UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

ESCUELA DE POSGRADO

TESIS PARA OPTAR EL GRADO ACADÉMICO DE

MAESTRO EN INGENIERÍA DE SISTEMAS

MENCIÓN: EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

CUMPLIMIENTO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LA NORMA ISO 27000 EN LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR. AÑO 2017.

TESISTA: IGNACIO RUBEN TACZA VALVERDE

ASESOR: Mg. MÓNICA RICARDINA ESPINOZA NARCISA

HUÁNUCO - PERÚ

2018

DEDICATORIA

A mis padres ya que ellos son la fuerza que me permiten continuar en el desarrollo de mi carrera profesional, a mi hermana y sobrinas por su apoyo emocional y estimulo.

AGRADECIMIENTO

Al personal trabajador de la Universidad Nacional Tecnológica de Lima Sur, por su apoyo para el logro de la presente investigación.

RESUMEN

El estudio tuvo como objetivo determinar el cumplimiento de la norma ISO 27000 en la Universidad Nacional Tecnológica de Lima Sur.

El estudio básicodescriptivo y correlacional se realizó con una muestra de 80 trabajadores con acceso a la información de la Universidad Nacional Tecnológica de Lima Sur. Se localizaron las fuentes de información como bibliografía, revistas, Internet, asociaciones de profesionales, de egresados, investigaciones de campo, tesis, etc.

Del resultado de la hipótesis principal obtenido se infiere que existe relación significativa del plan de seguridad de información y la norma ISO/IEC).Por tanto, es necesario adaptarse a la Norma ISO 27001:2005 y plantear un plan de aseguramiento de la información. Se concluye, que la UNTELS no ha cumplido la implementación adecuada de un plan de seguridad de la información, según lo normado por al ONGEI, por tanto, dicha institución está en grave riesgo y constante amenaza con respecto a la gestión adecuada de sus repositorios de información así como los mecanismos y políticas que enmarcan dichos procesos.

Palabras clave: seguridad de la información, sistema de seguridad de la información, ISO 27000, plan de seguridad de la información, riesgos en seguridad de información, disponibilidad de información, distribución de información, diagnóstico de la seguridad de la información, condiciones de la seguridad de la información.

SUMMARY

The study aimed to determine compliance with ISO 27000 at the Universidad Nacional Tecnológica de Lima Sur.

The study is of descriptive basic type and correlational according to the objective that it wants to achieve, with a population of 80 workers with access to the information of the National Technological University of Lima Sur. Information sources such as bibliography, journals, Internet, professional associations, alumni, field research, theses, etc. were located. The results were: From the result of the main hypothesis obtained it is inferred that there is no significant relationship between the information security plan and the ISO / IEC standard according to the results obtained from the hypothesis test.

Therefore, it is necessary to adapt to the ISO 27001: 2005 Standard and to propose an information assurance plan. It is concluded: that UNTELS has not complied with the proper implementation of an information security plan, as regulated by ONGEI, therefore, this institution is at serious risk and constant threat with respect to the proper management of its repositories Information and the mechanisms and policies that frame these processes.

Key words: information security, information security system, ISO 27000, information security plan, information security risks, information availability, information distribution, information security diagnostics

.

INTRODUCCIÓN

En toda organización, el recurso que origina la vida de la misma, es la información, la cual es considerada como un recurso estratégico, y su gestiónes vital para la subsistencia de la institución. La toma de decisiones se orienta en base a la cantidad y calidad de información con que se cuenta.

La confidencialidad, disponibilidad y la totalidad de la información son aspectos que deben estar presentes en el momento de implementar procesos, políticas o sistemas de gestión de la seguridad de la información. Este trabajo tiene por objetivo estudiar un caso en concreto, el de la Universidad Nacional Tecnológica de Lima Sur (UNTELS), en donde luego de muchos inconvenientes se implementó un plan de acciones y políticas a fin de salvaguardar la información de la institución como recurso estratégico basándose en la familia ISO 27000.

El presente trabajo comenzará por entender con claridad que aspectos de seguridad de la información propone la norma ISO 27001:2005 y lo que el estado peruano necesita que las entidades públicas implementen, haciendo una revisión de proyectos similares y entrevistando a personas relacionas al tema, gobierno electrónico, personal de la PCM, etc.

De acuerdo a esto, se hará una comparación con el esquema planteado en la UNTELS, identificando los puntos de controversia, puntos fáciles, puntos problemáticos, a fin de establecer soluciones y ajustes documentados que permitan definir con claridad un camino al éxito de la implementación de la seguridad de la información, en este tipo de organización, por último se discutirán los resultados llegando a conclusiones que permitirán definir mejoras y otras investigaciones.

Considerando lo anterior expuesto se planteó la pregunta: ¿De qué manera el plan de seguridad de la información se relaciona a lo establecido en la norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur?

Esta investigación es necesaria pues pretende aportar con ajustes a modelos concretos la implementación de un sistema de seguridad de la información en universidades públicas especialmente en la UNTELS. Así también, busca aumentar la cultura de las personas trabajadoras de las diferentes organizaciones gubernamentales en asuntos relacionados a la seguridad de la información haciendo hincapié en la necesidad imperiosa de contar con un sistema de seguridad de información. Y al mismo tiempo contribuir a cumplir con la normatividad peruana respecto a la Seguridad de la Información.

La investigación para su desarrollo se constituye en los siguientes capítulos:

Capítulo I: El problema de investigación, Capitulo II: Marco Teórico, Capítulo III: Marco Metodológico, Capítulo IV: Resultados, Capítulo V: Discusión de Resultados, Conclusiones y Sugerencias, para finalmente considerar las referencias Bibliográficas y anexos.

ÍNDICE

Pág.

INDICE DE TABLAS

INDICE DE GRÁFICOS

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Descripción del problema

La información es un recurso valioso para cualquier organización, está caracterizada por poseer características de confidencialidad, integridad y disponibilidad, estos atributos deben ser considerados al momento de diseñar y operar un sistema de seguridad de información. Existen enfoques que mencionan de manera muy general el contenido operativo que debe poseer los sistemas de información (ISO 27000), pero no establecen con claridad formatos o procesos concretos respecto del tema.

En la Universidad Nacional Tecnológica de Lima Sur (UNTELS), a raíz de la Resolución Ministerial N°187-2010-PCM del 15 de junio de 2010, se decidió organizar el sistema de seguridad de la información, para tal efecto se designó un comité encargado de implementar políticas y procesos de trabajo con la finalidad de salvaguardar la información de la universidad. Dicho trabajo desencadenó diferentes documentos, tal como resolución de aprobación del reglamento de designación del comité de seguridad de la información de la UNTELS, el listado de políticas de tratamiento de la información, etc. Un trabajo arduo que demando casi dos años de labor. Sin embargo, pese a todo el trabajo, surge la interrogante ¿se ha logrado implementar adecuadamente el sistema de seguridad de la información basado en ISO 27000?, actualmente es fácil detectar problemas en cuanto a la gestión de este recurso, como la falta de rapidez en detectar un expediente, el tiempo empleado (en exceso) para realizar algunos trámites, se presume que hasta cinco días hábiles dependiendo del proceso. ¿Qué ajustes son necesarios para

lograr que los procesos de seguridad de la información sean más eficientes? Y estén conforme a lo solicitado por el gobierno e ISO 27000.

De acuerdo a la ley N° 30220 las universidades son autónomas, pero se rigen bajo la misma ley y en convergencia de procesos; el estado rige las universidades del país, a través dela SUNEDU, la cual puede supervisar el funcionamiento de las mismas, es decir es posible que los problemas encontrados en el proceso del presente estudio y las mejoras que se propongan sirvan para otras instituciones similares a esta.

1.2. Formulación del problema.

1.2.1 Problema general:

¿Qué relación existe entre cumplimiento del plan de seguridad de la información con lo establecido por la norma ISO/IEC 27001:2005, en lo que respecta al personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017?

