sgsi 68
4.1.5 Política de seguridad de la información 75
4.1.6 Metodología de evaluación y tratamiento de riesgos 97
4.1.7 Declaración de aplicabilidad 110
4.1.8 Plan de tratamiento de riesgos 122

4.1.9 Plan de capacitacion y concienciacion 126
V. DISCUSIÓN 145
VI. CONCLUSIONES. 146
REFERENCIAS BIBLIOGRÁFICAS. 147
ANEXOS. 149
ANEXO N°1: Check-List Sobre Políticas De Seguridad En La Institución Policial Comisaria Del Norte Pnp – Chiclayo. 149
ANEXO N°2: chick-List Sobre Gestión De Activos En La Institución Policial Comisaria Del Norte Pnp – Chiclayo. 150
ANEXO N°3: Entrevista 01 151
ANEXO N°4: Tabulación De Las Encuestas / Pre-Test 152
ANEXO N°5: Tabulación De Las Encuestas / Post-Test 155

Lista de Figuras:

Figura 1. Estructura que referencia un SGSI. 19
FIgura 2. Estructura piramidal de los distintos niveles de un SGSI. 20
Figura 3: Estructura de iso/iec 27001 29
Figura 5: Fases del proceso de implementación de iso/iec 27001 30
Figura 4: Alcance de iso/iec 27001 31
FIgura 6: Marco de trabajo para gestionar los riesgos 34

Lista de cuadros:

Cuadro n°1 Requerimientos en la institución policial. 54
Cuadro n°2: Activos de la institución. 56
Cuadro n°3: Dimensiones de seguridad 57
Cuadro n°4: Ámbito y activos. 57
Cuadro n° 5: Controles de salvaguardas 59
Cuadro n°6: Requerimientos de la institución 66
Cuadro n°7. Responsables de información 67
Cuadro N°8: Infraestructura de ti de la institución 73
Cuadro N°9: Activos de información 79
Cuadro N°10: Estructuración y valor de los activos 80
Cuadro N°11: Descripción y valor critico de los activos 80
Cuadro N°12: Resumen del análisis diferencial 95
Cuadro N°14: Valoración de la vulnerabilidad 106
Cuadro N°15: Valoración de la criticidad y sus rangos 106
Cuadro N°16 Impacto y sus rangos 107
Cuadro n°17 Variación del impacto y la vulnerabilidad 107
Cuadro n°18 Nivel de aceptación del riesgo 108

RESUMEN.

El presente trabajo de investigación se enfoca en elaboración de una Guía de implementación de la seguridad basada en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas de información en la institución Policial Comisaria del Norte – Chiclayo.

Para la obtención de dicha información y recolección de datos se consideró conveniente el uso de las técnicas de recolección de datos tales como encuestas, entrevistas, así como fichas de observación, como medio para poder extraer la información y su posterior interpretación; y de esta manera medir la realidad problemática apoyado en el uso de la Norma ISO/IEC 27001, lográndose determinar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información de dicha institución.

Los resultados obtenidos permitieron determinar de forma real que, al incorporar la norma ISO/IEC 27001 basada en una Guía de Implementación. Se logró incrementar los procedimientos utilizados en favor de la Institución permitiéndole la detección de anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla. Con el Plan de tratamiento de Riesgos, se permitió la disminución de los niveles de riesgos con respecto a los activos de información, considerados amenazas y vulnerabilidades en la institución, esto manifestado en un plan adecuado para abordarlos y tomar las precauciones necesarias que minimicen sus impactos. Finalmente con el Plan de Capacitación y Concienciación puesto en marcha en la Institución, se pudo incrementar el porcentaje de conocimiento por parte del personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la institución, teniendo como resultado personal comprometido con la seguridad en favor de la institución.

Una correcta implementación de la Guía desarrollada en el presente trabajo de investigación permite incrementar el nivel de la seguridad en las aplicaciones informáticas de la institución policial, lo cual se manifiesta en el incremento de políticas de seguridad puestas en marcha que benefician a la institución y ayudan a incrementar el nivel de seguridad en la misma.

.

PALABRAS CLAVE: Gobierno TI, Políticas de Seguridad, SGSI, Estrategias de Seguridad, Gestión de Recursos, Evaluación de Riesgos, Auditable, SIDPOL, Híbrica, Ingeniería de Seguridad.

ABSTRACT.

This work contains real and reliable information, a guide focused on security implementation based on ISO / IEC 27001, to improve levels of safety and reliability in information systems and use of the Applications within the institution Police Commissioner North - Chiclayo.

To obtain such information and data collection was considered appropriate use of data collection techniques such as surveys, interviews and observation sheets as a means to extract information and then be processed for interpretation, and to measure the problematic reality supported by the use of ISO / IEC 27001. Standard Achieving identify gaps thus improving levels of safety and reliability in the information systems of the institution.

The results determine actual form, incorporating the ISO / IEC 27001 -based Guide to Implementation , was able to increase the level of safety in applications of the police , and this was manifested in increasing security policies that were implemented that benefited the institution and helped increase the level of security in it.

With the implementation of this proposal will be able to increase the procedures used for the institution enabling the detection of anomalies in information security, reflected in different security mechanisms to safeguard it. With the Risk Treatment Plan , the decreased levels of risk with respect to information assets , threats and vulnerabilities considered in the institution is allowed , it said in a suitable plan to meet them and take precautions to minimize their impacts . And finally, with the Plan of Training and Awareness launched in the institution, it could increase the percentage of knowledge by staff in thematic oriented policies, security strategies that benefit the institution, having as a personal outcome committed to safety on behalf of the institution.

KEYWORDS: Government IT Security Policy, ISMS, Security Strategies, Resource Management, Risk Assessment, Auditable, SIDPOL, Híbrica, Safety Engineering.

I. INTRODUCCIÓN.

Actualmente, en las organizaciones es de suma importancia determinar si los controles implementados son eficientes y suficientes, identificar las causas de los problemas existentes en los sistemas de información y a su vez las áreas de oportunidad que puedan encontrarse, identificando causas y soluciones a problemas específicos de los sistemas de información, que pueden estar afectando a la operación y a las estrategias del negocio; así como las acciones preventivas y correctivas necesarias para mantener a los sistemas de información confiables y disponibles.

Hoy en día las empresas privadas se han sistematizado y están utilizando herramientas, equipos informáticos y personal capacitado para facilitar los procesos de trabajo y obtener así un mayor rendimiento laboral. La mayoría de estas empresas no le dan la suficiente importancia a la auditoría de sistemas, creyendo que este tipo de herramienta no les corresponde y lo ven como un gasto y no como una inversión; es por eso que este enfoque es básico y necesario como es el de una Guía de Implementación en la seguridad de sistemas información.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

A través de una Guía de Implementación para la seguridad en las aplicaciones se puede gestionar la tecnología de la información en las entidades, a través de auditorías internas y externas. El presente trabajo propone una Guía de Implementación que apoye a la seguridad de los Sistemas de Información con la finalidad de medir los riesgos y evaluar los controles en el uso de las tecnologías de información, haciendo uso de técnicas y estrategias de análisis, que permitan una mejor gestión de tecnologías de información, a disposición de las entidades públicas.

En la Entidad donde se desarrolla el presente trabajo de investigación, Comisaria del Norte de la PNP de la ciudad de Chiclayo, se ha venido trabajando diferentes enfoques que corresponden a Guías de Implementación apoyadas a la seguridad de la Información; así se pudo encontrar la siguiente situación problemática, la cual mencionaremos a continuación especificando las causas que ocasionan estos inconvenientes o problemas, los cuales citaremos a continuación:

- Del total del personal encuestado en la comisaria el 76% manifestó que existe un alto grado de inseguridad en el uso de sus aplicaciones. Esta inseguridad está reflejada en varios aspectos como por ejemplo: desactualización de equipos, ausencia de políticas de seguridad, activos vulnerables, etc.(Ver Anexo N°4)

- En lo que hace referencia al tiempo y uso de sus aplicaciones, de acuerdo a la información recopilada en la comisaria cuentan por lo menos entre 5 años a mas

con el uso de sus aplicaciones, llámense estas para registro de denuncias, investigaciones, donde se obtuvo un 40% del personal encuestado que manifestó ese tiempo de uso en las aplicaciones, excepto el nuevo sistema de denuncia policial conocido como SIDPOL, el cual entró en vigencia hace un año. 2013. (Ver Anexo N°4)

- En lo que respecta a los equipos de cómputo con los que cuenta la comisaria están desactualizados, y en algunos casos estos suelen estar malogrados o inoperativos. Así también, en cuanto al mantenimiento de los mismo se realizan anualmente; lo cual fue manifestado por el 67% del total de encuestados. La causa presente es de que no existe una política adecuada de actualización periódica, y que esta causa genera un efecto en las deficiencias y vulnerabilidades en el uso de los sistemas de información.(Ver Anexo N°4)

- Solamente el 27% del personal es capacitado en algún curso o charla correspondiente al uso de las nuevas tecnologías y aplicaciones en informática, la causa presente es el deficiente nivel adecuado en las capacitaciones esto genera un efecto en el personal no del todo positivo ya que se limita en muchos casos el conocimiento. no a todos se les brinda este nivel de capacitación, lo que genera en muchos casos una inversión de los propios bolsillos de algunos efectivos que no son beneficiados con las capacitaciones correspondientes, para de alguna manera enterarse y actualizarse por su propia cuenta. (Ver Anexo N°4)

- En lo que respecta a mecanismos de seguridad para las aplicaciones y los sistemas, de acuerdo a la encuesta realizada el 80% hace uso de los conocidos Antivirus como medios de protección, pero que a su vez no son licenciados, sino versiones de prueba. Así como los sistemas operativos no licenciados. (Ver Anexo N°4)

- En cuanto a las acciones o actividades que se toman en cuenta frente a posibles problemas e inconvenientes que puedan presentarse en los equipos, o activos de información en la institución. Un 47% del total de encuestados coincidió que frente a estos inconvenientes se contactan con un experto que no necesariamente está dentro de la institución, un 23% los encuestados manifestó que frente a esos inconvenientes se hace uso de un plan de contingencia. (Ver Anexo N°4)

- En lo que respecta al conocimiento de Políticas de seguridad, Estrategias y niveles de riesgo enfocados a la institución. Un 93% de los encuestados afirmó no conocer acerca de estos temas, por lo que tan solamente un 7% conoce sobre los mismos .(Ver Anexo N°4)

- En cuanto al índice de fallas en las Aplicaciones, y los sistemas informáticos de acuerdo a la encuesta el 53% manifestó que a veces se suelen presentar fallas de seguridad, problemas con la información, en cuanto a la disponibilidad, integridad, etc. o en otros casos problemas técnicos muy puntuales, en las aplicaciones, como por ejemplo la vulnerabilidad de las mismas. (Ver Anexo N°4)

- En cuanto a los motivos y causas que generan las fallas, demoras, e inconvenientes en las aplicaciones que hace uso la comisaria, los resultados que obtuvimos fueron dos motivos más resaltantes como son: el problema de mayor recurrencia se manifestó en los equipos desactualizados y en mal estado con un 53%, seguido de problemas en la conexión y accedo a la red (internet) con un 47%. Estos problemas encontrados se manifiestan en causas de carecimiento de políticas, estrategias, y mecanismos de seguridad adecuados. Toda esta problemática y causas se ven manifestadas en un efecto que conlleva a deficiencias en el uso de las aplicaciones, los niveles de seguridad vulnerables, etc. Cabe mencionar que no todo el local de la comisaria cuenta con acceso a internet, solamente el área de investigación, y aun así la velocidad es muy pobre tan solo 500 megas que no le son suficientes, mientras que las otras áreas no cuentan con internet. Es por eso que algunos efectivos tienes que llevar sus propias maquinas (laptops), para así agilizar el trabajo de manera más eficiente en algunos casos. (Ver Anexo N°4)

- En cuanto al proceso utilizado para la detección de ciertas anomalías en la seguridad de la información y causas que puedan generan algunos inconvenientes con la misma, del total de los encuestados un 10%, aseguro que el proceso utilizado cuenta con mecanismos del control, como por ejemplo algunas políticas de control, integridad de la información, etc. Mientras que un 90% afirmo que el proceso es deficiente para poder detectar ciertas anomalías y salvaguardar la información.(Ver Anexo N°4)

Los policías muchas veces deben asociarse para contratar el servicio de Internet. A esta realidad se suma que sólo 23 de las 114 comisarías en la ciudad de Chiclayo tienen acceso a Reniec; cinco de cada diez al sistema de requisitorias, y ninguna a la información de procesos judiciales. Por esto, cuando se realiza un operativo de control de identidad, estas dependencias deben esperar la información de una unidad especializada.

Por todo lo anterior expuesto, se planteó el siguiente tema de investigación: ¿Cómo ayudar en la mejora de la Seguridad de los Sistemas Informáticos de la Comisaria del Norte en la Ciudad de Chiclayo?

Seguidamente de una Hipótesis: Con una Guía de Implementación de la Seguridad de la Información basado en la Norma ISO/IEC 27001, se apoyará en la mejora de la Seguridad en las Aplicaciones Informáticas de la comisaria del Norte –Chiclayo.

Entre los Objetivos que se plantearon tenemos, como Objetivo General: Contribuir a mejorar el nivel de seguridad de la Información, apoyado en la norma ISO/IEC 27001, en la institución Policial Comisaria del Norte – Chiclayo.

Como Objetivos Específicos tenemos a los siguientes:

- Incrementar el nivel de seguridad en las aplicaciones de la institución Policial.
- Mejorar el proceso utilizado para detectar anomalías en la seguridad de la información.
- Disminuir los niveles de riesgos, respecto a los activos de información considerados amenazas y vulnerabilidades.

- Mejorar el nivel de capacitación en temas de seguridad informática en el personal.

La Justificación de la presente investigación se da en el ámbito Tecnológico, Económico, Social, y Científico, las cuales se detallan a continuación:
Tecnológica: Ya existen antecedentes orientados a este tipo de investigación y en áreas especifica de las organizaciones, pero con otra perspectiva y otro uso de metodologías. A través de esta investigación se pretende hacer uso de las tecnologías estrictamente orientadas a la seguridad de los sistemas de información, a la auditoria de los Sistemas de información, ya que se pretende solucionar un problema en la organización orientada al nivel de seguridad en el uso de sus sistemas de información que manejan en sus actividades, generando como consecuencia una mejora en el uso de las aplicaciones con mejores y mayores niveles de seguridad en los sistemas de información respectivamente.

Económica: A través del desarrollo de este tema de tesis, se pretende ayudar en cierto modo a la organización, ya que cuenta con inconvenientes en el nivel de seguridad y uso de sus sistemas de información y en sus aplicaciones, con el desarrollo de la siguiente guía se podrían obtener beneficios económicos a través de las políticas destinadas y orientadas a mejorar esa realidad existente de la institución.

Social: Entre los factores, por los cuales se propone el siguiente tema de investigación y desarrollo, es porque a través del mismo se podrá ayudar al personal que labora en la Institución y hace uso de los sistemas y tecnologías de información con los que esta cuenta, así mismo el poder tener un mejor y mayor control en la seguridad de su información , y por ende un mejor nivel de seguridad en el uso de las aplicaciones que apoyan su labor diaria, permitiéndole bridar un servicio de calidad a los ciudadanos.

Científica: Con el desarrollo de esta investigación, se pretende servir de apoyo a futuras investigaciones relacionadas con los temas de seguridad y niveles de seguridad de la Información, y así mismo aportar nuevos conocimientos con el uso de nuevas aplicaciones y metodologías de trabajos para concretar fines específicos relacionados con el uso de las tecnologías y sistemas de información. A si mismo aprovechar con la Auditoria de sistemas y tecnologías de información como herramienta fundamental de poyo, y que esta no sea vista como un gasto extremo sino más bien como una inversión a mediano y largo plazo, que podría colaborar en próximos intentos por mejorar cada vez más los servicios apoyados en los Sistemas de Información.

II. MARCO TEÓRICO.

2.1 Antecedentes.

2.1.2 Antecedentes Internacionales.

Según los Autores: Antoni Lluís Mesquida, Antonia Mas, Esperanza Amengual, Ignacio Cabestrero. Con el tema de investigación: Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. De la Universidad Rafael Belloso Chacín- Venezuela, Año 2008. Sostienen que:

Dada la gran aceptación que tuvo en su momento la implantación de un Sistema de Gestión de Calidad (SGC) de acuerdo con la norma ISO 9001, actualmente la mayoría de organizaciones que deciden implantar una nueva norma para gestionar sus servicios, como ISO/IEC 20000, o la seguridad de su información, como ISO/IEC 27001, normalmente ya cuentan con un SGC basado en ISO 9001. Con el objetivo de facilitar a las empresas la implantación de estas normas se ha realizado un estudio, tanto para analizar las posibles relaciones existentes entre los requisitos de los sistemas de gestión propuestos por estas normas, como para identificar los requisitos no compartidos entre ellos. En este artículo se presenta un nuevo Sistema de Gestión Integrado que amplía los requisitos de un SGC según ISO 9001 con los requisitos específicos de los otros dos estándares antes mencionados.

El mencionado antecedente se relaciona con dicha investigación en la parte que referencia a los Sistema de Gestión y Guías de Implementación en la seguridad, en este caso en particular se utiliza una metodología especifica conocida la de Piattini, aplicando así mismo un enfoque de la norma ISO 17799 -2005 la cual está estipulando los dominios de control y políticas de seguridad. Ya que la mencionada tesis esta inclinada en Auditar el servicio de red, vos y datos de la universidad en su servicio Telemático.

Según los Autores: Enrique Martín Méndez, Miguel Ángel Aguilar Proyecto Sanitas – con el tema de investigación: Sistema de Gestión de Seguridad de la Información y certificación UNE 71502 e ISO 27001. Del Grupo Sanitas, Año 2006. Sostiene que:

En la mencionada empresa en el sector de asistencia sanitaria, ha culminado con éxito la implantación de un Sistema de Gestión de Seguridad de la Información y la consiguiente obtención de los certificados UNE 71502 e ISO 27001. El proyecto se ha llevado a cabo con el apoyo de la consultora especializada en seguridad de la información ESA Security, la cual a su vez ha aportado su experiencia en la implantación de estos sistemas. El Departamento de Seguridad de Sanitas, perteneciente a la Dirección General de Sistemas de Información, ha sido el impulsor de este proyecto con el objetivo de mejorar continuamente en su gestión.

El desarrollo del proyecto en Sanitas le permitió ser certificable, esto debido a la confianza y colaboración de querer salir adelante; también al reconocer que los activos de información de su empresa son muy importantes en el desarrollo de sí misma, por ello busco métodos para salvaguardar y proteger su información y por ende la seguridad de sus sistemas de información de dicha organización.

2.1.3 Antecedentes Nacionales.

Según Arturo Fernando Granados Rodríguez, en su tema de investigación "Auditoria del Desarrollo de Sistemas de Información en el Gobierno Regional de Cajamarca", Universidad Privada del Norte (2012), sostiene que:

Dicha investigación surge a raíz que en todo ámbito institucional se requiere información oportuna y confiable, para la toma de decisiones, esta realidad ha permitido el desarrollo de Sistemas de información. Usualmente, la mayoría de las instituciones, en este caso específico como lo es el Gobierno Regional de la ciudad de Cajamarca, en cuanto al desarrollo de sistemas de información carece de un análisis adecuado, técnico y profesional, lo cual ha generado como consecuencia el contar con la información poco confiable y veraz, inoportuna e inconsistente a la hora de tomarlas decisiones por la gerencia. Es por eso que en esta tesis la propuesta está orientada a mejorar el nivel orientado a la seguridad de sus datos y a la información que procesa y maneja el gobierno regional de Cajamarca, haciendo uso de metodologías específicas y estándares de calidad como el 27001 que apunta al nivel de seguridad, para analizar toda la problemática y propone un plan de acción que permita administrar su información de la mejor manera posible en el corto y mediano plazo para mejorar la calidad y servicios que ofrece a la ciudadanía.

Según Emigdio Antonio Alfaro Paredes, con el tema de investigación "Metodología para la Auditoria Integral de la Gestión de la Tecnología de Información". Pontificia Universidad Católica del Perú (2008), sostiene que:

De la revisión de la literatura sobre estándares internacionales de calidad relacionados a la gestión de tecnología de información (COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 (ITIL), PMBOK, ISO/IEC 27001, IEEE 1058-1998, ISO 9001:2000 e ISO 19011:2002), MoProSoft 1.3, y las normas relacionadas a la auditoría informática en el Estado Peruano, se concluye que no existe una metodología para la auditoría integral de la gestión de la tecnología de información. Los enfoques actuales están basados sobre el proceso general de auditoría sumándoles las inclusiones no integradas de los diversos estándares de calidad internacional, o las normas vigentes para las entidades que son sujetas de evaluación en una auditoría.

El objetivo de la tesis fue el desarrollo de una metodología para la auditoría integral de la gestión de las tecnologías de información (MAIGTI), con un enfoque de procesos, basado en estándares de calidad internacionales. MAIGTI enlaza los diversos conceptos de COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 (ITIL), Y PMBOK, sobre la base de una simplificación del proceso general de auditoría descrito en la norma ISO 19011:2002, y sobre la base de una adaptación del esquema de procesos de la ISO 9001:2000 (ISO, 2000). MAIGTI comprende los siguientes elementos: (a) objetivo (la finalidad de la auditoría), (b) alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría), (c) entradas (requerimientos de información), (d) proceso de MAIGTI (evaluaciones a realizar) y (e) salidas (papeles de trabajo e informe de auditoría). Asimismo, cada uno de los procedimientos para la evaluación de los principales objetivos de control dentro de los subprocesos de MAIGTI, comprende la siguiente estructura: (a) objetivo (la finalidad del procedimiento de auditoría), (b) alcance (detalle de lo que está incluido y lo que no está incluido como parte de la auditoría a realizarse a través del procedimiento), (c)

entradas (requerimientos de información para ejecutar el procedimiento de auditoría), (d) proceso (detalle de los pasos a seguir en el procedimiento de auditoría), y (e) salidas (hallazgos evidenciados como resultado de la ejecución del proceso).

En los procedimientos descritos en el anexo 1, se ha detallado como salidas, algunos hallazgos posibles que se derivan como resultado de la experiencia de las aplicaciones de MAIGTI en auditorías realizadas por el autor de la tesis. MAIGTI ha sido aplicada principalmente a 2 empresas de seguros y de manera parcial 8 entidades más, auditadas por el autor de la tesis, siendo aplicable para entidades usuarias de tecnología de información. Se recomienda ampliar MAIGTI o crear otra metodología, para la auditoría integral de la gestión de tecnología de información en entidades proveedoras de servicios de tecnología de información.

2.1.4 Antecedentes Locales.

Ana Pilar de Jesús Maco Chonate, en su investigación "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 utilizando el software pilar2". Universidad Católica Santo Toribio de Mogrovejo (2008), sostiene que:

De acuerdo al análisis realizado a la Caja Sipán de la ciudad de Chiclayo en lo que respecta la seguridad de su información que esta maneja y opera, se pudo encontrar indicios de que la Caja Sipán no cuenta con un equipo encargado de analizar y gestionar la seguridad de la información en esta, por lo que siendo una entidad financiera debe tener un plan de seguridad de su información, el encargado de realizar esta labor es el Jefe del Área de Tecnologías de Información. Así mismo otro de los problemas encontrados en la Caja Sipán es la disconformidad que se tiene en cuanto a la calidad de equipo técnico que respalda la seguridad de la información. Se encontró también que la Caja Sipán cuenta con un plan de seguridad de la información, el cual no contaba con todas sus políticas documentadas, e incluso que este plan de seguridad de la información no era conocido por el personal que labora en la empresa. Este tipo de faltas o de carencias en cuanto a la seguridad conllevan a la empresa a tener grandes pérdidas. Los trabajadores de la Caja Sipán al desconocer estas políticas, están incumpliéndolas, lo que ocasiona la falta de eficiencia en el trabajo. Sobre esta descripción se puede definir que el problema principal de la empresa es la carencia de un Plan de Seguridad sujeto a normas de calidad que garanticen la seguridad, integridad, confiabilidad y eficiencia de la información.

2.2 Bases Teóricas Científicas.

2.2.1 Gestión de la Seguridad de la Información.

a) Definición de Seguridad de Información.

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. (Wolfgang 2009).

b) Importancia de Seguridad de 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 saboteada. 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. (Wolfgang 2009).

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. (Álvarez 2008)

c) Objeto de la Seguridad de la Información.

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 usados 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. (Álvarez 2008)

2.2.2 Aspectos Fundamentales en la Seguridad de la Información.

Tenemos los siguientes aspectos como son los que se detallaran a continuación como: La Confidencialidad, La Integridad, La Disponibilidad, y La Autentificación. En seguida hablaremos de cada una de ellas:

a) La Confidencialidad.

Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. A groso modo, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.
La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad. (Álvarez 2008)

b) La Integridad.

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información (Álvarez 2008)

c) Disponibilidad.

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo

requieran. En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La Alta disponibilidad sistemas objetivo debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con un sistema de gestión que permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera. Tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc. Mediante el uso de clúster o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

d) Autenticación.

Es la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.

2.2.3 Gestión de Riesgos en la Seguridad Informática.

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo, es así que tenemos a los siguientes parámetros como son los que detallaremos a continuación:

1) Análisis del Riesgo.
Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.

2) Clasificación.
Determina si los riesgos encontrados y los riesgos restantes son aceptables.

3) Reducción.
Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.

4) Control:
Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sancionar el incumplimiento.
Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de:

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.
- Orientar el funcionamiento organizativo y funcional.
- Garantizar comportamiento homogéneo.
- Garantizar corrección de conductas o prácticas que nos hacen vulnerables.
- Conducir a la coherencia entre lo que pensamos, decimos y hacemos.

2.2.4 Sistema de Gestión de la Seguridad de la Información (SGSI).

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. 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 (a las que puede acceder directamente a través del submenú de la izquierda o siguiendo los marcadores de final de página) se desarrollarán los conceptos fundamentales de un SGSI según la norma ISO 27001. (Chi-Hsiang Wang 2010)

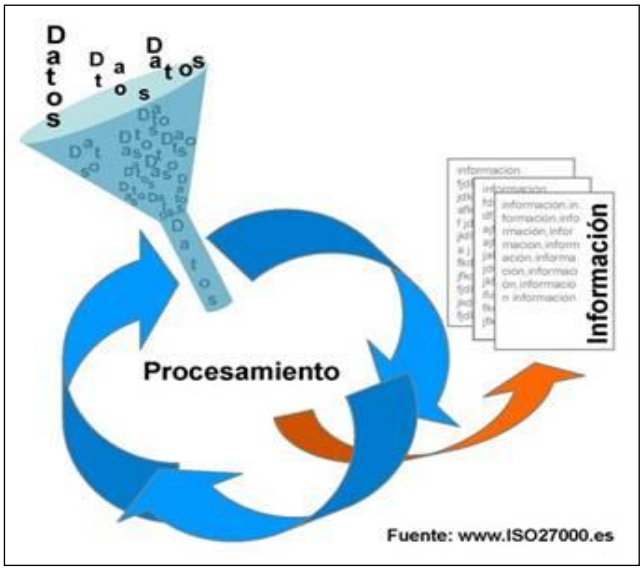
2.2.5 Que se entiende por un SGSI.

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 Información 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. (ISO27001.es).

Figura 1.Estructura que referencia un SGSI.



Fuente: www.ISO27001.es

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.

2.2.6 Que 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 2.Estructura Piramidal de los distintos Niveles de un SGSI.

Fuente: www.ISO27001.es

1. 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.

2. 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.

3. 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.

