UNIVERSIDAD AUTÓNOMA DE ICA

FACULTAD DE INGENIERÍA, CIENCIAS Y ADMINISTRACIÓN

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS

TESIS:

FORMULACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 17799 PARA LA GESTION DE LA INFORMACION DE LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL EN CHINCHA EN EL AÑO 2018

TESIS DESARROLLADA PARA OPTAR EL TITULO

PROFESIONAL DE INGENIERA DE SISTEMAS

LÍNEA DE INVESTIGACIÓN

NORMAS Y ESTÁNDARES

PRESENTADO POR:

ORÉ CRISÓSTOMO, WHENDY RUBY

DOCENTE ASESOR:

DR. ARMANDO JOSÉ MORENO HEREDIA

CÓDIGO ORCID N°0000-0002-6564-3344

CHINCHA, 2020

DEDICATORIA

La siguiente tesis está dedicada en primer lugar a Dios quien me ha dado las fuerzas para continuar con este camino universitario tan largo, a mis padres Richard Wilmer Oré Paredes y Heidy Liz Crisóstomo Villa que sin su consejo y apoyo no podría ser el tipo de persona que soy hoy en día, a las personas que llegaron a mi vida, y me apoyan constantemente con mucho amor, todo ello me llevó a poder alcanzar muchos de los objetivos de mi vida, los que ya he conseguido y los que están por conseguir.

Whendy Ruby Oré Crisóstomo

AGRADECIMIENTO

A mis padres por instarme día a día y que a pesar de mis errores siempre me han apoyado, a mis hermanos que siempre han estado alentándome en los momentos difíciles, a todas las personas que han pasado por mi vida y las enseñanzas que me han dejado, a los docentes que, con su perseverancia y dedicación, me han ayudado a formar profesionalmente.

Whendy Ruby Oré Crisóstomo

INDICE

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

RESUMEN

En la estructura de la organización del área informática y control de activos TI la seguridad, es esencial para el correcto desarrollo de una entidad u organización, y llevarla a cabo es algo nuevo en nuestro país.

La metodología expuesta en este trabajo, idea planear, incurriendo en formular políticas para lograr una correcta estructura de organización y gestión de Activos TI por medio de la estimación en riesgos de TI.

ABSTRACT

In the organization structure of the IT area and IT asset control, security is essential for the proper development of an entity or organization, and carrying it out is something new in our country.

The methodology presented in this work, planning idea, incurring in formulating policies to achieve a correct structure of organization and management of IT Assets through the estimation of IT risks.

INTRODUCCIÓN

La innovación de tecnología de la mayoría de organizaciones, muy distinto al rubro al que ellos se dediquen, ha venido ejecutándose en la mayoría de ocasiones con un control en nivel incorrecto y esto ha provocado que en la actualidad la mayoría de empresas no conozcan la forma de cómo se ha estructurado su área informáica, de igual manera también desconoce de la cantidad, sus características y los estados de sus diversos activos informático, y esta situación genera un alto riesgo de desaprovechar los mismos.

Por este motivo la presente tesis nos apoyará a la formulación de lineamientos en general para una buena estructura de organización y un correcto tratamiento de riesgos incluidos en un ámbito de TI, reconociendo sus posibles vulnerabilidades y amenazas. Así mismo mientras se desarrolla e implementa este método, se facilitará a las organizaciones cumpli con lo que se norma por la ONGEI con relación al tema de implementar la NTP ISO/IEC 17799, particularmente en este caso de dominios de control llamados a la Estructura de Organización y a la Clasificación y Control en activos.

CAPÍTULO I

ASPECTO INFORMATIVO

1.1. ASPECTOS ORGANIZACIONALES

1.1.1. DESCRIPCIÓN DE LA ORGANIZACIÓN

La Unidad de Gestión Educativa Local de Chincha, es la encargada de garantizarnos el servicio de educación con una calidad en todos los niveles o modalidades que haya en el sistema de educación del país.

Actualmente su representante es el señor Aristedes Gonzales Zagaceta identificado con DNI 21829597.

La UGEL Chincha cuenta con 8 áreas a disposición de cada proceso que se requiera.

DATOS DE LA ENTIDAD

- **Número de RUC:** 20410275849 – LA UNIDAD DE GESTION EDUCATIVA DE CHINCHA – UNIDAD EJECUTORA 301
- **Tipo Contribuyente:** INSTITUCIONES PUBLICAS.
- **Fecha de Inscripción:** 20/01/2000
- **Estado del Contribuyente:** ACTIVO
- **Condición del Contribuyente:** HABIDO
- **Dirección:** AV. BENAVIDES NRO. 207 ICA - CHINCHA - CHINCHA ALTA
- **Actividad Económica:** Principal – CIIU 80904 – EDUCACION DE ADULTOS Y OTROS.