1.2.2 Problemas específicos

1. ¿Qué relación existe entre la situación actual de la seguridad de la información (Diagnóstico) con lo establecido por la norma ISO/IEC 27001:2005, respecto del personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017?
2. ¿Qué relación existe entre la seguridad de la información (respecto del cuidado y distribución de la información) con lo establecido por la norma ISO/IEC 27001:2005 en el personal administrativo dela Universidad Nacional Tecnológica de Lima Sur en el 2017?

3. ¿Qué relación existe entre el cumplimiento del plan de seguridad de la informaciónestablecidomediante la identificaciónde los puntos fuertes y débiles de los sistemas de información (riesgo) y lo establecido por la norma ISO/IEC 27001:2005 respecto del personal administrativo que manejan dichos sistemas en la Universidad Nacional Tecnológica de Lima Sur en el 2017?
4. ¿Qué relación existe entre el conocimiento de los accesos a la información, internos y externos (condiciones), con lo establecido por la norma ISO/IEC 27001:2005 enlo referente al personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017?
5. ¿Qué relación existe entre la seguridad de información (controles que garanticen la confidencialidad, integridad y disponibilidad de la información) con lo establecido por la norma ISO/IEC 27001:2005, respecto de su manejo por el personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017?

1.3. Objetivo general y objetivos específicos

1.3.1. Objetivo General

Determinar la relación de cumplimiento del plan de seguridad de la información con la norma ISO/IEC 27001:2005 por el personal administrativo de la Universidad Nacional Tecnológica de Lima Sur.

1.3.2. Objetivos Específicos

1. Verificar la relación entre la situación actual de la seguridad de la información (Diagnostico) con lo establecido por la norma ISO/IEC 27001:2005, respecto del personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017.

2. Evaluar la relación dela seguridad de la información (respecto del cuidado y distribución de la información) con lo establecido por la norma ISO/IEC 27001:2005 en el personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017.

3. Identificar la relación entre el cumplimiento del plan de seguridad de la información establecido mediante la identificaciónde los puntos fuertes y débiles de los sistemas de información (riesgo) y lo establecido por la norma ISO/IEC 27001:2005 respecto del personal administrativo que manejan dichos sistemas en la Universidad Nacional Tecnológica de Lima Sur en el 2017.

4. Conocer la relación entre el conocimiento de los accesos a la información, internos y externos (condiciones), con lo establecido por la norma ISO/IEC 27001:2005 en lo referente al personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017

5. Verificar la relación entre la seguridad de información (controles que garanticen la confidencialidad, integridad y disponibilidad de la información) con lo establecido por la norma ISO/IEC 27001:2005, respecto de su manejo por el personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017.

1.4. Hipótesis y/o Sistemas de hipótesis:

1.4.1. Hipótesis General

Existe una relación significativa entre el plan de seguridad de la información con la norma ISO/IEC 27001:2005, enla Universidad Nacional Tecnológica de Lima Sur.

1.4.2. Hipótesis Específicas

1. Existe una relación directa y significativa entre la situación actual de la seguridad de la información (Diagnostico) con lo establecido por la norma ISO/IEC 27001:2005, respecto del personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017.

2. Existe una relación directa y significativa entre la seguridad de la información (respecto del cuidado y distribución de la información) con lo establecido por la norma ISO/IEC 27001:2005 en el personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017

3. Existe una relación directa y significativa entre el cumplimiento del plan de seguridad de la información establecido mediante la identificaciónde los puntos fuertes y débiles de los sistemas de información (riesgo) y lo establecido por la norma ISO/IEC 27001:2005 respecto del personal administrativo que manejan dichos sistemas en la Universidad Nacional Tecnológica de Lima Sur en el 2017

4. Existe una relación directa y significativa entre el conocimiento de los accesos a la información, internos y externos (condiciones), con lo establecido por la norma ISO/IEC 27001:2005 en lo referente al personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017.

5. Existe una relación directa y significativa entre la seguridad de información (controles que garanticen la confidencialidad, integridad y disponibilidad de la información) con lo establecido por la norma ISO/IEC 27001:2005, respecto de su manejo por el personal administrativo de la Universidad Nacional Tecnológica de Lima Sur en el 2017.

1.5. Variables

1. Variable independiente : Plan de seguridad de información

- DIMENSIONES
    - Diagnóstico de la situación actual
    - Distribución de la información
    - Riesgo
    - Condiciones de acceso
    - Controles de seguridad de información

2. Variable dependiente : Norma ISO/IEC 27001:2005

- DIMENSIONES
    - Conocimiento de aspectos normados y valorados por ISO 27000

1.6. OPERACIONALIZACION DE VARIABLES

TABLA A: Variables

VARIABLE	DIMENSIONES	INDICADORES	PUNTAJE O VALORACIÓN	TIPO DE INSTRUMENTO
Plan de seguridad de información	Diagnostico	Cobertura de servicios Promedios Calidad Índices Promedios	Escala Likert: 1. Totalmente en desacuerdo 2. En desacuerdo 3. Neutral 4. De acuerdo 5. Totalmente de acuerdo	Test para medir sobre el plan de seguridad de la información
	Cuidado y distribución	Actividades desarrolladas		
	Riesgos	Aspectos críticos		
	Condiciones	Contexto actual		
	Controles	Resultados		

Fuente: elaboración propia

1.7. Justificación e importancia

La seguridad de la información es quizás, una de las razones más importantes del existir de un profesional en tecnologías de información, un ingeniero de sistemas buscará orientar de manera eficiente los procesos de información de Una determinada organización, haciendo énfasis en su objetivo, como insumo primordial en la toma de decisiones.

Esta investigación es necesaria pues pretende aportar con ajustes a modelos concretos de la implementación de un sistema de seguridad de la información en universidades públicas especialmente en la UNTELS. Así también, busca aumentar la cultura de las personas trabajadoras de las diferentes organizaciones gubernamentales en asuntos relacionados a la seguridad de la información haciendo hincapié en la necesidad imperiosa de contar con un

sistema de seguridad de información. Y al mismo tiempo contribuir a cumplir con la normatividad peruana respecto a la Seguridad de la Información.

1.8. Viabilidad

Es viable esta investigación por las siguientes razones:

a) El objeto de estudio son los trabajadores administrativos de la UNTELS.
b) Los objetivos del estudio son alcanzables por la participación de los trabajadores administrativos de la UNTELS que se ofrecieron a participar en dicho estudio.
c) .Disponibilidad de bases teóricas y antecedentes de estudios relacionados al tema de investigación con nivel de evidencia.
d) Existencia de recursos humanos, técnicos, económicos y materiales para la ejecución de la tesis.
e) El investigador posee los conocimientos teóricos y prácticos que pueden llevar a realizar el presente trabajo por su formación profesional.

1.9. Limitaciones

Se han encontrado los siguientes obstáculos:

A. EN CUANTO AL OBJETO DE ESTUDIO

- Lostrabajadores administrativos, que concentran grandes problemas laborales, propios de su labor.
- Los jefes de los trabajadores no permitían mucho las entrevistas y cuestionarios a sus operativos, pese a ser solicitadas con anticipación.

- La universidad se encontraba en periodos largos e intermitentes de huelgas.

- El plan de seguridad de la información de la UNTELS, fue elaborado bajo la norma ISO/IEC 27001:2005, y por ello el estudio de cumplimiento se realizó bajo lo determinado en la norma mencionada.

B. EN CUANTO AL ENFOQUE.

- Poco acceso a las fuentes primarias por que las bibliotecas de las universidades son ilimitadas al público en general.

- Escasas bibliografías y estudios de investigación actualizados para el área de docentes a nivel superior.

- Los trabajadores sentían el estudio como una fuente de ataque a su labor, puesto que se les preguntaba acerca del conocimiento y aplicación de una norma internacional.