4. 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. (ISO27001.es)

2.2.7 Gestión de la Seguridad de la Información.

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información. La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. (Burnett. 2004)

También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible. A raíz de la importancia de la norma ISO 27001, muchas legislaturas han tomado esta norma como base para confeccionar las diferentes normativas en el campo de la protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc. (Dussan 2004)

2.2.8 Fases del Sistema de Gestión de Seguridad de Información.

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información.
Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información. (Gómez Fernández 2012).

Las fases son las siguientes:

a) **La Fase de planificación**: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).

b) **La Fase de implementación**: esta fase implica la realización de todo lo planificado en la fase anterior.

c) **La Fase de revisión**: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos "canales" y verificar si los resultados cumplen los objetivos establecidos.

d) **La Fase de mantenimiento y mejora**: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI. (Gómez Fernández 2012)

a) La Fase de planificación.

Esta fase está formada por los siguientes pasos:

- Determinación del alcance del SGSI;
- Redacción de una Política de SGSI;
- Identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos;
- Identificación de activos, vulnerabilidades y amenazas;
- Evaluación de la magnitud de los riesgos;
- Identificación y evaluación de opciones para el tratamiento de riesgos;
- Selección de controles para el tratamiento de riesgos;
- Obtención de la aprobación de la gerencia para los riesgos residuales;
- Obtención de la aprobación de la gerencia para la implementación del SGSI;
- Redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables. (Wang 2010)

b) La Fase de verificación.

Esta fase incluye los siguientes pasos como:

- Implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.;
- Revisiones periódicas de la eficacia del SGSI;
- Medición la eficacia de los controles;
- Revisión periódica de la evaluación de riesgos;
- Auditorías internas planificadas;
- Revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras;
- Actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión;
- Mantenimiento de registros de actividades e incidentes que puedan afectar la eficacia del SGSI.

c) La Fase de mantenimiento y mejora.

Esta fase incluye los siguientes pasos como:

- Implementación en el SGSI de las mejoras identificadas;
- Toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros;
- Comunicación de actividades y mejoras a todos los grupos de interés;
- Asegurar que las mejoras cumplan los objetivos previstos.

2.2.9 Lista de Verificación de la Norma ISO 27001.

La Organización Internacional de Normalización (ISO, por sus siglas en inglés) publicó la norma ISO 27001 para establecer, supervisar y mejorar la gestión de seguridad de la información en las organizaciones. La lista de verificación la norma ISO 27001 ayuda a las empresas desarrollar y mantener un programa de seguridad que impida las fugas de información y otras violaciones de seguridad de la información. La lista cubre una amplia gama de medidas de control legales, físicas y técnicas que van desde la clasificación sensitiva de los datos a la entrada de restricción de las personas con malas intenciones.

A. Política de seguridad

La lista de verificación de la norma ISO 27001 debe analizar si una empresa tiene un sistema de información del programa de seguridad que está aprobado por la dirección y se comunica a todos los empleados de la compañía. La administración debe manifestar su compromiso con la seguridad y el enfoque de la organización para la gestión de seguridad de la información. La política debe revisarse a intervalos. Esto es para asegurar la continua estabilidad, suficiencia y efectividad de la tecnología de la información del sistema. Todas estas cuestiones deben abordarse en la lista.

B. Coordinación de seguridad

Las actividades de seguridad de la información deben ser coordinadas por representantes de diversos departamentos de la empresa. La necesidad de la organización de acuerdos de confidencialidad o no divulgación debe estar claramente definida y revisada con regularidad. Los empleados deben entender que la violación del acuerdo de no divulgación tiene sus consecuencias. Por ejemplo, un analista de inteligencia de EE.UU. fue detenido en Irak en junio de 2010 por filtrar un video clasificado de las tropas disparando contra civiles. Bradley Manning filtró el vídeo a los denunciantes del sitio web Wikileaks. El liderazgo organizacional también debe identificar los riesgos a los servicios de información antes de conceder acceso a terceros. Las medidas de control deben ser implementadas antes de concederse el acceso. La información debe ser clasificada también en términos de su valor y la sensibilidad de la empresa.

C. Protección contra la entrada maliciosa

Necesitas tener la capacidad para detectar y prevenir intentos maliciosos internos o externos para acceder a tu información. Si se trata de un negocio en línea, por ejemplo, los clientes deben ser capaces de comprar de forma segura la mercancía. El programa que transfiere datos de un ordenador a otro debe ser capaz de funcionar efectivamente por su cuenta. Con el fin de evitar poner en peligro información valiosa, la red de una organización debe ser adecuadamente gestionada y controlada para evitar cualquier amenaza y mantener la seguridad de los sistemas y aplicaciones en toda la red de la organización. Sin ese mecanismo, la información de la organización está en riesgo de abuso por parte de delincuentes que se benefician con datos en línea. (Alvares 2012)

2.2.10 Como Implementar la ISO 27001.

La ISO 27001 es un estándar de calidad general desarrollado por ISO (International Standards Organization - Organización Internacional de Estándares) enfocado en la seguridad de la información. La seguridad de la información varía por organización; sin embargo, en general incluye todas las formas de datos, comunicaciones, conversaciones, grabaciones, documentos e incluso fotografías. Incluye todo desde correos electrónicos a faxes y conversaciones telefónicas. La implementación del ISO 27001 es utilizada específicamente para obtener certificación para el sistema de administración de seguridad de la información (ISMS o Information Security Management System) de una organización. El ISMS define el estándar para toda la organización, proveyendo objetivos marcados por un plan accionable para lograr y mejorar sobre ellos de acuerdo al estándar de la administración.

Instrucciones:

1) **Establece objetivos**. Cada sistema de administración de seguridad de la información debería tener un conjunto de ISMS hacia el cual trabajar. Los objetivos exactos dependerán de la organización y el entorno regulador de la industria en la que la industria trabaja. Por ejemplo, un banco que trabaje con clientes con un alto patrimonio neto necesitará establecer objetivos más rigurosos en relación a la seguridad de la información que una compañía de ganado.

2) **Define el alcance y los límites de los objetivos de tu ISMS**. Para cada objetivo, asigna un valor que te ayude a medir el alcance de su éxito. Por ejemplo, si quieres reducir el fraude en relación a la seguridad de la información, puedes establecer un objetivo que incluya una reducción del fraude de un 5 al 10 por ciento por año. Además, puede que quieras establecer diferentes objetivos para diferentes departamentos dentro de la organización. Por ejemplo, el personal de ventas puede tener una tasa más alta de fraudes que otras funciones como administración o soporte. Definir el alcance y establecer los límites mejorará el éxito de la implementación.

3) **Identifica la mejor manera de abordar la evaluación de riesgos**. Los riesgos para el ISO 27001 son eventos que pueden comprometer la seguridad de la información de una organización. Por ejemplo, tu compañía puede querer realizar una auditoria o contabilización interna para evaluar riesgos regularmente en conjunto con sus tareas normales. Estos grupos tienden a trabajar objetivamente con toda la organización y usualmente ayudan a establecer y monitorear controles internos.

4) **Identifica los mayores riesgos de seguridad en tu organización**. Luego de evaluar los riesgos, tendrás una lista de eventos de seguridad. Prioriza estos riesgos para el equipo de implementación.

5) **Evalúa tu entorno de seguridad de la información actual y mide la amenaza de cada riesgo de seguridad**.
   Cada riesgo de seguridad también debe estar conectado a un objetivo específico para medir el desempeño a lo largo del tiempo.

6) **Crea un plan para tratar y mejorar sobre estos riesgos**. Cada riesgo debe tener una lista de acciones y opciones que pueda ser seguida por el equipo de evaluación de riesgos. Las acciones deben proveer una forma clara de alcanzar los objetivos, y también controles definidos para poder monitorear los riesgos. Para una organización grande, separa el plan en diferentes secciones. Por ejemplo, puede que quieras empezar con un piloto y luego desplegar el plan a la organización.

7) **Obtén aprobación de la gerencia**. La gerencia debe formalmente ratificar el plan antes de implementarlo. Pide hacer un anuncio general del plan a la organización. También provee una línea de tiempo para que la implementación se apruebe y disemine a lo largo de la organización.

8) **Comienza la implementación**. Realiza auditorías internas con regularidad y reporta los resultados a la gerencia con la misma regularidad. Actualiza tus objetivos y planes de seguridad de manera apropiada.

III. MATERIALES Y MÉTODOS.

3.1 Diseño de investigación.

3.1.1 Tipo de Investigación.

El tipo de investigación es Tecnológica Aplicada, en razón que se hará el estudio bajo conocimientos de Gestión y Guías de Implementación para seguridad de Sistemas de Información, transformando ese conocimiento puro en un conocimiento útil, así mismo se generan conocimientos o métodos dirigidos, ya sea con el fin de mejorarlos y hacerlos más eficientes, o con el fin de obtener productos nuevos y competitivos.

3.1.2 Hipótesis.

Con una Guía de Implementación de la Seguridad de la Información basada en la Norma ISO/IEC 27001, se apoyará en la mejora de la Seguridad en las Aplicaciones Informáticas de la comisaria del Norte –Chiclayo.

3.1.3 Diseño de Contrastación.

El diseño de contrastación según el nivel de conocimiento que se pretende alcanzar el diseño de la investigación es el de una Investigación Cuasi-Experimental, ya que en esta se analiza el efecto producido por la acción o la manipulación de una o más variables independientes sobre una o varias dependientes. (Ramírez Zuluaga- 2004)

3.1.4 Variables e Indicadores.

3.1.4.1 Variables

a) Variable Independiente.

Guía de Implementación de la seguridad de información, bajo la Norma ISO/IEC 27001.

b) Variable Dependiente.

Nivel de Seguridad

3.1.4.2 Indicadores.

Cuadro 1: Indicadores de objetivos.

OBJETIVOS ESPECÍFICOS	INDICADOR	DESCRIPCIÓN	UNIDAD DE MEDIDA	INSTRUMENTO	OPERACIONALIZACION
Incrementar el nivel de seguridad en las aplicaciones de la institución policial.	Nivel de seguridad	Valor en una escala de nivel aceptable: nivel alto, nivel medio, nivel bajo.	Nivel Porcentual	Reporte del sistema sobre los índices de inseguridad	Porcentaje de cumplimiento de nivel aceptable / Cantidad total niveles
Mejorar el proceso para la detección de anomalías en la seguridad de la información.	Número de procesos	Instrumento para medir el Nº de procesos implementados, con los ya existentes: alto, medio, y bajo.	Numero	Entrevistas realizadas la personal involucrado en temas de seguridad	N° Proceso implementados - N° procesos existentes
Disminuir los niveles de riesgos, respecto a los activos de información considerados amenazas y vulnerabilidades.	Nivel de Riesgo	Niveles de riesgos, con referencia a los activos de información de la institución.	Valor escalar	Encuesta dirigida al personal involucrado en los sistemas de información	Activos información con riesgos / Total de activos de información
Mejorar el nivel de capacitación en temas de seguridad informática en el personal	Nivel de programas de capacitación	Nivel de programas destinados a la capacitación del personal.	Nivel	Encuesta dirigida a los efectivos acerca del número de capacitaciones recibidas	Nivel de capacitación implementado - Nivel de capacitación existente.

Fuente: Elaboración Propia

3.1.5 Población y Muestra.

La población de la presente investigación lo constituirá los 30 trabajadores de la Comisaria del Norte de la PNP de la ciudad de Chiclayo, que además son efectivos policiales.
Según Hernández y Fernández 1991: Debido a que la población es muy pequeña (n<=30) se tomarán a los 30 trabajadores de la Entidad mencionada. La selección de la muestra será en base a un muestreo no probabilístico, de tipo intencional o por conveniencia; que para el caso la muestra será el total de la población.

3.1.6 Técnicas de Procesamiento de Datos.

Cuadro2: Detalle de Técnicas en el proceso de los datos.

MÉTODO/ TÉCNICA	INSTRUMENTO	ELEMENTOS DE LA POBLACIÓN	DESCRIPCIÓN
Observación	Ficha de Observación	Proceso de denuncia del ciudadano.	Con el uso de esta ficha se procede al llenado de la denuncia indicando, los motivos, el denunciado, la hora del hecho, etc.
Encuestas	Cuestionario de preguntas (abiertas y cerradas) Anexo-encuesta 01	Personal efectivo policial	Este cuestionario estuvo dirigido al personal que labora en la comisaria, para recoger información acerca de los problemas que suceden en la comisaria, para así conocer y determinar el nivel de conocimiento en temas de seguridad en el uso de sus aplicaciones.
Entrevistas	Guía de entrevistas (formato de entrevistas) Anexo – entrevista 01	Jefe del departamento de denuncias policiales (violencia familiar – delitos robos)	Esta entrevista con preguntas abiertas estuvo dirigida al encargado del dpto. De denuncias policiales que a sus vez esta las orientadas al tipo de denuncias familiares y abuso y maltrato infantil y a la mujer y las denuncias típicas por robo. Para así conocer que tanto pueden saber y conocer temas orientados a políticas y mecanismos de seguridad en el uso de las aplicaciones, ya que en este departamento se usa el Sistema de Denuncia Policial con SIDPOL.
Reportes	Guía de reportes	Jefe encargado del uso del sistema policial	Con el uso de esta técnica se procede al conocimiento del desempeño y uso del sistema de denuncias policiales de la institución policial.

Fuente: Elaboración propia

3.2 Metodología.

3.2.1 Metodología Norma ISO/IEC 27001.

A. Aspectos Básicos de la Norma ISO/IEC 27001.

La ISO/IEC 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO), la que a su vez describe cómo gestionar la seguridad de la información adecuada en una empresa. ISO/IEC 27001 puede ser a su vez implementada en cualquier tipo de organización, la misa que a su vez puede ser, con o sin fines de lucro, privada o pública, pequeña o grande. Está norma a su vez está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.

B. Como funciona ISO/IEC 27001.

Cabe mencionar que a su vez el eje central de ISO/IEC 27001 es proteger la confidencialidad, la integridad y disponibilidad de la información en una determinada empresa. Para dicha actividad se encarga de investigar y revisar cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego define lo que es necesario hacer para evitar que estos problemas se produzcan o se terminen manifestando (es decir, mitigación o tratamiento del riesgo). Por lo tanto, la filosofía principal de la norma ISO/IEC 27001 es basada en la gestión de riesgos: investigándolos y luego tratarlos sistemáticamente.

En cuanto a las medidas de seguridad (o controles) que se van a implementar estos se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Figura 3: Estructura de ISO/IEC 27001

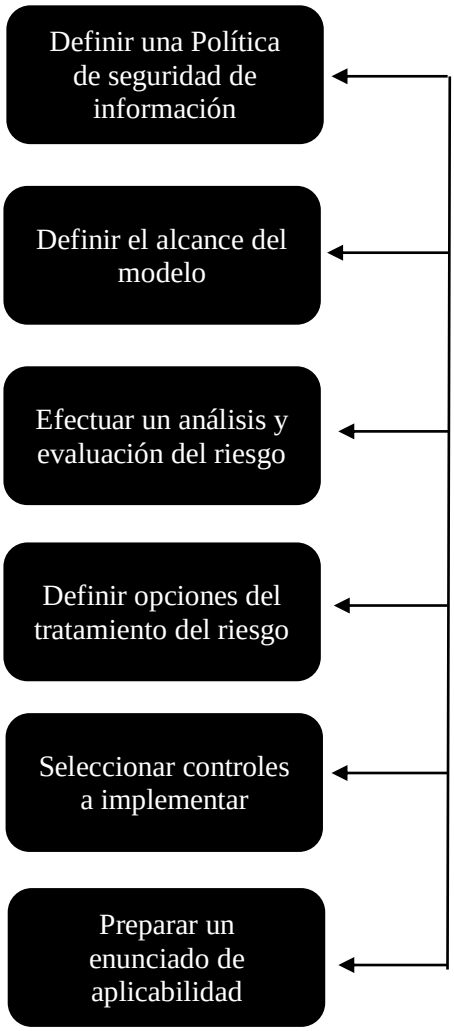
Fuente: www.iso27001standard.com

C. Proceso de implementación de la ISO/IEC 27001 – Enfoque de las seis fases o pasos esenciales del proceso.

Dentro del proceso de implementación de la ISO/IEC 27001, podemos mencionar el siguiente enfoque para su posible implementación como son los siguientes:

- Definir una Política de seguridad de Información
- Definir el Alcance del Modelo
- Efectuar un Análisis y Evaluación del Riesgo
- Definir Opciones del Tratamiento del Riesgo
- Seleccionar Controles a Implantar
- Preparar un enunciado de Aplicabilidad

Figura 5: Fases del proceso de implementación de ISO/IEC 27001



Fuente: www.iso27001standard.com
Fuente: Burnett. 2004

D. Beneficios que brinda ISO/IEC 27001

Existen 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información, las que a su vez son las siguientes:

- Cumplir con los requerimientos legales.
- Obtener una ventaja comercial.
- Menores costos.
- Una mejor organización.

E. Donde interviene ISO/IEC 27001.

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

Figura 4: Alcance de ISO/IEC 27001

Fuente: www.iso27001standard.com

F. Entregables definidos por ISO/IEC 27001.

Los diferentes entregables que se tomaron en cuenta con esta Metodología utilizada como la ISO/IEC 27001 para la institución policial Comisaría del Norte PNP-Chiclayo, son los siguientes que detallaremos a continuación brevemente:

E1 Entregable 01: Procedimiento para el control de documentos y registros.

- Objetivo del entregable: Establecer las pautas para la elaboración y control de los documentos y registros asociados al Sistema integrado de Gestión de Seguridad en la Institución Policial PNP Comisaria del Norte Chiclayo.

E2 Entregable 02: Plan del proyecto.

- Objetivo del entregable: El objetivo del Plan del proyecto es definir claramente el propósito del proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), los documentos que se redactarán, los plazos y las funciones y responsabilidades del proyecto.

E3 Entregable 03: Procedimiento para la identificación de requisitos.

- Objetivo del entregable: El objetivo del presente documento es definir el proceso de identificación de las partes interesadas, de los requisitos legales, normativos, contractuales y de otra índole relacionados con la seguridad de la información y con la continuidad del negocio, como también las responsabilidades para su cumplimiento.

E4 Entregable 04: Documento sobre el alcance del SGSI.

- Objetivo del entregable: El objetivo de este documento es definir claramente los límites del Sistema de gestión de seguridad de la información (SGSI) en la Institución Policial Comisaria del Norte – Chiclayo. Este documento se aplica a toda la documentación y actividades dentro del SGSI.

E5 Entregable 05: Política de seguridad de la información.

- Objetivo del entregable: El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información. Esta Política se aplica a todo el Sistema de gestión de seguridad de la información (ISMS), según se define en el Documento del Alcance del SGSI.

E6 Entregable 06: Metodología de evaluación y tratamiento de riesgos.

- Objetivo del entregable: El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en la Institución Policial Comisaria del Norte –Chiclayo y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001

E7 Entregable 07: Declaración de aplicabilidad.

- Objetivo del entregable: El objetivo del presente documento es definir qué controles son adecuados para implementar en la Institución Policial Comisaria del Norte -Chiclayo, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.

E8 Entregable 08: Plan de tratamiento del riesgo.

E9 Entregable 09: Plan de capacitación y concienciación.

- Objetivo del entregable: Capacitación y Concienciación del Personal Efectivo Policial de la Institución Policial Comisaria del Norte PNP-Chiclayo.

3.2.2 Metodología Magerit.

A. Aspectos Básicos de la Metodología Magerit.

Esta metodología hace referencia al análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión en las organizaciones respectivamente.

B. Estructura de la Metodología Magerit.

Esta metodología tiene una estructura adecuada la cual se describirá a continuación como:

- El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

- El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.

- El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.

- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

- El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.

- El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

- El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos

C. Objetivos de Magerit.

Entre los distintos objetivos que persigue la siguiente metodología tenemos a los siguientes objetivos Directos como son:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

D. Fundamentos de Magerit

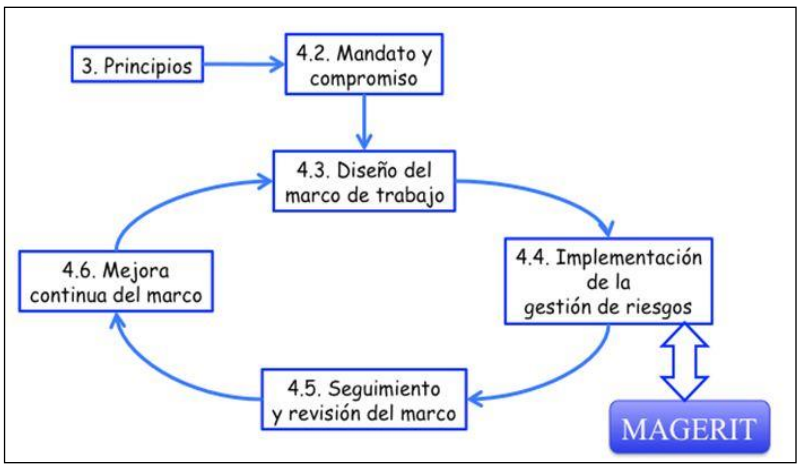
Puntualmente esta metodología se basa fuertemente en analizar el impacto que puede tener para la empresa la violación de su seguridad, busca la identificación de las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Lo interesante de esta metodología, es que presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos.

E. Ventajas de la Metodología Magerit

La metodología Magerit permite saber cuánto valor está en juego en las organizaciones y por ende ayuda a protegerlo. Así mismo conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con esta metodología, se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Figura 6: Marco de trabajo para gestionar los riesgos



Fuente: PAE: Portal de Administración Electrónica.

IV. RESULTADOS.

En los resultados de la Tesis, daremos a conocer los distintos entregables asociados a la norma ISO/IEC 27001, que se consideraron para el desarrollo realizado en la Institución policial PNP "Comisaria del Norte" – de la ciudad de Chiclayo.
A continuación mencionaremos una lista de los distintos entregables, que posteriormente se detallarán respectivamente en el documento.

4.1 Entregables realizados.

- Entregable 01; Procedimiento para el control de documentos y registros.
- Entregable 02; Plan del proyecto
- Entregable 03; Procedimientos para identificación de requisitos.
- Entregable 04; Documento sobre el alcance del SGSI.
- Entregable 05; Políticas de seguridad de la información.
- Entregable 06; Metodología de evaluación y tratamiento de riesgos.
- Entregable 07; Declaración de aplicabilidad.
- Entregable 08; Plan de tratamiento de riesgos.
- Entregable 09; Plan de capacitación y concienciación.

A continuación detallaremos el desarrollo de los distintos entregables que se trabajaron para la institución policial, basados en la norma ISO/IEC 27001, respectivamente.

COMISARIA DEL NORTE PNP –CHICLAYO

PROCEDIMIENTO PARA CONTROL DE DOCUMENTOS Y REGISTROS

Código	CPCDR
Versión:	001
Fecha de la versión:	2014-05-05
Creado por:	Alcántara Flores Julio Cesar
Aprobado por:	Cap. PNP- Medina
Nivel de confidencialidad:	Nivel Intimo / Nivel Intermedio / Nivel Superficial.

TABLA DE CONTENIDO

1. Objetivos y Usuarios……41
2. Alcance……41
3. Procedimiento de Control de Documentos Internos……41
   3.1. Formato de los Documentos……....42
   3.2. Cuerpo del Documento……42
   3.3. Portada……..42
   3.4. Encabezados……..43
   3.5. Cierre del Documento……...45
   3.6. Control de Cambios……..46
4. Procesos de Control de Documentos Externos……47
5. Procedimiento de Control de Registro……47

1. OBJETIVOS Y USUARIOS.

1.1 GENERAL

- Establecer las pautas para la elaboración y control de los documentos y registros asociados al Sistema integrado de Gestión de Seguridad en la Institución Policial PNP Comisaria del Norte Chiclayo.

1.2 OBJETIVOS ESPECIFICOS

- Definir los pasos a seguir en la Producción Documental del Sistema de Seguridad de Información en la Institución Policial.
- Permitir que el manejo de la documentación del SGSI refleje una adecuada Imagen Institucional, contribuyendo al fortalecimiento de la Identidad Visual.
- Permitir un control eficaz y eficiente de la información y documentación, por medio de actividades de seguimiento, control y verificación adecuadamente.
- Permitir el conocimiento a todo el personal que forma parte de la Institución Policial Comisaria del Norte, en temas orientados a elaboración y control de documentos.

2. ALCANCE.

Aplica a todos los documentos que soportan el Sistema de Gestión de la Seguridad de la Información (SGSI) de la Institución Policial PNP Comisaria del Norte en la ciudad de Chiclayo. En el cumplimiento de la Norma ISO 27001.

3. PROCEDIMIENTO DE CONTROL DE DOCUMENTOS INTERNOS.

Procedimiento establecido con el fin de determinar las actividades concernientes a la elaboración, aprobación, actualización, distribución y conservación de los documentos de la Institución Policial: COMISARIA DEL NORTE - CHICLAYO, con el fin de disponer de la información de manera ágil y eficiente, contribuyendo a

La correcta preservación de la documentación del Sistema de Gestión del Sistema de Información.
Los Parámetros a cumplir en la elaboración de los documentos son los siguientes:

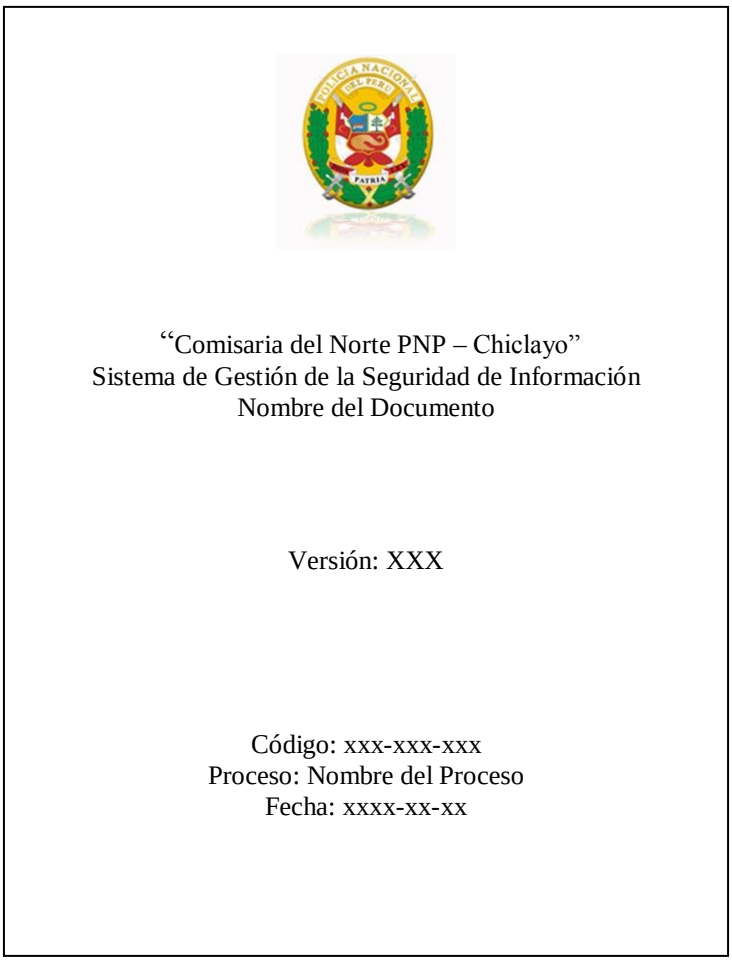
3.1 Formatos de los Documento.

3.2. Cuerpo del Documento.

Los Documentos del SGSI, tales como Manuales, Instructivos, Guías, Informes, Protocolos y Programas se deben elaborar en papel Bond blanco tamaño carta, con márgenes superior e izquierda 3 cm, inferior y derecha 2,5 cm, fuente tipográfica Arial tamaño 12 y los siguientes elementos.