Ubicación

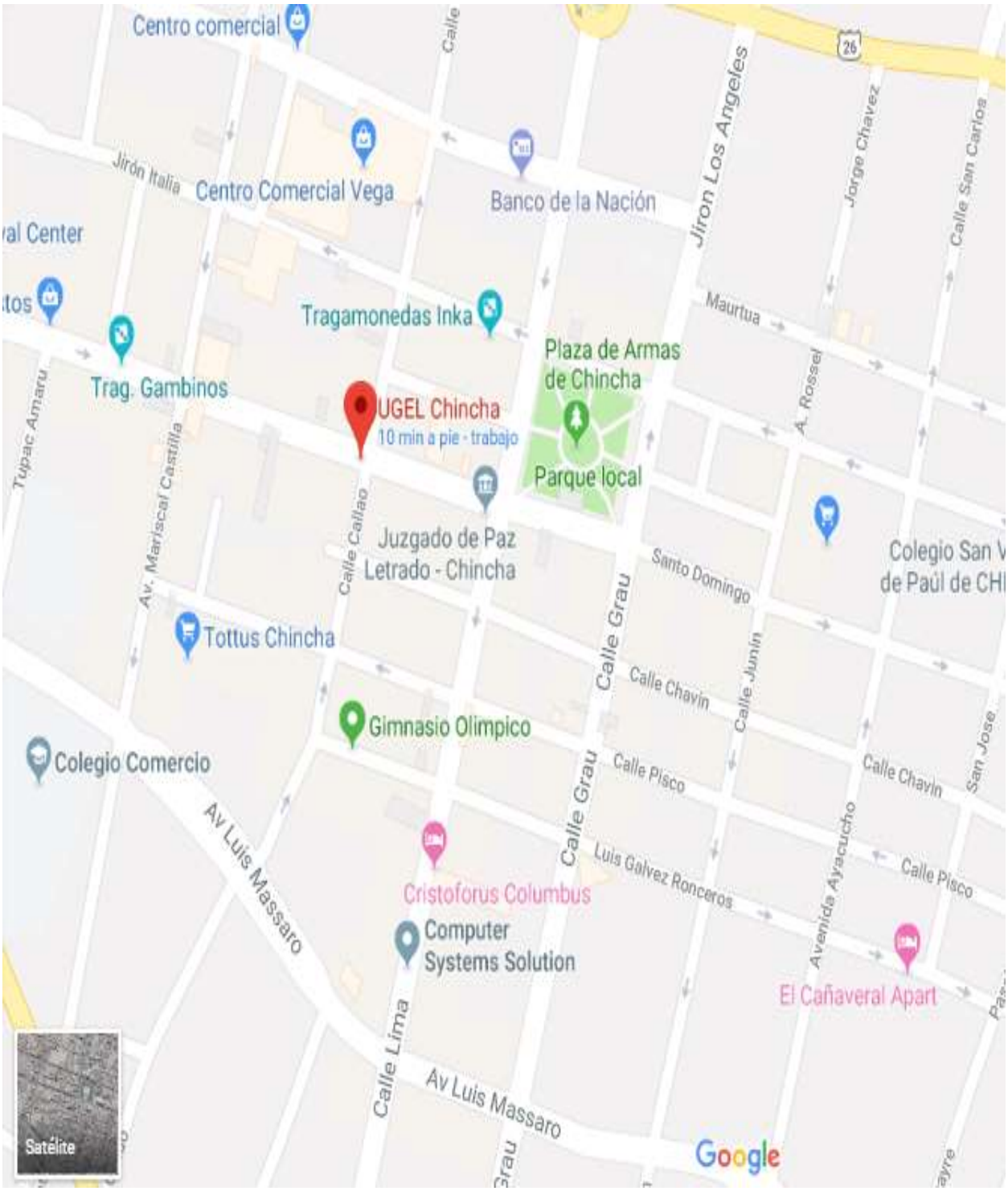


Imagen 1: Mapa de la Ubicación de la UGEL Chincha

FUENTE: G. MAPS

1.1.2. ESTRUCTURA ORGÁNICA

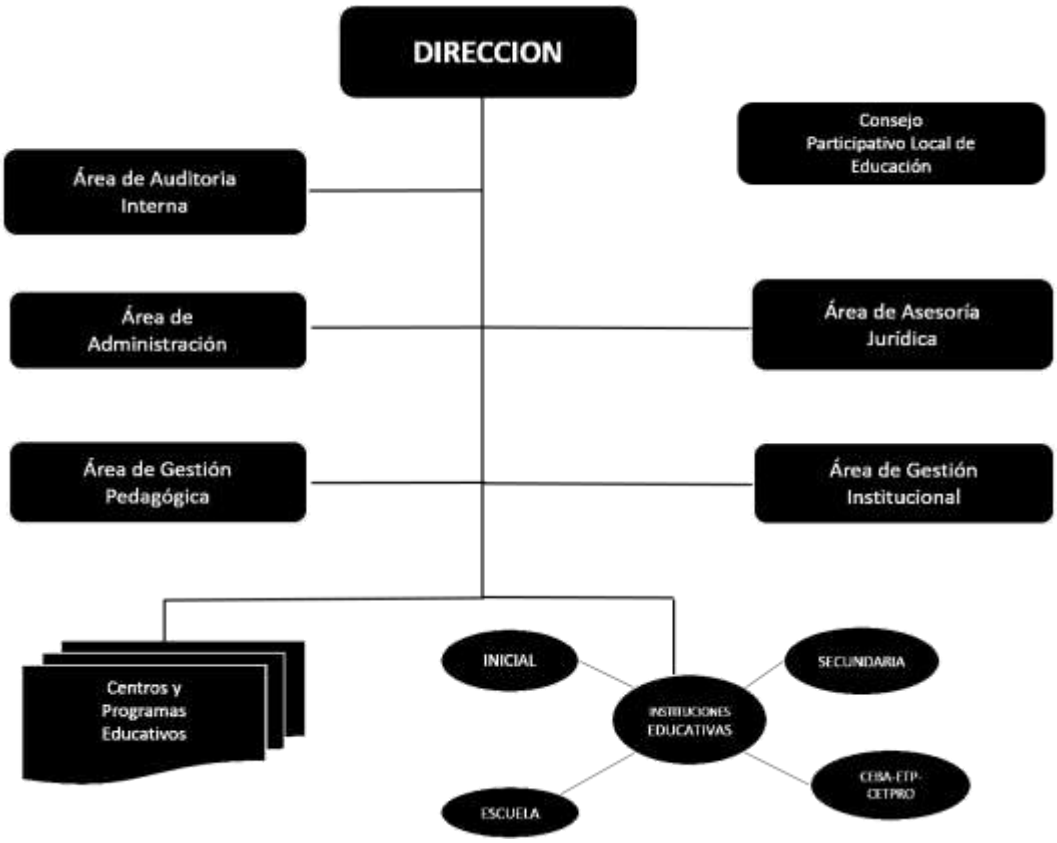


Imagen 2: Organigrama de la UGEL Chincha

FUENTE: Ugel Chincha

1.1.3. FACTORES ESTRATÉGICOS

1.1.3.1. VISIÓN

La Unidad de Gestión Educativa Local de Chincha, tiene por visión al 2021 alcanzar el nivel de competitividad y modernización, brindando servicio de calidad a las instituciones educativas públicas y privadas, y con ella Contar con una Educación Básica Regular de calidad, que incorpore y articule los niveles de inicial, primaria y secundaria , sustentada en valores de solidaridad y respeto a los derechos humanos y medio ambiente, integrando la cultura y el deporte, estrechamente vinculada con el desarrollo de la ciencia y mejora de los aprendizaje. (Unidad de Gestión Educativa Local [UGEL], 2016).

1.1.3.2. MISIÓN

Fomentar el desarrollo y formación integral de los niños, adolescentes y jóvenes adultos, en el logro de sus aprendizaje, asegurando la oferta del servicio educativo de calidad con participación de las Instituciones Públicas y Privadas que brinden formación integral y permanente al educando, sustentado a una cultura de valores que favorezca el desarrollo de sus capacidades, que le permita condiciones para el desarrollo social y emocional mediante la ciencia la tecnología, cultura y deporte, con una implementación de la infraestructura adecuada y pertinente en las Instituciones Educativas. (Unidad de Gestión Educativa Local [UGEL], 2016).

1.1.4. ANÁLISIS FODA

FORTALEZAS - Personal con experiencia en la administración. - Acceso a Internet, que permite la trasmisión de los logros y avances.	**DEBILIDADES** - Falta de espacio físico para el archivo de documentos que generan las diferentes oficinas de la UGEL. - Personal no capacitado en el Sistema de Trámite Documentario.
OPORTUNIDADES - Convenios con grandes entidades de apoyo a la educación, para capacitar al personal. - Las nuevas tecnologías que salen al mercado.	**AMENAZAS** - Incremento de la Competencia. - Actitudes negativas por parte de personal de área.

TABLA 1: Análisis FODA de la UGEL Chincha

FUENTE: Elaboración Propia

CAPÍTULO II

ANALISIS DE LA INVESTIGACIÓN

2.1. SITUACIÓN PROBLEMÁTICA

La Unidad de Gestión Educativa Local ubicada en Chincha Alta, tiene en su equipo de personal de informática que actualmente labora dentro de la entidad está conformado por un especialista; el cual tiene a cargo muchas funciones referidad al mantenimiento y soporte tecnológico, al desarrollo de los sistemas en infomación, a la administración de base de datos, también a la administración de redes, y por esta razón se ha visto necesario formular políticas para los recursos y habilidades informáticas.

Las Políticas de Seguridad Informática tiene como objetivo el de establecer medidas de manera técnica y organizacionales que son necesarias para poder garantizar la seguridad de TI (redes, equipos de cómputo o sistemas) y también a las personas que interactúan y usan los servicios que se asocian entre ellos y están aplicados a los usuarios de sistemas ed la Ugel-Chincha.

Las Políticas de Seguridad Informática se han fundamentado en base a la norma ISO/IEC 17799, se han planteado, analizado, y revisado con el objetivo de ofrecer garantía l usuario y esta se está mostrando de buena manera para resguardar los sistemas con seguridad, siempre manteniendo el respeto por los reglamentos y estatutos de la Ugel.

Esta Política de Seguridad Informática se aplicará a los empleados, usuarios externos o terceros, contratados y toda persona que tenga un equipo vinculado a la red de la empresa.

2.2. PROBLEMA

2.2.1. PROBLEMA PRINCIPAL

¿La formulación de Políticas de Seguridad Informática influirá en la gestión de información de la Unidad de Gestión Educativa Local de Chincha?

2.2.2. PROBLEMAS ESPECÍFICOS

- ¿La formulación de Políticas de Seguridad Informática permitirá la realización de un inventario de activos en la Gestión de la Información de la Unidad de Gestión Educativa Local de Chincha?
- ¿La formulación de Políticas de Seguridad Informática permitirá la elaboración de un plan de protección en la Gestión de la Información de la Unidad de Gestión Educativa Local de Chincha?
- ¿La formulación de Políticas de Seguridad Informática permitirá la ejecución de análisis en riesgos en la Gestión de la Información de la Unidad de Gestión Educativa Local de Chincha?