C. EN CUANTO A LA LOCALIZACIÓN

- La localización del estudio, trabajadores administrativos de la UNTELS.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes:

- **Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT**

  Investigación tecnológica realizada por De la Cruz Guerrero, César Wenceslao y Vásquez Montenegro, Juan Carlos (2008). Elaboran y aplican un Sistema de Gestión de Seguridad de la Información (SGSI) para mejorar la seguridad de las tecnologías de información y las comunicaciones en la Universidad Católica Santo Toribio de Mogrovejo, efectuando un diagnóstico de la situación actual de la seguridad de información en la organización, evaluando las áreas encargadas del cuidado y distribución de la información y realizando un análisis de riesgos de los puntos fuertes. Logrando desarrollar en la organización el modelo de Sistema de Gestión de Seguridad de la Información (SGSI) protegiendo la información y los activos de la USAT a través de la confidencialidad, integridad y disponibilidad de los datos.

- **Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013**

  Proyecto realizado por Talavera Álvarez, Vasco Rodrigo (2015), en el que se realiza el análisis y diseño de un SGSI para el Instituto Nacional Materno Perinatal, conforme a la normativa referida a la seguridad de la información. En este trabajo se verificó que existe un gran retraso

respecto a la programación establecida por la ONGEI con respecto al proceso de implementación de la NTP ISO/IEC 27001:2008. Y se llega a la conclusión de que en la institución sobre la cual se realizó el proyecto existe una brecha considerable respecto a seguridad de la información y la norma, considera que la principal falencia que debe ser resuelta es involucrar a la alta dirección de la institución en el proceso de implementación del SGSI institucional para así se pueda contar con el apoyo de las diferentes direcciones y áreas de la institución.

- **Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano**

  Trabajo de investigación tecnológica, realizado por Huamán Monzón, Fernando Miguel (2014). En este proyecto se elaboran procedimientos basados en COBIT 5.0 para realizar auditorías que verifiquen el cumplimiento de la NTP-ISO/IEC 27001 en las instituciones públicas del Perú. Se definen los controles que se deben definir e implementar por la entidad, así también, el inventario de activos de información y un mapeo del marco COBIT 5.0 versus la NTP 17799. Luego de realizar las pruebas de los procedimientos se llega a concluir que los procedimientos representan una herramienta muy útil en el proceso de evaluación del cumplimiento de la NTP-ISO/IEC 1779 y NTP-ISO/IEC 27001. Debido a que los procedimientos se enfocan para escenarios de organizaciones del estado peruano, y se recomienda que puedan ser trasladados a empresas del sector privado para que se cuente con una

mejor calidad en lo que respecta a seguridad de la información beneficiando a los ciudadanos y a las organizaciones.

- **Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.**

  Proyecto de Espinoza Aguinaga, Hans Ryan (2013). En este trabajo se toma en cuenta los aspectos más importantes de la ISO/IEC 27001:2005 y desarrolla las etapas del diseño de un SGSI para ser aplicado por una empresa dedicada a la producción de alimentos de consumo masivo en Perú, a fin de cumplir con las normas de regulación vigentes en lo que respecta a seguridad de la información. Concluye que es necesario el apoyo de la alta dirección como promotor activo para el logro de una adecuada gestión de la seguridad de la información. También, recomienda la sensibilización de los empleados sobre seguridad de la información y su importancia así como también, recomienda ejecutar evaluaciones periódicas a los indicadores de seguridad de la empresa de los riesgos que fueron encontrados.

- **Proyecto PYMETICA, ETICOM, asociación de Empresarios de Tecnologías de la Información y Comunicaciones de Andalucía (2002).**

  Orientado a la implementación y certificación de un SGSI en las PYMES de Andalucía según la norma ISO 27001, busca introducir elementos de continuidad de negocio tratando de mejorar la gestión interna de la seguridad de la información. Representó la primera experiencia

agrupada en España orientada a la implementación de un SGSI en las PYMES, orienta a evaluar toda implementación de un plan de seguridad de la información.

2.2. Bases teóricas

La gestión de la información en el contexto de red de usuarios, es una puerta para accesos intrusos. Protegerse de este peligro implica tener un especial cuidado con todo el software empleado, desde el sistema operativo hasta la última de las aplicaciones instalada, cuidando especialmente la configuración de los programas de computadora (Peter, 1996)

Es necesario, no olvidar, que existe la posibilidad que, en estos momentos, existan intrusos informáticos que pueden acceder de manera física al sistema. El avance en las telecomunicaciones ha desembocado en el hecho que se preste una gran vigilancia a la suceso de accesos remotos, sin embargo, de nada sirve evitar esta posibilidad, si se permite el acceso físico al sistema a personas que no están autorizadas. Es por esto que, en algunos casos pueda ser necesario tomar las medidas de seguridad adecuadas sobre el hardware para evitar robos, o pérdidas de información por estos accesos inadecuados.

En resumen, un buen sistema de seguridad debe proteger los sistemas vulnerables ante el posible acceso físico o remoto de intrusos no autorizados. Indiscutiblemente, el nivel de seguridad establecido tendrá que ser consecuente con un análisis previo de los riesgos, tomando en cuenta el impacto de dicho acceso no deseado contra las posibilidades de que este se produzca.

Se pueden adoptar algunas gestiones de seguridad como el cifrado de información sensible para impedir el acceso sin la clave adecuada, métodos físicos de destrucción de la información en caso de manipulación mecánica de la misma, etc.

2.2.1. Norma ISO/IEC 27001:2005

El origen de la Norma ISO/IEC 27001, se remonta desde 1901, y como primera entidad de normalización a nivel mundial se tiene a BSI (British StandardsInstitución), quien es responsable de la publicación de importantes normas como:

- **1979 Publicación BS 5750 - ahora ISO 9001**
- **1992 Publicación BS 7750 - ahora ISO 14001**
- **1996 Publicación BS 8800 - ahora OHSAS 18001**

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa británica un conjunto de buenas prácticas para la gestión de la seguridad de su información. La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de gestión de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte la adoptó ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información (Echeverry & Trujillo, 2009).

2.2.2. La Serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- ISO 27000: contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma es gratuita, a diferencia de las demás de la serie.
- ISO 27001: Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean

seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007.

- ISO 27002: Desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. La norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

Actualmente el ISO-27001:2005 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad. ISO 27001 le permite:

Diseñar una herramienta para la implementación del sistema de gestión de seguridad de la información teniendo en cuenta la política, la estructura organizativa, los procedimientos y los recursos.

A la dirección gestionar las políticas y los objetivos de seguridad en términos de integridad, confidencialidad y disponibilidad.

Determinar y analizar los riesgos, identificando amenazas, vulnerabilidades e impactos en la actividad empresarial.

Prevenir o reducir eficazmente el nivel de riesgo mediante la implementación e implantación de los controles adecuados, preparando

la organización ante posibles emergencias, garantizando la continuidad del negocio(IEC- ISO, 2015)

2.2.3. Normativa

Normatividad peruana sobre seguridad de la información. En el aspecto normativo peruano, se puede relatar como reseña histórica sobre la Norma Técnica Peruana que fue desarrollada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos (EDI), mediante el sistema uno o adopción, entre mayo y octubre del 2008, usando como antecedente la ISO/IEC 27001:2005 Informationtechnology Security techniques – Informationsecuritymanagementsystems –Requiremenst.

El Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos–EDI presentó a la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias -CNB-, con fecha 2008-10-22, el PNTP-ISO/IEC 27001:2008, para su revisión y aprobación, siendo sometido a la etapa de Discusión Publica el 28 de noviembre de 2013. No habiéndose presentado observaciones fue oficializado como Norma Técnica Peruana PNTP-ISO/IEC 27001:2008 EDI.