3.3. Portada.

El texto de la portada se escribe en fuente Arial tamaño 12, el nombre del documento en tamaño 14, negrita y alineado al centro. La estructura de la portada debe estar como se indica en la siguiente gráfica:



En la parte superior del documento, seis (6) interlineaciones bajo el margen superior, encontramos el logo símbolo de la Institución, compuesto por el escudo, de la Policía Nacional del Perú. Aprobado mediante Acuerdo del Ministerio del Interior el 30 de Agosto del año 1988. El escudo debe tener un tamaño de 4,01 cm de alto por 3,78 de ancho, el nombre debe estar escrito con fuente Humanst 521 BT y se escribirá cumpliendo el Manual de Identidad del siguiente modo:

Comisaria del Norte PNP Chiclayo.

Comisaria en tamaño de fuente 14 negrita, del en tamaño de fuente 12, Norte en tamaño de fuente 14, PNP en mayúsculas tamaño 12, y Chiclayo en tamaño 14.
Seis (6) interlineaciones bajo el logo símbolo encontraremos los datos requeridos por el documento como tal. Estos datos son: El texto "Sistema de Gestión de Sistemas de Información" en fuente Arial negrita tamaño 12. Tres (3) interlineaciones después, encontramos el nombre del documento en fuente Arial negrita tamaño 14. Tres (3) interlineaciones bajo el nombre del documento, se encuentra la versión del documento, cinco (5) interlineaciones después se encuentra el código que identifica al documento, cinco (5) interlineaciones abajo, se registra el nombre del Proceso del que hace parte el documento y finalmente, tres (3) interlineaciones abajo, se registra la fecha de vigencia del documento como tal. Estos últimos datos se registran con fuente Arial negrita con tamaño 12.

Nota: La interlineación de la Portada debe ser sencilla, tenga en cuenta las Normas ICONTEC para la elaboración de documentos.

3.4. Encabezado

El encabezado de los documentos del SGSI se encuentra en todas las hojas que conforman el documento, excepto la portada, deben estar registrados en fuente tipográfica Arial tamaño 9 y debe tener el siguiente contenido:

- **Extremo izquierdo.**

Se encuentra el escudo de la Institución Policial PNP y el nombre de la Comisaria en fuente tipográfica Humanst BT en la parte inferior del Escudo, tal como lo ordena el Manual de Identidad Visual Institucional de la Universidad.

- **Centro.**

Se registrara los nombres de la dependencia o Proceso, según sea el caso y del documento. De este modo, los documentos de uso general llevarán el texto "Sistema de Gestión de Seguridad de Información", los de uso por Proceso llevarán el nombre que los identifica y los de uso por Dependencia llevarán el nombre de la misma.

- **Extremo derecho.**

Se debe registrar los siguientes datos:

Código: conjunto de caracteres asignados por la Unidad de Archivo y Correspondencia, que se determina de acuerdo al proceso y tipo de documento de acuerdo al siguiente orden:

- **Documentos de uso general**

Los documentos que son aplicables a toda la Institución se codificarán de la siguiente manera:

Los primeros tres dígitos tienen las iniciales del Sistema de Gestión de Seguridad (SGS), los dos siguientes al tipo documental, seguidos de su consecutivo.

- **Documentos de uso por Procesos:**

Los documentos que son aplicables por Proceso se codificarán así:
Las tres primeras letras corresponden al proceso, los dos siguientes al tipo de documento y los dos últimos al consecutivo.

- **Documentos de uso por Dependencia:**

Los documentos que son sustantivos de las funciones de cada dependencia y no son aplicables a Otras, se codificarán de la siguiente manera: Los tres primeros dígitos corresponden a la dependencia, los tres siguientes al proceso, los dos siguientes al tipo de documento y los dos últimos al consecutivo.

Nota: los códigos que se asignan a los documentos asociados al SGSI corresponden al Instructivo de Codificación de Documentos, código SGSI-IN-01 y se registran el Listado Maestro de Documentos Internos, código SGSI-FR-17.

Página: debe evidenciar el número de la página actual frente al número total de páginas. Por ejemplo: 1 de 10.

Versión: corresponde al número de publicaciones aceptadas del documento.

Vigente a partir de: se refiere a la fecha de aceptación de la versión del documento, la cual se registra de acuerdo al sistema internacional: año, mes, día; separados por un guion (xxxx-xx-xx), de este mismo modo se registrará en el cierre y en el control de cambios.

Nota: Dado el tamaño variable de los formatos de la Institución, no se estipula un tamaño exacto de encabezado, pero se debe respetar los requerimientos del Manual de Identidad Visual. El tipo de letra de los datos registrados en el centro e izquierda del encabezado deben ser en fuente tipográfica Arial, negrita, mayúscula sostenida para los nombres e inicial para los datos, tamaño de fuente 9.

3.5. Cierre de Documento.

Los datos contenidos en el Cierre de Documento nos permiten verificar quién lo creó, quién lo revisó y quién lo aprobó, de este modo se identifican los responsables del documento.

- **Elaborado por:** En esta casilla se registra el responsable de la elaboración o creación del documento, o autor del mismo.

- **Revisado por:** En esta casilla se registra el asesor del proceso y el Representante por la Dirección para el Sistema Integrado de Gestión de Calidad.

- **Aprobado por:** En esta casilla se registra el nombre del Líder del Proceso, quien es el responsable de la verificación final del contenido de los documentos. Dado el valor técnico de los Documentos, es necesario que aquellos que lo posean, se aprueben por el Comisario o su segundo subordinado inmediato, de la Dependencia respectiva.

Cada una de estas casillas debe especificar cargo, nombre, firma y fecha en su respectiva columna. Cabe resaltar que el uso de Firmas Digitales únicamente está autorizado para el Comisario de la Institución Policial. La fuente tipográfica a utilizar en el cierre del documento es Arial tamaño 9, negrita y mayúscula inicial.

Gráfica del Cierre de Documento.

	ELABORADO POR:	**REVISADO POR:**	**APROBADO POR:**
CARGO:	Responsable del Procedimiento	Representante de la Dirección	Líder del Proceso o Director de la Dependencia
NOMBRE:	Alcántara Flores Julio Cesar.	Cap. PNP Medina G.	Comisario PNP Cesar Espadín.
FIRMA:			
FECHA:			

3.6. Contenido del Documento.

El contenido del documento debe ser claro, conciso, evitando redundancias y errores gramaticales y ortográficos, teniendo en cuenta que los documentos son la carta de presentación de la Institución ante las entidades con las que se tiene relación. Por razones de variación en los formatos, se recomienda que la fuente sea Arial, el tamaño de fuente depende del tipo y tamaño del formato.

3.7. Control de Cambios.

El Control de Cambios consiste en una tabla que permite llevar control sobre las solicitudes de modificación del documento, cuántas veces se ha llevado a cabo las modificaciones y por qué se las realizó. Esta tabla se debe incluir al final del documento, bajo los Datos de Elaboración y genera un Formato denominado Control de Cambios, código SGSI-FR-19. Los datos contenidos en el Control de Cambios son los siguientes:

- **Versión:** corresponde al número de versiones existentes del mismo Documento. Cabe resaltar que la última versión es la que se toma en cuenta para difusión.
- **Fecha de Aprobación:** Corresponde a la fecha de aprobación de la versión que se encuentra.
- **Descripción del Cambio:** Referencia de la razón por la cual fue modificado el documento.

Gráfica del Control de Cambios:

CONTROL DE CAMBIOS		
VERSION N°	FECHA DE APROBACION	DESCRIPCION DEL CAMBIO

Nota:
Los datos de Cierre del Documento y Control de Cambios únicamente se registran en los Documentos y no en los Registros.

4. PROCEDIMIENTO DE CONTROL DE DOCUMENTOS EXTERNOS.

Procedimiento establecido con el fin de establecer controles para la identificación y control de los documentos externos que afectan al SGSI, con el fin de disponer de la información de manera adecuada, evitando el uso de documentos obsoletos, contribuyendo al mejoramiento continuo de los Procesos y Procedimientos en la Institución.

Los Documentos Externos que afectan al SIGC son:

Documentos Legales, entre ellos, la Constitución Política del Perú, Leyes, Acuerdos, Decretos y Códigos Peruanos de diferente naturaleza.

Manuales de funcionamiento, directrices y demás documentos que se relacionen con el manejo de equipos propios de la Institución Policial de la Comisaria del Norte –Chiclayo.

Documentos generados, por otras Instituciones y que tengan relación directa con las actividades y funciones realizadas por las diferentes Dependencias.

Documentos implementados, por una Dependencia pero que son generados por otra, como por ejemplo, las Resoluciones Ministeriales o los Acuerdos del Concejo Superior de Inspectoría que aplican a varias dependencias.

Los documentos externos se identifican con el sello de copia controlada del SGSI y se incluyen en el Listado Maestro de Documentos Externos SGSI-FR-18. Los líderes de los procesos deben reportar al Asesor de Seguridad, asignado los documentos externos que utilicen y que se hayan modificado o actualizado en cumplimiento de sus funciones para la actualización del Listado Maestro de Documentos Externos. A su vez, el Asesor debe reportar dentro de los 5 últimos días de cada mes los cambios realizados a la Unidad de Archivo y Correspondencia para consolidar el Listado Maestro de Documentos Externos de la Institución Policial.

5. PROCEDIMIENTO CONTROL DE REGISTROS

Procedimiento que establece las actividades necesarias para la identificación, el almacenamiento, la conservación, la recuperación, la retención y la disposición de los registros que se generan en cumplimiento de las funciones y procedimientos establecidos por el SGSI.

Diligenciamiento.

El diligenciamiento de los Registros puede llevarse a cabo de manera digital o manual.

- En los casos en que el formato se diligencie de manera manual, se deben tener en cuenta los siguientes aspectos:
- Escribir con letra clara y legible
- Usar tinta indeleble
- Diligenciar todas las casillas que el formato solicita.
- Evitar tachones y enmendaduras.
- Cuando ocurra un error que requiera la anulación del documento debe tacharse con una sola línea diagonal y dejar constancia mediante la firma y fecha del funcionario responsable.
- Cuando una casilla del formato que requiera diligenciamiento, no se diligenció, debe trazarse una línea para evitar diligenciamientos posteriores de información.

Responsabilidad.

Para identificar quién es el responsable de diligenciar el documento es necesario implementar la Línea de Responsabilidad que se encuentra al final de los formatos establecidos, dicha línea de responsabilidad contiene los siguientes datos, de acuerdo a la naturaleza de cada formato:

	DILIGENCIADO POR
NOMBRE	
CARGO	
FIRMA	
FECHA	

	DILIGENCIADO POR	APROBADO POR
NOMBRE		
CARGO		
FIRMA		
FECHA		

	DILIGENCIADO POR	REVISADO POR	APROBADO POR
NOMBRE			
CARGO			
FIRMA			
FECHA			

Los Registros se relacionan en un Listado Maestro de Registros, código SGSI-FR-16, Formato en el que se registra los siguientes datos:
Código, Nombre, Versión, Vigencia, Fecha de Vigencia, Ubicación o Dependencia, Lugar de Almacenamiento, Cargo del Responsable del Manejo del Archivo, Medio de Almacenamiento, Nivel de Acceso de la Información, Tiempo de Retención, Disposición Final y Observaciones. El responsable del diligenciamiento del listado maestro de registros es el líder de cada proceso o su delegado, quien debe reportar dentro de los cinco (5) últimos días de cada mes a la Unidad de Archivo y Correspondencia los cambios realizados en el Listado.

COMISARIA DEL NORTE PNP -CHICLAYO

PLAN DEL PROYECTO
PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código	CPPISGSI
Versión:	001
Fecha de la versión:	2014-05-05
Creado por:	Alcántara Flores Julio Cesar
Aprobado por:	Cap. PNP -Medina
Nivel de confidencialidad:	Nivel Intimo / Nivel Intermedio / Nivel Superficial.

TABLA DE CONTENIDOS

1. Objetivos, Alcance y Usuarios……..52
2. Documentos de Referencia……52
3. Proyecto de Implementación del SGSI……..52
   3.1. Objetivo del Proyecto……52
   3.2. Resultado del Proyecto……...53
   3.3. Plazos……..53
   3.4. Organización del Proyecto……54
4. Gestión de Riesgos guardados en base a este Documento……55
5. Validez y Gestión de Documentos……55
6. Diagnóstico de la Situación Actual……...56
7. Situación Actual……56

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del Plan del proyecto es definir claramente el propósito del proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), los documentos que se redactarán, los plazos y las funciones y responsabilidades del proyecto.
El Plan del proyecto se aplica a todas las actividades realizadas en el proyecto de implementación del SGSI.

El Plan del proyecto se aplica en una primera etapa a los datos, sistemas de información, medios de enlace y redes de comunicación, infraestructura tecnológica, soportes de información, infraestructura física y funcionarios que apoyan la ejecución de los tres (3) primeros procesos identificados como críticos dentro de la Institución Policial, lo cual nos permitirá identificar de una implementar la metodología adecuada, para cada año adaptar los demás procesos críticos del negocio con el SGSI, hasta obtener un grado de madurez que luego nos permita gestionar de una manera adecuada todos los procesos en la Institución Policial Comisaria del Norte.

Los usuarios de este documento son los miembros de la [alta dirección] y los miembros del equipo del proyecto. Para este caso los Miembros de la Alta dirección está compuesta por el encargado de la Institución Policial y el que toma las decisiones como es el Comisarios PNP Cesar Espadín, seguido del Cap. PNP Medina, y los miembros del equipo del Proyecto está conformado por el Sr Alcántara Flores J.C

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001
- Norma ISO 22301

3. PROYECTO DE IMPLEMENTACIÓN DEL SGSI

3.1. Objetivo del proyecto

Para implementar el Sistema de Gestión de Seguridad de la Información en conformidad con la norma ISO 27001, se realizará a más tardar, hasta finales del mes de Julio del 2014, la implementación de los documentos necesarios que permitan gestionar de manera segura el flujo de información derivado de los diferentes procesos de la Institución Policial.

3.2. Resultados del proyecto

Durante el proyecto de implementación del SGSI, se redactarán los siguientes documentos:

a. Situación actual

b. Políticas que incluyen controles para:

1. Aspectos Organizativos de la seguridad de la información.
2. Gestión de Activos.
3. Seguridad relacionada al personal.
4. Gestión de comunicaciones y operaciones.
5. Control de Acceso.
6. Adquisición, desarrollo, mantenimiento de sistemas informáticos.
7. Gestión de los Incidentes de Seguridad.
8. Gestión de la Continuidad del Negocio.
9. Cumplimiento.

c. Compromiso firmado por parte de los miembros del Comité de Administración Integral de Riesgo (CAIR), de apoyar decididamente a la implementación del SGSI.

d. Enfoque de evaluación de riesgos cuya metodología debe contemplar inventario de activos, identificación de amenazas y vulnerabilidades, identificación de impactos, análisis y evaluación de riesgos, y tratamiento de riesgos.

e. Declaración de aplicabilidad SOA.

f. Estrategias para Formación y concienciación.

g. Planes de acción correctiva/preventiva.

h. Planes de monitoreo y revisión.

i. Revisión del SGSI por parte de la Dirección.

j. Planes de auditoría.

3.3 Plazos

El Sistema de Gestión de Seguridad de la Información tiene como fecha límite en sus desarrollo en el mes de Julio del 2014, fecha en la cual se habrá pasado por las fases del ciclo de Deaming o PDCA (Plan - Do - Check - Act) que nos permitirá, como la mejor práctica, hacer una mejora continua de las fases que son necesarias a fin de llevar a cabo una satisfactoria implementación del SGSI.

3.4. Organizacion del Proyecto

3.4.1 Promotor del Proyecto

El promotor y responsable del presente proyecto será el Oficial CAP PNP Medina, quien deberá coordinar cada una de las fases, solicitar, organizar o generar la documentación que sea necesaria a fin de dar cumplimiento a la implementación satisfactoria del SGSI.

3.4.2 Gerente del Proyecto

El Oficial CAP PNP Medina, informará de los avances en el desarrollo del presente proyecto al Gerente de la Unidad de Administración Integral de la Institucion Policial Comisario PNO Cesar Espadin.

3.4.3 Equipo del Proyecto

Para el desarrollo del presente proyecto será necesario contar con la colaboración de un miembro de la Unidad de Planificación y Desarrollo Organizacional, Administrador de Seguridad de la Información, y el visto bueno de los Gerentes de cada Área con la finalidad de involucrar a sus colaboradores de una manera planificada mientras se desarrolla el presente plan.

3.5 Principales Riesgos del Plan

En cualquier proyecto, el recurso más importante son las personas. Idealmente un proyecto debería tener disponibles a un número adecuado de personas, con las habilidades y experiencia correctas, y comprometidos y motivados con el proyecto. Sin embargo, las cosas pueden ser diferentes, por lo que hemos identificado estos riesgos.

- ¿El personal del proyecto está comprometido con la entera duración para lo que son necesarios?
- ¿Todos los miembros del equipo están disponibles a tiempo completo?
- ¿El movimiento de personal de un mismo proyecto es suficientemente bajo como para permitir la continuidad del proyecto?
- ¿Se han establecido los mecanismos apropiados para permitir la comunicación entre los miembros del equipo?
- ¿El entorno de trabajo del equipo es el apropiado?

3.6 Herramientas para Implementación del Proyecto y Generación de Informes.

Se ha evaluado varias herramientas, una de las mejores opciones de código abierto ha sido **"Securia"** SGSI es una herramienta integral que cubre el proceso automático de implantación, puesta en funcionamiento, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma internacional ISO 27001.
La herramienta seleccionada es actualizada periódicamente y cuenta con manuales de implementación y uso en español, adicional al uso de Securia, se usará hojas de cálculo lo cual permitirá llevar un control del avance de la implementación del SGSI.

4. GESTIÓN DE RIESGOS GUARDADOS EN BASE A ESTE DOCUMENTO.

Se realizará una revisión de los documentos de políticas y archivos generados del desarrollo e implementación del SGSI, se gestionará la implementación de un sistema de versionamiento que permita validar los cambios documentales y las versiones finales de adicionalmente se llevará el control de la documentación en las herramientas seleccionadas.

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS.

Todos los documentos serán debatidos por los involucrados, recoger los comentarios ayudará a enriquecer las políticas que se definan, solo entrara en vigencia cuando se los apruebe por los canales establecidos en la Institución Policial, y una vez que se tenga implementadas todas las correcciones solicitadas por los involucrados del SGSI.

DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

6. SITUACIÓN ACTUAL.

6.1 Objetivos.

- Verificar la implementación de una metodología que permita gestionar los riesgos de la Institución Policial, la identificación y valoración de activos y las amenazas sobre éstos.
- Verificar la administración de accesos lógicos a los servicios internos y externos.
- Verificar las configuraciones de los servicios y la documentación generada.
- Evaluación de la arquitectura de red implementada.
- Seleccionar los controles que nos van a permitir cubrir los distintos aspectos al implementar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Revisar las políticas, normas, procedimientos y documentos de control que nos permiten determinar el grado de cumplimiento en la implementación del SGSI.

6.2 Metodología.

La metodología seleccionada para la implementación se basa en la metodología EISA la cual nos permitirá aplicar un método riguroso y comprensivo para describir el comportamiento de los procesos de seguridad de la Institución Policial, sistemas de seguridad de información y subunidades de personal y organizativas, para que se alineen con las metas comunes de la organización y la dirección estratégica.

Preguntas que responde la EISA

Un proceso de Arquitectura de Seguridad de Información en la Empresa ayuda a Contestar preguntas básicas como:
¿Está la arquitectura actual apoyando y añadiendo valor a la seguridad de la Organización?
¿Cómo podría una arquitectura de seguridad ser modificada para que añada más Valor a la organización?

Para implementar una arquitectura de seguridad de información en la Institución Policial Comisaria del Norte, mediante la cual la arquitectura se alinee con la estrategia de la organización y otros detalles necesarios tales como dónde y cómo opera, es necesario competencias esenciales, procesos de negocio, y cómo la organización interactúa consigo misma.

Cuadro N°1 Requerimientos en la Institución Policial.

REQUERIMIENTO	DOCUMENTADO	ACTUALIZADO
Cuadros de organización, actividades, y flujo de procesos sobre cómo TI de la organización operan.	SI	NO
Ciclos, periodos y distribución en el tiempo de la organización.	NO	NO
Proveedores de tecnología hardware, software y servicios.	SI	NO
Inventarios y diagramas de aplicaciones y software	SI	NO
Interfaces entre aplicaciones; esto es: eventos, mensajes y flujo de datos.	NO	NO
Intranet, Extranet, Internet, comercio electrónico	NO	NO
Clasificación de datos, bases de datos y modelos de datos soportados.	NO	NO
Hardware, plataformas, servidores, componentes de red y dispositivos de seguridad y dónde se conservan.	NO	NO
Redes de área local y abiertas, diagramas de conectividad a internet	NO	NO

Fuente: Elaboración propia

Para el desarrollo del presente plan se utilizarán los siguientes procedimientos:

- Reuniones con los involucrados en el Plan de implementación del SGSI, que nos permitirá debatir y contar con la aceptación de los controles de la norma ISO 27002 a implementar en la Institución Policial Comisaria del Norte.

- Reunión para establecer el compromiso y delegados en el proceso de implementación del SGSI.

El objetivo de ésta etapa es sentar las bases del proceso de mejora continua en materia de seguridad, permitiendo a la Comisaria del Norte, conocer el estado del mismo y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales. Para ello se abordarán las siguientes fases:

- Documentación normativa sobre las mejores prácticas en seguridad de la información.
- Identificación y valoración de los activos y amenazas sobre los activos de la Institución Policial Comisaria del Norte.
- Auditoría de cumplimiento de la ISO/IEC 27002:2005.
- Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- Presentación de resultados.

Para adaptar el Sistema de Gestión de Seguridad de la Información será importante que el proyecto se ajuste a las 4 fases definidas por la serie de normas ISO 27000 como la mejor práctica para poder implementar el SGSI, en el siguiente esquema se presenta las etapas. En las cuales el SGSI será adaptado a la Institución Policial, las mismas etapas serán la guía para la presentación de avances.

6.3. Documentación Normativa sobre las Mejores Prácticas en Seguridad de la Información.

Para la ejecución de la presente etapa se selecciona a **"Magerit V2"** como metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, también es posible que para la consecución de los objetivos sea necesario implementar otras fuentes de buenas prácticas como ITIL.

6.4 Identificación y Valoración de los Activos y Amenazas sobre los Activos de la Institución Policial Comisaria del Norte.

6.4.1 Inventario de Activos.

Como primera actividad a ejecutar es necesario realizar la evaluación de los activos de información en los procesos seleccionados, considerando las dependencias entre éstos y realizando una valoración.

Cuadro N°2: Activos de la Institución.

Inventario de Activos	Detalle
INSTALACIONES	Ubicación de equipos informáticos y de comunicaciones
HARDWARE (HW)	Equipos que alojan datos, aplicaciones y servicios
APLICACIONES (SW)	Aplicativos que permiten manejar los datos
DATOS	El principal recurso, todos los demás activos se identifican alrededor de éste activo
RED	Equipamiento que permite intercambiar datos
SERVICIOS	Que se brindan gracias a los datos y que se necesitan para gestionar los datos
EQUIPAMIENTO AUXILIAR	Todo aquello que complemente al material informático
SOPORTES DE INFORMACION	Dispositivos que permiten el almacenamiento de datos (temporal)
PERSONAL	Quienes explotan u operan todos los demás elementos

Fuente: Elaboración propia

Cuadro N°3: Dimensiones de seguridad

DIMENSIONES DE SEGURIDAD		
VA	VALOR	CRITERIO
MA	10	Daño muy grave a la organización
A	7-9	Daño grave a la organización
M	4-6	Daño importante a la organización
B	1-3	Daño menor a la organización
MB	O	Daño irrelevante para la organización

Fuente: Magerit V2

Cuadro N°4: Ámbito y Activos.

AMBITO	ACTIVO	VALOR
DATOS	Información personal cliente	MA
	Transacción cliente	M
SERVICIO	Tramites policiales	M
	Denuncias policiales	MA
SW	SIDPOL	MA
HW	Servidor BBDD Principal – Oracle	MA
	IBM Blade Server	MA
	Servidor Formas - Oracle Forms 6	MA
	Terminal de Usuario	M
REDES Y COMUNICACIONES	Red Lan	MA
SOPORTE DE NFORMACION	Papeletas	M
INSTALACIONES	Oficinas	A
	Data Center (Sala servidores)	MA
PERSONAL	Oficial Operativos y Administrativos	M
	Jefe de Operaciones	B
	Personal técnico	B

Fuente: Elaboración propia

6.4.2 Análisis de Amenazas.

Para el entendimiento de la presente etapa es necesario indicar que se establecen según Magerit V2, ciertas amenazas típicas identificadas y que reducen la utilización del activo en diferentes ámbitos de los pilares de la seguridad de la información, éstos activos están frecuentemente expuestos a las amenazas, por lo cual la frecuencia de ocurrencia se expresará como como tasa anual o incidencias por año; finalmente la frecuencia con la que una amenaza se materialice sobre un activo hará que éste activo disminuya en un porcentaje de su valor.

6.4.3 Calculo del Riesgo

El cálculo del riesgo actual es una valoración en la que interviene el valor que le hemos dado a los activos en cada una de las dimensiones, la frecuencia con la que una amenaza puede degradar a aun activo, y el impacto de daño o disminución que la amenaza puede causarle al activo.

6.4.4 Selección de Controles – Salvaguardas.

Para ejecutar la actividad de selección de salvaguardas, debemos tomar en consideración los elementos de protección actual que tienen nuestros activos, y los posibles elementos de control de los que podemos dotar a nuestros, activos, es decir a los grupos de activos que hemos definido, validar los controles del Anexo a la Norma UNE-ISO/IEC 27001:2005 son aplicables en el contexto de nuestras capacidades, para esto se ha considerado 2 ámbitos esenciales con los que debemos trabajar las salvaguardas, los aspectos de y el tipo de protección de las salvaguardas que vamos a implementar, los cuales resumimos en los siguientes cuadros.

Cuadro N° 5: Controles de Salvaguardas

Aspecto de las salvaguardas	
PR	Procedimientos
PP	Política Personal
SW	Aplicaciones
HW	Dispositivos Físicos
SF	Seguridad Física

Tipo de protección	
PTG	Protección de Tipo General
PdS	Protección de Servicios
PDI	Protección de Datos/Información
PSW	Protección de Aplicaciones
PHW	Protección de Equipos
PdC	Protección de Comunicaciones
PSF	Seguridad Física
PRP	Relativas al Personal

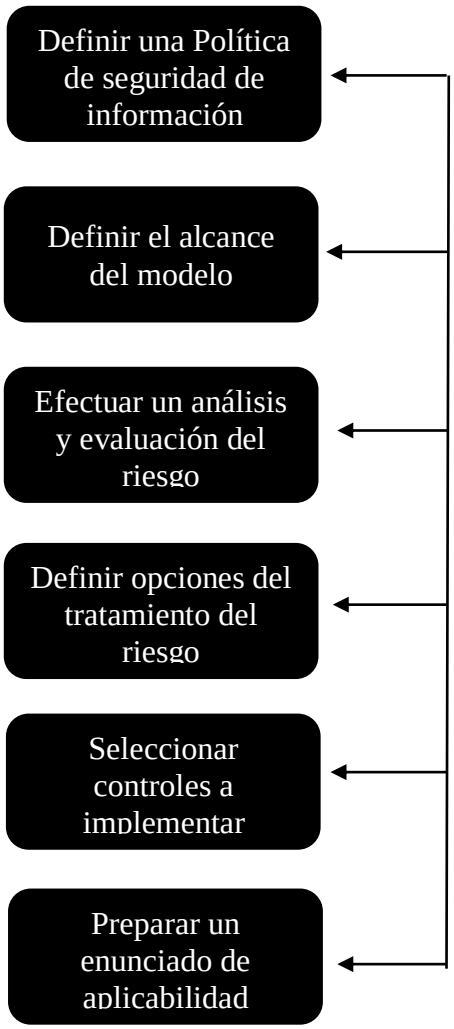
Fuente: Magerit V2

6.4.5 Auditoria de Cumplimiento de la ISO 27001.

Con el propósito de proteger la información de la Institución Policial, y como futura guía para implementar o mejorar las medidas de seguridad, ésta etapa nos va a permitir obtener una radiografía de la situación actual entorno a la Seguridad de la Comisaria.