2.3. HIPÓTESIS

2.3.1. HIPÓTESIS GENERAL

La formulación de políticas de seguridad informática contribuye a la gestión de la información en la Unidad de Gestión Educativa Local de Chincha.

2.3.2. HIPÓTESIS ESPECÍFICAS

- La formulación de Políticas de Seguridad Informática permite la realización de un inventario de activos en la gestión de la Información de la Unidad de Gestión Educativa Local de Chincha.

- La formulación de Políticas de Seguridad Informática permite la elaboración de un plan de protección en la gestión de la Información de la Unidad de Gestión Educativa Local de Chincha.

- La formulación de Políticas de Seguridad Informática permite la rejecución de análisis de riesgos en la gestión de la Información de la Unidad de Gestión Educativa Local de Chincha

2.4. OBJETIVOS

2.4.1. OBJETIVO GENERAL

Formular Políticas de Seguridad Informática para mejorar la Gestión de la Información de la Unidad de Gestión Educativa Local de Chincha

2.4.2. OBJETIVOS ESPECÍFICOS

- Realizar un inventario de activos identificando los controles de seguridad en la gestión de la información de la Unidad de Gestión Educativa Local de Chincha a través de la Formulación de Políticas de Seguridad Informática.
- Elaborar un plan de protección adecuado para la gestión de la Información de la Unidad de Gestión Educativa Local de Chincha a través de la Formulación de Políticas de Seguridad Informática.

- Realizar un análisis de riesgos a los que se expone en la gestión de la Información de la Unidad de Gestión Educativa Local de Chincha, a través de la Formulación de Políticas de Seguridad Informática.

2.5. JUSTIFICACIÓN E IMPORTANCIA

La justificación consiste, en considerar que se necesita que toda institución tiene que contar con una Política de Seguridad Informática, la cual nos servirá para poder administrar toda la información podible, y podremos garantizar muchos aspectos de confidencialidad, disponibilidad e integrad que deberían de cumplirse.

En linas generales, esta investigación es de mucha importancia ya que la información de toda empresa es el activo que más valor tiene, y por este motivo debemos darle prioridad e implementar las Políticas que se formularán más adelante.

2.6. TIPO Y NIVEL DE LA INVESTIGACIÓN

La investigación que se va a realizar es de tipo Tecnológico Aplicada Formal, ya que nos hemos planteado la necesidad de hallar efectividad en una gestión de información que se basa a formular Políticas de Seguridad Informática según todos los estándares que se acepten nde manera nacional o internacional ya sea el caso de la NTP-ISO/IEC17799.

CAPÍTULO III
MARCO TEÓRICO

3. BASES TEÓRICAS

3.1. ANALISIS DE RIESGOS

Analizar y Gestionar riesgos nos da un enfoque para poder identificar diversos factores dentro de la empresa, esto hace que haya una alteración a la seguridad de la organización. Por este motivo es de suma importancia que se establezcan medidad de seguridad que nos permita la reducción de pérdidas de activos en información.

EXPOSICIÓN A RIESGOS

Se debedeterminar el nivel de exposición de cada proceso que se haya podido identificar.

FORMAS DE ESTIMACIÓN DE PROBABILIDAD DE PÉRDIDA

- Disposición del personal de informática.
- Calibrar objetivos mefiante involucrados.

3.2. CONTROL INTERNO

Podemos decir que el control interno parte de la necesidad de poder evaluar la eficiencia , razón, oprtunidades, confiabilidad en proteger, salvaguardar y también ofrecer seguridad de los recursos de una organización, también nos podrá ayudar a dar control al desarrollo de actividades o resultados que desean tener al desempeñar sus funciones en la empresa.

Este Control se adquiere partiendo de los objetivos de la organización.

Entonces podríamos asumir que el objetivo principal del control, es, cuidar el mantenimiento de cualquier organización y ayudar a su desarrollo, implementar, y aplicar al interior de la organización.

3.3. POLÍTICA DE SEGURIDAD

Las políticas de seguridad están dirigidas primordialmente al personal interno de la organización, en algunas ocasiones también personas externas quedan sujetas a estas políticas.

Proponer o idetificar la Políticas de Seguridad Informática necesita un compromiso con la empesa, observar bien las debilidades y ser constante para la renovación y actualización de la Política con respecto a deinir la empresa moderna.

La mayoría de las empresas han documentado y recomendado orientar en usar adecuadamente los recursos tecnológicos para sacar provecho y no ocasionar problemas en los activos de las empresas.

En tal sentido, la Política de Seguridad Informática, nos sirve como herramienta para dar conciencia a todos los usuarios de la empresa sobre cuan importante y sensible es la información de la misma.

Las Políticas de Seguridad informática nos enfoca y da a conocer muchas normas, reglas y procedimientos que debemos seguir y aplicar, y también nos indica las medidas que se deben aplicar para dar protección al sistema.

La Política de Seguridad Informática, deben explicarnos comprensiblemente sobre las decisiones que se han de tomar y también explicar su importancia.

También es importante que las Políticas se establezcan o formulan de una manera sencilla y comprensible sin caer en la exageración o la ambigüedad.

Por último, estas Políticas deben actualizarse periódicamente en base a los cambios que haya en la organización.

OBJETIVO:

Las Políticas de Seguridad tienen como objetivo la protección de la información asegurando la confidencialidad, disponibildad e integridad en los sistemas de instalaciones de cómputo, redes, etc.

DEFINICIONES DE LA PSI:

Algunas de las definiciones se tienen:

- La PSI se puede definir como conjunto de requerimientos que se definen por los autores reponsables de los sistemas, en líneas generales lo que se permite y no se permite en el ámbito de seguridad mientras se opera el sistema.

- La PSI se puede definir como una manera de establecer comunicación con los empleados o usuarios, ya que estos son los canalizadores formales para poder actuar con respecto a los servicios de informática que nos ofrece la empresa u organización.

- La norma o estándar ISACA también lo define como establecer intención en nivel alto y esto nos da la seguridad a los servicios o sistemas informático y de esta manera establecer las responsabilidades dentro de la organización.

Resumiendo podríamos definirlo como un conjunto que contiene la aplicación de reglas a cada actividad que se relacione con el uso de la información en la empresa, sin descuidar nuestro objetivo de dar protección a la información, y su reputación.

ELEMENTOS DE LA PSI:

- Alcance
- Objetivos
- Responsabilidades de servicios.
- Requerimientos
- Definición de sanciones
- Responsabilidad para los usuarios.

La Política de Seguridad Informática, debe explicar comprensiblemente sobre el motivo de tomar algunas decisiones y dar explicaciones sobre su importancia.También deben designar lo que la empresa tiene como expectativas con respecto a la seguridad y establecer la persona reponsable para dar seguimiento de cumplimientos y sanciones.

Es importante decir también, que esta Política de Seguridad debe actualizarse periódicamente para que siempre vaya acorde con los cambios o mejor que se apliquen a la empresa pero para todo esto se debe realizar un proceso que este estandarizado, y definirlo con un lenguaje sencillo y que sea entendible y manejable ni con términos ambiguos, sin caer en la exageración de la precisión.

PROPÓSITO:

La Política de Seguridad Informática tiene como propósito cuidar la información de la empresa y sus activos. Estas Políticas son una guía para asegurarnos proteger y tener en integridad los datos de los distintos recursos informáticos.

3.4. ISO 17799

Es recomendable usar este ISO en las áreas a analizar, es por ello que más adelante se aplicará la metodología presente con el objetivo de formular las Políticas de Seguridad Informática.

En toda empresa que tenga implementada recursos de tecnología de información es recomendable la implementación de buenas prácticas para dar seguridad, pues en la mayoría de veces cuando no se sigue un proceso para implementarlo adecuadamanete como nos indica la norma ISO 17799 pueden haber vacíos ya que es muy complejo esta o los procesos en la empresa u organización y esta situación puede generar el aumento de riesgos en los activos de información.