Esta norma técnica peruana reemplaza a la NTP 821.101:2005 EDI. Sistemas de gestión de seguridad de la información. Especificaciones con guía de uso y es una adopción de la ISO/IEC 27001:2005. La presente norma técnica peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995(FONCODES, 2015)

Esta norma ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener y optimizar un efectivo Sistema de Gestión de Seguridad de la Información ISMS, por sus siglas en Ingles (Information Security Management System). La adopción de un ISMS de una organización está influenciada por las necesidades y objetivos de una organización, requisitos de seguridad, procesos, tamaño y estructura del negocio. Se espera que estos y sus sistemas de aporte cambien a lo largo del tiempo, así como que las situaciones simples requieran soluciones ISMS simples. La norma técnica peruana puede usarse en el ámbito interno y externo de las organizaciones.

Asimismo la norma técnica peruana promueve la aceptación de un enfoque del proceso para establecer, implementar, operar, monitorear, mantener y optimizar la efectividad de un ISMS en la organización.

Una organización debe identificar y administrar varias actividades con el fin de desempeñarse efectivamente. Cualquier actividad que administre y use recursos para lograr la transformación de entradas y salidas, puede ser considerada como un proceso. Con frecuencia la salida de un proceso se convierte en la entrada del proceso siguiente.

El funcionamiento de un sistema de procesos dentro de una organización, junto con la identificación e relaciones de estos procesos y su administración se define como un enfoque de proceso.

El enfoque de proceso motiva a sus usuarios a enfatizar la importancia de:

- Entender los requisitos de seguridad de información de negocios, implementar políticas y objetivos para la seguridad de la información.
- Implementar y operar controles para poder administrar el riesgo total de la organización.
- Monitorear y revisar el desempeño y efectividad del ISMS.
- Mejora continua, que se basa en la medición de objetivos.

2.2.4. Valorativa

El aspecto valorativo de la Tecnología de la Información está basado en el “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información” en entidades del Sistema Nacional de Informática.

A. ISO 27001:2005:

La norma internacional ha sido preparada para proporcionar un modelo que permita establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para la organización. Se espera que la escala de implementación de un SGSI se establezca de acuerdo a las necesidades de la organización, es decir, una situación sencilla requiere una solución de SGSI sencilla (Palacios, 2015).

B. ISO 27002:2005 (anterior ISO 17799:2005):

- Introducción: conceptos generales de seguridad de la información y SGSI.

- Campo de aplicación: se especifica el objetivo de la norma.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- Estructura del estándar: descripción de la estructura de la norma.
- Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- Política de seguridad: documento de política de seguridad y su gestión.
- Aspectos organizativos de la seguridad de la información: organización interna; terceros.
- Gestión de activos: responsabilidad sobre los activos; clasificación de la información.
- Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.
- Seguridad física y ambiental: áreas seguras; seguridad de los equipos.
- Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.
- Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de

acceso a las aplicaciones y a la información; computadoras portátiles y teletrabajo.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.
- Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.
- Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorias de los sistemas de información.

C. Beneficios

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.

- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 1800).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías(Cortés, Marcela, Guzmán, & Victoria, 2012).

2.3. Definiciones conceptuales

2.3.1. Activo de Información

Son recursos que poseen valor o utilidad para la organización. Para que la organización funcione y logre los objetivos que plantea la dirección, son necesarias sus operaciones comerciales y su continuidad. (Fernández, Medina, Moya y Plattini, 2003).

2.3.2. Política de Seguridad de la Información

Es un conjunto de leyes, reglas y prácticas que definen lo que está permitido y lo prohibido regulando la forma de dirigir, proteger y distribuir los recursos en una organización. Permiten definir procedimientos y herramientas necesarias para llevar a cabo los objetivos en cuanto a seguridad informática respecta dentro de la organización (López, 2016).

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

Para que una empresa proteja sus activos de información es necesario seguir algunos pasos. Lo primero es identificar aquellos activos de información que tengan algún impacto significativo en el negocio, después realizar un análisis y evaluación de riesgos de cada activo identificado y finalmente determinar las alternativas más óptimas a implementar para el tratamiento del riesgo y minimizar las posibilidades de que las amenazas puedan causar daño (Alexander G., 2007).

2.3.4. Riesgos

Cualquier cosa que amenace el progreso de un proyecto; algo que bajo ciertas circunstancias puede interferir o interrumpir la buena marcha del proyecto. Está relacionado con algún evento que podría ocurrir y que en caso ocurriese tendría un impacto negativo para el progreso del proyecto (Llorens, 2005).

Se puede realizar un análisis agrupando los fallos de seguridad que se pueden dar en el software. El análisis va a enfocar, más adelante cómo distintos tipos de software ayudan a solventarlos. De una forma simple, se pueden dividir en tres bloques:

- Los defectos debidos a errores desconocidos en el software, o conocidos sólo por terceras entidades atacantes.
- Los defectos debido a errores que no se han arreglado en el software.
- Los defectos que aparecen debido a una inacertada configuración, lo cual puede ocasionar puntos débiles (en cuanto a seguridad) en el sistema

El primer fallo se debe a la calidad del código, el segundo fallo a la efectividad del arreglo de errores en el código, el tercer fallo puede deberse a una falta de documentación del software o un desequilibrio en las capacidades de los administradores para adaptar de manera eficiente el software (Stoneburner, 2001).

Los fallos originan un mal funcionamiento del software, en cuanto a los aspectos de seguridad de la información es alarmante por las siguientes razones

- Es posible implementar rutinas que no funcionen bien, lo cual origina una pérdida de seguridad (por ejemplo, un algoritmo de cifrado que utilice un patrón conocido).
- Es posible que se generen servicios que ofrezcan, de manera involuntaria (por una mala especificación), funcionalidades que no estaban previstas o que puedan vulnerar la seguridad del servidor en donde este alojado el software.
- Es posible que no se hayan seguido las normas de seguridad de la información por tanto, pueden, no existir, medidas de precaución que aseguren el adecuado tratamiento de los inputs al

procesos de la información recibida por la organización. En el sistema puede originar que un atacante destruya la información que reguarda el sistema informático.

2.3.5. Amenaza

Es todo aquello que pueda causar un incidente no deseado generando daños a la organización y a sus activos como por ejemplo la pérdida de información, de la privacidad o un fallo en los equipos físicos (Tupia, 2011).

2.3.6. Vulnerabilidad

Es una debilidad asociada con los activos de la organización. Las debilidades pueden ser explotadas por una amenaza causando incidentes no deseados. La vulnerabilidad no causa daño, es una condición que permite que una amenaza afecte a un activo (Alexander, 2005).

2.3.7. Controles

Para los controles en la implementación y gestión del sistema de seguridad informática, se efectúa un estudio de la situación de la información desde el punto de vista de la seguridad, con el objetivo de identificar las actividades que se han de ejecutar en función de las necesidades detectadas y con ello establecer las políticas, los objetivos, procesos y procedimientos de seguridad de la información según ISO 27000, los cuales apuntan a gestionar el riesgo y mejorar los niveles de seguridad informática, posibilitando obtener resultados conformes con las políticas y objetivos estratégicos de la organización.

Los elementos que manejan la información dentro de una organización no tienen el mismo valor, de la misma manera, no se exponen a los mismos problemas (riesgos), así pues, es necesario realizar un análisis de riesgo que permita valorar los elementos de la información y las amenazas a las que están sometidos, así también los mecanismo y maneras de actuar a fin de reducir los problemas o riesgos detectados(Rodríguez, 1995).

El objetivo de todo este aspecto (controles) es establecer las prioridades en las acciones a trabajar con el objetivo de minimizar los riesgos, esto teniendo como base la premisa de que los riesgos jamás desaparecerán totalmente, la dirección es el ente que asume el posible riesgo producido a pesar de la implementación anterior.

La seguridad de la información basada en ISO 27000, en los departamentos de sistemas (o tecnologías de información) es un tema que está incrementando su popularidad, así pues, se está en aumento la necesidad de evaluar la seguridad y protección de la información, mediante mecanismo claros para efectuar la manipulación de la información contenida en sus archivos y en los dispositivos de almacenamiento digital, la seguridad de las instalaciones donde resguardan las máquinas y archivos de información de la organización, del personal y los usuarios de sistemas y de toda la institución, así como de todo lo relacionado con el resguardo de los sistemas software.