PROCESO DE IMPLEMENTACION DE LA NORMA ISO 27001 – ENFOQUE DE LAS SEIS FASES ESENCIALES DEL PROCESO.

- Definir una Política de seguridad de Información
- Definir el Alcance del Modelo
- Efectuar un Análisis y Evaluación del Riesgo
- Definir Opciones del Tratamiento del Riesgo
- Seleccionar Controles a Implantar
- Preparar un enunciado de Aplicabilidad



Definir una Política de seguridad de información

Los riesgos a los que se ve expuesta la institución policial Comisaria del Norte – Chiclayo, llevan consigo la creación de directrices que orienten hacia un uso responsable de los recursos y evitar su uso indebido, lo cual puede ocasionar serios problemas a los activos de la mencionada institución. Las políticas de seguridad son documentos que constituirán la base del entorno de seguridad para la institución policial en donde se definen así mismo las responsabilidades, los requisitos de seguridad, las funciones, y las normas a seguir por los trabajadores - efectivos de la institución policial.

Definir el alcance del modelo

En esta parte o fase de implementación de la norma definimos muy bien el alcance del proyecto, en lo que respecta áreas implicadas, procesos, procedencia de los documentos a incorporar en el modelo, formato de los documentos, tipo de documento físicos o electrónico, tipo de información que se considera documento, o selección de herramienta tecnológica (metodologías a utilizar). En muchos casos son recomendables alcances reducidos pero viables antes que proyectos demasiado complejos y que nunca acaban de implantarse y que corren el riesgo de quedarse incompletos.

Efectuar un análisis y evaluación del riesgo

En esta fase de implementación de la norma efectuamos un análisis minucioso de los riesgos a los que está sujeta la institución, así como las amenazas y vulnerabilidades, los mismos que a su vez pueden ser analizados a través de los distintos métodos de análisis, así mismo para la evaluación de los riesgos se incluye características del puesto de trabajo y del personal que lo realiza, el proceso a seguir en la evaluación de riesgos,

Cuenta con los siguientes pasos, en primero lugar con la identificación del peligro, la estimación del riesgo, y la deducción de la tolerancia del riesgo.

Definir opciones del tratamiento del riesgo

En esta fase de implementación de la norma definimos las opciones y medidas para el tratamiento del riesgo para sí poder reducirlo, es así que existen seis medidas que han sido tomadas en cuenta para el tratamiento del o los riesgos, así mismo las 3 primeras orientadas al control del riesgo, y las otras 3 orientadas a la financiación del riesgo. Así mismo en las tres primeras se puede evitar, prevenir y proteger, mientras que en la segunda se puede aceptar, retener y transferir el riesgo. El diseño de las medidas de tratamiento puede reflejar la cultura organizacional de la institución. La historia de la institución, la forma en que está organizada y su operación, y el medio en el cual se desempeña.

En el desarrollo del presente trabajo de Tesis de Pre grado, se ha podido avanzar hasta la etapa que respecta el Definir opciones del tratamiento de los riesgos, la cual hace referencia a la 4ta etapa de implementación de la Norma ISO 27001.

COMISARIA DEL NORTE PNP -CHICLAYO

PROCEDIMIENTO PARA IDENTIFICACIÓN DE REQUISITOS

Código	CPIR
Versión:	001
Fecha de la versión:	2014-05-05
Creado por:	Alcántara Flores Julio Cesar
Aprobado por:	Cap. PNP Medina
Nivel de confidencialidad:	Nivel Intimo / Nivel Intermedio / Nivel Superficial.

TABLA DE CONTENIDOS

1. Objetivo, Alcance y Usuarios……68
2. Documentos de Referencia……68
3. Identificación de Requisitos y Partes Interesadas……..68
4. Responsabilidades……..70

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir el proceso de identificación de las partes interesadas, de los requisitos legales, normativos, contractuales y de otra índole relacionados con la seguridad de la información y con la continuidad del negocio, como también las responsabilidades para su cumplimiento. Este documento se aplica a todo el Sistema de gestión de seguridad de la información (SGSI).Los usuarios de este documento son todos los empleados de la Institución Policial Comisaria del Norte – Chiclayo.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, punto 4.2; control A.18.1.1
- Norma ISO 22301, punto 4.2
- Política del sistema de gestión de seguridad de la información
- Política de la Continuidad del Negocio

3. IDENTIFICACIÓN DE REQUISITOS Y PARTES INTERESADAS

El Comisario y jefe de la Institución Policial Cesar Espadín, será el responsable, en brindar toda la información requerida para la determinación y levantamiento de Requisitos.

Cuadro N°6: Requerimientos de la Institución

REQUERIMIENTO	DOCUMENTADO	ACTUALIZADO
Cuadros de organización, actividades, y flujo de procesos sobre cómo TI de la organización opera.	SI	SI
Ciclos, periodos y distribución en el tiempo de la organización.	NO	NO
Proveedores de tecnología hardware, software y servicios.	SI	NO
Inventarios y diagramas de aplicaciones y software	NO	NO
Interfaces entre aplicaciones; esto es: eventos, mensajes y flujo de datos.	NO	NO
Intranet, Extranet, Internet, comercio electrónico	NO	NO
Clasificación de datos, bases de datos y modelos de datos soportados.	NO	NO
Hardware, plataformas, servidores, componentes de red y dispositivos de seguridad y dónde se conservan.	SI	NO
Redes de área local y abiertas, diagramas de conectividad a internet	NO	NO

Fuente: Comisaria del Norte

4. RESPONSABLES.

Cuadro N°7. Responsables de información

	Jefatura	CTSG
Recopilación de legislación de seguridad		R
Identificación de requisitos legales de seguridad		R
Evaluación del riesgo de cumplimiento		R
Adopción de medidas para asegurar el cumplimiento	C	R
Actualización de lista de requisitos legales		R
Comunicación	R	C
Cumplimentación y archivos de registros		R

Fuente: Comisaria del Norte
R: Responsabilidad – C: Colaboración

COMISARIA DEL NORTE PNP -CHICLAYO

DOCUMENTO SOBRE EL ALCANCE DEL SGSI

Código	CASGSI
versión:	001
fecha de la versión:	2014-05-05
creado por:	Alcántara Flores Julio Cesar
aprobado por:	Cap. PNP- Medina
nivel de confidencialidad:	Nivel Intimo /Nivel Intermedio / Nivel Superficial.

TABLA DE CONTENIDO

1. Objetivo, Alcance y Usuarios……72
2. Documentos de Referencias……..73
3. Definición del Alcance del SGSI……...73
   3.1. Proceso y Servicios……73
   3.2. Unidades Organizativas……..75
   3.3. Redes e Infraestructura de T.I……77

1. OBJETIVO, ALCANCE Y USUARIOS.

El objetivo de este documento es definir claramente los límites del Sistema de gestión de seguridad de la información (SGSI) en la Institución Policial Comisaria del Norte – Chiclayo. Este documento se aplica a toda la documentación y actividades dentro del SGSI. Los usuarios de este documento son los miembros de la dirección de la Comisaria del Norte - Chiclayo, los miembros del equipo del proyecto que implementa el SGSI y los colaboradores que formaran parte de la organización en mención.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, punto 4,3
- [Documento del Plan del proyecto para la implementación de la norma ISO 27001]
- [Lista de requisitos legales, normativos, contractuales y de otra índole]

3. DEFINICIÓN DEL ALCANCE DEL SGSI

La organización necesita definir los límites del SGSI para decidir qué información quiere proteger. Esa información deberá ser protegida independientemente de si además es almacenada, procesada o transferida dentro o fuera del alcance del SGSI. El hecho de que determinada información esté disponible fuera del alcance no significa que no se le aplicarán las medidas de seguridad; esto solamente implica que la responsabilidad por la aplicación de las medidas de seguridad serán transferidas a un tercero que administre esa información. Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del SGSI se define de acuerdo a los siguientes aspectos:

3.1. Procesos y servicios

Dentro de los procesos que se dan en la Institución Policial Comisaria del Norte – Chiclayo tenemos los siguientes como son:

- Recibir denuncias ya sean estas de índole por robo, casos de violencia intrafamiliar, y/o abuso infantil.
- Brindar la asesoría jurídica, psicológica y social en todos los temas de familia.
- Realización de audiencias de conciliación en casos de:

  -Alimentos
  -Fijar cauciones de comportamiento conyugal
  -Suspensión de la vida en común

-Exoneración de la cuota alimentaria
-Custodia de los niños, niñas y cuidado personal
-La existencia de la unión marital de hecho

- Recibir denuncias de violencia intrafamiliar y maltrato infantil
- Brindar atención a los niños, niñas y adolescentes que se encuentren en situación irregular.
- Funciones en la prevención y promoción:
- Realizar talleres, brigadas, seminarios y visitas a establecimientos públicos con el fin de prevenir, detectar y atender la problemática de la violencia intrafamiliar.
- Funciones operativas, policivas y de protección.

EQUIPO INTERDISCIPLINARIO.

- Comisario de Familia
- Psicóloga
- Trabajadora Social
- Jurídica
- Citador

Dentro del proceso de alimentos, custodia y visitas se solicita a los convocantes los siguientes documentos:

• Copia del Registro civil de Nacimiento
• Copia de la tarjeta de Identidad si son mayores de 7 años
• Copia del carnet de Vacunación
• Certificado de control y crecimiento para menores de ocho años con vigencia no mayor de tres meses junto con última cita odontológica.
• Certificación Médica y odontológica para mayores de 9 años.

SERVICIOS PSICOLOGICOS

Realiza valoraciones psicológicas, ofrece intervención en situación de crisis a través de terapias individuales, familiares y de pareja; así como también hace seguimiento a los casos atendidos por las demás instituciones del Centro de Convivencia Ciudadana, apoyando, entre otras, la labor de los comisarios de familia y la fiscalía. El apoyo psicológico también involucra un importante rango de actividades con la comunidad. Desarrolla programas de capacitación para los funcionarios del Centro de Convivencia Ciudadana y los usuarios.

3.2. Unidades Organizativas

La División General Técnica de la Institución Policial Comisaria del Norte-Chiclayo sé estructura en las siguientes Brigadas:

a) Brigada de Desarrollo Tecnológico.
b) Brigada de Administración de Medios.

Asimismo, se adscriben directamente a la División General Técnica los siguientes Grupos, conformados por los siguientes:

a) Grupo de Jefatura.
b) Grupo de Gestión Administrativa.
c) Grupo de Recursos Humanos.
d) Grupo de Formación.

Los mencionados Grupos tendrán carácter central.

Brigada de Administración Policial.

1. Corresponde a la Brigada de Administración Policial la realización de las tareas siguientes:

- Recepción, registro y distribución de toda la documentación de la institución policial.
- Gestión de la comunicación interna y externa de la institución Policial en coordinación con las unidades competentes en la materia de la Administración.
- Secretaría del Jefe de la Policía Foral.
- Atención de las relaciones institucionales con otros Cuerpos de Policía y organizaciones y protocolo.
- Recopilación y divulgación de normativa y procedimientos aplicables a la operatividad policial.
- La elaboración de informes jurídicos y asesoramiento.
- Centralización y apoyo a las Áreas y Comisarías de todas las tareas generales de carácter administrativo correspondientes a la institución.
- Gestión y control de toda la documentación de la institución Policial inspeccionando su correcta tramitación en plazo y forma, así como su registro, archivo y custodia.

- Identificación y atención de las necesidades de la institución Policial en recursos humanos en coordinación con la unidad competente de la Dirección General de Interior.
- Gestión y tramitación de todo lo relacionado con licencias, permisos, vacaciones, situaciones administrativas, control de horarios, provisión de puestos de trabajo así como velar por el cumplimiento de las disposiciones vigentes en esta materia.
- Gestión y control de los expedientes personales de los componentes de la institución.
- Desarrollo de una cultura preventiva de riesgos laborales, impulsando aquellas acciones oportunas de acuerdo a la legislación específica, la elaboración de los planes de prevención de riesgos laborales y coordinación con las unidades competentes de la Administración.
- Gestión económica y presupuestaria de la institución Policial en coordinación con los órganos competentes de la Secretaría General Técnica.
- Tramitación y control de desplazamientos y viajes practicados por la institución policial.
- Gestión de los ingresos recabados en concepto de elaboración de informes policiales, tasas, acompañamientos y servicios especiales.
- Identificación y definición de las necesidades de formación de la Policía.
- Revista de armas en colaboración con la División de Régimen Interno.

Grupos.

1. Para la mejor especialización en la ejecución de sus tareas, la Brigada de Administración de la institución Policial, se estructura en los siguientes grupos:

a) Grupo de Jefatura.
b) Grupo de Gestión Administrativa.
c) Grupo de Recursos Humanos.
d) Grupo de Formación.

2. Los grupos del apartado anterior tendrán carácter central.

3.3. Redes e Infraestructura de TI

Cuadro N°8: Infraestructura de TI de la Institución

GRUPO	TIPO	DESCRIPCION	UNDS
Hardware	Equipos de oficina	PCs de escritorio	25
		Portátiles	5
		Tablets	1
	Impresoras	Impresora láser B/N	4
		Impresora multifuncional Oficina	4
	Dispositivos de Red	Switches C3 distribucion oficinas	10
		Switches C3 distribución CPD	5
		Routers CPD	5

Fuente: Comisaria del Norte

GRUPO	TIPO	DESCRIPCION	UNDS
Infraestructura	CPD	Generador eléctrico	1
		Cámara de vigilancia	3
		Armarios comunicaciones	6
		Armarios	12

Fuente: Comisaria del Norte

GRUPO	TIPO	DESCRPCION
Información	TI	Contratos TIC

Fuente: Comisaria del Norte

COMISARIA DEL NORTE PNP -CHICLAYO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código	CPSI
Versión:	001
Fecha de la versión:	2014-05-05
Creado por:	Alcántara Flores Julio Cesar
Aprobado por:	Cap. PNP- Medina
Nivel de confidencialidad:	Nivel Intimo / Nivel Intermedio / Nivel Superficial.

TABLA DE CONTENIDO

1. Objetivo, Alcance y Usuarios……....80
2. Documentos de referencia…….80
3. Terminología básica sobre Seguridad de la Información……..80
4. Objetivos de la Gestión de la Seguridad de la Información……..81
   4.1. Objetivo General……81
   4.2. Objetivos Específicos……81
5. Alcance de la Política de Seguridad de la Información……81
   5.1. Alcance General…….82
   5.2. Definición de los Activos de Información…….83
   5.3. Definición de la Seguridad de la Información……83
6. Políticas y Objetivos de Seguridad de la Información……..84
   6.1. Política de Control de acceso…….84
   6.2. Política de No repudio……86
   6.3. Política de Privacidad y confidencialidad……..87
   6.4. Política de Integridad…….87
   6.5. Política de Disponibilidad del servicio……..88
   6.6. Política de Disponibilidad de información……89
   6.7. Política de Protección del servicio…….89
   6.8. Política de Registro y auditoria……..90
7. Marco General de las Políticas de Seguridad Institucional……...91
   7.1. Aspectos generales……91
   7.2. Aprobación de la política……91
   7.3. Difusión de la política……....91
   7.4. Revisión de la política……92
   7.5. Evaluación del cumplimiento de la política……...92
   7.6. Análisis diferencial de la institución policial…….93

1. OBJETIVO, ALCANCE Y USUARIOS

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información. Esta Política se aplica a todo el Sistema de gestión de seguridad de la información (ISMS), según se define en el Documento del Alcance del SGSI. Los usuarios de este documento son todos los empleados de La Institución Policial Comisaria del Norte - Chiclayo, como también terceros externos a la organización.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales

3. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN

Confidencialidad: característica de la información que está disponible solo para personas o sistemas autorizados.

Integridad: característica de la información que es modificada solo por personas o sistemas autorizados y de una forma permitida.

Disponibilidad: característica de la información a la cual pueden acceder solo las personas autorizadas cuando sea necesario.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de gestión de seguridad de la información: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. OBJETIVOS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACION

4.1. Objetivo General.

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad operacional de los procesos y servicios que desarrolla y maneja la Institución Policial Comisaria del Norte - Chiclayo, mediante el resguardo de los activos de información asociados a los procesos críticos del negocio y su soporte.

4.2. Objetivos Específicos.

- Identificar, clasificar y asignar los dueños de los activos de información de la Institución, en orden lograr niveles adecuados de integridad, confidencialidad y disponibilidad de éstos.
- Controlar, prevenir y/o mitigar los riesgos de seguridad de la información, identificando las vulnerabilidades y amenazas que enfrentan los activos, en orden a asegurar la continuidad del negocio.
- Establecer políticas, normativas y procedimientos que permitan resguardar y proteger los activos de información de la Institución Policial.
- Definir un Plan de Difusión, Sensibilización y Capacitación que permita difundir los alcances y buenas prácticas asociadas a la seguridad de la información institucional.

5. ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

5.1. Alcance General

- La Política General de Seguridad de la Información de la Institución Policial – Comisaria del Norte, se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información.
- La presente política debe ser conocida y cumplida por todo el personal de la Institución Policial llámense efectivos Policiales Administrativos y efectivos involucrados en el uso de los sistemas y tecnologías de Información.
- Esta Política se aplica en todo el ámbito de la Institución Policial, a sus recursos y a la totalidad de los procesos, internos y externos, vinculados a la entidad a través de contratos o acuerdos con terceros.

- De acuerdo a lo anterior, la información que genera y gestiona la institución Policial constituye un activo estratégico clave para asegurar la continuidad del negocio, por lo que la Seguridad de la Información es una herramienta para garantizar su integridad, disponibilidad y confidencialidad.

5.2. Definición de los Activos de Información.

Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución, en la que se distinguen tres niveles:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- Los Equipos/Sistemas/infraestructura que soportan esta información
- Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

Cuadro N°9: Activos de Información

ACTIVOS DE INFORMACION	ACTIVOS FISICOS	ACTIVOS DE SERVICIOS DE T.I	ACTIVOS HUMANOS
Base de Datos	Infraestructura de TI	Servicios de autentificación	Personal policial
Datos Digitales	Oficinas, muebles	Servicios de red	Agentes externos
Copias de Seguridad	Estaciones de trabajo PC, Portátiles		Otros empleados

Fuente: Elaboración propia

Capital Humano

Cuadro N°10: Estructuración y valor de los activos

GRUPO	DESCRIPCION	UNDS	VALOR	VALOR S/	CRITICIDAD
Empleados	Mandos	22	Muy alta	44.000 S/	Critico
	Especialista	2	Muy alta	5.000 S/	Critico
	Operadores	4	Muy alta	8.000 S/	Critico
	Administración	2	Muy alta	6.000 S/	Critico

Fuente: elaboración propia

Cuadro N°11: Descripción y valor critico de los activos

TIPO	DESCRIPCION	UNDS	VALOR	VALOR S/	CRITICIDAD
Equipos de oficina	Equipos	25	Media	50.000 S/	Medio
	Portátiles	5	Baja	7.500 S/	Bajo
	impresoras	6	Baja	2.500 S/	Bajo
	tablets	1	Muy baja	0.00S/	Bajo

Fuente: elaboración propia

5.3. Definición de la Seguridad de la Información.

La institución Policial Comisaria del Norte - Chiclayo, entiende que la Seguridad de la Información es la protección de los activos de información contra una amplia gama de amenazas para asegurar la continuidad de las operaciones, minimizar el daño de la Institución y maximizar la eficiencia y las oportunidades de mejora de la gestión de la misma.

6. POLÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN.

Las políticas de seguridad que se plantean en este documento, están basadas en un análisis estratégico acorde con cada una de las fases de la Estrategia de la Organización. Estas políticas representan directrices generales de alto nivel que deben ser adoptadas por todos los participantes e integrantes en la cadena de prestación de servicios durante las fases de la evolución de la Estrategia de la Institución Policial. Para asegurar el cumplimiento de las políticas de seguridad para la Institución, se establecieron objetivos de control asociados a cada política:

6.1. Políticas de Control de Acceso.

Se requiere mayor nivel de seguridad como resultado de un análisis y evaluación del riesgo, deben implementar mecanismos y controles que aseguren un efectivo registro, identificación y autenticación de los clientes y usuarios de dichos servicios. Así mismo, deben implementar mecanismos y controles que aseguren el acceso bajo el principio del menor privilegio, necesario para realizar únicamente las labores que a cada cliente o usuario de dichos servicios corresponden. Igualmente, se deben implementar controles para realizar una efectiva administración de usuarios y derechos de acceso

Objetivos Control.

PS1.1

Otorgar acceso a servicios que requieren mayor nivel de seguridad, sólo para usuarios autorizados. Se requiere limitar el acceso solo para usuarios identificados y autenticados apropiadamente.

PS1.2

Otorgar los mínimos privilegios de acceso a servicios que requieren mayor nivel de seguridad. Se requiere minimizar el daño potencial causado por usuarios autorizados lo cual implica establecer segregación de funciones para separar usuarios de los servicios y usuarios con roles administrativos.

PS1.3

Otorgar acceso a servicios que requieren mayor nivel de seguridad condicionado a la presentación de un token de acceso expedido por un tercero en representación de la

Entidad proveedora del servicio. Se debe fortalecer el control de acceso para las transacciones que requieran mayor nivel de seguridad.

PS1.4

Otorgar acceso a servicios que requieren mayor nivel de seguridad condicionado a la presentación de información que soporte la identidad del individuo que requiere el acceso y sus credenciales de autenticación. Se debe implementar la autenticación personal más allá de la posesión del token.

PS1.5

Otorgar privilegios de acceso a servicios de la Institución, sólo cuando se satisfaga la verdadera identidad del usuario, es decir que el usuario sea quien realmente dice que es y no esté registrado bajo otra identidad con un acceso legítimo. Se debe prevenir la creación de múltiples identidades. Un usuario puede tener múltiples roles con respecto a los servicios de la Institución, pero solo puede poseer una única identidad.

PS1.6

Otorgar acceso a los usuarios sobre los servicios y o activos necesarios para soportar el servicio específico requerido. Se deben fortalecer los controles de acceso a nivel de objeto o aplicación, de manera que un usuario legítimo, una vez otorgado el acceso, no pueda alterar datos no requeridos por el servicio solicitado.

PS1.7

Implementar una administración efectiva de los derechos de acceso de usuarios y asignar dicha responsabilidad al personal apropiado (administradores de accesos).

PS1.8

Implementar la vigencia de los derechos de acceso y su revocación, una vez finalice el período asignado, o haya pérdida de las credenciales, o se detecte uso indebido de los recursos por parte de los usuarios. Las credenciales de acceso y los tokens deben quedar inválidos ante eventos de revocación.

6.2. Políticas de No Repudio.

Se debe garantizar la no repudiación de las transacciones poniendo en práctica mecanismos de seguridad que permitan crear un ambiente de confianza entre los clientes (ciudadanos, funcionarios públicos, empresas), los proveedores de servicios, los

Organismos de certificación y la entidad estatal, con relación a la autenticidad, trazabilidad y no repudiación de las transacciones electrónicas.

Objetivos Control.

PS2.1

Proveer evidencia del origen y la integridad del mensaje, es decir, se deben implementar mecanismos en el servicio para crear una prueba de origen de manera que se pueda evitar que una de las partes (usuario o servicio) niegue su responsabilidad en el envío del mensaje. Así mismo, se deben implementar mecanismos para probar si el mensaje ha sido alterado.

PS2.2

Proveer evidencia del acuse del mensaje, es decir, se deben implementar mecanismos en el servicio para crear una prueba de recibo y almacenarla para su recuperación posterior en caso de una disputa entre las partes (usuario y servicio).

PS2.3

Proveer evidencia que el servicio es proporcionado realmente por una entidad pública. Se deben implementar credenciales del servicio y ser presentadas al cliente para la autenticación del sistema de acceso al cliente.

PS2.4

Proveer evidencia de la fecha y hora de la transacción electrónica efectuada a través del servicio.

6.3. Política de Privacidad y Confidencialidad.

Los datos personales de los clientes, ciudadanos y demás información enviada a través de los servicios de la Institución Policial, deben ser protegidos y manejados de manera responsable y segura.

Objetivos de Control:

PS3.1

Proveer protección adecuada de la información personal y privada contra divulgación no autorizada cuando se transmite a través de redes vulnerables.

PS3.2

Proteger la información personal y privada de uso indebido y divulgación no autorizada cuando se procesa y almacena dentro del dominio de implementación de los servicios de la Institución Policial.

6.4. Política de Integridad.

La información que se recibe o se envía a través de los servicios de la Institución Policial, debe conservar los atributos de correcta y completa durante la transmisión, el procesamiento y el almacenamiento. Deben garantizar la integridad de la información.

Objetivos de Control:

PS4.1

Proteger la información que se transmite a través de redes públicas contra modificación, borrado o repetición accidental o intencional. Se debe asegurar la fuerte integridad de las comunicaciones para prevenir contra manipulación de datos en tránsito o contra pérdida y corrupción causada por fallas de equipos y comunicaciones.

PS4.2

Proteger la información que se almacena en el dominio del cliente contra modificación accidental o intencional. Se deben implementar mecanismos para prevenir que usuarios y atacantes manipulen la información del servicio almacenada en su estación de trabajo con el fin de obtener algún beneficio.

PS5.3

Proteger la información almacenada dentro de los servicios de la Institución Policial contra modificación o destrucción intencional por parte de atacantes externos. Se deben implementar fuertes medidas para frustrar la alteración mal intencionada de los datos de usuarios o de información de dominio público que puedan disminuir la confianza de los

Servicios. Los proveedores de servicios tienen la obligación del debido cuidado, para asegurar que la información proporcionada sea veraz.

PS5.4

Proteger la información trasmitida o almacenada dentro de la Institución Policial contra pérdida o corrupción accidental. Se deben implementar procedimientos probados de respaldo y recuperación de datos y asegurar que se mantienen las listas de usuarios y clientes autorizados.

6.5. Política de Disponibilidad del Servicio.

Es de suma importancia el poder asegurar la disponibilidad continua de los servicios bajo un control estricto y adecuado.

Objetivos de Control:

PS5.1

Proteger los servicios de la Institución Policial contra daños o negación del servicio (DoS –Denial of service) por parte de atacantes externos.

PS5.2

Proteger los servicios de la Institución Policial contra daños o provisión intermitente del servicio por fallas internas de los equipos y/o redes. Se deben implementar mecanismos de redundancia y alta disponibilidad acordes con la criticidad de la provisión continua del servicio y la capacidad para realizar reparaciones rápidas.

PS5.3

Proteger los servicios de la Institución Policial contra pérdida de datos, pérdida de equipos y otros eventos adversos. Se debe implementar un plan de continuidad del

Negocio (BCP –Business Continuity Plan), para asegurar que se toman las medidas necesarias y evitar en lo posible, la pérdida de información por ocurrencia de incidentes.