La seguridad tiene como objetivo brindarnos y asegurarnos la continuidad de todo operación que se realice dentro de la organización, tener una mínima cantidad de daños que nos haya procado unna contingencia, y asegurarnos una óptima inversión en la seguridad y sus tecnologías.

Como toda norma estandarizada, esta ISO 17799 nos da una guía sobre qué métodos, estándar o norma técnica se pueden aplicar a un sistema que administre la seguridad en la información, podría entenderse que estas normas son para uso auxiliar y pueden ser aplicadas en su implementación.

Toda política, estándar local y procedimiento está adaptada a la necesidad que se haya visto en la empresa u organización ya que el procesamiento de elaborarloincluye demostrar a la empresa el estado de su seguridad, y esto es muy importante según indica las normas.

Implementar la ISO 17799 nos obliga a seguir estándares y procedimientos en la cual, en un inicio, analizando los riesgos nos permitirá poder identificar los activos inform´páticos y algunos riesgos o amenazas en la que se expone la empresa.

Analizar los riesgos nos llevará a poder deleccionar correctamente un control que se pueda aplicar en la organización o empresa, y se podrá definir como controles para poder proporcionar niveles de seguridad y hacer seguimiento de su cumplimiento.

Otra de las ISO que nos brinda seguridad de información es la ISO 27000, este es un documento que consta de tipicidad en su vocabulario, definición y términos técnicos del mismo tema que también sigue la estandarización en el ámbito de gestionar la seguridad.

En su nueva serie nos da a conocer los estándares internacionales para el Sistema de Gestión de la Seguridad de la Información, y este nos propone algunos requisitos del SGSI, su mejora contínua y la gestión de riesgos.

Por otro lado, también encontramos la ISO 27001, aquí nos indican como realizar la aplicación de algunos controles que se nos propuso en la ISO 17799, y establece algunos requerimientos para poder auditar y certificar un correcto SGSI,

El SGSI en la ISO 27001 les da la potestad de poder dar la prevención y reducción en eficacia del alto nivel en riesgo con ayuda de implantar estos adecuados controles, para mejorar la empresa y poder garantizar su continuidad.

BENEFICIOS DE IMPLANTACIÓN:

- Establece una clara y correcta estructuración para la Gestión de Seguridad.
- Reducir riesgos en la información.
- Revisión constante de riesgos y controles.
- La empresa y sus servicios pueden continuar sus operciones.
- Confianza al personal.
- Concientización
- Establece seguridad.

NTP-ISO/IEC 17799

Existe una Normativa Peruana para esta ISO, si bien es cierto existen muchas normas a nivel mundial que se han creado para implementarse las buenas prácticas de seguridad.

Han existido y existen actualmente organizaciones que tienen la responsabilidad de establecer y brindarnos normas, estándares para orientarnos a tener buenas prácticas en Tecnología de Información.

En Perú, se puede observar que también hau organizaciones encargadar de brindarnos normas mediante resoluciones, decretos, etc. Y depende de cada empresa u organización su aplicación de buenas prácticas.

Con el Objetivo de crear una Sociedad de Información en Perú, y que nos garantice la eficiencia, y disponibilidad de todo tipo de información, de manera electrónica, servicos muy aparte de tipo de empresa que sea, en el sector educativo, industrial, financiero, etc.

3.5. COSO

Esta metodología debe aplicarse a diferentes áreas ya que enfoca principalmente al estudio de control interno, y analiza los riesgos tanto internos como externos, y estos también pueden ser por causas humanas, y por lo mismo nos enfatiza al contrato de personal responsable y de igual manera a la correcta asignación de las responsabildades para pedir su compromiso de gerencia para aplicar esta metodología.

COSO está basado en el control interno y en el análisis de riesgo ya sea externo o interno, y que puedan haber sido provocados po fallar humanas, por este motivo se pone alto énfasis a la contratar responsablemente los empleados y asignar responsablemente sus funciones, y considerar que cada persona cumple un papel importante en la empresa por tanto dbe tener un compromiso de parte gerencial para la aplicación y seguimiento del control interno dentro de la empresa.

Esta metodología también nos indica que debe mantenerse de manera conveniente una documentación favorable y correcta con el fin de poder analizar su alcande en sentido de evaluar, su nivel de autorización, impacto de deficiencia, inidcador de su despeñoo, todos esto análisis deben actuar en función de conseguir una correcta evaluación.

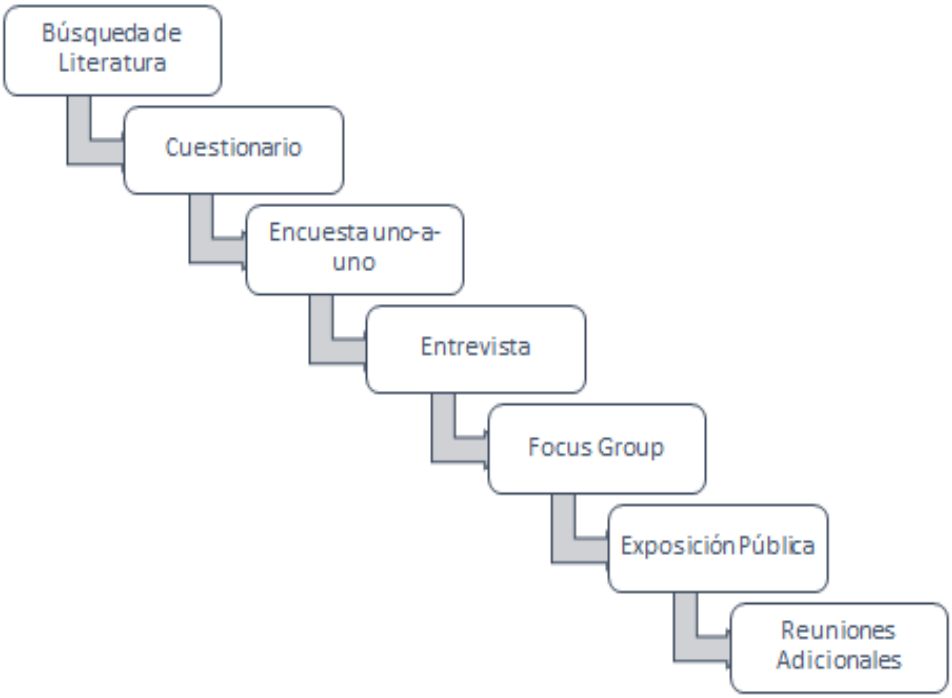
OBJETIVO

- Comunicarse fluidamente con los interesados de la investigación, en todas sus etapas de la metodología.

ALCANCE

Esta metodología nos permite considerar todos los puntos de vista de los interesados, y de esta maneranos permite diferenciar y clasificar la información que nos brindaron y gestionar conclusiones de acuerdo a la problemática.

PARTES DE LA METODOLOGÍA



Todos estos procedimientos han sido aplicados las siguientes personas:

Director del Area de Auditoría Interna	01
Director de la Unidad de Asesoría Jurídica	01
Director de la Unidad de Gestión Pedagógica	01
Director de la Unidad de Gestión Institucional	01
Director de la Unidad de Gestión Administrativa	01
Total	05

COMITÉ DE GESTIÓN

En toda empresa u organización, su estructura debe proporcionar conceptualmente y planear, ejecutar, controlar y monitorear las actividades para conseguir objetivos.

Existen aspectos que significan mucho para establecer una conrrecta estructura en la organización y estas incluyen definir las responsabilidades y establecer lineamientos para de información.

RESPONSABILIDAD Y ROLES

Toda persona en una empresa u organización tiene responsabilidades con respecto al control interno. Por ejemplo: El área de administración debe ser el responsable del control interno en la empresa u organización.
El director general es quien debe controlar la seguridad en toda la emprea, y finalmente todos los empleadores o colaboradores son resoinsables de controlar su actividad diaria.

FINALIDAD

Comprender el control interno de cada empresa u organización puede ayudarla a cumplir logros muy importantes con mucha eficacia, eficiencia tomando en cuenta los indicadores ya sea tomar decisiones, analizar y cumplir metas.