Las áreas comprometidas con la seguridad de la información están enmarcadas dentro de una acción de auditoría, entre las principales evaluaciones se tiene:

- **Evaluación de la seguridad física de la información.**

Se estudian y evalúan los mecanismos de protección física que tiene la información, en archivo y de manera digital, los sistemas software que gestionan los datos, el hardware y su configuración, las personas involucradas, todo los descrito y demás deben estar dentro de los límites permitidos por las políticas establecidas.

- **Evaluación de la seguridad lógica de la información.**

Esta evaluación se concentra en los aspectos de usabilidad que se le da a los sistemas software que se emplean en la organización, la protección de los datos, mediante mecanismos propios del software y de los sistemas gestores de base de datos, y los usuarios con sus respectivos accesos.

- **Evaluación de la seguridad del personal que manipula la información.**

La evaluación de los aspectos de seguridad en el preciso instante del trabajo con la información, ya sea digital o en papel, así también de los equipos a fin de tener un adecuado uso de parte de los empleados, esto es necesario que se tome en cuenta

- **Evaluación de la seguridad de la información y las bases de datos.**

La evaluación de la protección de la información debe enmarcarse dentro de los aspectos de confidencialidad, disponibilidad e integridad. Desde el momento de su acopio, la información deberá estar clasificada, a la mano de quien la desee y tenga los permisos de acceder a ella, y debe permanecer inmutable hasta que por

privilegio, un trabajador pueda cambiar la información(Tipton& Krause, 2007)

Los mecanismos que permitan lo anteriormente descrito deberán estar documentados y aprobados por un comité de seguridad informática.

Evaluación de la seguridad en el acceso y uso del software.

Cuando se busca evaluar la seguridad en la operación del software, debemos identificar las principales vulnerabilidades del software de la entidad, entre los cuales, mencionamos los aspectos siguientes:

- Errores de aplicaciones.
- Errores de sistemas operativos.
- Rutinas de acceso no autorizados.
- Servicios no autorizados(Santos, 2010).

Evaluación de la seguridad en la operación del hardware.

Cuando se evalúa la seguridad en la operación del hardware, se debe identificar las principales vulnerabilidades de hardware, de las cuales se pueden mencionar a continuación:

- Inapropiada operación.
- Fallas en mantenimiento.
- Inadecuada seguridad física.
- Falta de protección contra desastres naturales

Evaluación de la seguridad en las telecomunicaciones.

En las políticas de la organización deben reconocerse que los sistemas, redes y mensajes transmitidos y procesados son propiedad de la organización y no deben usarse para otros fines no autorizados,

por seguridad y por productividad, salvo en emergencias concretas, si allí se ha especificado y mejor dicho, para comunicaciones con voz. Los usuarios tendrán cierta limitación de accesos según dominios, únicamente podrán cargar los programas autorizados, y únicamente podrán cambiar las configuraciones y componentes los técnicos autorizados(Maiwald, 2005).

Se revisarán especialmente las redes cuando existan repercusiones económicas porque se trata de la transferencia de fondos o comercio electrónico. Puntos a revisar:

- Los tipos de redes y conexiones
- Los tipos de transacciones.
- Los tipos de terminales y protecciones: físicas, lógicas, llamadas de retorno.
- La transferencia de ficheros y controles existentes.
- Consideración especial respecto a las conexiones externas a través de pasarelas (gateway) y encaminadores (routers).

2.3.8. Sistema de gestión de la seguridad de la información

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

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe usar un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un 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 modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en un análisis y evaluación de riesgos y en una medición de la eficacia de estos. Por lo tanto el SGSI ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. La aceptación de este estándar debe ser tomada en cuenta como una decisión estratégica para la organización; se pretende que el SGSI se extienda con el tiempo en relación a las necesidades de la organización.

El enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional impulsa que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño del Sistema de Seguridad de la Información.
- Mejoramiento continuo en base a la medición del objetivo(Palacios, 2015).

2.4. Bases epistémicas

La base epistemológica del presente trabajo se presenta como la entidad del conocimiento científico que se ha de tratar, y se enfoca en el cómo, y cuál ha sido el proceso de constitución y desarrollo de los conocimientos científico.

Mediante este proyecto se desea generar un conocimiento de tipo conceptual sobre lo que acontece en la universidad nacional respecto de la implementación de mecanismos referidos a gestionar la información que produce esta; se pretende obtener conocimiento de tipo cualitativo, a partir del análisis de los procesos implementados bajo la norma ISO 27000.

CAPÍTULO III

MARCO METODOLOGICO

3.1 Tipo de investigación

El presente trabajo pertenece a una investigación de tipo básica descriptiva y es correlacional conforme al objetivo que desea lograr:

Descriptiva: Pues hace un intento de determinar los problemas actuales, emplea para ello una descripción y una comprensión de forma íntegra del contexto que actual.

De acuerdo a la técnica de contrastación: la investigación se clasifica en aplicada; pues busca una aplicación de los conocimientos que se acumularán durante el desarrollo del proyecto.

3.2 Diseño y esquema de la investigación.

En este punto se describen los individuos que participaran y apoyaran la investigación, las características de la población o universo de nuestro estudio, así como otras variables que se consideren necesarias.

La presente investigación se lleva a cabo gracias a la investigación de teorías y procesos ya establecidos; personal trabajador de la UNTELS para brindar la información necesaria, con la ayuda de encuestas y entrevistas. También, se trabajara con el personal encargado de la gestión efectiva de la información de la UNTELS (oficina de tecnologías de información) y por ende de la seguridad de la misma, el personal de esta área es más capaz de brindar

información vital, ya que conoce los procesos, instalaciones, las locaciones de cada área, las áreas peligrosas y vulnerables que guardan o transportan la información.

En la UNTELS, en la oficina de tecnologías de información existen 35 personas laborando en la jefatura de sistemas de información, para satisfacer las necesidades de información de la institución, cuenta con un jefe de sistemas. 3 Subjefes de sistemas los cuales se dividen en, operación de sistemas, desarrollo de sistemas y soporte a la red, los que trabajan directamente con la seguridad de información son el área de operación de sistemas y soporte a la red ya que ellos crean los sistemas de transmisión, acceso y almacenamiento de la información, el área de desarrollo de sistemas crea programas para uso interno que le permiten al usuario no experto en sistemas visualizar la información de una manera sencilla.

A su vez cada subjefatura de sistemas de información cuenta con 1 investigador y desarrolladores o ingenieros de soporte, que forman parte del área y hacen posible la realización de las tareas, el área de desarrollo de sistemas cuenta con 9 programadores, las áreas de soporte a la red y operación de sistemas cuentan con 11 ingenieros de soporte cada subjefatura.

La universidad cuenta con 1 dirección general y 12 jefaturas las cuales son finanzas, atención a clientes, planta exterior, sistemas de información, mercadotecnia, ventas, compras e ingeniería, sumando entre todos aproximadamente 120 empleados activos en la organización los cuales aproximadamente 100 son usuarios de los sistemas de información.

De estos sujetos descritos anteriormente obtendremos una muestra de 80 individuos a ser entrevistados para buscar responder nuestros objetivos de investigación y una entrevista para complementar estos datos realizada al Jefe del área de sistemas de información.

3.3 Población y muestra.

La población está conformada por el personal administrativo de la Universidad Nacional Tecnológica de Lima Sur, en un total de 100 (N = 100) administrativos usuarios de los sistemas de información y la muestra de investigación está formada por 80 (n = 80) trabajadores administrativos de la UNTELS.