6.6. Política de Disponibilidad de Información.

Las entidades que provean servicios de Gobierno, deben asegurar que los datos de los usuarios y clientes se mantienen protegidos contra pérdida, alteración o divulgación por actos accidentales o malintencionados, o por fallas de los equipos y/o redes.

Objetivos de Control:

PS6.1

Recuperar los datos personales o críticos que han sido dañados, destruidos, alterados o modificados por acciones malintencionadas o accidentales. Se deben implementar procedimientos de copias de respaldo y recuperación, para asegurar que exista recuperación de los datos sensitivos y que puedan ser restaurados en el evento de una falla. También se deben Implementar mecanismos para que los datos personales no sean divulgados sin autorización expresa del dueño de la información.

PS6.2

Recuperar la información protegida en el evento que un cliente u otro usuario no pueda suministrar las credenciales de acceso necesarias. Se deben implementar procedimientos para recuperar datos de usuario en el evento que un token de acceso o la contraseña se pierdan. Esto permite soportar investigaciones de posible uso indebido del sistema

6.7. Política de Protección del Servicio.

Se debe asegurar que los servicios y sus activos de información relacionados, estén adecuadamente protegidos contra ataques externos o internos.

Objetivo de Control:

PS7.1

Proteger los sistemas de información, equipos y redes que soportan los servicios de la Institución Policial contra ataques a la provisión continua y segura del servicio. Se deben asegurar los equipos y las redes implementando medidas tales como:

Aseguramiento de servidores, implementación de topologías seguras de red y escaneo de vulnerabilidades. Los sistemas de información y las aplicaciones, deben ser diseñados e implementados de manera que se minimicen las vulnerabilidades y los ataques externos e internos se reduzcan a un nivel aceptable.

6.8. Política de Registro y Auditoria.

Es importante el poder mantener y proteger los registros de las transacciones electrónicas como evidencia para los requerimientos de las auditorias (internas o externas) y como mecanismo para establecer responsabilidades de los clientes y usuarios.

Objetivo de Control:

PS8.1

Mantener un registro de transacciones que pueda ser requerido después del análisis de eventos y/o incidentes. Se deben mantener registros y pistas de auditoria con el fin de establecer Responsabilidad por las transacciones, reconstruir transacciones fallidas y suministrar registros apropiados en caso de conflictos o disputas por el servicio. Debe existir trazabilidad de los registros de transacciones según sea apropiado.

ENFOQUE DE LAS 6 FASES ESENCIALES DEL PROCESO DE IMPLANTACION ISO 27001

- Definir una Política de seguridad de Información
- Definir el Alcance del Modelo
- Efectuar un Análisis y Evaluación del Riesgo
- Definir Opciones del Tratamiento del Riesgo
- Seleccionar Controles a Implantar
- Preparar un enunciado de Aplicabilidad

7. Marco General de las Políticas de Seguridad Institucional

7.1. Aspectos Generales

- La Política General de Seguridad de la Información ha sido elaborada en concordancia con la legislación vigente en el país, considerando además su compatibilidad con las prácticas sugeridas por la Norma ISO 27001.

- La Dirección de la Policía Nacional del Perú se compromete a realizar las acciones que estén a su alcance para permitir la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger

- los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

7.2. Aprobación de la Política

- Las políticas de seguridad de la información serán aprobadas por el Comisario Cesar Espadín Jefe de la Institución Policial –Comisaria del Norte, reflejando claramente su compromiso, apoyo e interés en el desarrollo de una cultura de seguridad de la información en la institución.

7.3. Difusión de la Política

- Será responsabilidad del Comisario PNP Cesar Espadín encargado y jefe de esta institución el difundir los temas relevantes en materia de seguridad. Las políticas de seguridad de la información serán comunicadas a todo el personal y efectivos policiales de la Institución, y a terceros que presten servicios en la institución y a las entidades externas relevantes.

- Para la difusión de los contenidos de las políticas de seguridad de la información al interior de la institución se deberán utilizar los medios de difusión que disponga la Institución Policial Comisaria del Norte (intranet, boletín, etc.), así como también instancias de capacitación llevadas a cabo para este efecto.

Los principales medios utilizados serán:

- Intranet institucional
- Circulares informativas de la Institución
- Inducción a personal (planta, contrata y honorarios) que ingresen al servicio. Comunicaciones a través de charlas y reuniones
- Para lo anterior se deberá definir, implementar y evaluar las acciones e iniciativas contenidas en un Plan de Difusión, Sensibilización y Capacitación en materia de seguridad de la información.

7.4. Revisión de la Política

- La Política General de Seguridad de la Información será revisada de manera Anual o en las siguientes circunstancias: a requerimiento del/de la Director Jefe - Comisario, frente a cambios en el ambiente de la institución, debido a las circunstancias del servicio, a las condiciones legales y al ambiente técnico.

- La modificación del presente documento está a cargo del Comité de Seguridad de la Información y será aprobado por el Comisario encargado de la Institución Policial Comisaria del Norte.

7.5. Evaluación del Cumplimiento de la Política

- Todos los Jefes de Departamento y Unidades son responsables de la implementación de estas políticas de seguridad de la información, dentro de sus áreas de responsabilidad,

- así como el cumplimiento de las políticas, normativas y procedimientos por parte de su equipo de trabajo.

- La institución realizará auditorías internas anuales al sistema de seguridad de la información para verificar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

- El incumplimiento de la Política General de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características del aspecto no cumplido.

7.6. Análisis Diferencial de la Institución.

POLITICA DE SEGURIDAD POLITICA DE SEGURIDAD DE LA INFORMACION				
Documento de política de seguridad de la información	SEGURIDAD	Existen algunas normas que hacen referencia en cuanto al uso de los recursos informáticos de la institución. Pero una Política General de Seguridad, ya que la jefatura o dirección de la institución aun no la aprueba.	No existe	No se cumple
Revisión de la política de seguridad de la información	SEGURIDAD	No existen Políticas de Seguridad, tampoco ha sido aprobada por la jefatura de la institución, por lo que no se revisa, por ausencia de la misma.	No existe	No se cumple

ORGANIZACIÓN DE LA SEGURIDAD EN LA INSTITUCION POLICIAL PARTE DE LA ORGANIZACIÓN INTERNA				
Compromiso con la jefatura en temas de seguridad con la información	SEGURIDAD	Ausencia de un comité el cual gestione la seguridad de la información en la institución, en algunos casos la jefatura muestra su apoyo en temas de seguridad dentro de la comisaria, asigna algunas funciones, lo realiza a través de algunas áreas, tampoco se ha realizad un asignación adecuada y definida de responsabilidades.	No existe	No se cumple
Coordinación en temas de seguridad dentro de la institución	SEGURIDAD	En cuanto a las actividades orientadas a la seguridad, estas son coordinadas entre los diferentes roles y funciones, pero tampoco existen procedimientos documentados.	repetible	No se cumple
Responsables en temas de seguridad de información en la institución	SEGURIDAD	En algunos casos los activos de información no están muy claros definidos, y aunque en algunos casos existe alguna asignación de responsabilidades, esta no es o se da de manera formal.	Inicializado	No se cumple
Autorización de recursos asociados a la seguridad de la información	SEGURIDAD	Se da un proceso de autorización, para los nuevos recursos orientados a procesos de información, pero este proceso no es del todo formal por lo que no	Proceso definido	No se cumple

		existe una documentación correspondiente.		
Niveles y acuerdos en temas de confidencialidad	SEGURIDAD	En algunos casos dentro de la institución se han realizado algunos acuerdos en temas de confidencialidad, pero muchas veces estos no se monitorean de manera periódica, mucho menos cuando se incorporan nuevos activos de información en la institución policial.	Repetible	No se cumple
Relación con Autoridades competentes	SEGURIDAD	Existen algunos procedimientos referenciados a prevenir algunos riesgos y accidentes en las labores del personal de la institución. Pero en el caso de la seguridad de la información no se establece un procedimiento formal adecuado.	Repetible	Cumple
Revisión independiente referente a la seguridad de la información	SEGURIDAD	No específicamente en todas las áreas de la institución se realizan revisiones orientadas a temas de seguridad, ya que no cuentan con una política clara específica que termine definiendo la frecuencia y la metodología de la revisión adecuada en la institución policial.	Repetible	No se cumple

GESTION DE ACTIVOS RESPONSBLES DE LOS ACTIVOS EN LA INSTITUCION				
Inventario de activos	SISTEMAS / REDES	Se realiza un inventario de equipos, infraestructura y otros dispositivos que son propiedad de la institución policial, pero no se da un inventario en sus activos de información correspondiente y adecuada.	Proceso definido	Cumple
Propietario de los activos	SISTEMAS/ REDES	Para el inventario existente, es asignado un propietario al activo, pero no es especificado de manera razonablemente ya que se hacer de forma genérica y no especifica.	Proceso definido	No se cumple
Uso aceptable de los recursos informáticos en la institución	RR .HH	En la institución existe una publicación orientada a términos de conducta y guía generalizada sobre el buen uso adecuado de los recursos de información con los que cuenta la organización.	Gestionada y evaluado	Cumple

CLASIFICACION DE LA INFORMACION INFORMACION DE LA INSTITUCION				
Directrices de clasificación	RR .HH	Se cuenta con una clasificación de información del personal efectivo de la institución, clasificando los activos de información que no contengas datos personales y tampoco se identifican según su criticidad para la institución.	Proceso definido	Cumple
		La información clasificada en muchos casos suele estar etiquetada y tiene un		

Etiquetado y tratamiento en temas de seguridad	SEGURIDAD FISISCA	tratamiento adecuado a las características, aunque con lagunas limitaciones ya que a veces no está correctamente clasificada.	Proceso definido	No se cumple

CUMPLIMIENTO DE LAS POLITICAS Y NORMAS DE SEGURIDAD POLITICAS DE SEGURIDAD				
Cumplimiento de las políticas y normas de seguridad	AUDITORIA	Ausencia de informes formales, sobre las revisiones del cumplimiento por parte de las autoridades de la institución, aunque en algunos casos de manera informal se suele realizar este seguimiento.	Gestionado y evaluable	Cumple
Comprobación del cumplimiento técnico	AUDITORIA	En los últimos años, se han realizados algunas auditorias técnicas y procedimentales, la institución posee los informes, se analizan los resultados e informes y se implementan los resultados para beneficios de la institución.	Optimizado	Cumple

Cuadro N°12: Resumen del Análisis Diferencial

DOMINIO	CUMPLE	NO CUMPLE
Política de seguridad	10%	90%
Organización de la seguridad y la información	30%	70%
Gestión de activos	50%	50%
Seguridad ligada a los RR.HH	65%	35%
Seguridad física y ambiental	40%	60%
Gestión de las comunicaciones y operaciones	30%	70%
Control de acceso	40%	60%
Adquisición, desarrollo, mantenimiento de sistemas de información	35%	65%
Gestión de incidencias de la seguridad de la información	10%	90%
Cumplimiento	36%	64%

Fuente: Elaboración propia

GLOSARIO DE TERMINOS.

- **Evaluación de Riesgos**

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

- **Administración de Riesgos**

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

- **Comité de Seguridad de la Información**

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

- **Responsable de Seguridad Informática**

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

- **Incidente de Seguridad**

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

COMISARIA DEL NORTE PNP –CHICLAYO

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

Código	CMETR
Versión:	001
Fecha de la Versión:	2014-05-05
Creado por:	Alcántara Flores Julio Cesar
Aprobado por:	Cap. PNP- Medina
Nivel de Confidencialidad:	Nivel Intimo / Nivel Intermedio / Nivel Superficial.

TABLA DE CONTENIDOS

1. Objetivo, Alcance y Usuarios……..101
2. Documentos de referencia……...101
3. Metodología de Evaluación y Tratamiento de Riesgos……...101

3.1 Evaluación de Riesgo…….101

3.1.1 El Proceso……..101

3.1.2 Activos, Vulnerabilidades y Amenazas…….101

3.1.3 Identificación de los Propietarios de Riesgos……....102

3.1.4 Funciones y Obligaciones……..102

3.2 Personal con Acceso Privilegiado y Personal Técnico……..103

3.3 Personal con Perfila de Usuario……104

3.4 Funciones y Obligaciones del Responsable de Seguridad……....105

3.5 Metodología y Análisis del Riesgo……106

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en la Institución Policial Comisaria del Norte –Chiclayo y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

La evaluación y tratamiento de riesgos se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los activos que se utilizan dentro de la organización o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

Los usuarios de este documento son todos los empleados de la Institución Policial Comisaria del Norte –Chiclayo que participan en la evaluación y tratamiento de riesgos.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos 6.1.2, 6.1.3, 8.2, y 8.3
- Política de Seguridad de la Información
- Lista de requisitos legales, normativos y contractuales y demás requisitos
- Política de seguridad para proveedores
- Declaración de aplicabilidad

3. METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

3.1 Evaluación de riesgos

3.1.1 El proceso

La evaluación de riesgos se implementa a través del Cuadro de evaluación de riesgos. El proceso de evaluación de riesgos es coordinado por El Oficial Cap. Medina encargado de la parte del control de los Activos, la identificación de amenazas y vulnerabilidades la realizan los propietarios de los activos, mientras que la evaluación de consecuencias y probabilidad es realizada por los propietarios de los riesgos.

3.1.2 Activos, vulnerabilidades y amenazas

El primer paso en la evaluación de riesgos es la identificación de todos los activos dentro del alcance del SGSI; es decir, todos los activos que pueden afectar la

Confidencialidad, integridad y disponibilidad de la información en la organización. Los activos pueden ser documentos en papel o en formato electrónico, aplicaciones y bases de datos, personas, equipos de TI, infraestructura y servicios externos o procesos externalizados. Al identificar los activos también es necesario identificar a sus propietarios: la persona o unidad organizativa responsable de cada activo.

El siguiente paso es identificar todas las amenazas y vulnerabilidades relacionadas con cada activo. Las amenazas y vulnerabilidades se identifican utilizando los catálogos incluidos en el Cuadro de evaluación de riesgos. Cada activo puede estar relacionado a varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades.

3.1.3 Identificación de los Propietarios de Riesgos.

En la institución policial conocida como Comisaria del norte – Chiclayo, está compuesta por los siguientes propietarios de Riesgos como son:

- Representante de la Dirección o Jefatura de la comisaria.
- Responsable de la seguridad en la institución policial.
- Responsable de la explotación de sistemas
- Responsable de desarrollo y proyectos institucionales
- Responsable de la infraestructura de TI
- Responsable y asesor jurídico
- Responsable de la administración del personal policial
- Equipo de asesores externos, expertos en temas de seguridad

3.1.4 Funciones y Obligaciones del Personal.

Las funciones que los empleados de la institución policial comisaria del norte desarrollen en relación de los sistemas de información, serán aquellas para las que hayan sido expresamente autorizados, independientemente de las limitaciones, que se establecen para controlar su acceso.

Todo el personal policial y efectivos y las entidades relacionas con los sistemas de información estarán obligados a respetar las normas, tanto las de carácter general y la de carácter específico. Con la finalidad de hacer cumplir estas obligaciones, se ha creído conveniente definir una política general contenida en el presente documento.

Independientemente de las funciones y responsabilidades especificas asignadas a los usuarios y/o entidades sobre los respectivos sistemas de información a cualquier empleado de la institución se le exige con carácter general:

1. Confidencialidad, con respecto a la documentación e información que reciben /o usan perteneciente a la institución o de su responsabilidad.
2. No incorporar a la institución información o datos sin ninguna autorización previa y antes coordinada con la institución.
3. Comunicar al responsable de seguridad cualquier incidencia respecto a la seguridad de la información.

3.2 Personal con acceso Privilegiado y personal técnico

El personal técnico que tiene acceso y administra los sistemas de información, no tiene por qué estar presente en todos los casos, siendo en algunos casos sub contratados o asumido por otros roles ahora bien en cualquiera de los dos casos se puede clasificar en las siguientes categorías de acuerdo a sus funciones tenemos:

Administradores: estos tendrán a su cargo la responsabilidad de los máximos privilegios, por lo cual manejaran un riesgo alto de que una acción equivocada o errada afecte al sistema directamente, este personal podrá acceder a todo el sistema para poder desarrollar su función y dar solución a los problemas que surjan.

Operadores: personal con algunas limitaciones dentro del sistema de información por lo general estos serán supervisados por los administradores, estos no deberán tener acceso a los ficheros que contengan datos personales y de alto compromiso, salvo sean requeridos.

Mantenimiento de los sistemas y aplicaciones: este personal será el responsable de resolver los inconvenientes o incidencias orientadas al software y hardware. En principio estos no deberían tener acceso a los datos de los sistemas de información salvo sea requerido.

Ahora bien tanto el personal con acceso privilegiado y personal técnico deberán cumplir con las obligaciones establecidas detalladas en este documento, para estas categorías laborales serán de aplicación las normas y obligaciones establecidas para todo el personal con perfil de usuario. A continuación se identificarán algunas de las funciones y responsabilidades exclusivas del personal técnico y con acceso privilegiado:

1. Procurar que la Integridad, Autentificación, Control de acceso, auditoria y registro se contemplen y se incorporen en el diseño, en la implementación y operación de los sistemas de información.

2. Procurar la confidencialidad y disponibilidad de la información almacenada en los sistemas de información (ya sea de forma electrónica o no), así como su protección mediante copias de seguridad de una manera periódica.

3. Conceder a los usuarios acceso únicamente a los datos y recursos a los que estos están autorizados y para el desarrollo de su trabajo.

4. No acceder a los datos aprovechando sus privilegios sin tener autorización alguna del responsable de seguridad.

5. Custodiar con especial cuidado los identificadores de contraseñas que den acceso al o a los sistemas con privilegios de administrador.

6. Notificar las incidencias oportunamente ante cualquier incidente que violente las normas de seguridad o vulnerabilidades detectadas en los sistemas.

7. No revelar a terceras personas ajenas a la institución ninguna posible debilidad que haga referencia a seguridad de los sistemas sin previa autorización del responsable de seguridad y con el propósito de su corrección.

3.3 Personal con perfil de usuario

El personal con acceso al sistema de información solo podrán acceder aquellos que estén previamente autorizados y sea necesarios para el desempeño en su función. Por lo tanto, todo el personal o usuario involucrado en el uso de sistemas de información deberán cumplir con las siguientes obligaciones, dependiendo de la función que realicen:

1. Guardar el secreto de la información a la cual tiene acceso, e incluso después de haber finalizado la relación con la institución.

2. Conocer y cumplir la normativa interna en cuestión de seguridad de la información y especialmente la referida a la protección de los datos de índole personal.

3. Respetar los procedimientos, mecanismos y dispositivos de seguridad, para así evitar cualquier intento de acceso no autorizado a los recursos no permitidos.

4. Utilizar de manera adecuada los procedimientos, mecanismos y controles de identificación y autentificación ante los sistemas de información. En el caso particular de usuarios y contraseñas.

5. Utilizar las contraseñas según las instrucciones recibidas al respecto, tampoco informarlas ni cederlas a terceras personas ya que estas son de carácter personal y con uso exclusivo por parte del o los titulares.

6. De darse el caso de que un usuario tiene sospechas de que su acceso autorizado, ha sido comprometido o viene siendo utilizado por otra persona, deberá proceder al cambio de su contraseña y así comunicar la correspondiente incidencia de seguridad.

7. Proteger especialmente los datos personales de la organización que con carácter excepcional tuviera que almacenarse, usarse o transportarse fuera de la institución.

8. Salir o bloquear el acceso de los ordenadores u otros dispositivos similares, cuando se encuentre ausente de su puesto de trabajo.

9. El personal de la institución deberá notificar al responsable de la seguridad de la institución cualquier incidencia detectada la cual comprometa los datos de los sistemas de información.

10. Entregar cuando sea requerido por la organización, y de manera especial cunado cause baja en la empresa, las llaves, claves, tarjetas de identificación, documentación, equipos, dispositivos, los cuales sean propiedad de la institución.

3.4 Funciones y obligaciones del responsable de seguridad.

El responsable de seguridad en la institución es el personal que va a coordinar y controlar las medidas de seguridad que serán aplicadas en la institución policial. A continuación se enumeraran las principales funciones asociadas a los responsables de la seguridad:

1. Asesorar en la definición de los requisitos sobre las medidas orientadas a la seguridad que se deben adoptar.
2. Validar la implantación de los requisitos de seguridad necesarios.
3. Revisar de manera periódica el sistema de información y elaborar un informe de las revisiones realizadas y problemas detectados.
4. Verificar la ejecución de los controles establecidos, según lo dispuesto en el documento de seguridad.
5. Mantener actualizadas las normas y procedimientos en materia de seguridad que afecte a la institución.
6. Definir y comprobar la aplicación del procedimiento de copias de respaldo y recuperación de datos.
7. Definir y comprobar la aplicación del procedimiento de notificación y gestión de incidencias.
8. Controlar que la auditoria de seguridad se realice con la frecuencia necesaria.
9. Analizar los informes de auditoría y si lo considera necesario modificar las medidas correctivas para prevenir incidencias.
10. Trasladar los informes de auditoría a la dirección.
11. Establecer los controles y medidas correspondientes para así asegurar los sistemas de información.
12. Gestionar y analizar las incidencias de seguridad en la organización y su registro según el procedimiento indicado en el documento de seguridad.
13. Coordinar la puesta en marcha de las medidas de seguridad y colaborar con el cumplimiento y la difusión del documento de seguridad.

3.5 METODOLOGIA DE ANLISIS DEL RIESGO.

El análisis de riesgos realizado en la institución policial obedece a una metodología, en este documento se detalla el método del análisis de riesgo utilizado. Para este caso de la institución policial, la metodología de análisis de riesgo está basada en MAGERIT.

Aunque se personalizaran alguno de los aspectos atendiendo las características de la institución policial.

FASE 1. Toma de datos y proceso de información: en esta fase se define el alcance y se analizara los resultados de la organización, durante el desarrollo de este proceso se toma en cuenta la granularidad del análisis ya que impactara directamente en el coste del análisis de riesgo.

FASE 2. Establecimiento de Parámetros: durante esta actividad de identifican los parámetros que se utilizaran durante el análisis de riesgo; serán los siguientes:

- Valor de los Activos: se asignara un valor económico al objeto analizado. A la hora de asignar el valor económico se tendrá en cuenta el valor de reposición, configuración, uso y pérdida de oportunidad.

Cuadro N°13: Valoración de los Riesgos

VALORACION	RANGO	VALOR
Muy Alta	**Valor > 2000 s/**	**3000 s/**
Alta	**1000 s/ < valor > 2000s/**	**1500s/**
Media	**500s/ < valor > 1000s/**	**750s/**
Baja	**100s/ <valor > 500s/**	**300s/**
Muy Baja	**Valor < 100s/**	**100s/**

Fuente: Magerit v2

La Vulnerabilidad: es entendida como frecuencia de la ocurrencia de una amenaza. Esta valoración numérica se realizara mediante estimaciones anuales, para ello se aplicara la siguiente formula: (Vulnerabilidad =Frecuencia estimada / días año)

Cuadro N°14: Valoración de la vulnerabilidad

VULNERABILIDAD	RANGO	VALOR
Frecuencia extrema	1 vez al día	1
Frecuencia alta	1 vez cada 2 semanas	26/365
Frecuencia media	1 vez cada 2 meses	6/365
Frecuencia baja	1 vez cada 6 meses	2/365
Frecuencia muy alta	1 vez cada año	1/365

Fuente: Magerit v2

Criticidad: es entendida como el impacto en la organización, si se produjera un problema sobre el activo.

Cuadro N°15: Valoración de la criticidad y sus rangos

CRITICIDAD	RANGO	VALOR
Critico	100 - 90%) Parada total de todos los servicios o un servicio esencial de la institución. Afecta a la imagen de la institución causando daños económicos muy elevados.	95%
Alto	89 - 76%) Parada de un servicio no esencial de la organización, causando daños económicos elevados.	75%
Medio	75 – 26%) Parada en un departamento o equipo de trabajo, causa daños económicos medios.	50%
Bajo	25 – 0%) Parada de un puesto de trabajo. No causa daños económicos apreciables.	25%

Fuente: Magerit v2

Impacto: es entendido como el tanto por ciento del activo que se pierde en caso de que un impacto suceda sobre él.

Cuadro N°16 Impacto y sus rangos

IMPACTO	RANGO
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: Magerit v2

Efectividad de control de seguridad: entendido como el parámetro indicador de la efectividad de las medidas de protección de los riesgos, pueden reducir la vulnerabilidad o el impacto dependiendo del control.

Cuadro N°17 Variación del impacto y la vulnerabilidad

VARIACION IMPACTO / VULNERABILIDAD	VALOR
Muy alto	95%
Alto	75%
Medio	50%
Bajo	30%
Muy bajo	10%

Fuente: Magerit v2

FASE 3. Análisis de los Activos: aquí se identifican los activos de la institución que serán requeridos para llevar a cabo la actividad. Los distintos activos encontrados en la institución son: activos físicos, lógicos, de personal, de infraestructura, intangibles, etc.) Estos serán valorados teniendo en cuenta los parámetros de valoración de activos.

FASE 4. Análisis de Amenazas: estas pueden provocar un problema de seguridad. Las amenazas dependen del tipo de organización así como de su configuración y características. Según MAGERIT, las amenazas se pueden clasificar en 4 grupos según esta metodología como son:

- Accidentes
- Errores
- Amenazas intencionales presenciales
- Amenazas intencionales remotas

FASE 5. Establecimiento de las Vulnerabilidades: como aquellas que permiten explotar una amenaza dañando un activo, en este caso para la metodología MAGERIT, no es necesario lista las vulnerabilidades pero si tenerlas identificadas para de ese modo poder estimar la frecuencia de la ocurrencia de una determinada amenaza sobre un activo.

FASE 6. Valoración de Impactos: es importante y necesario cuantificar el impacto de las amenazas sobre los activos.

FASE 7. Análisis de riesgos intrínseco: una vez después de haber identificado los valores anteriores podemos realizar el estudio de riesgos actuales de la institución, para ello vamos a valernos del uso de la siguiente formula como:

Riesgo = Valor del activo * Vulnerabilidad * Impacto

Nivel aceptable de riesgos. Durante esta fase se establecerá el nivel aceptable de riesgos que se basaran en la siguiente tabla:

Cuadro N°18 Nivel de aceptación del riesgo

NIVEL ACPETABLE DEL RIESGO	VALOR
Alto	75%
Medio	50%
Bajo	25%

FASE 8. Influencia de las Salvaguardas: después de tener los riesgos identificados iniciamos la fase de la gestión del riesgo donde analizamos cada uno de los riesgos y aplicar la solución más óptima y técnica que nos permita reducirlos al máximo.

Para ello utilizaremos dos tipos de salvaguardas como son:

- **Preventivas:** (reducen las vulnerabilidades): Nueva vulnerabilidad = vulnerabilidad * % disminución vulnerabilidad.
- **Correctivas:** (reducen el impacto): Nuevo impacto = impacto * % disminución impacto.

FASE 9. Análisis de riesgos efectivos: después de haber finalizado la aplicación de salvaguardas se calcula el riesgo efectivo incluyendo la reducción resultante después de la aplicación de las salvaguardas. Para este cálculo del riesgo efectivo se utilizara la siguiente formula como:

"Valor efectivo * Nueva vulnerabilidad * Nuevo impacto = Valor activo * (Vulnerabilidad * % disminución de vulnerabilidad) * (impacto * % disminución de impacto) = Riesgo intrínseco * % disminución de vulnerabilidad * % disminución de impacto".