Esta metodología nos permite verificar la información manifestada y poder establecer conclusiones de acuerdo a la problemática existente, relacionadas a las etapas o fases.

ÁREAS INVOLUCRADAS

ÁREA DE AUDITORÍA INTERNA

Esta área es responsable de la programación y ejecución de acciones de control posteriores por medio de auditorías, investigaciones y/o exámenes especiales, y deben proporcionarnos una seguridad con razón de poder lograr buenos resultados.

ÁREA DE GESTIÓN ADMINISTRATIVA

Esta área está encargada de administrar y desarrollar el talento humano, también de la parte financiera y afines de la UGEL.

ÁREA DE ASESORÍA JURÍDICA

Esta área es la que asesora a la UGEL en la parte técnica y jurídica, así como sus dependencias en todo el ámbito legal.

ÁREA DE GESTIÓN PEDAGÓGICA

Esta área se encarga de asesorar y evaluar las acciones educativas que se vienen desarrollando en todas las Intituciones Educativas de área local.

ÁREA DE GESTIÓN INSTITUCIONAL

Esta área se encarga de ver la parte estadística de está organización, desde su planeamiento hasta su Infraestructura.

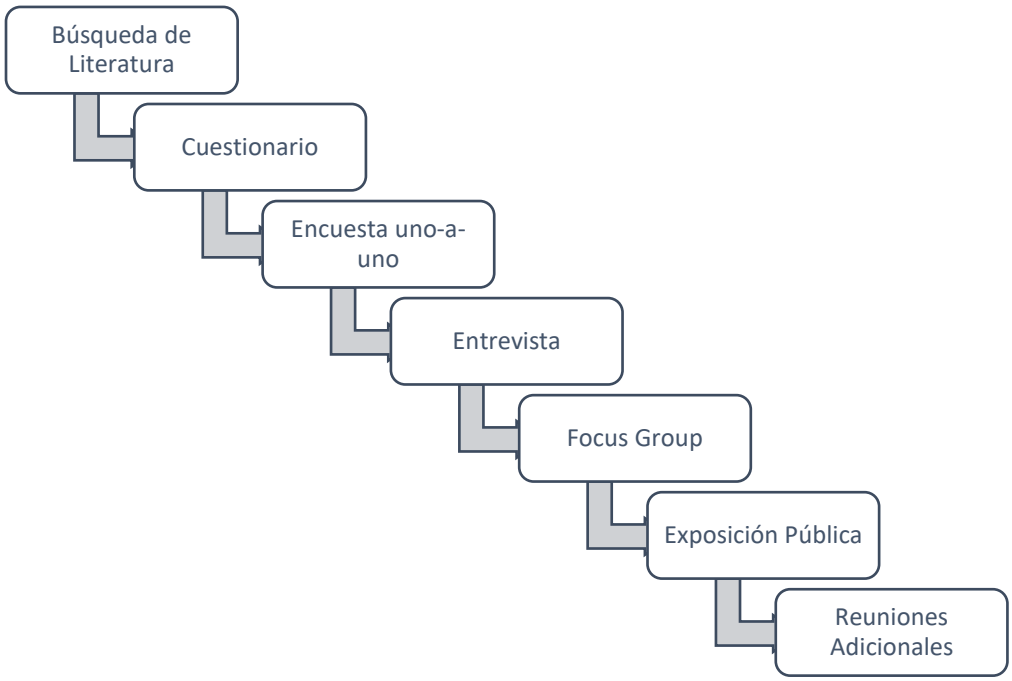
CAPITULO IV
METODOLOGÍA Y PROCEDIMIENTOS

4.1. METODOLOGÍA COSO

Esta metodología nos permite verificar la información manifestada y poder establecer conclusiones de acuerdo a la problemática existente, relacionadas a las etapas o fases.

4.2. DESARROLLO DE METODOLOGÍA

Las diversas áreas que se mencionaron en el capítulo anterior y sus respectivos encargados, serán analizados con respecto a estos 7 pasos:



Todos estos procedimientos han sido aplicados las siguientes personas:

Director del Area de Auditoría Interna	01
Director de la Unidad de Asesoría Jurídica	01
Director de la Unidad de Gestión Pedagógica	01
Director de la Unidad de Gestión Institucional	01
Director de la Unidad de Gestión Administrativa	01
Total	05

La investigación se ha desarrollado en 7 partes de la metodología COSO:

1. Búsqueda de Literatura

En este punto hemos tomado de apoyo a libros, publicaciones, tesis, archivos de la web.

Se realiza una amplia búsqueda de información y luego se ha seleccionado los más eficientes conceptos para poder tener una fuerte base teórica y de esta maner poder desarrollar el proyecto de tesis.

2. Cuestionario

Se entregó un cuestioario a las jefaturas de las 6 áreas que ha tomado en cuenta y se mencionaron anteriormente, se seleccionaron estas personas ya que estarán relacionados a concientizar a los demás usuarios o empleados de sus áreas.

3. Encuesta

La encuesta fue diseñada para obtener información más clara y detallada.

4. Entrevista uno a uno

Se realizaron entrevistas por el equipo investigador y con un formato de ayuda para la entrevista.

5. Focus Group

Se ha realizado Focus Group y de esta manera se expusieron los resultados que se encontró en las partes que se mencionaron anteriormentey también para informales la importancia del tema, y también para tomar nota de los comentarios y lo que nos podrían recomendar para ser más ojetivos.

Este Focus Group incluyó la genarlización del proyecto y todas sus partes así como también las conclusiones que se identificaron tantos los jefes como el equipo investigador.

6. Exposición Pública

Se hizo la exposición para poder mostrarles unas posibles acotaciones que s deben tomar en cuenta con relación a la estructura de la organización y también el control de los activos de información para que se pueda llegar a un acuerdo.

7. Reuniones Adicionales

Estas reuniones permitieron la determinación de alguna modificación desde que se realizó la exposición.

El equipo investigador tomó en cuenta todas las recomendaciones y de esa manera se adapte una mejor estructura en la organización.

4.3. ANÁLISIS DE PROCEDIMIENTOS

4.3.1. ANÁLISIS DE CUESTIONARIOS

Para analizar las respuestas de las preguntas planteadas en el cuestionario se ha considerado conveniente, la creación de categorías que se puedan calificar como: Bajo, Regular, Alto.

El análisis de resultados se da a conocer a continuación:

I. DE LA ESTRUCTURA ORGANIZACIONAL Y FUNCIONES

1. **¿Tiene usted conocimiento de que se estén aplicando normas o estándares que nos permitan definir las políticas y sus métodos de trabajo?**

   En las respuestas de esta pregunta se puede notar que nos existen estándares que nos permitan definir las políticas y métodos de trabajo en la entidad.

II. DEL CONTROL DE ACTIVOS

1. **¿Tiene usted conocimiento de que exista una clasificación o quizás una técnica para evaluar los activos de informática o recursos en la entidad?**

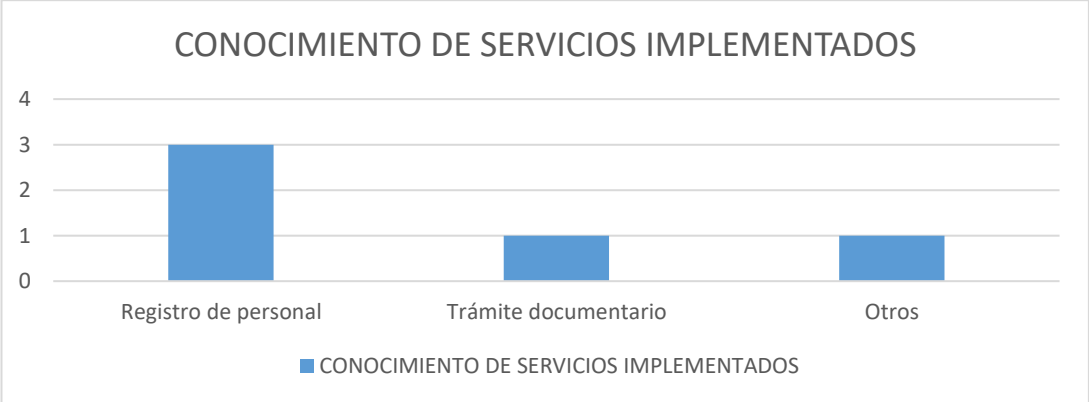
   Podemos notar que existe un conocimiento Bajo sobre la clasificación o ya sea una técnica para evaluar los activos de informática o recursos, entre los cuales se mencionan a COSO, COBIT, o la norma ISO 17799 a los que nos referimos.