La investigación se basará en una entrevista al jefe de la oficina de tecnologías de información de la UNTELS, 80 encuestas cerradas realizadas a la muestra de 80 usuarios de sistemas de información y colaboradores del área de sistemas, denominados usuarios expertos, las entrevistas se crearán con base en los objetivos para conocer los diferentes puntos de vista de cada una de las partes en lo que refiere al trabajo referido a la seguridad de la información, según la norma ISO 27000.

Muestreo probabilístico: La muestra de estudio n = 80 está conformada por los administrativos usuarios de los sistemas de información, la muestra representativa fue seleccionada por muestreo probabilístico en la Universidad Nacional Tecnológica de Lima Sur – UNTELS, 2015.

Tabla A: personal administrativo UNTELS

Universidad Nacional Tecnológica de Lima Sur – UNTELS	Cantidad
Personal Administrativo usuario de los sistemas de información.	100

Fuente: Información de la UNTELS

Se aplicó el muestreo aleatorio simple para proporciones con un margen de error de 5% y un nivel de confiabilidad de 95%

Formula:

$$n = \frac{N(P)(Q)(Z^2)}{(N-1)e^2 + (P)(Q)Z^2}$$

Dónde:

N: Población muestreada del estudio (N=100)

P: Probabilidad de éxito obtenido 0.5

Q: 1-0.5 = 0.5 complemento de P

Z: Coeficiente de confiabilidad al 95% igual a 1.96

E: Máximo error permisible en la investigación e = 0.05

Aplicando la fórmula:

$$n = \frac{100(0.5)(0.5)(1.96^2)}{(100-1)0.05^2 + (0.5)(0.5)1.96^2} = 80$$

La muestra en lainvestigación está conformada de n = 80 administrativos del área de sistemas de información de la UNTELS. Este tipo de muestreo en el cual los elementos son escogidos por métodos aleatorios, y en donde todos los elementos tienen la misma probabilidad de ser escogidos como parte de la muestra.

3.4 Instrumentos de recolección de datos:

Las encuestas se aplicaron aleatoriamente a 80 usuarios de los sistemas de información, será una encuesta cerrada eligiendo preguntas que respondan a los objetivos generales y particulares y por supuesto a las hipótesis, posteriormente se graficará y realizará una tabulación completa de los datos obtenidos.

Las preguntas son una manera general de informar y alimentar la investigación para justificar la continuación del trabajo, ya que son una manera abierta de aportar a la exploración en caso de la entrevista (Anexo 4) y una manera complementaria para saber que tanto los usuarios están involucrados con la manera en que se forma la seguridad de la información (Anexo 3).

También, se describe el estudio de la investigación, para fundamentar el análisis y comunicar los resultados obtenidos de los instrumentos y procedimientos de la metodología. Se mostrará los reportes de los resultados del proceso cualitativo con su metodología descriptiva de manera narrativa ya que eso sería el reporte cualitativo.

La entrevista, se aplicó de manera abierta, directamente al jefe de la oficina de tecnologías de información de la institución en investigación, para complementar la información, además de las gráficas y tabulaciones que presentaremos más adelante.

Los resultados obtenidos son producto de una entrevista abierta, serán reales de una muestra cualitativa de lo que para él entrevistado, es la seguridad informática en una organización gubernamental, la entrevista será aplicada el día 30 de julio del 2015,

en las instalaciones de la UNTELS para así tener una idea de que se espera del departamento de sistemas y de la presente investigación.

3.5 Técnicas de recojo, procesamiento y presentación de datos

Después de haber planeado la forma en que se buscaría la información en las distintas fuentes, se organizó la aplicación de los siguientes instrumentos:

TABLA C: Técnicas, instrumentos, fuentes e informantes

TÉCNICA/ MÉTODO	JUSTIFICACIÓN	HERRAMIENTAS	APLICACIÓN
Entrevista	Permite conocer más acerca de los procesos de la institución,sus problemas, objetivos y requerimientos	Una grabadora, Cuestionarios	Trabajadores de las áreas en estudio, personal administrativo de la UNTELS.
Observación	Es el método en la cual enfocamos la perspectiva de los problemas que existen en las áreas a trabajar.	Fichas o guías de observaciones	Trabajadores de las áreas en estudio, personal administrativo de la UNTELS.
Encuestas	Permite conocer las expectativas que tienen los usuarios respecto a los nuevos procesos y necesidades de Información de los usuarios.	Cuestionario del Plan de Seguridad de Información. Escala de Likert con 5 niveles de respuesta. Preguntas abiertas. Cuestionario de la Norma ISO/IEC 27001:2005 Escala dicotómica. Preguntas Cerradas	Trabajadores de las áreas en estudio, personal administrativo de la UNTELS.

Fuente: Elaboración propia

Fuentes de información, equipos y paquetes de cómputo.

Se localizaron las fuentes de información como bibliografía, revistas, Internet, asociaciones de profesionales, de egresados, investigaciones de campo, tesis, etc. Se utilizará un equipo de cómputo e impresoras con software que permite realizar gráficas, tablas, letras y colores con el fin de darle presentación a este proyecto de investigación.

Todos los datos informativos recopilados en fichas de trabajo, bibliográficos, etcétera, se estructurarán en una computadora por medio de herramientas como tablas, graficas, diagramas conforme se fueron dando la planeación, organización, dirección y control para darle forma al proyecto. Con la información ya reflejada será necesario reestructurar las demás partes de la misma sobre la base de los resultados.

El instrumento que se empleará para la recolección de la información, consta de dos instrumentos el cuestionario del Plan de Seguridad de Información (Escala de Likert con 5 niveles de respuesta) y preguntas abiertas, en este tipo de escalas se ofrece una afirmación al sujeto y se pide que la califique del 1 al 5 según su grado de acuerdo con la misma. Cuestionario de la Norma ISO/IEC 27001:2005 Escala dicotómica con preguntas Cerradas para la segunda variable en investigación.

Para la presente investigación se emplearán, además, la ficha textual y el análisis documental. El análisis documental se aplicará a la elaboración del marco teórico, planteamiento metodológico de la investigación y a las estrategias utilizadas para el presente estudio.

Técnicas, Instrumentos, fuentes e informantes

Para la obtención de información se hará uso de herramientas como son: entrevista, encuestas y observación.

Indicadores:

- Para determinar la contrastaciónde la investigación entre las operaciones antes del diseño del SGSI y después del mismo, se han tomado en cuenta los indicadores recomendados por Rodríguez (1995):
- Porcentaje de evaluación de riesgos de seguridad identificados y evaluados con niveles de importancia alta, media o baja.
- Grado de aplicación de políticas de seguridad en la organización.
- Porcentaje de empleados que han recibido y aceptado formalmente, roles y responsabilidades con respecto a seguridad de la información.
- Número de informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización.
- Número y costes acumulados de incidentes por software malicioso como virus, gusanos, troyanos o spam detectados y bloqueados.
- Porcentaje de backups y archivos con datos sensibles o valiosos que se encuentran protegidos dentro y fuera de la empresa.

- Número de incidentes de seguridad de red identificados en los meses anteriores, dividido por categorías de leve importante y grave importancia.
- Número de peticiones de cambios de acceso por parte del personal que labora en la empresa.
- Estado de la seguridad en el entorno portátil (laptops, PDAs, teléfonos móviles, etc.).
- Porcentaje de sistemas para los cuales los controles de validación de datos se han definido e implementado y demostrado eficaces mediante pruebas.
- Porcentaje de sistemas evaluados de forma independiente conforme a estándares de seguridad básica.
- Numero de informes sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo.
- Número de chequeos (a personas a la salida) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.
- Porcentaje de nuevos empleados relacionados con las tecnologías de información y comunicaciones (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar

CAPÍTULO IV

RESULTADOS

4.1 Resultados del trabajo de campo

Luego de haber concluido la etapa de recolección de los datos, se tabulan para ser presentados en cuadros de frecuencia y gráficos correspondientes, para finalizar con algunas recomendaciones que se obtuvieron después de nuestra investigación y análisis de los datos, que como ya se dijo antes la cual tratará la interpretación de los resultados, conclusiones y recomendaciones. En esta parte se dará una discusión de los resultados la cual traducirá e interpretará los hallazgos obtenidos en la investigación y su relación con los objetivos y la hipótesis.