FASE 10. Gestión de riesgos: esta última fase consiste en la toma de decisiones por parte de la institución ante las medidas de seguridad a aplicar. Ante la selección de las medidas de seguridad se debe tener presente el umbral del riesgo aceptable y el coste de la aplicación de las medidas de seguridad. Así mismo establecer un plan de acción que contenga al menos la siguiente información:

- Establecimiento de prioridades
- Análisis de coste / beneficio
- Selección de controles
- Asignación de responsabilidades
- Implantación de controles

COMISARIA DEL NORTE PNP –CHICLAYO

DECLARACIÓN DE APLICABILIDAD

Código	CDA
Versión:	001
Fecha de la Versión:	2014-05-05
Creado Por:	Alcántara Flores Julio Cesar
Aprobado Por:	Cap. PNP- Medina
Nivel de Confidencialidad:	Nivel Intimo / Nivel Intermedio / Nivel Superficial.

TABLA DE CONTENIDOS

1. Objetivos, Alcance y Usuarios……...115
2. Documentos de Referencia……115
3. Aplicabilidad de los Controles……...115
4. Funciones y Obligaciones del Personal……120

1. OBJETIVO, ALCANCE Y USUARIOS.

El objetivo del presente documento es definir qué controles son adecuados para implementar en la Institución Policial Comisaria del Norte -Chiclayo, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.

Este documento incluye todos los controles detallados en el Anexo A de la norma ISO 27001. Los controles se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI).

Los usuarios de este documento son todos empleados de la Institución Policial Comisaria del Norte -Chiclayo que cumplen una función dentro del SGSI.

2. DOCUMENTOS DE REFERENCIA.

- Norma ISO/IEC 27001, capítulo 6.1.3 d)
- Política de Seguridad de la Información
- Metodología de evaluación y tratamiento de riesgos
- Informe de evaluación y tratamiento de riesgos

3. APLICABILIDAD DE LOS CONTROLES.

Son aplicables los siguientes controles del Anexo A de la norma ISO 27001:

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Objetivos del control	Método de implementación	Estado
A.5	Políticas de la seguridad de la información	SI	Políticas de seguridad de la información	La dirección y jefatura de la institución dará apoyo a la seguridad de la información, de acuerdo con los requisitos del negocio y las normas aplicables.	Planificado
A.5.1	Dirección de la gerencia para la seguridad de la información	SI	Documento de política de seguridad de la información	La dirección deberá aprobar un documento de políticas de seguridad de la información, publicarlo y distribuirlo a todos el personal de la institución y terceros afectados	Planificado
A.5.1.1	Políticas para seguridad de la información	SI	Políticas de seguridad de la información	La dirección y jefatura de la institución dará apoyo a la seguridad de la información, de acuerdo con los requisitos del negocio y las normas aplicables. Todas las políticas indicadas bajo esta columna	Planificado
A.5.1.2	Revisión de políticas para seguridad De la información.	SI	Revisión de políticas para seguridad De la información.	Cada política tiene un propietario designado que deberá revisar el documento según un intervalo planificado.	Planificado
A.6	Organización de la seguridad de la información	SI	Organización Interna	Gestionar la seguridad de la información dentro de la institución, a través de jerarquías dentro de la institución.	Planificado

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Objetivos del control	Método de implementación	Estado
A.6.1	Organización interna	SI	Organización Interna	Gestionar la seguridad de la información dentro de la institución, a través de jerarquías dentro de la institución.	Planificado
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	SI	Responsabilidades sobre los Activos de información	Asegurar el funcionamiento correcto y seguro de los recursos de tratamiento de la información.	Planificado
A.6.1.2	Segregación de deberes	SI	Asignación de responsabilidades relativas a la seguridad de la información	Cualquier actividad que incluya información sensible es aprobada por una persona e implementada por otra. Donde se definirán claramente las responsabilidades y deberes relativos a la seguridad de la información.	Planificado
A.6.1.3	Contacto con autoridades	SI	Contacto con las Autoridades	[Estrategia de continuidad del negocio], [Plan de respuesta a los incidentes], Se deben mantenerse los contactos adecuados con las autoridades competentes de la institución.	Planificado

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Objetivos del control	Método de implementación	Estado
A.6.1.4	Contacto con grupos de interés especial	SI	Contacto con grupos de especial interés	El jefe de seguridad de la institución es el responsable de supervisar [detallar los nombres de grupos de interés y foros de seguridad], donde se mantendrán los contactos adecuados con grupos de interés especial u otros, asociaciones profesionales especializadas en seguridad.	Planificado
A.6.1.5	Seguridad de la información en gestión de proyectos	SI		El gerente de proyecto debe incluir las reglas correspondientes sobre seguridad de la información en cada proyecto, así como las acciones y tareas a cumplir que le sean asignadas a cada integrante del grupo.	Planificado
A.6.2	Dispositivos móviles y tele-trabajo	SI	Ordenadores portátiles, comunicaciones móviles y tele-trabajo	Se implantar aun política formal, adoptando las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de ordenadores portátiles y dispositivos móviles.	Planificado

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Objetivos del control	Método de implementación	Estado
A.6.2.1	Política sobre dispositivos móviles	SI	Ordenadores portátiles y comunicaciones móviles	[Política de uso aceptable] / [Política sobre computación móvil y tele-trabajo], [Política Trae tu propio dispositivo (BYOD) El equipamiento mencionado precedentemente puede ser llevado fuera de las instalaciones solamente en caso sea requerido pero no se podrá filtrar ni copiar ninguna información que salga de los sistemas de información de la institución, así como el uso de tarjetas de memoria, medios de trasferencia de datos.	Planificado
A.6.2.2	Tele-trabajo	SI	Tele trabajo	[Política de uso aceptable] / [Política sobre computación móvil y tele-trabajo], se redactara e implementar una política de actividades de tele trabajo así como los planes y procedimientos de operación correspondiente.	Planificado

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL.

En este apartado se recogen las funciones y obligaciones, para el personal efectivo con acceso a los sistemas de información de la institución policial. Así como la previa definición de las funciones y obligaciones del personal, teniendo como objeto:

- Proteger los sistemas de información, así como las redes de comunicación propiedad de la institución o bajo su responsabilidad, contra el acceso o uso que no sea autorizado, así como la alteración indebida, destrucción o mal uso.
- Proteger la información perteneciente o proporcionada a la organización en contra de revelaciones no autorizadas o de modo accidental.

A efecto de dar cumplimiento con estas obligaciones independientemente de su función o responsabilidad, la institución exige un carácter general a cualquier empleado o efectivo el cumplimiento de los siguientes aspectos:

- Confidencialidad de la información
- Propiedad intelectual
- Control de acceso físico
- Salidas y entradas de información
- Incidencias
- Uso apropiado de los recursos
- Software
- Hardware
- Conectividad a la red de internet

4.1 Confidencialidad de la Información.

1. Se debe proteger la información propia o confiada de la institución evitando el uso indebido o su envió no autorizado al exterior a través de cualquier medio de comunicación.

2. Se deberá guardar máxima reserva, por un tiempo indefinido, la información, documentos, claves, análisis, programas y el resto de información a la cual se tenga acceso dentro de la institución policial.

3. En caso de manejar información confidencial, en cualquier tipo de soporte, se deberán entender que la posesión de la misma es temporal, con una obligación de secreto por parte

4. del personal y son que ello le considere derecho alguno de posesión, titularidad o copia de la misma, inmediatamente después de haber realizado y finalizado las tareas que se hubieran originado, esta debería devolverse a la institución.

4.2 Propiedad Intelectual.

Queda totalmente prohibido en los sistemas de información de la institución:

1. El uso de aplicaciones informáticas sin la correspondiente licencia. Así como los programas informáticos propiedad de la institución, están protegidos por la propiedad intelectual por lo tanto queda rotundamente prohibida su reproducción, modificación, cesión, o comunicación sin ninguna autorización previa.

2. El uso, reproducción, modificación, cesión o comunicación de cualquier otro tipo de obra protegida por la propiedad intelectual sin la debida autorización correspondiente.

4.3 Control de Acceso Físico.

Las normas orientadas al acceso físico de las instalaciones de la institución que albergan los sistemas de información y los locales de tratamiento son los siguientes:

1. El acceso a las instalaciones de la institución donde se encuentran los sistemas de información y locales de tratamiento, será realizado previo paso por un sistema de control de acceso físico o con la autorización del responsable (s) de las instalaciones de la institución.

4.4 Salidas y Entradas de Información.

1. Todo tipo de salida y entrada de información de la institución sea esta de carácter personal, deberá ser realizada por el personal autorizado y será necesaria la autorización formal del responsable del fichero de donde provienen los datos.

2. Para la salida de la información de Alto nivel – confidencial, se deberán cifrar los mismos o utilizar cualquier otro mecanismo que no permitan el acceso o su manipulación durante el transporte.

4.5 Incidencias.

1. El personal de la organización y de terceras partes, tiene como obligación la comunicación de cualquier incidencia que se pueda producir la cual esté relacionada con los sistemas de información o de cualquier otro recurso informático de la institución.

2. La comunicación, gestión y resolución de las incidencias de seguridad se realizaran mediante el sistema de gestión de incidencias es cual es habilitado por la institución.

4.6 Uso Apropiado de los Recursos.

Los recursos informáticos ofrecidos por la institución (datos, software, comunicaciones, etc.), están disponibles exclusivamente para cumplir con las obligaciones labores y con una finalidad corporativa. Por lo que queda terminantemente prohibido cualquier uso distinto del indicado, algunos ejemplos:

1. El uso de los recursos de la institución, así como los que están bajo su supervisión para actividades no relacionadas con la finalidad de la institución.

2. El uso de los equipos, dispositivos o aplicaciones los cuales no estén especificados como parte de software y/o hardware contenidos en la institución.

3. Introducir en los sistemas de información o red corporativa contenidos ilegales, inmorales u ofensivos y en general, sin utilidad alguna en los procesos del negocio de la institución policial.

4. Introducir voluntariamente programas, virus, spyware o cualquier otro software malicioso que sean susceptibles de causar alteraciones en los recursos informáticos de la institución hacia terceros.

5. Desactivar o inutilizar los programas antivirus y de protección de los equipos y sus actualizaciones.

6. Intentar eliminar, modificar, inutilizar los datos, programas o cualquier otra información propios de la institución.

7. Conectarse la red corporativa a través de otros medios que no sean los definidos y administrados por la institución.

8. Intentar descubrir o descifrar las claves de acceso o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la institución policial.

4.7 Software.

1. Los usuarios deben utilizar únicamente las versiones de software facilitadas por la institución y así seguir las normas de utilización.

2. El servicio de informática, es el responsable de definir los programas de uso estandarizado en la institución y de realizar las instalaciones en los PCs.

3. Los usuarios no deben instalar ni borrar ningún tipo de programa informático en su PC.

4.8 Hardware.

1. El personal en su actividad laboral, deben hacer uso únicamente del hardware instalado en los equipos propiedad de la institución y cuya función lo requiere para el trabajo que desempeña.

2. El personal en ningún caso accederá físicamente al interior del equipo que tiene asignado para su trabajo o que pertenezca a la propiedad de la institución. En caso necesario se comunicara la incidencia, según el protocolo habilitado, para que el departamento indicado o en su defecto el encargado de su función, realice las tareas de reparación, instalación o mantenimiento.

3. Los usuarios no manipularan los mecanismos de seguridad que la organización implemente en los dispositivos (equipos, portátiles, móviles, etc.)

4. No sacar equipos, dispositivos o soportes de las instalaciones sin la autorización necesaria, y en todo caso, con los controles y medidas que se hayan establecido para cada supuesto.

4.9 Conectividad a la red de Internet.

Las normas referentes al correo electrónico son:

1. El servicio de correo electrónico o cunetas de correo que la organización pone a disposición de los usuarios tiene un uso estrictamente profesional y destinado a cubrir las necesidades del puesto.

2. Queda terminantemente prohibido intentar leer, copiar o borrar mensajes de correo electrónico de otros usuarios.

3. El personal no debe enviar mensajes de correo electrónico de manera masiva o de tipo primordial con fines publicitarios o comerciales. En el caso que sea necesario, dada la función del usuario, este tipo de mensajes se gestionara con la dirección de la institución y con el responsable de seguridad.

COMISARIA DEL NORTE PNP –CHICLAYO

PLAN DE TRATAMIENTO DE RIESGOS

Código	CPTR
Versión:	001
Fecha de la Versión:	2014-05-05
Creado Por:	Alcántara Flores Julio Cesar
Aprobado Por:	Cap. PNP- Medina
Nivel de Confidencialidad:	Nivel Intimo / Nivel Intermedio / Nivel Superficial.

Para cumplir los objetivos del SGSI, es necesario realizar las siguientes actividades

Actividad	Recursos generales y financieros necesarios	Recursos Humanos necesarios	Recursos de capacitación	Control del riesgo (evitar, prevenir, proteger)	Función del riesgo (aceptar, retener, transferir)	Opciones del riesgo
Políticas para seguridad de la información	Documentación en papel o formato electrónico, recursos asumidos por el gobierno en el presupuesto asignado a las comisarias del departamento	Personas encargadas de gestionar la documentación referente a las políticas de seguridad a seguir en la institución.	Programas de capacitación al personal efectivo, dado por personal experto en temas de seguridad.	Prevenir	Transferir	Elección de controles
Revisión de las políticas para seguridad de la información	Documentación establecida y finalizada acerca de políticas establecidas anteriormente	Personal de la alta dirección gerencial o de la jefatura de la institución policial experta en temas de seguridad.	Programas de capacitación dirigida a los efectivos de la institución que interactúan con los sistemas de información	Proteger	Retener	Evitar el riesgo
Inventario de activos	Inventario de los activos de la institución, personal externo especializado en temas de inventarios.	Personal experto en levantamiento de políticas de la seguridad de la información	registros para entender mejor las necesidades de seguridad de información y determinar los controles para asegurar la confidencialidad, integridad y disponibilidad de la información	Prevenir	Aceptar	Elección de controles

Mantenimiento de equipo	Recursos del presupuesto alcanzado a la jefatura o dirección de la institución, destinado para los equipos e infraestructura de la institución policial.	Personal técnico especializado en el área de tecnologías de información e infraestructura de hardware y software.	Mantenimiento para los equipos de la institución policial bajo tres aspectos de capacitación tales como son: el mantenimiento preventivo, el correctivo y el predictivo.	Prevenir	Aceptar	Evitar el riesgo
Procedimientos y políticas sobre transferencia de información	Recursos utilizados por la institución policial asignados en el presupuesto del gobierno destinado a las comisarias del departamento	Personal encargado de velar en el cumplimiento de procedimientos y transferencia y registros de información	Cursos y charlas de capacitación orientadas a definir y mejorar procedimientos orientados a manejo de información así como el uso adecuado de la misma.	Evitar	Retener	Evitar el riesgo
Cumplimiento con las políticas y estándares de seguridad	Recursos utilizados por la institución policial asignados en el presupuesto del gobierno destinado a las comisarias del departamento	Personal encargado de velar en el cumplimiento de procedimientos y transferencia y registros de información	Cursos y charlas de capacitación orientadas a definir y mejorar procedimientos orientados a manejo de información así como el uso adecuado de la misma.	Evitar	Retener	Evitar el riesgo
Revisión independiente de la seguridad de la información	Documentación en papel o formato electrónico, recursos asumidos por el gobiernos en el presupuesto asignado a las comisarias del departamento	Personas encargadas de gestionar la documentación referente a las políticas de seguridad a seguir en la institución.	Programas de capacitación al personal efectivo, dado por personal experto en temas de seguridad.	Prevenir	Transferir	Elección de controles

Reporte de debilidades en la seguridad de la información	Documentación establecida y finalizada acerca de políticas establecidas anteriormente	Personal de la alta dirección gerencial o de la jefatura de la institución policial experta en temas de seguridad.	Programas de capacitación dirigida a los efectivos de la institución que interactúan con los sistemas de información	Proteger	Retener	Evitar el riesgo
Análisis y especificación de los requerimientos de seguridad de la información	Recursos utilizados por la institución orientados al levantamiento de requisitos de seguridad para la institución policial y próximamente para su implantación	Personas expertos en toma de requerimientos y necesidades de la institución enfocados a la seguridad en los sistemas de información	Programas de capacitación al personal efectivo, dado por personal experto en temas de seguridad.	Evitar	Aceptar	Elección de controles
Procedimientos documentados de operación	Recursos necesarios apoyados por la alta dirección o jefatura de la institución policial.	Personal efectivo capacitado en labores de documentación y operación.	Recurso asignado por el gobierno orientado a brindar capacitación al personal adecuado en términos documentarios.	Proteger	Transferir	Elección de controles

COMISARIA DEL NORTE PNP –CHICLAYO

PLAN DE CAPACITACION Y CONCIENCIACION

Código	CPCC
Versión:	001
Fecha de la Versión:	2014-05-05
Creado Por:	Alcántara Flores Julio Cesar
Aprobado Por:	Cap. PNP- Medina
Nivel de Confidencialidad:	Nivel Intimo / Nivel Intermedio / Nivel Superficial.

FICHA TECNICA

1. DENOMINACIÓN.

Capacitación y Concienciación del Personal Efectivo Policial de la Institución Policial Comisaria del Norte PNP- Chiclayo.

2. FINALIDAD.

a) Capacitar al personal efectivo policial que hace uso de los sistemas y tecnologías de información en la Comisaria del Norte - Chiclayo en el uso y manejo de la seguridad del Sistema así como en su Gestión Documentaria.

b) Acreditar al personal policial involucrado, que han llevado y aprobado el Curso de Capacitación y concienciación en temas de seguridad del Sistema, así como en la Gestión Documentaria de la institución Policial Comisaria del Norte – Chiclayo.

3. BASE LEGAL.

- Ley especial sobre delitos informáticos (Ley N°30096), el Gobierno de la Republica Peruana.
- Ley de Transparencia y Acceso a la Información Pública (LEY Nº 27806.)
- Resolución Ministerial 129-2012-PCM – Implementación incremental de NTP-ISO/IEC 27001:2008.
- Norma Técnica Peruana "NTP-ISO/ IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad.

4. DESCRIPCIÓN.

Este programa de CAPACITACION Y CONCIENCIACION, requiere ser aprobado por el Titular de la Unidad de la Jefatura de la Institución Policial, convocante a la Capacitación, por lo cual se debe asegurar un Área específica dentro de la Institución o como puede ser un Laboratorio de Cómputo donde se desarrolle la capacitación, Así mismo gestionar toda la logística del evento.

Reclutar a los Capacitadores por parte de la Jefatura de la institución Policial, donde se Procederá a capacitar a los participantes bajo la forma de taller, es decir de manera teórico y práctica, llegando a finalizar con la capacitación en una evaluación programada posterior a la capacitación, con vista a la acreditación del participante.

5. PLANEAMIENTO.

5.1.Laboratorio

El Laboratorio con computadoras personales y con acceso a Internet, será asignado para el dictado de clases teórico – prácticas, en horarios previamente programados.

5.2.Computadoras Personales

Las PC's a utilizar cumplen con los siguientes requisitos técnicos:
a) Hardware: Procesador Intel Core I3 y Memoria RAM 4 Gb.
b) Software: Sistema Operativo: Ubuntu o Windows en cualquier versión.
c) Navegador Web: (Mozilla Firefox, Chrome o Explorer)

5.3.Capacitador

Perfil de Capacitador para la Labor:

a. Bachiller o Ingeniero de Sistemas, Computación o Informática.
b. Disponibilidad de tiempo en los turnos de mañana y/o tarde, entre lunes y viernes de cada semana.
c. Conocimiento de Software Libre, Licenciado y herramientas de diseño Web.
d. Proactivo(a), trabajo en equipo y establecimiento de metas diarias.

El proceso de reclutamiento e instrucción de los Capacitadores estará a cargo de la Oficina de Tecnologías de la Información y Área de Informática de la Institución Policial.

5.4.Manual de apoyo

El Manual Práctico del Usuario (archivo digital) servirá de ayuda inmediato al personal policial al momento de interactuar con el Sistema.

5.5.Lista de Asistencia

Se llevará un control de asistencia por capacitación efectuada, en el entendido que éstas han sido agrupadas por día y hora de manera programada adecuadamente.

5.6.Carpeta de trabajo

Cada usuario al momento de la capacitación recibirá como material del curso: un archivo digital del manual, usuario y clave, instrucciones.

5.7.Esquema del Curso

a) Registro de asistencia.
b) Introducción al curso
c) Explicación sobre el curso y la Acreditación.
d) Desarrollo del contenido del curso. (Parte Teórica / Parte Práctica)
e) Preguntas.
f) Cronograma de Evaluación para Acreditación.

5.8. Material de trabajo

El Capacitador tendrá los siguientes recursos y materiales:

a) Carnet de Identificación
b) Proyector multimedia.
c) Laptop.
d) Pizarra acrílica y Puntero láser.
e) Dos plumones (colores azul y rojo).

5.9. Usuario y contraseña

En la capacitación cada participante ingresará al Sistema de Práctica con su respectivo nombre de usuario y contraseña asignada por el capacitador.

5.10. Prueba y Evidencia

La capacitación brindada a los participantes debe probarse con la realización de ejercicios prácticos, y debe evidenciarse con la filmación o fotografías del evento.

6. INSTRUCCIÓN A CAPACITADORES.

Es la explicación a detalle del proceso del Sistema de Gestión Documentaria absolviendo inquietudes de los capacitadores en forma coherente y siendo anotado en un Banco de Preguntas.
Al final del Programa cada capacitador recibirá del Organizador un Certificado por haber participado como "Capacitador" con el número de horas dictadas.

7. ACREDITACIÓN.

A. Posterior a la capacitación y en plazo no mayor a dos semanas, el participante, mediante solicitud llenado en formato pre-establecido y presentado en la Oficina de Tecnologías de la Información, podrá solicitar la evaluación teórico – práctico para obtener la Acreditación del Sistemas y mecanismo de seguridad, citando un correo electrónico de uso personal, brindado por los capacitadores, en donde se le remitirá el día y hora programado para realizar el examen.

B. Para el participante que decida rendir el examen para obtener la Acreditación del Sistemas y mecanismo de seguridad, sin asistir a la capacitación, podrá solicitarlo en los mismos términos y condiciones mencionados en el párrafo anterior.

C. La acreditación es personal y será suscrita por el Jefe de la Oficina Regional de Administración conjuntamente por el Gerente Regional de Educación, a propuesta de la Jefatura de la Oficina de Tecnologías de la Información, vía Oficina Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial.

D. Para la Acreditación requiere que la asistencia del Participante sea en un 100%, es decir que permanezca todo el tiempo que dure la capacitación, salvo lo previsto en el numeral 7.2.

E. Si el participante que desaprueba el examen para la acreditación solo tiene una nueva oportunidad de solicitarlo, si persiste la desaprobación, el participante puede solicitar llevar el curso de capacitación utilizando el formato que refiere el numeral 7.1 de la presente Ficha.

8. METODOLOGÍA

Para asegurar que las actividades de Trabajo en la Jefatura de Tecnologías de la Información – JTI continúen de manera regular, la Capacitación para la Acreditación se llevará a cabo en dos estados:

1) El primer estado está a cargo de Capacitadores instruidos previamente para tal fin que se pretende alcanzar en la Institución.

2) El segundo estado está a cargo del personal de la JTI quienes tendrán el trabajo de evaluar al personal capacitado para su acreditación. La evaluación será mediante examen con puntaje vigesimal, siendo la nota aprobatoria igual o mayor a catorce (14).

Ambos estados se llevaran a cabo en un Laboratorio asignado en la institución Policial, por la Unidad Ejecutora que aprueba el evento.

PLAN DE CAPACITACIÓN Y CONCIENCIACIÓN

Con el objetivo de preparar al personal para que pueda cumplir una función en la seguridad de la información, se debe llevar a cabo la siguiente capacitación:

1. PROGRAMACION.

   Dentro de la programación, los eventos a realizar en esta actividad serán los siguientes:

NO.	EVENTO	UNID MED	META	PERÍODO (DÍAS)
01	Determinación de Laboratorio	# Laboratorio	1	1
02	Gestión para la logística de materiales	# Pedido	1	1
03	Convocatoria y selección de capacitadores	# Capacitador	2	1
04	Instrucción a capacitadores	# Capacitador	2	1
05	Capacitación a participantes	# Personal	40	2
06	Acreditación a trabajadores	# Personal	40	2

(*) Estará en función al N° de trabajadores de la Unidad Ejecutora

Cabe hacer de mención que las capacitaciones al personal efectivo se harán efectivas los días martes y jueves de las semanas en un período de tiempo de 10 semanas el equivalente a 2 meses y medio respectivamente. Los Horarios para la capacitación son:

TURNO/HORARIO	CAPACITADOR	SUPERVISOR
Mañana: 08:00 - 09:00	A	Ing. Marco Ignacio Valverde R.
Mañana: 09:00 – 10:00	B	Ing. Marco Ignacio Valverde R.
Tarde: 17:00 – 18:00	A	Ing. Roncal Ramírez Iván A.
Tarde: 18:00 – 19:00	B	Ing. Roncal Ramírez Iván A.

MODULO - TEMATICA	FECHA	HORARIO
Seguridad en las SI/TI	05/07/2014	08:00-09:00 am
Control de logística y almacén	05/07/2014	09:00-10:00 am
Control documentario	12/07/2014	17:00-18:00 pm
Fiabilidad y confidencialidad en la seguridad de la información	12/07/2014	18:00-19:00 pm
Elementos vulnerables en los sistemas de información	19/07/2014	08:00-09:00 am
Amenazas en las tecnologías y sistemas de información	26/07/2014	09:00-10:00 am
Personas y Amenazas logísticas	02/08/2014	17:00-18:00 pm
Amenazas físicas y Lógicas en los sistemas de información	09/08/2014	18:00-19:00 pm
Implementación de Políticas de seguridad	16/08/2014	08:00-09:00 am
Estándares de seguridad, estrategias y niveles de riesgo	23/08/2014	09:00-10:00 am

Para que el personal comprenda la importancia de la gestión de la seguridad de la información y de su propio aporte al SGSI, y para que acepte las políticas y planes y comprenda las consecuencias de violar las normas de seguridad de la información, se deben aplicar los métodos de concienciación mencionados anteriormente en el documento.

V. DISCUSIÓN.

De acuerdo a lo obtenido en los resultados de la Tesis, se referenciará el análisis de los datos que fueron tomados en cuenta, a su vez demostraremos el cumplimiento y satisfacción de los objetivos de la Tesis que fueron planteados en un inicio, evidenciando los cambios que se han podido suscitar correspondientemente a una realidad que se pudo encontrar en su momentos y que a través de unos objetivos planteados mostraremos los porcentajes de medición para poder entender lo que sucedió en la institución.

CONTRASTACIÓN DE HIPÓTESIS PARA LOS INDICADORES.

Indicador A1: Nivel de seguridad en las aplicaciones, de la institución Policial.

$\mathbf{N_{AG}}$ = Nivel de seguridad en las aplicaciones de la institución policial antes de la Guía de Implementación para la institución. (Pre test/encuesta).

$\mathbf{N_{DG}}$ = Nivel de seguridad en las aplicaciones de la institución policial con la Guía de Implementación para la institución. (Post test/encuesta)

Donde:

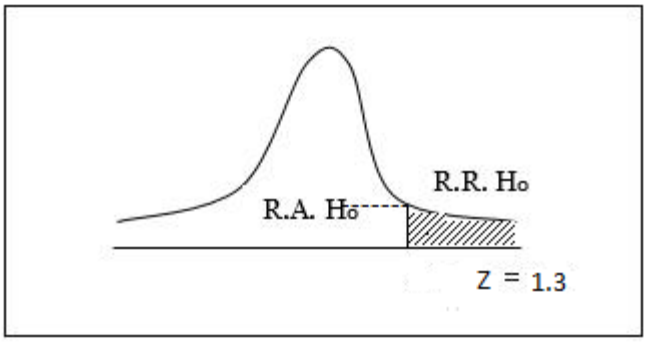
AG: Antes de la Guía de implementación.
DG: Después la Guía de Implementación.