4.3.2. ANÁLISIS DE ENCUESTA

1. **¿Tiene usted conocimiento sobre algunos servicios de informática que se han venido implementando en la UGEL**

a)	Registro personal	3
b)	Trámite documentario	1
c)	Otros	1

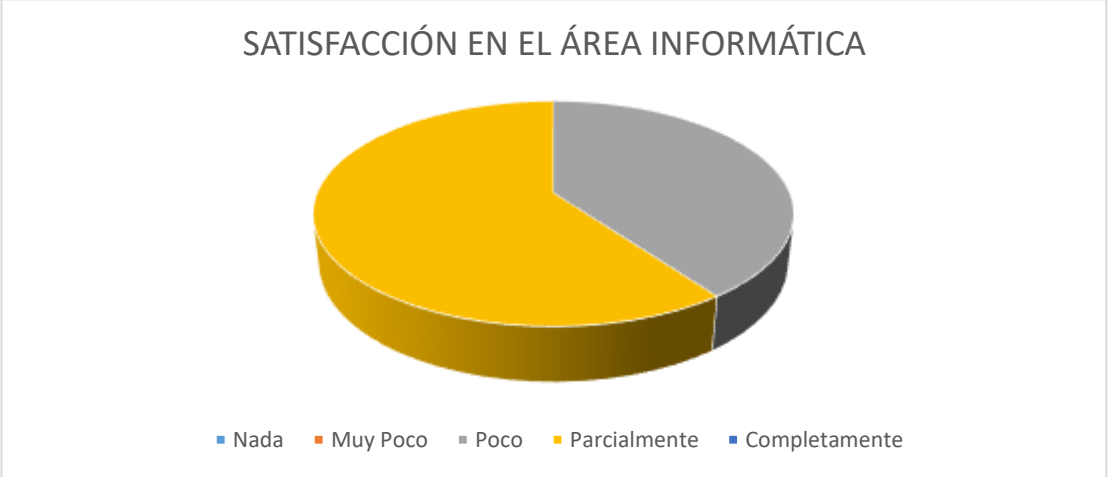
Chincha?



- El 60% (3 personas) opinan que se ha implementado Registro de Personal.
- El 20% (1 persona) ha opinado que se ha implementado Trámite documentario.
- El 20% (1 persona) ha opinado que se ha implementado otros servicios.

2. ¿Podría usted decirnos si los procesos que nos brinda el área informática cumple sus expectativas?

a)	Nada	0
b)	Muy Poco	0
c)	Poco	2
d)	Parcialmente	3
e)	Completamente	0



- El 40% de las personas encuestadas tiene POCO grado de satisfacción.
- El 60% de las personas encuestadas tiene PARRCIALMENTE grado de satisfacción.

4.3.3. ANÁLISIS DE ENTREVISTA UNO - A – UNO

PERSONAL

- No existen Políticas de Seguridad de las cuales se pueda regir la UGEL, por lo tanto se desarrollan de manera rutinaria.
- La UGEL actualmente no cuenta con normas para poder regularizar su área informática, por este motivo se trabaja como ellos crean conveniente, dejándose llevar por los años de experiencia, por tal razón se puede decir que no existe un mecanismo que nos ayude a definir sus controles o de hacerlos cumplir.

DIRECCIÓN

- La UGEL debe confiar en el método de informatizar, ya sea desde usar la tecnología que por cierto nos ayuda mucho a resolver aquellas necesidades en la organización, también tener un orden en los sistemas en información y formalizar estos para poder hacernos más fácil el tomar decisiones, ya que estos deben hacerse de manera responsable y nos deben brindar credibilidad.

CAPITULO V
FORMULACIÓN DE POLÍTICAS

FORMULACIÓN DE POLÍTICAS DE SEGURIDAD

1. FINALIDAD

La finalidad de estás políticas es dar soporte y dirigir la gestión de TI en acuerdo con lo que requiera la UGEL Chincha.

2. JUSTIFICACIÓN

Las políticas que se recomendarán están con base en las NTP ISO/IEC 17799:2004, el cual su uso es de forma obligatoria con:

. RESOLUCIÓN MINISTERIAL N° 224-2004-PCM, de 23-07-2004, en el cual nos manifiesta que es de uso obligatorio esta norma.

Cabe recalcar, que este documento será trabajado conforme a la actualización de la norma.

3. ESTRUCTURA

- **Cláusula:**
  - Aspectos Organizacionales de Seguridad
  - Control y Clasificación de Activos
- **Categorías:**
  - Objetivo de control con base en la NTP ISO/IEC 17799.
  - Dar a conocer estado actual de la UGEL conforme a la NTP.
  - Planteamiento de Política.

4. ALCANCE

Las Políticas de Seguridad en el presente documento serán aplicados por los directores de las áreas que tienen relación con el manejo de TI/SI en la entidad.

POLÍTICAS DE SEGURIDAD INFORMÁTICA

1. ASPECTOS ORGANIZACIONALES DE SEGURIDAD

1.1. Organización Interna

A. Según la NTP ISO/IEC 17799

El objetivo es Gestionar la SI en la organización.

Se debería establecer una correcta estructura para poder iniciar y tener un control de la implantación de la SI en la organización.

Se deben organizar foros con las jefaturas para que se aprueben las Políticas de SI, a su vez la asignación de roles y la coordinación de implantación de SI en la organización.

B. Descripción actual de UGEL.

La UGEL hace una gestión de SI que se basa en la experiencia de cada trabajador, debemos tener en cuenta que esta entidad no ctien documentación formal que se haya aprobado por la dirección o que se hayan elaborado con base a normas para tener una base fuerte de trabjo en cada área.

C. Planteamiento de política

En lo que norma la NTP ISO/IEC 17799, en lo que corresponde a este punto, se debe recalcar que tiene sub-categorías, que se trataran a continuación para que nos permita analizar y plantear mejor las políticas.

1.1.1. Comité de Gestion de SI

A. Según la NTP ISO/IEC 17799

Según la norma nos dice que debe tener las siguientes funciones:

a. Asegurarnos que la meta de SI sea identificada y relacionada a lo que exige la organización.
b. Revisar que se efectivo el implementar la política de información.
c. Aprobar la asignación de rol y responsabilidad para SI en la organización.
d. Asegurarnos que implementar control de SI sea en coordinación con la organización.

B. Descripción actual de UGEL.

La UGEL no establece un Comité de SI, la cual debería estar integrado por jefes de área y personal administrativo con poder de tomar decisiones en la organización, para poder hacer cumpli lo que nos dice la norma.

C. Planteamiento de política

Cabe señalar que si es posible formar este Comité con las siguientes observaciones:

- Es de Sugerencia que el Comité, debe estar integrado por el Especialiosta en Informática, jefes de áreas y personal administrativo.
- El Comité debe estar informado de los cambios o mejoras de la norma.

1.1.2. Coordinación de SI

A. Según la NTP ISO/IEC 17799

Normalmente, la coordinación de la SI debe tener la colaboración de las jefaturas, de usuarios, y personal administrativo. Esta debe:

- Identificar como podemos manejar los incumplimientos.
- Identificar las amenazas de exponer la información.
- Asegurarnos que las actividades que se hayan organizado para la segurdad seas ejecutadas.
- Evaluar y coordinar la implementación de control de SI.
- Promoción la conciencia de SI.

B. Descripción actual de UGEL.

La UGEL trata de coordinar la SI pero no existe medio de coordinación con respecto a la SI y esta debe ser realizada por el especialista de informática.