Al finalizar el Plan para la Implementación de la ISO/IEC 27001:2005, se obtendrá los siguientes resultados:

- Contar con un sistema de gestión permite ordenar las actividades de la organización y dirigirlas hacia el objetivo que la empresa busca.
- Lograr alcanzar todos los puntos establecidos en los objetivos propuestos.
- Contar con una política de seguridad de la información, que permita alinear las normas y procedimientos definidos por la organización.

- Gestionar el sistema de gestión de seguridad de la información, de acuerdo a lo definido en las normas ISO 27001 - ISO 27002.
- Cerrar los hallazgos encontrados en las auditorías internas realizadas al SGSI.
- Certificarse en la Norma ISO-27001:2005
- Administrar de forma eficiente los riesgos detectados en la organización y mitigarlos adecuadamente antes de que lleguen a ser un problema.
- Conseguir que el 100% del personal que labora en UNTELS, reporten los incidentes de seguridad de la información, con el fin de prevenir eventos que puedan afectar la continuidad de la formación académica.
- Afianzar los procesos, procedimientos y controles definidos en la continuidad del negocio

4.2 PROCESAMIENTO DE DATOS:

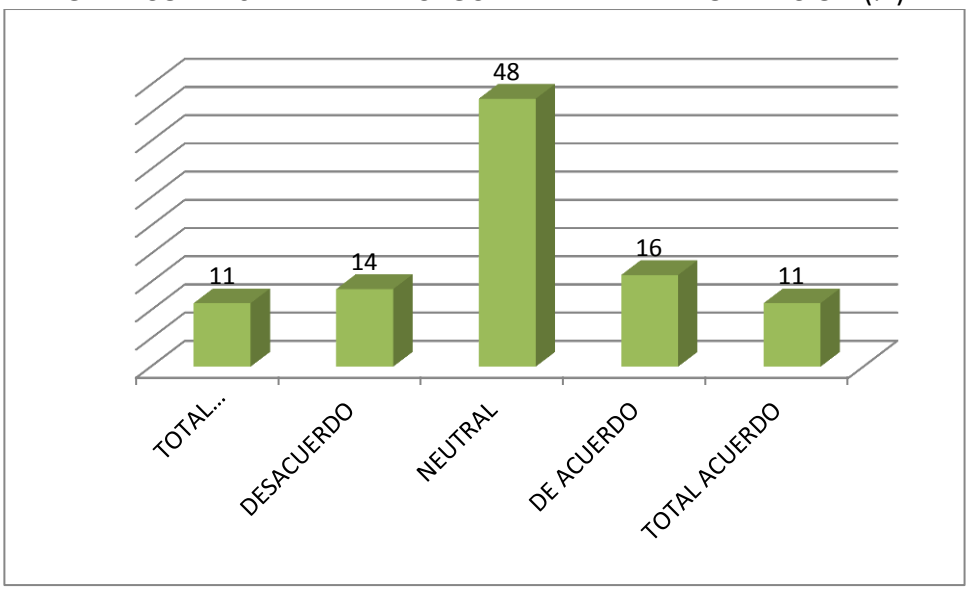
4.2.1. Cumplimiento del plan de seguridad de la información con relación a la norma ISO 27000 en la universidad nacional tecnológica de lima sur.

TABLA Nº 01: PLAN DE SEGURIDAD DE LA INFORMACION

	Frecuencia	Porcentaje
1.- En total Desacuerdo	9	11
2.- En Desacuerdo	11	14
3.- Neutral	38	48
4.- De Acuerdo	13	16
5.- Totalmente de Acuerdo	9	11
Total	80	100

Fuente: Datos obtenidos de la investigación.

GRÁFICO Nº 01: PLAN DE SEGURIDAD DE LA INFORMACION (%)



Fuente: Elaborado por el autor en base al cuadro Nº 01

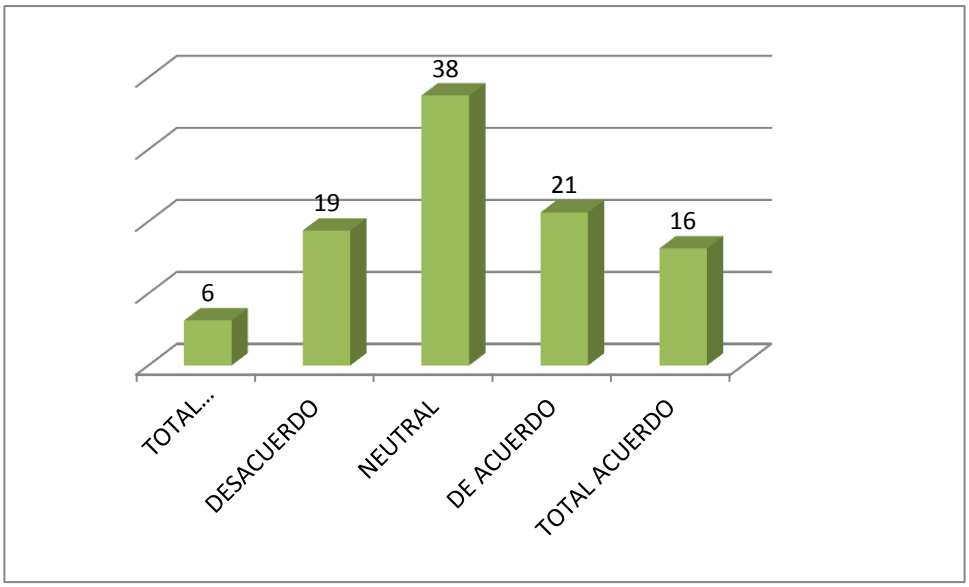
Se observa que el 48% de los encuestados es neutral al plan de seguridad implementado en la UNTELS, el 16 % está de acuerdo, el 11%, está totalmente de acuerdo, mientras que solo el 11% está en total desacuerdo y el 14% en desacuerdo; por lo que podría considerarse que el 75% de los encuestados están de acuerdo con el plan de seguridad de la información, mientras que solo el 25% no está de acuerdo.

TABLA Nº 02: DIAGNOSTICO DEL PLAN DE SEGURIDAD DE LA INFORMACION

	Frecuencia	Porcentaje
1.- En total Desacuerdo	5	6
2.- En Desacuerdo	15	19
3.- Neutral	30	38
4.- De Acuerdo	17	21
5.- Totalmente de Acuerdo	13	16
Total	80	100

Fuente: Datos obtenidos de la investigación

GRÁFICO Nº 02: DIAGNOSTICO DEL PLAN DE SEGURIDAD DELAINFORMACION (%)



Fuente: Elaborado por el autor en base al cuadro Nº 02.

En la información anterior se observa que el 21% de los trabajadores administrativos encuestados están de acuerdo con el diagnóstico del plan de seguridad de la información, el 38% es neutral a ello, el 19% está en desacuerdo, el 16% está totalmente de acuerdo y solo el 6% está en desacuerdo; por lo que podría afirmarse que el 75% de los encuestados están de acuerdo con el diagnóstico realizado y solo el 25% no lo está.