A) Hipótesis estadística.

$$H_0: N_{AG} = N_{DG} \Rightarrow N_{AG} - N_{DG} = 0$$
$$H_1: N_{AG} > N_{DG} \Rightarrow N_{AG} - N_{DG} > 0$$

	Antes	**Después**	**Dif: A-D**
Indicador A1	17%	20%	+3

B) Región critica.



C) Estadística de prueba.

$$z = \frac{\bar{X} - \mu_0}{\sigma/\sqrt{n}} \rightarrow N(0, 1)$$

Rechazar si: Z >= 1.96 o Z<= -1.96
Aceptar si: -1.96 < Z < 1.96

D) Calculo.

$$z = \frac{\bar{X} - \mu_0}{\sigma/\sqrt{n}} = \frac{113-100}{30/\sqrt{9}} = 1.3$$

Z=1.3

E) Se acepta H_0.

F) Decisión y Conclusión:

Como 1.3 es < 1.96 aceptamos el H_0.
La evidencia suficiente aconseja no rechazar, según la regla de decisión adoptada, la hipótesis de que la media poblacional sea igual a 100. Para decir que el nivel de seguridad se mostró un incremento en el nivel de seguridad. Eso quiere decir que con la Guía de implementación podemos reducir el nivel de inseguridad en el uso de las aplicaciones de la institución.

Indicador A2: Mejorar el proceso utilizado para detectar anomalías en la seguridad de la información.

P_{AG} = Mejorar el proceso utilizado para detectar anomalías en la seguridad de la información. (Pre test/encuesta).

P_{DG} = Mejorar el proceso utilizado para detectar anomalías en la seguridad de la información. (Post test/encuesta)

Donde:

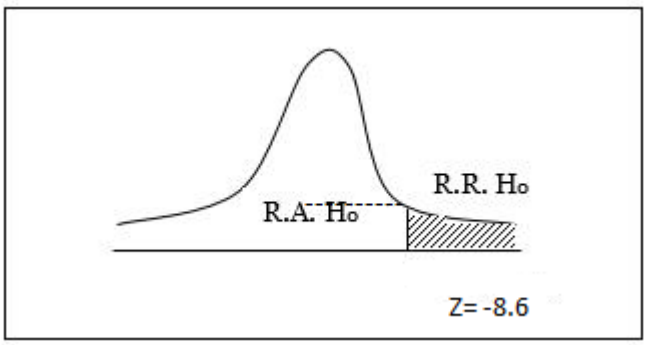
AG: Antes de la Guía de implementación.
DG: Después la Guía de Implementación.

A) Hipótesis estadísticas.

$$H_0: P_{AG} = P_{DG} \Rightarrow P_{AG} - P_{DG} = 0$$
$$H_1: P_{AG} > P_{DG} \Rightarrow P_{AG} - P_{DG} > 0$$

	Antes	**Después**	**Dif: A-D**
Indicador A2	10%	14%	+4

B) Región critica.



C) Estadística de prueba.

$$z = \frac{\bar{X} - \mu_0}{\sigma/\sqrt{n}} \rightarrow N(0, 1)$$

Rechazar si: Z >= 1.96 o Z<= -1.96
Aceptar si: -1.96 < Z < 1.96

D) Calculo.

$$z = \frac{\bar{X} - \mu_0}{\sigma/\sqrt{n}} = \frac{35 - 100}{30/\sqrt{16}} = -8.66$$

Z= -8.66

E) Se rechaza H_0.

F) Decisión y Conclusión:

Como -8.66 es < -1.96 aceptamos el H_0.
La evidencia suficiente aconseja rechazar, según la regla de decisión adoptada, la hipótesis de que la media poblacional sea igual a 100. Para decir que se mejoró el proceso utilizado en la detención de anomalías en la información. Eso quiere decir que con la Guía de implementación podemos mejorar el proceso para la detención de anomalías en la seguridad dela información.

Indicador A3: Disminuir los niveles de riesgo, respecto a los activos de información, considerados amenazas y vulnerabilidades.

N_{AG} =Disminuir los niveles de riesgo, respecto a los activos de información, considerados amenazas y vulnerabilidades. (Pre test/encuesta).

N_{DG} =Disminuir los niveles de riesgo, respecto a los activos de información, considerados amenazas y vulnerabilidades. (Post test/encuesta)

Donde:

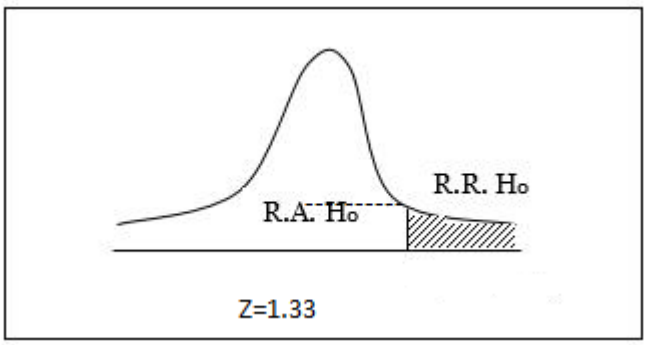
AG: Antes de la Guía de implementación.
DG: Después la Guía de Implementación.

A) Hipótesis estadísticas.

$$H_0: N_{AG} = N_{DG} \Rightarrow N_{AG} - N_{DG} = 0$$
$$H_1: N_{AG} > N_{DG} \Rightarrow N_{AG} - N_{DG} > 0$$

	Antes	**Después**	**Dif: A-D**
Indicador A3	67%	57%	-10

B) Región critica.



C) Estadística de prueba.

$$z = \frac{\bar{X} - \mu_0}{\sigma/\sqrt{n}} \rightarrow N(0, 1)$$

Rechazar si: Z >= 1.96 o Z<= -1.96
Aceptar si: -1.96 < Z < 1.96

D) Calculo.

$$z = \frac{\bar{X} - \mu_0}{\sigma/\sqrt{n}} = \frac{124 - 100}{30/\sqrt{100}} = 1.33$$

Z= 1.33

E) Se acepta H_0.

F) Decisión y Conclusión:

Como 1.33 es < 1.96 aceptamos el H_0.
La evidencia suficiente aconseja aceptar, según la regla de decisión adoptada, la hipótesis de que la media poblacional sea igual a 100. Para decir que se disminuyeron los niveles de riesgos. Eso quiere decir que con la Guía de implementación podemos disminuir los nivele de riesgos en los activos de información de la institución.

Indicador A4: Mejorar el nivel de capacitación en temas de seguridad informática en el personal.

N_{AG} =. Mejorar el nivel de capacitación en temas de seguridad informática en el personal. (Pre test/encuesta).

N_{CG} =.Mejorar el nivel de capacitación en temas de seguridad informática en el personal (Post test/encuesta).

Donde:

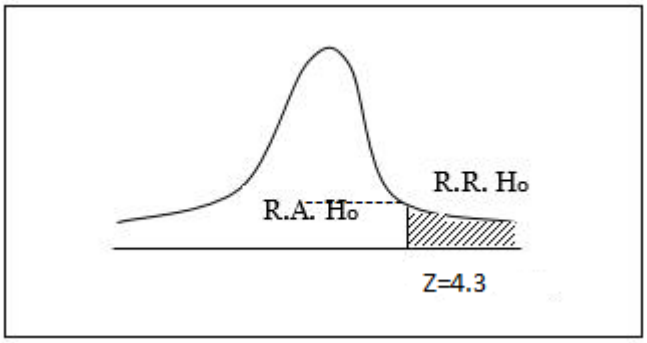
AG: Antes de la Guía de implementación.
CG: Con la Guía de Implementación.

A) Hipótesis estadísticas.

$$H_0: N_{AG} = N_{CG} \Rightarrow N_{AG} - N_{CG} = 0$$
$$H_1: N_{AG} > N_{CG} \Rightarrow N_{AG} - N_{CG} > 0$$

	Antes	**Después**	**Dif: A-D**
Indicador A4	27%	30%	+3

B) Región critica.



C) Estadística de prueba.

$$z = \frac{\bar{X} - \mu_0}{\sigma/\sqrt{n}} \rightarrow N(0, 1)$$

Rechazar si: Z >= 1.96 o Z<= -1.96
Aceptar si: -1.96 < Z < 1.96

D) Calculo.

$$z = \frac{\bar{X} - \mu_0}{\sigma/\sqrt{n}} = \frac{57 - 100}{30/\sqrt{9}} = 4.3$$

Z= 4.3

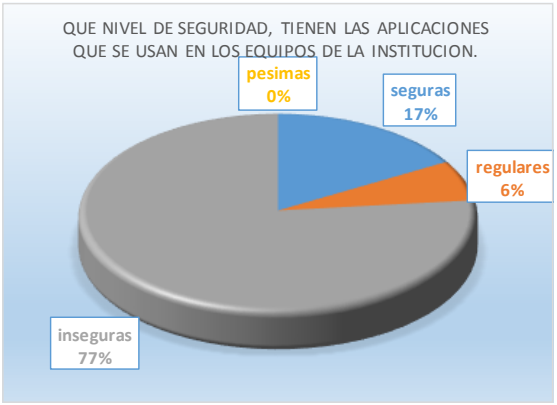
E) Se rechaza H_0.

F) Decisión y Conclusión:

Como 4.3 es >1.96 aceptamos el H_0.
La evidencia suficiente aconseja rechazar, según la regla de decisión adoptada, la hipótesis de que la media poblacional sea igual a 100. Para decir que se pudo mejorar el nivel de capacitación. Eso quiere decir que con la Guía de implementación podemos mejorar el nivel de capacitación en temas de seguridad hacia el personal.

Indicador A1: Nivel de seguridad en las aplicaciones de la institución Policial.
Respecto a la implementación de políticas de seguridad, orientadas a mejorar los niveles de seguridad en el uso de las aplicaciones, las cuales hace uso el personal de la institución policial y de gran importancia para las demás instituciones del mismo sector. Al iniciar el trabajo de investigación se percibían ciertos inconvenientes reflejados en problemas con los recursos de la organización, como es el caso de la información, las comunicaciones, el hardware y el software; lo cual quedó reflejado en los datos obtenidos en las encuestas realizadas, donde un 17% de los encuestados señaló que existe ese porcentaje de seguridad en cuanto al uso de las aplicaciones, generando molestias e inconvenientes por parte del personal de la institución demostrado en el porcentaje de insatisfacción. Así mismo al aplicar el Pos-test en la institución, el porcentaje de seguridad se vio incrementado en un 3%, con respecto al valor inicial obtenido en el Pre-test. Este pequeño incremento de porcentaje obtenido benefició a la institución, en lo relacionado a las medidas para salvaguarda de su información; a fin de permitirle contar con la información necesaria y disponible, que se refleja en una adecuada y certera toma de decisiones.

Anexo 04 - Fig. 01
Antes



Fuente propia de Análisis

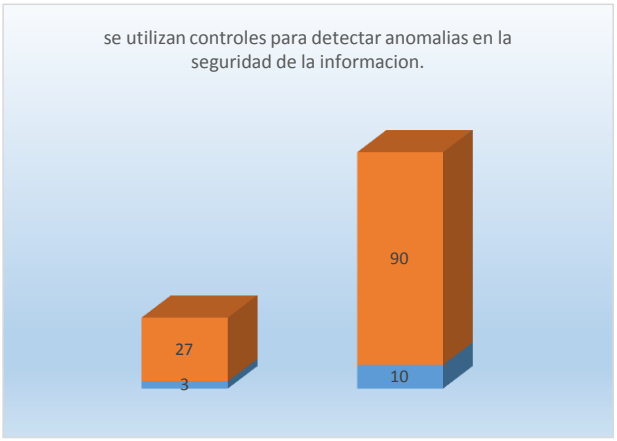
Anexo 05 – Fig.01
Después

Fuente propia de Análisis

Indicador A2: Mejorar el proceso utilizado para detectar anomalías en la seguridad de la información.-
En cuanto a los controles tomados en cuenta para detectar deficiencias o anomalías en la seguridad de la información con la que cuenta la institución para protegerse, se pudo encontrar ciertas deficiencias, teniendo como consecuencia una información no oportuna y veraz en algunos casos alterada, lo cual queda demostrado con los datos obtenidos en las encuestas realizadas, el 10% de los encuestados señaló que se debería mejorar el proceso que se viene utilizando la ausencia de controles adecuados y específicos para proteger la información considerado si el mas importantes de sus activos, como es el caso de tener acceso a la misma, modificarla, alterarlas, etc. Definiendo los límites de acceso al personal adecuado e idóneo a la hora de manipular la información. Con la aplicación del pos-test en la institución, el porcentaje de seguridad se vio incrementado en un 4%, respecto al valor inicial obtenido en el pre-

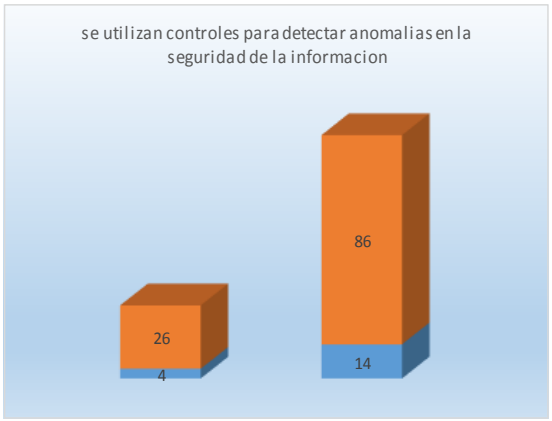
test. A su vez este pequeño incremento de porcentaje obtenido colabora con el beneficio al momento de requerirse la información en el momento adecuado y exacto para la institución; y así evitar que la información pueda perderse o ser alterada y no ser oportuna.

Anexo 04 - Fig. 11
Antes



Fuente propia de Análisis

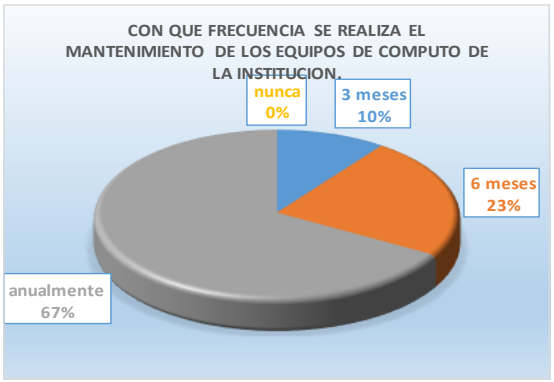
Anexo 05 – Fig.11
Después



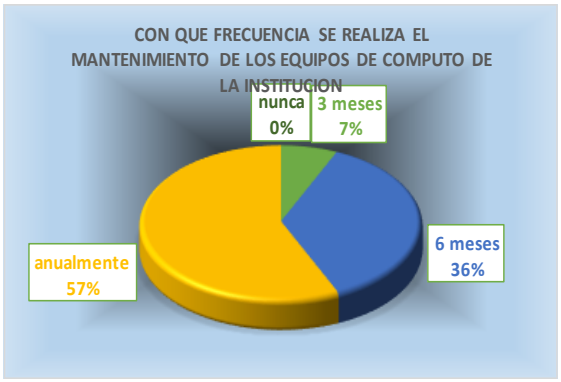
Fuente propia de Análisis

Indicador A3: Disminuir los niveles de riesgo, respecto a los activos de información, considerados amenazas y vulnerabilidades.
El nivel de riesgo, con respecto a los activos de información es de suma importancia en el funcionamiento y los procesos de la institución. Cabe indicar que el soporte y mantenimiento que reciben los activos de la institución, no viene siendo los más adecuados por lo que resulta insuficiente; a su vez el no poder disminuir estos riesgos con respecto a los activos puede generar inconvenientes, algunas inconsistencias que se pueden ver manifestadas en las vulnerabilidades y amenazas para la institución. Al iniciar el trabajo de investigación se percibían ciertos inconvenientes reflejados en problemas con los activos de la organización, lo cual quedó en evidencia con los datos obtenidos en las encuestas realizadas. En cuanto al mantenimiento de los activos se da anualmente en un 67%, lo cual no es el más adecuado para disminuir los impactos en la organización. Al aplicar el Pos-test en la institución, el porcentaje de riesgos disminuyó en un 10% con respecto al valor inicial ya que se considera prudente un mantenimiento de los activos de manera semestral en mayor porcentaje para monitorear y contralar de manera mucho más adecuada los activos de la institución. Se pudo notar también a su vez un incremento del 16% en conocimiento de políticas de seguridad, que ayudan a disminuir los riesgos en la institución, esto debido al conocimiento que tiene ahora el personal. A su vez este incremento de porcentaje obtenidos va a colaborar y beneficiar a la institución en tomar las medidas del caso adecuadas para controlar sus riesgos y evitar pérdidas de información que perjudiquen el negocio y los proceso respectivamente.

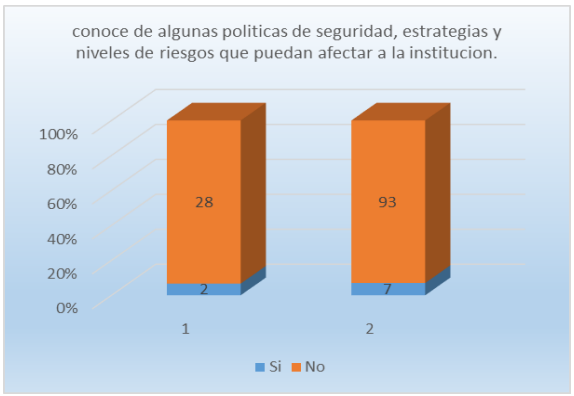
Anexo 04 - Fig. 03
Antes



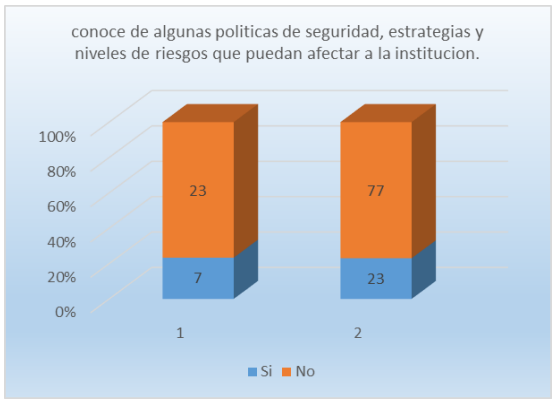
Anexo 05 – Fig.03
Después



Anexo 04 - Fig. 07
Antes



Anexo 05 – Fig.07
Después



Fuente propia de Análisis

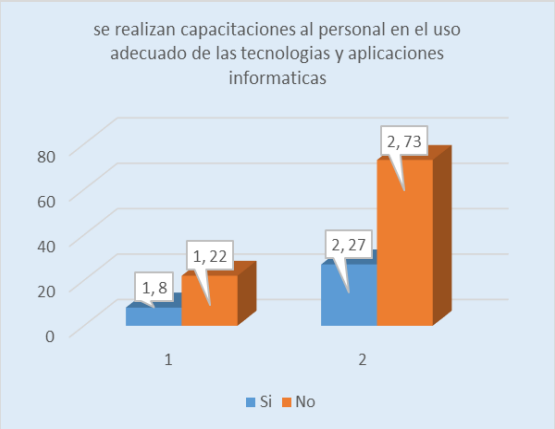
Fuente propia de Análisis

Indicador A4: Mejorar el nivel de capacitación en temas de seguridad informática en el personal.

El uso y puesta en marcha de programas orientados a capacitar al personal que forma parte de la institución policial los cuales hacen uso de los sistemas de información, dirigidos al personal efectivo de la institución, y orientados a dar a conocer y poner en práctica los conocimientos en temas específicamente de seguridad en el uso de las aplicaciones que utiliza la institución. Estos programas de capacitación son muy importantes para las demás instituciones del mismo sector, lo que a su vez el no aprovecharlos podría limitar los conocimientos del personal. Se percibían ciertos inconvenientes reflejados en problemas con el ejercicio de las buenas prácticas recomendadas en los procesos qué realiza la institución, por lo cual se evidenció en el pre-test, pues tan solo el 27% de los encuestados era capacitado en temas específicamente sobre seguridad y políticas para mejorar el desempeño en los proceso que realiza la institución, por lo cual esto genera cierto desconocimiento sobre políticas, planes específicos a seguir, etc. Al aplicar el Pos-test en la institución, sobre esta misma situación se pudo notar que el porcentaje sufrió un incremento del 3% con respecto al valor inicial obtenido. A su vez este pequeño incremento de porcentaje obtenido genera un cierto conocimiento mucho más específico, y de gran nivel al estar

dirigidos para el personal que hace uso de los sistemas de información lo cual se va a ver reflejado en mejores resultados en formas y maneras de proceder adecuadamente, acompañado de una concienciación a la hora de hacer efectivas estas capacitaciones respectivamente.

Anexo 04 - Fig. 04
Antes



Fuente propia de Análisis

Anexo 05 – Fig.04
Después

Fuente propia de Análisis

En lo que respecta a la contratación de la Hipótesis, podemos afirmar que se pudieron satisfacer los diferentes objetivos e indicadores de la misma. El poner en marcha la aplicación de la Guía de Implementación de Seguridad de la Información basada en la Norma ISO/IEC 27001, se pudo comprobar una cierta mejoría en la seguridad de las aplicaciones de la institución, acompañada de cambios que se perciben como es el caso del incremento de políticas de seguridad, incremento en mayor número de control para monitorear anomalías en la información, la disminución de niveles de riesgos con respecto a los activos de información de la institución, y finalmente un incremento en programas de capacitación que dan conocimientos al personal en el uso de los sistemas de información , por todas estas características podríamos decir que se pudo contrastar la hipótesis que se planteó en su inicio al abordar el presente tema de investigación.

VI. CONCLUSIONES.

1. Con la Guía de Implementación, se logró incrementar el nivel de la seguridad en las aplicaciones informáticas de la institución policial, y esto se vio reflejado en el incremento de políticas de seguridad que fueron puestas en marcha que beneficiaron a la institución y ayudaron a incrementar el nivel de seguridad en la misma.

2. El uso de la Guía de Implementación, se logró mejorar el proceso para detectar las anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla y prevenir su mal uso y divulgación no adecuada que perjudiquen a la institución.

3. Con el Plan de tratamiento de Riesgos, se permitió la disminución de los niveles de riesgos con respecto a los activos de información, considerados amenazas y vulnerabilidades en la institución, esto manifestado en un plan adecuado para abordar estos riesgos, con mecanismos preventivos y correctivos, tomando las precauciones necesarias que minimicen los impactos respectivamente.

4. Con el Plan de Capacitación y Concienciación puesto en marcha en la Institución, se logró incrementar el conocimiento, y su vez mejorar el nivel de capacitación para el personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la institución, teniendo como resultado personal comprometido con la seguridad en favor de la institución.

VII. REFERENCIAS BIBLIOGRÁFICAS.

Antoni Lluís Mesquida, Antonia Mas, Esperança Amengual, (Clavijo 2008), Ignacio Cabestrero. Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001 REICIS Revista Española de Innovación, Calidad e Ingeniería del Software, vol. 6, núm. 3, noviembre, 2010, pp. 25-34, Asociación de Técnicos de Informática España.

Arturo Fernando Granados Rodríguez: Auditoria del Desarrollo de Sistemas de Información en el Gobierno Regional de Cajamarca. De la Universidad Privada del Norte. Año 2012.

Enrique Martín Méndez, Miguel Ángel Aguilar Proyecto Sanitas: Sistema de Gestión de Seguridad de la Información y certificación UNE 71502 e ISO 27001. Del Grupo Sanitas, Año 2006

Emigdio Antonio Alfaro Paredes: Metodología para la Auditoria Integral de la Gestión de la Tecnología de Información. De la Pontificia Universidad Católica del Perú. Año 2008.

Ana Pilar de Jesús Maco Chonate: 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 utilizando el software pilar2. De la Universidad Católica Santo Toribio de Mogrovejo. Año 2008.

Wolfgang BOEHMER. Cost-benefit trade-off analysis of an ISMS based on ISO 27001.IEEE. Año 2011.

Luis Gómez Fernández y Ana Andrés Álvarez Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.
2. ª edición © AENOR (Asociación Española de Normalización y Certificación), 2012

Carlos S. Álvarez C. La ley y la seguridad de la información: una perspectiva regional. ACIS. Año 2012.

Chi-Hsiang Wang. Integrated Installing ISO 9000 and ISO 27000 Management Systems on an Organization IEEE, Año 2010.

Burnett. Metodología de 8 etapas, et al. (2004) Ingeniería Industrial/ISSN 1815-5936/Vol. XXXIII/No. 3/septiembre-diciembre/2012/p. 260-271

Madelayne L. Vega García Las Auditorias de información en las organizaciones. 2001. Ciencias de la Información, vol. 37, núm. 2-3, mayo-diciembre, 2006, pp. 3-14.

Castellano Castellano, Diana. Auditorías de Sistemas Informáticos en la Empresa Minga S.A y su sucursal utilizando Cobit (Tesis de Titulación en Ingeniería Informática). Chicago: Universal S.A, 2009.
Ciro Antonio Dussan Clavijo Políticas de seguridad informática Entramado, vol. 2, núm. 1, pp. 86-92, Universidad Libre Colombia, 2004.

Marianella Villegas, Marina Meza, Pilar León Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática Télématique, vol. 10, núm. 1, enero-abril, 2011, pp. 1-16, Universidad Rafael Belloso Chacín Venezuela, 2006.

Soy i Aumatell. Metodología - Auditorias de los Sistemas de Información y las Tecnologías de la Información. (2003)

http://www.iso27001standard.com/es/

Barker, R. L. (1990). Information audits: Designing a methodology with reference to the R & D división of a pharmaceutical company. Occasional publications series no. 8 (pp. 5–34). Sheffield: Department of Information Studies, University of Sheffield.

Instituto de Información Científica y Tecnológica (IDICT). La Habana, Cuba
Dra. Gloria Ponjuan .LAS AUDITORÍAS DE INFORMACIÓN Y DEL CONOCIMIENTO Y SUS CONTEXTOS Facultad de Comunicación Universidad de La Habana. (2008)

VIII. ANEXOS.

Check-List sobre Políticas de Seguridad en la Institución Policial Comisaria del Norte PNP – Chiclayo. (Anexo N°1)

CHECK-LIST SOBRE POLITICAS DE SEGURIDAD			
Auditoria en Seguridad Informatica		Proceso: Norma ISO 27001	
EVALUACION DE POLITICAS DE SEGURIDAD	FECHA:		
Con el objetivo de evaluar politicas de seguridad informatica y de conocer, la percepcion de las personas entrevistadas en el Area de sistemas de informacion, se desea conocer sus opiniones evaluativas de esta actividad.			
Datos Generales:			
FECHA DE AUDITORIA	PROCESO AUDITADO	1. consideraciones 2. medidas, controles, normas, estandares de seguridad. 3. perido de vida de contraseñas 4. privilegio de informacion 5. cifrado de informacion	
NOMBRE DEL AUDITOR A EVALUAR			
NOMBRE DEL EVALUADOR			
PERFIL		FIRMA	
A continuacion encontrara una seria de preguntas cuya respuesta se debe señalar con una X en una escale de valores asi:			
PREGUNTAS		**SI**	**NO**
1. ¿existen, medidad, controles, procedimientos, normas y estandares de seguridad?			
2. ¿existe un documento donde este especificado la relacion de las funciones y obligaciones del personal?			
3. ¿existen procedimientos de notificacion y gestion de insidencias?			
4. ¿existen procedimientos de realizacion de copias de seguridad y recuperacion de datos?			
5. ¿existe una relacion del personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?			
6. ¿existe una relacion de controles periodicos a realizar para verificar el cumplimiento del documento?			
7. ¿existen medidad a adoptar cuando un soporte vaya hacer desecho o reutilizado?			
8. ¿existe una relacion del personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales?			
9. ¿existe una relacion de personal autorizado a acceder a los soportes de datos?			
10. ¿existe un periodo maximo de vida de las contraseñas?			
11. ¿existe una relacion de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos?			
12. ¿los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encaminadas, las cuales a su vez se encuentran o deben estar documentadas en el documento de seguridad?			
13 ¿hay dadas de alta en el sistema cuentas de usuarios genericas, es decir utilizadas por mas de una persona no permitiendo por tanto la identificacion de la persona fisica que las ha utilizado?			
14 ¿en la practica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el documento de seguridad?			
15 ¿el sistema de autenticacion de usuarios guarda las contraseñas encriptadas?			
16 ¿en el sistema estan habilitadas para todas las cuentas de usuario las opciones que permiten establecer: un numero maximo de intentos de conexión. un periodo maximo de vigencia para contraseña			
17 ¿existen procedimientos de asignacion y distribucion de contraseñas?			