En la actualidad, los usuarios toman malas decisiones ocn respecto a la SI, ya sea de manera interna con las documentaciones o en re/ internet que va en contra de las buenas prácticas, y esto debe ser regtringido o limitado.

C. Planteamiento de política

Deben implementarse mecanismo para coordinar la aprobación de la Dirección de la organización y entre las áreas que se tomaran en cuenta, para de esta manera respetar lo estipulado en las normas, por este motivo:

- Las personas que van a estar encargadas de coordinar la SI tedrán que encargarse de entrenar y concientizar a los jefes y usuarios finales para que se vayan inculcando al cultura de SI.
- Se debe tener en cuenta las funciones según lo que dice la norma, y se debe estar al tanto de las actualizaciones de la norma.
- Se deben tener reuniones periódicamente, al menos uan vez por mes, con las jefaturas de las áreas.

1.1.3. Asignación de responsables sobre SI

A. Según la NTP ISO/IEC 17799

Esta asignación debe hacerse en acuerdo con la información que contenga la Política de Seguridad.

Esta asignación dene definirse de manera clara para saber y delegar, es esencial que hayan áreas en las que cada jefe es responsable, para ser precesiso serían las siguientes:

a. Deberían definirse y documentar los niveles existentes de autorización.
b. Se debería nombrar un responsable por ada proceso de SI y documentarlo.
c. Se debería identificar los activo TI y sus procesos de SI.

B. Descripción actual de UGEL.

La UGEL no cuenta con normas o documentos que les permitan identificar la responsabilidad de cada persona en su áre de trabajocon respecto a la SI. Pero si tiene responsabilidades que se asignan en base a la experiencia de cada personal.

C. Planteamiento de política

En la UGEL si es posible realizar la asignación de responsabilidaes de SI, pero debemos tener en cuenta:

- Para elaborar y asignar responsabilidades, se debe tener presente las políticas que ha elaborado el Comité SI y que ya se han aprobado por la Dirección de la organización.
- Los encargados de coordinar la SI son quienes deben hacer seguimiento y verificar que se cumplan.
- Los documentos deben contener: descripción de activos TI/SI, niveles de autización, restricciones, y también sanciones a quien no cumpla.

1.1.4. Proceso para autorizar el Tratamiento de información

A. Según la NTP ISO/IEC 17799

Se debe considerar:

a. Debe autorizar y evaluar usar los medios de informática que son personales, ya sean computadores portátiles como, equipos móviles, puede tener vulnerabilidades.
b. Los medios deben ser aprobados por sus jefaturas, justificando su propósito.
c. Se debe comprobar que tanto el software como el hadware sean compatiebles con el sistema.

B. Descripción actual de UGEL.

En la UGEL, cuando se necesitan equipos nuevos se debe fundamentar el pedido a la dirección y junto con el área de Administrción para evaluar la financia y aprobar.

Pero esto podría ser más rápido si hubiera documentos para planificar activo y asignar el finaciamiento.

C. Planteamiento de política

En la UGEL si se puede agilizar la autorización si se tomara en cuenta:

- La Dirección debe coordinar con el Comité de SI la entrega de POI.
- La UGEL debe elaborar un POI, en el cual debe indicar como adquirirlo y su grado de importancia o necesidad.

1.1.5. Auerdo de Confidencialidad

A. Según la NTP ISO/IEC 17799

Para poder identificar requerimientos de confidencia debe considerarse:

- Duración del acuerdo.
- Proceso para notificarlle y reportar un acceso in autorización.
- Términos o acuerdos cuando cese el acuerdo.
- Acciones y responsabilidad para poder evitar un acceso sin autorización.

B. Descripción actual de UGEL.

La UGEL no hace acuerdos de confidencialidad por este motivo se puede divulgar información privada fuera de la organización, sin embargo esto debería guardarse en secreto.

C. Planteamiento de política

Estos acuerdos se deben implementar, pero tomar en cuenta:

a. Se debería exigir la confidencia y no divulgar los datos para todo el personal que tengo acceso a información importante.

b. Estos acuerdos deben tener: la información que se va a proteger, cuanto durará, acciones al finalizar.

c. El personal debe de firmar el acuerdo para probar que lo ha recibido.

d. El comité debe auditar el cumplimiento del acuerdo.

1.2. Seguridad en acceso a terceros

A. Según la NTP ISO/IEC 17799

El objetivo es el de garantizar la seguridad de que los recursos informáticos sean accesibles a terceros, pero este acceso debe ser controlado al máximo.

B. Descripción actual de UGEL.

En la UGEL no hay documentación formal que figure el acceso de terceros.

Tampoco hay controles que se puedan encargar de hacer seguimiento del trato que se hace a la información de la organización por parte de estos terceros.

C. Planteamiento de política

En la UGEL, si puede ser factible hacer cumplir esta norma, pero se debe tener en cuenta la meta de mantener en todo tiempo la seguridad de los activos TI/SI.

Asimismo según se norma, hay subcategorías que se deben tener en cuenta:

1.2.1. Identificar los riesgos

A. Según la NTP ISO/IEC 17799

Se deben identificar los riesgos que ocasione el dar acceso a terceros y se debe tener en cuenta:

- El tipo de acceso
- La información

Hay que asegurarse que estos terceros estén pendientes y enterados de las obligaciones y/o responsabilidades que les implica este privilegio de tener este aceso a la información de la organización.

B. Descripción actual de UGEL.

En la UGEL no se ha realizado una identificación de riesgos por estos accesos o tapoco hay documentación formal aprobada.

C. Planteamiento de política

Es de mucha importancia, que la UGEL identifique los riesgos que pueda ocasionar el dar acceso a la información de la organización a terceros, y se debe tenr en cuenta lo siguiente:

- La UGEL, debe encargarse de la documentación correspondiente.
- Cuando se habla de terceros pueden ser: servicio, proveedores, consultores, y personal que no es permante ya sean estudiantes o practicantes.

2. CONTROL DE ACTIVOS

2.1. Responsabilidad sobre Activos

A. Según la NTP ISO/IEC 17799

El objetivo es el de tener una adecuada protección sobre la información de la organización.

B. Descripción actual de UGEL.

La UGEL debe tener en cuenta que no existe documentación formal basada en estándares cobre Control de Activos a su personal que haga uso de la informática.

C. Planteamiento de política

En la UGEL, si puede ser posible hacer esta aplicación, asimiso hay subcategorías que se deben tener en cuenta:

2.1.1. Inventario de Activos.

A. Según la NTP ISO/IEC 17799

Toda organización debe saber reconocer los documentos que son de mucha importancia y tener un plan de contingencia, el inventario debe estar totalmente asegurando que la información estará alineada.

B. Descripción actual de la UGEL.

La UGEL no tiene una lista en donde se detallen sus activos de TI/SI, y esto origina que haya disponibildad de información para poder asignar niveles para proteger el valor de estos mimos.

C. Planteamiento de política

En la UGEL, es de mucha importancia tener inventariado los activos y este nos dará la seguridad que haya una adecuada protección con estos, para realizar debemos tener en cuenta lo siguiente:

. El área que se enargará de hacer el inventario debe ser el área de informática, que debe asignar un personal encargado.

. Este inventario debe actualizarse anualmente.

. El documento que nos resulte será dirigado al Comité de SI y aprobado por la Dirección.

. Se debe realizar una Gestión de Riesgo para ordenar los activos de la organización.

2.1.2. Propiedad de activo

A. Según la NTP ISO/IEC 17799

La responsabilidad recae en:

- Definir y revisar los accesos y sus restricciones, se debe tomar en cuentas las políticas.
- Asegurarnos que su información son clasificadas.

B. Descripción actual de UGEL.

En la UGEL no existe de manera formal una signación, y no hay un encargado de velar por la seguridad de los activos TI/SI de la organización.

C. Planteamiento de política

Es importante que haya responsables asignados y se de tener en cuenta lo siguiente:

. Los documentos deben decribir de manera detallada los activos.