Chick-List sobre Gestión de Activos en la Institución Policial Comisaria del Norte PNP – Chiclayo. (Anexo N°2)

CHECK-LIST SOBRE GESTION DE ACTIVOS INFORMATICOS			
Auditoria en Seguridad Informatica		Proceso: Norma ISO 27001	
EVALUACION DE POLITICAS DE SEGURIDAD	FECHA:		
Con el objetivo de evaluar politicas de seguridad informatica y de conocer, la percepcion de las personas entrevistadas en el Area de sistemas			
informacion, se desea conocer sus opiniones evaluativas de esta actividad.			
Datos Generales:			
FECHA DE AUDITORIA	PROCESO AUDITADO	1. inventario de soporte de actualizaciones 2. registro de actualizacion de entrada o salida 3. copias de seguridad y recuperacion de datos 4. almacenamiento de contraseñas 5. almacenamientos de copias de seguridad y	
NOMBRE DEL AUDITOR A EVALUAR			
NOMBRE DEL EVALUADOR			
PERFIL		FIRMA	
A continuacion encontrara una seria de preguntas cuya respuesta se debe señalar con una X en una escale de valores asi:			

PREGUNTAS	SI	NO
1. ¿existe control sobre el acceso fisico a las copias de seguridad?		
2. ¿existe un inventario de los recursos informaticos existentes?		
3. ¿dicho inventario incluye las copias de seguridad?		
4. ¿las copias de seguridad, o cualquier otro soporte se almacena fuera de la instalacion?		
5. ¿existe procedimientos de actualizacion de dicho inventario?		
6. ¿existen procedimientos de etiquetado e identificacion de los soportes informaticos?		
7. ¿existen procedimientos en relacion con la salida de soporte fuera de su alamacenamiento habitual?		
8. ¿existen estandares de distribucion y envio de estos soportes?		
9. ¿se tiene un documento que especifique los archivos que se envian fuera de la empresa?		
10. ¿existen controles para detectar la existencia de soporte recibido/enviados?		
11. ¿se realiza envios de soporte fuera de la empresa, con ficheros de nivel alto?		
12. ¿existen procedimientos para la realizacion de copias de seguridad		
13¿existen controles sobre el acceso fisico a las copias de seguridad?		
14 ¿hay dadas de alta en el sistema cuentas de usuarios genericas, es decir utilizadas por mas de una persona		
no permitiendo por tanto la identificacion de la persona fisica que las ha utilizado?		
14 ¿existe una politica para desechar un recurso con informacion importante?		
15 ¿existe algun programa que permita gestionar y almacenar claves secretas?		
16 ¿las contraseñas estan almacenadas en alguna carpeta compartida en red?		
17¿las contraseñas de usuarios estan almacenadas en algun fichero de claves?		
18¿existe algun estandar para etiquetar los soporte de datos?		
19¿existe un orden logico en el almacenamiento de soporte de datos?		
20.¿existe una estructura para crear una nueva cuneta de usuario?		
21¿hay en el sistema cuentas de usuarios genericas, usadas por mas de una persona		
22¿en el sistema hay o estan habilitadas para todas las cuentas de usuarios, las opciones que permiten establecer:		
un numero maximo de intentos de conexión, un perido maximo de vigencia en las contraseñas.		

ENTREVISTA 01 (Anexo N°3)

UNIVERSIDAD CATÓLICA
SANTO TORIBIO DE MOGROVEJO

Entrevista dirigido al Jefe del Dpto. de Denuncias de la Comisaría del Norte- Chiclayo.

Objetivo: determinar los niveles de conocimientos en el encargado del Dpto. de Denuncias a cerca de mecanismos, maneras, formas, y políticas de seguridad en las aplicaciones informáticas de la comisaria.

Fuente: cuestionario creado por Alcántara Flores Julio Cesar.

1. ¿Qué tan importantes cree Ud. Que sean los mecanismos de seguridad en las aplicaciones informáticas que usa la comisaria?

2. ¿Conoce de niveles y riesgos en el uso y funcionamiento de las aplicaciones con las que cuenta la comisaria?

3. ¿cree Ud. Que sea importante charlas, capacitaciones orientadas a motivar la psicología en el personal orientadas a la seguridad en los recurso de hardware y software de la comisaria?

4. ¿Conoce acerca de alguna Política de seguridad que se haya implantado en la comisaría en el uso de las aplicaciones informáticas?

5. ¿Qué tan a menudo se presenta la frecuencia o índice de errores en el uso de las aplicaciones informáticas de la comisaria?

6. ¿Realizan sistemáticamente copias de seguridad o buckups como formas de protección y seguridad en los datos o la información que se maneja en la institución?

7. Se realiza un análisis adecuado de riesgos, sabiendo que se podrían dar en la organización.

8. Entre estos tipos de riesgos que le mencionare a continuación, con que factor o ponderación los podría relacionar como: Alto, Medio, Bajo. como por ejemplo:

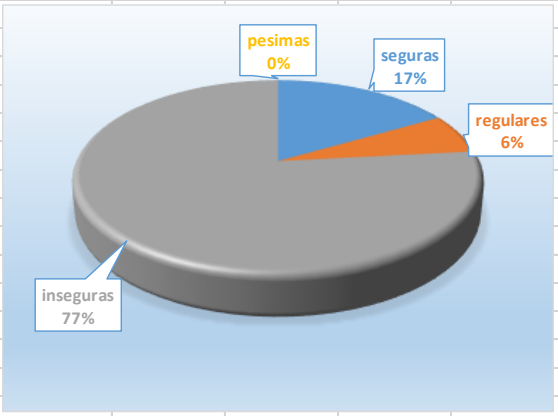
TIPO DE RIESGO	FACTOR
Robo de hardware	
Robo de información	
Vandalismo	
Fallas en los equipos	
Virus informáticos	
Equivocaciones	
Accesos no Autorizados	
Fraude	
Fuegos	
Terremotos	

9. Que estrategias de seguridad conoce que se pueden tomar en cuenta para proteger y garantizar la seguridad en las aplicaciones y la información.

Tabulación de las Encuestas / Pre-Test (Anexo N°4)

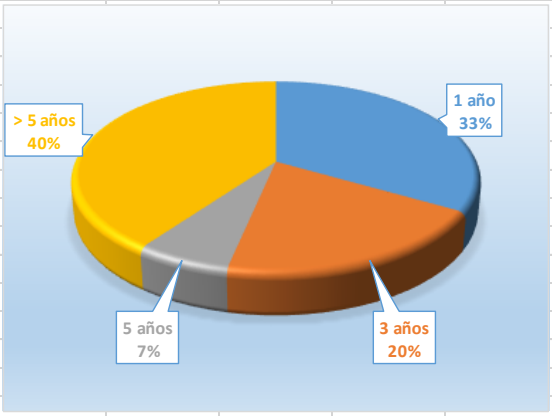
1. ¿Que nivel de seguridad, tienen las aplicaciones que se usan en los equipos de la institucion policial? (%)

	Items	N° Enc	Total en %
A	seguras	5	17
B	regulares	2	7
C	inseguras	23	76
D	pesimas	0	0
	TOTAL	**30**	**100**



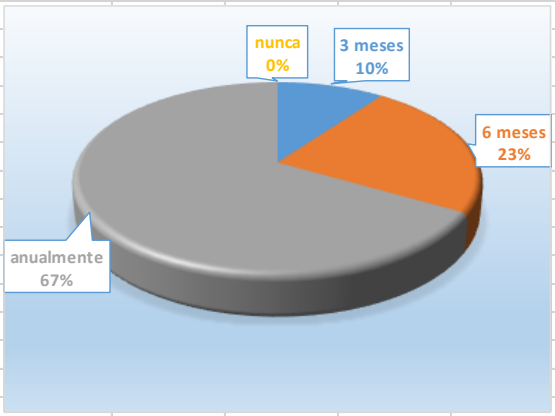
2. ¿Qué tiempo de uso tienen las aplicaciones con los que cuentan los equipos de computo de la institucion? (%)

	Items	N° Enc	Total en %
A	1 año	10	33
B	3 años	6	20
C	5 años	2	7
D	> 5 años	12	40
	TOTAL	**30**	**100**



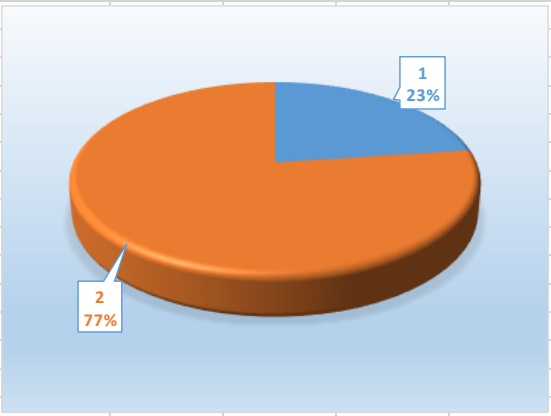
3. ¿con que frecuencia se realiza el mantenimiento de los equipos de computo de la institucion? (%)

	Items	N° Enc	Total en %
A	3 meses	3	10
B	6 meses	7	23
C	anualmente	20	67
D	nunca	0	0
	TOTAL	**30**	**100**



4. ¿se realizan capacitaciones al personal en el uso adecuado de las nuevas tecnologias y aplicaciones informaticas? (%)

	Items	N° Enc	Total en %
A	Si	8	27
B	No	22	73
	TOTAL	**30**	**100**

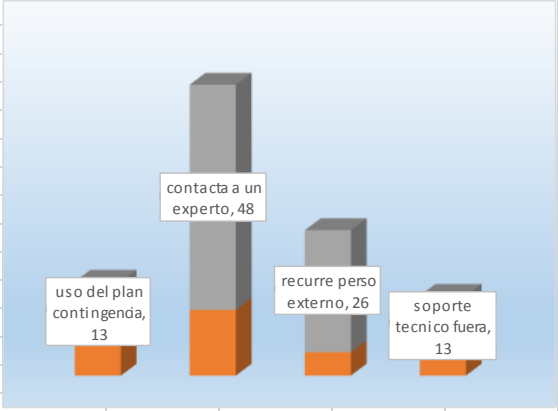


5. ¿Qué mecanismos de seguridad se utilizan en los equipos de computo de la institucion? (%)

	Items	N° Enc	Total en %
A	antivirus	27	90
B	polit segurid	1	3
C	acceso rem	0	0
D	plan de cont	0	0
E	cop segurid	2	7
	TOTAL	**30**	**100**

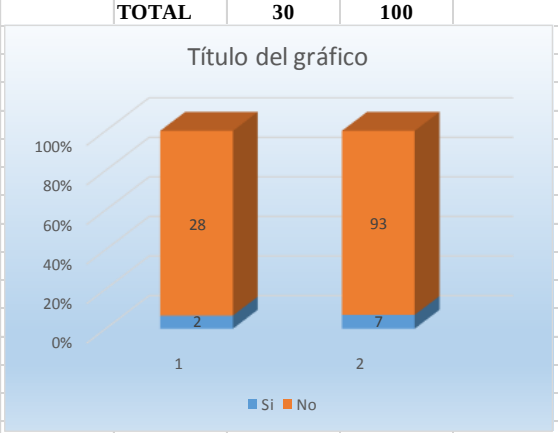
6 ¿Qué acciones se toman en cuenta, frente a posibles problemas que se pueden presentar en las aplicaciones y equipos? (%)

	Items	N° Enc	Total en %
A	uso del plan contingencia	7	13
B	contacta a un experto	14	48
C	recurre perso externo	5	26
D	soporte tecnico fuera	4	13
	TOTAL	**30**	**100**



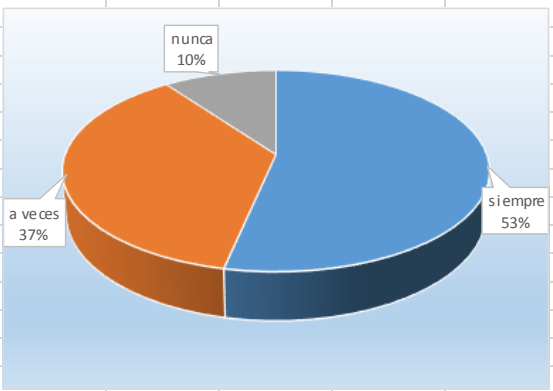
7. ¿Conoce de algunas politicas de seguridad, estrategias, y niveles de riesgos que puedan afectar a la institucion? (%)

	Items	N° Enc	Total en %
A	Si	2	7
B	No	28	93
	TOTAL	**30**	**100**



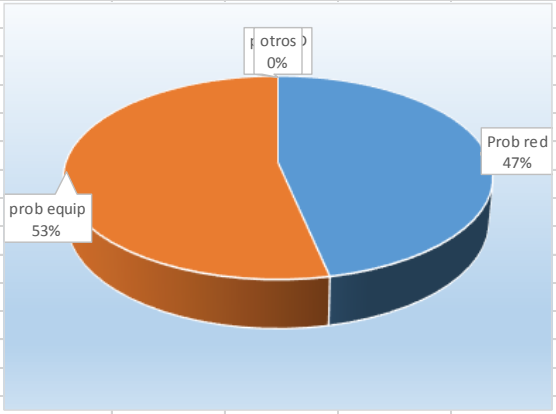
8. ¿cuan a menudo sulen presentarse fallas e inconvenientes en los sistemas informaticos o problemas tecnicos puntuales?

	Items	N° Enc	Total en %
A	siempre	16	53
B	a veces	11	37
C	nunca	3	10
	TOTAL	**30**	**100**



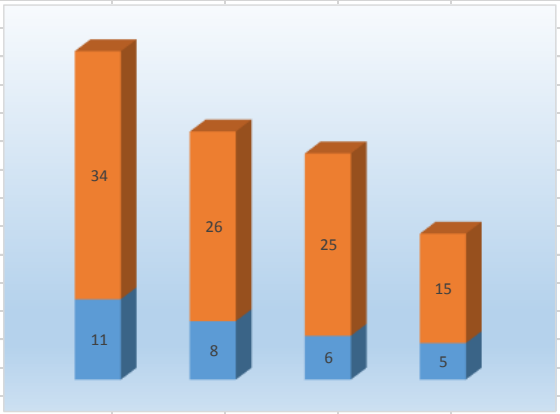
9. ¿A que cree que se deban las fallas e inconvenientes en los sistemas informaticos que se suelen presentar?

	Items	N° Enc	Total en %
A	Prob red	14	47
B	prob equip	16	53
C	prob BD	0	0
D	otros	0	0
	TOTAL	**30**	**100**



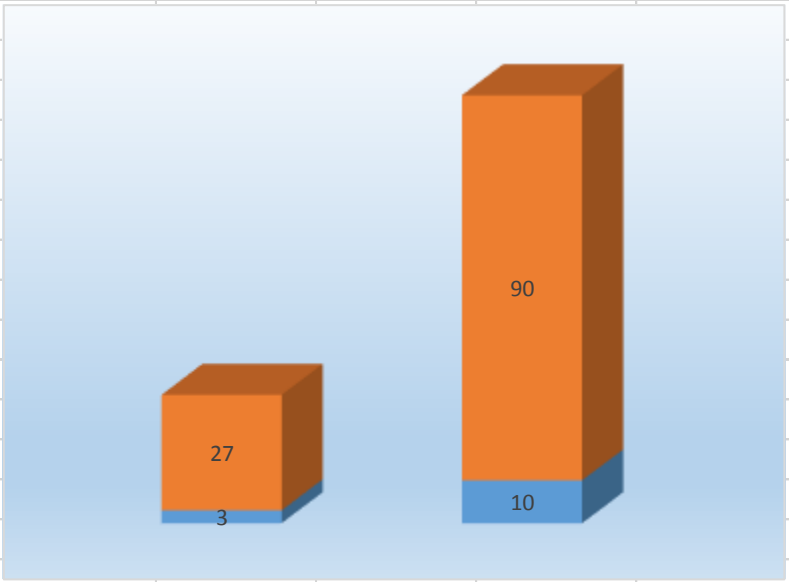
10. ¿Qué controles son tomados en cuenta para proteger la informacion de la institucion?

	Items	N° Enc	Total en %
A	C.accesos	11	34
B	permisos	8	26
C	P. autorizado	6	25
D	otros	5	15
	TOTAL	**30**	**100**



11. ¿su utilizan controles para detectar anomalias en la seguridad de la institucion?

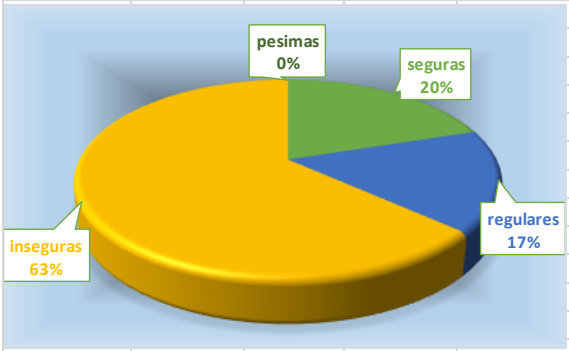
	Items	N° Enc	Total en %
A	Si	3	10
B	No	27	90
	TOTAL	**30**	**100**



Tabulación de las Encuestas / Post-Test (Anexo N°5)

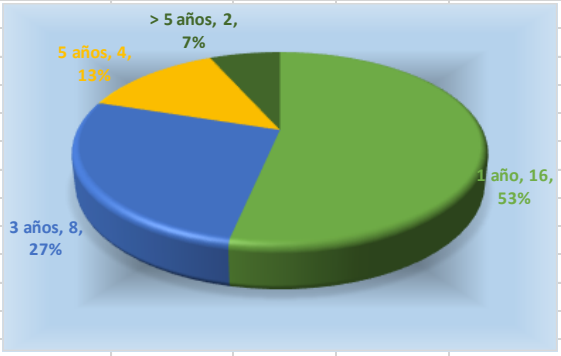
1. ¿Que nivel de seguridad, tienen las aplicaciones que se usan en los equipos de la institucion policial? (%)

	Items	N° Enc	Total en %
A	seguras	6	20
B	regulares	5	17
C	inseguras	19	63
D	pesimas	0	0
	TOTAL	**30**	**100**



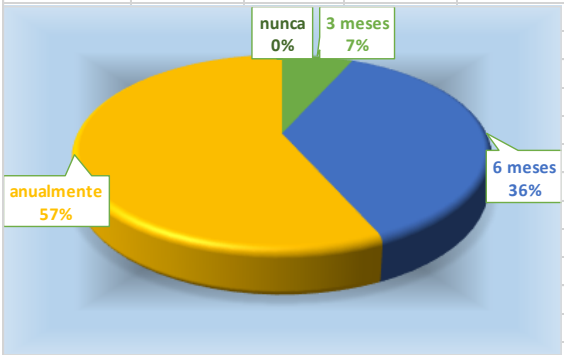
2. ¿Qué tiempo de uso tienen las aplicaciones con los que cuentan los equipos de computo de la institucion? (%)

	Items	N° Enc	Total en %
A	1 año	16	53
B	3 años	8	27
C	5 años	4	13
D	> 5 años	2	7
	TOTAL	**30**	**100**



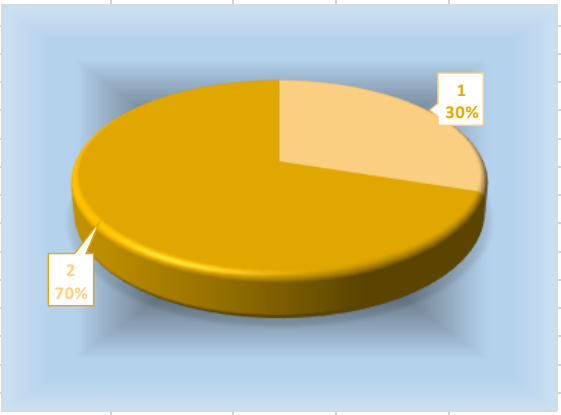
3. ¿con que frecuencia se realiza el mantenimiento de los equipos de computo de la institucion? (%)

	Items	N° Enc	Total en %
A	3 meses	2	7
B	6 meses	11	36
C	anualmente	17	57
D	nunca	0	0
	TOTAL	**30**	**100**



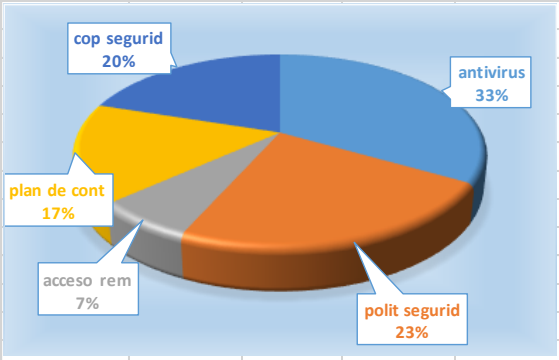
4. ¿se realizan capacitaciones al personal en el uso adecuado de las nuevas tecnologias y aplicaciones informaticas? (%)

	Items	N° Enc	Total en %
A	Si	9	30
B	No	21	70
	TOTAL	**30**	**100**



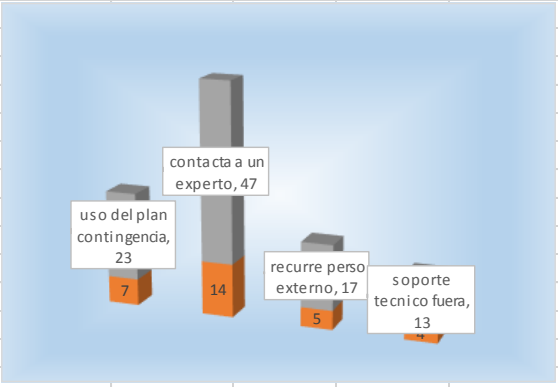
5. ¿Qué mecanismos de seguridad se utilizan en los equipos de computo de la institucion? (%)

	Items	N° Enc	Total en %
A	antivirus	10	33
B	polit segurid	7	23
C	acceso rem	2	7
D	plan de cont	5	17
E	cop segurid	6	20
	TOTAL	**30**	**100**



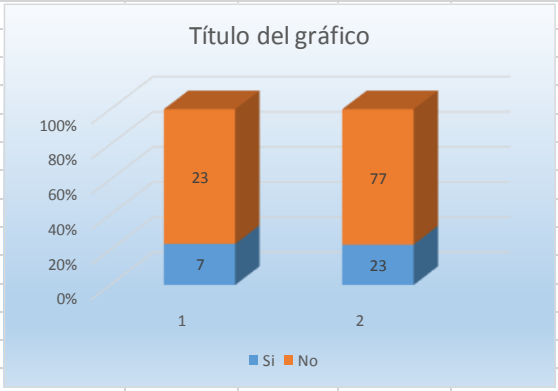
6 ¿Qué acciones se toman en cuenta, frente a posibles problemas que se pueden presentar en las aplicaciones y equipos? (%)

	Items	N° Enc	Total en %
A	uso del plan contingencia	7	23
B	contacta a un experto	14	47
C	recurre perso externo	5	17
D	soporte tecnico fuera	4	13
	TOTAL	**30**	**100**



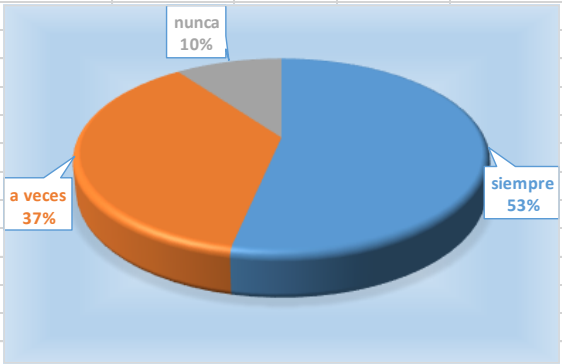
7. ¿Conoce de algunas politicas de seguridad, estrategias, y niveles de riesgos que puedan afectar a la institucion? (%)

	Items	N° Enc	Total en %
A	Si	7	23
B	No	23	77
	TOTAL	**30**	**100**



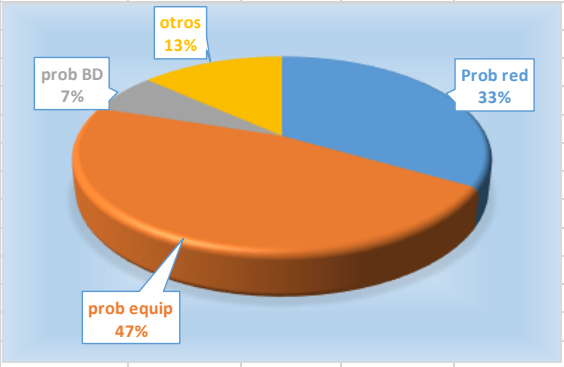
8. ¿cuan a menudo sulen presentarse fallas e inconvenientes en los sistemas informaticos o problemas tecnicos puntuales?

	Items	N° Enc	Total en %
A	siempre	16	53
B	a veces	11	37
C	nunca	3	10
	TOTAL	**30**	**100**



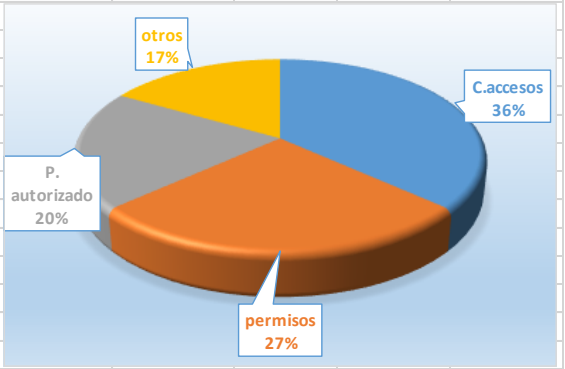
9. ¿A que cree que se deban las fallas e inconvenientes en los sistemas informaticos que se suelen presentar?

	Items	N° Enc	Total en %
A	Prob red	10	33
B	prob equip	14	47
C	prob BD	2	7
D	otros	4	13
	TOTAL	**30**	**100**



10. ¿Qué controles son tomados en cuenta para proteger la informacion de la institucion?

	Items	N° Enc	Total en %
A	C.accesos	11	37
B	permisos	8	27
C	P. autorizado	6	20
D	otros	5	16
	TOTAL	**30**	**100**



11. ¿su utilizan controles para detectar anomalias en la seguridad de la institucion?

	Items	N° Enc	Total en %
A	Si	4	14
B	No	26	86
	TOTAL	**30**	**100**