. Los que se encargan de los activos deben brindar la completa seguridad e la información.

. El comité de SI debe tener planificado programar capacitaciones con el fin de que estén cumpliendo el objetivo dea seguridad a la información de la organización.

2.1.3. Uso correcto de activos

A. Según la NTP ISO/IEC 17799

Todo el personal y contratados y terceros deben cumplir el reglamento de buen uso de la información de la organización, y deben incluir:

- Guias para el usuario.
- Reglas de acceso a internet.

B. Descripción actual de UGEL.

La UGEL no tiene reglas para el correcto uso de la información y por este motivo el personal no tiene limites al nocontar con un personal que se encargue de exigirle y aclararle el lineamiento para el uso responsable.

C. Planteamiento de política

Deben existir reglas para u ncorrecto uso de la información de la organización, esto también involucra que participe todo el personal que maneja información relevante de la empresa para un correcto uso se debe tener en cuenta lo siguiente:

. Las reglas deben incluir todo tipo de acceso a red o internet.
. Los encargados deben realizar las reglas de corecto uso de la información.
. Los encargados deben hacer seguimiento y deben verificar que se cumplan las reglas y a la vez hacer efectivas las sanciones.
. Estas reglas deben conocerse públicamente en cada área, para los nuevos personales que ingressen o para los que ya haya.

2.2. Clasificacón de información

A. Según la NTP ISO/IEC 17799

Debemos tener en cuenta que el objetivo es el de asegurar un alto nivel y adecuada protección al activo de información.

B. Descripción actual de la UGEL.

En la UGEL, toda su información no está correctamente clasificada por queno hay un sistema de clasificación que se haya establecido por lo tanto no existe un nivel adecuado para proteger los activos.

Por otro lado, ace señalar que todo su proceso de trámite documentario tampoco está digitalizado, y aún lo tienen en papel, y hay información muy im,portante que se encuentra el archivos físicos que deben digitalizarse ya que el materiales del papel no es bueno y se puede ir perdiendo información importante poco a poco.

C. Planteamiento de política

Según lo que indica la norma de este punto en mención nos dice que demebos saber que hay subcategorías:

2.2.1. Guía de Clasificación

A. Según la NTP ISO/IEC 17799

Se debe tener presente que la organización necsita restringir su información, así como clasificarla y tener un control de protección riguroso.

B. Descripción actual de UGEL.

En la UGEL no eiste formalización documental de como clasificar la información y por este motivo no puede garantizar que toda la información tiene medidas de protección.

C. Planteamiento de política

Es de importancia que la UGEL tenga guía de clasificar la información tomando en cuenta los siguientes criterios:

. Se debe establecer un sistema para que apoye en la clasificación de la información.
. Se debe establecer una Guia parala clasificación.

. Toda la documentación del Sistema creado debe ser enviada al Comité de SI y aprobada por la Dirección.

2.2.2. Tratamiento de información

A. Según la NTP ISO/IEC 17799

En los sistemas que se creen para realizar la clasificación de información, deben tener niveles de clasificación.
La información que se comparta con otras organizaciones debe tener dentro de ela procedimientos documentados que los garantice.

B. Descripción actual de UGEL.

En la UGEL no se tiene establecido este procedimiento formal de como tratar la información, por este motivo los recursos informáticos no tienen una medida de seguridad establecida y no tienen medida de seguridades especial.

C. Planteamiento de política

Es de vital importancia que la UGEL implemente esta norma en la organización ya que su información debe ser tratada de manera muy estricta con con un nivelde clasificación correcta.
Se debe tener en cuenta que:
. Se deben elaborar procediiento para tratar la información y deben marcarse por s univel de acceso.
. Las personas que están encargadas de coordinar el SI deben estar en constante monitoreo y verificar que se haga el marcado para clasificar de manera correcta la información.

CONCLUSIONES

1. Se hizo la formulación de la política con base en la NTP ISO/IEC 17799 para poder realizar un inventario de activas para la Gestión de Información de la Unidad de Gestión Educativa Local de Chincha.

2. Se hizo la formulación de la política con base en la NTP ISO/IEC 17799 para poder realizar el plan de Protección para la Gestión de Información de la Unidad de Gestión Educativa Local de Chincha.

3. Se hizo la formulación de la política con base en la NTP ISO/IEC 17799 para poder realizar un Análisis de Riesgos para la Gestión de Información de la Unidad de Gestión Educativa Local de Chincha.

RECOMENDACIONES

1. Se recomienda la ejecución de la formulación de la política con base en la NTP ISO/IEC 17799 para poder realizar un Inventario de activos y de esta manera tener un mejor control en Gestión de Información de la Unidad de Gestión Educativa Local de Chincha.

2. Se recomienda la ejecución de la formulación de la política en base a la NTP ISO/IEC 17799 para poder realizar el plan de Protección y tener un mejor control en Gestión de Información de la Unidad de Gestión Educativa Local de Chincha.

3. Se recomienda la ejecución de la formulación de la política con base en la NTP ISO/IEC 17799 para poder realizar un Análisis de Riesgos y tener un mejor control en Gestión de Información de la Unidad de Gestión Educativa Local de Chincha.

BIBLIOGRAFÍA

(s.f.). Obtenido de Unidad de Gestión Educativa Local de Chincha: www.ugelchincha.gob.pe
(s.f.). Obtenido de Unidad de Gestión Educativa Local de Chincha: www.ugelchincha.gob.pe
Aguilera López, P. (2010). Seguridad Informática. Argentina: EDITEX.

ANEXO

UNIVERSIDAD AUTÓNOMA DE ICA
FACULTAD DE INGENIERÍA CIENCIAS Y ADMINISTRACIÓN
PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS

"Investigación para desarrollar la tesis sobre Formulación De Políticas De Seguridad Informática Basado En La Norma ISO/IEC 17799 Para La Gestion De La Informacion De La Unidad De Gestión Educativa Local En Chincha"

INTRODUCCIÓN: El siguiente custionario va dirigido a las jefaturas de las 6 áreas a investigar para poder observar y analizar su estructura en la organización y su control de activos informáticos.

INSTRUCCIONES: Marcar la alternativa correcpondiente a su consideración.

I. DE LA ESTRUCTURA ORGANIZACIONAL Y FUNCIONES

1. ¿Tiene usted conocimiento de que se estén aplicando normas o estándares que nos permitan definir las políticas y sus métodos de trabajo?

a. Bajo
b. Regular
c. Alto

II. DEL CONTROL DE ACTIVOS

2. ¿Tiene usted conocimiento de que exista una clasificación o quizás una técnica para evaluar los activos de informática o recursos en la entidad?

a. Bajo
b. Regular
c. Alto

DATOS

Nombre: (Opcional)		
Cargo: (Obligatorio)		
Teléfono/ Celular: (Opcional)	Correo Electrónico: (Opcional)	Firma: (Obligatorio)

UNIVERSIDAD AUTÓNOMA DE ICA
FACULTAD DE INGENIERÍA CIENCIAS Y ADMINISTRACIÓN
PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS

"Investigación sobre Formulación De Políticas De Seguridad Informática Basado En La Norma ISO/IEC 17799 Para La Gestion De La Informacion De La Unidad De Gestión Educativa Local En Chincha"

INTRODUCCIÓN: La siguiente encuesta va dirigido a las jefaturas de las 6 áreas a investigar para poder observar y analizar su estructura en la organización y su control de activos informáticos.

INSTRUCCIONES: Marcar la alternativa correspondiente a su consideración.

1. **¿Tiene usted conocimiento sobre algunos servicios de informática que se han venido implementando en la UGEL Chincha?**

a. Registro Personal
b. Trámite documentario
c. Otros

2. **¿Podría usted decirnos si los procesos que nos brinda el área informática cumple sus expectativas?**

a. Nada
b. Muy Poco
c. Poco
d. Parcialmente
e. Completamente

Nombre: (Opcional)		
Cargo: (Obligatorio)		
Teléfono/ Celular: (Opcional)	Correo Electrónico: (Opcional)	Firma: (Obligatorio)