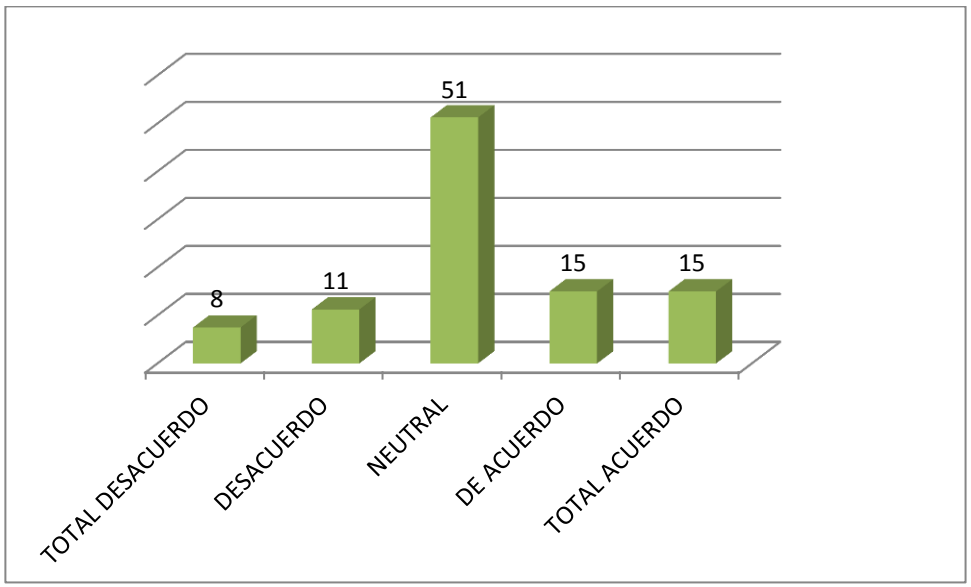
TABLA Nº 03: EVALUACION DE LAS AREAS ENCARGADAS DEL CUIDADO Y DISTRIBUCION DE LA INFORMACION

.

	Frecuencia	Porcentaje
1.- En total Desacuerdo	6	8
2.- En Desacuerdo	9	11
3.- Neutral	41	51
4.- De Acuerdo	12	15
5.- Totalmente de Acuerdo	12	15
Total	80	100

Fuente: Datos obtenidos de la investigación

GRÁFICO Nº 03: EVALUACION DE LAS AREAS ENCARGADAS DEL CUIDADO YDISTRIBUCION DE LA INFORMACION (%)



Fuente: Elaborado por el autor en base al cuadro Nº 03.

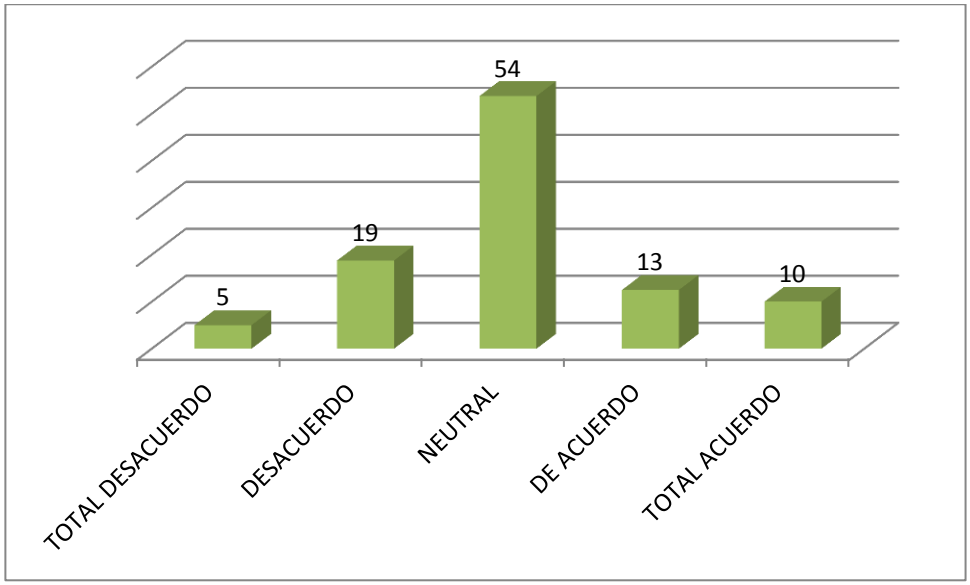
En la información anterior se observa que el 11% se encuentra en desacuerdo, el 15% está de acuerdo, el 51% es neutral, el 8% está en total desacuerdo y solo el 15% está totalmente de acuerdo con que se tiene cuidado y distribución con todo tipo de información en su área.

TABLA Nº 04: ANALISIS DE RIESGOS DE LOS PUNTOS FUERTES Y DEBILES DE LOS
SISTEMAS DE LA INFORMACION.

	Frecuencia	Porcentaje
1.- En total Desacuerdo	4	5
2.- En Desacuerdo	15	19
3.- Neutral	43	54
4.- De Acuerdo	10	13
5.- Totalmente de Acuerdo	8	10
Total	80	100

Fuente: Datos obtenidos de la investigación

GRÁFICO Nº 04: ANALISIS DE RIESGOS DE LOS PUNTOS FUERTES Y DEBILES DE LOS SISTEMAS DE LAINFORMACION (%)



Fuente: Elaborado por el autor en base al cuadro Nº 04.

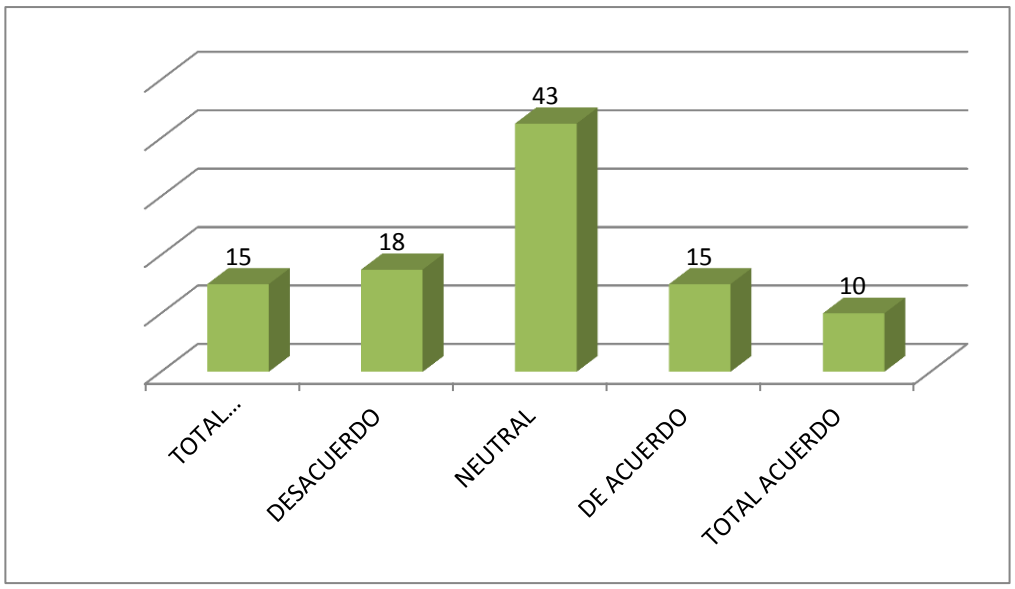
De la información anterior se deduce que el 54% es neutral, el 19% está en desacuerdo, el 13% está de acuerdo, el 10% está totalmente de acuerdo y el 5% está totalmente en desacuerdo; se puede concluir que el 77% está de acuerdo con el análisis de riesgos realizados, mientras que el 23% está en desacuerdo.

TABLA Nº 05: CONSIDERA QUE EXISTEN CONDICIONES DE ACCESO ADECUADAS
PARA LA MINIPULACION CORRECTA DE LA INFORMACION.

	Frecuencia	Porcentaje
1.- En total Desacuerdo	12	15
2.- En Desacuerdo	14	18
3.- Neutral	34	43
4.- De Acuerdo	12	15
5.- Totalmente de Acuerdo	8	10
Total	80	100

Fuente: Datos obtenidos de la investigación

GRÁFICO Nº 05: CONSIDERA QUE EXISTEN CONDICIONES DE ACCESO ADECUADAS PARA LA MINIPULACION CORRECTA DE LA INFORMACION (%)



Fuente: Elaborado por el autor en base al cuadro Nº 05.

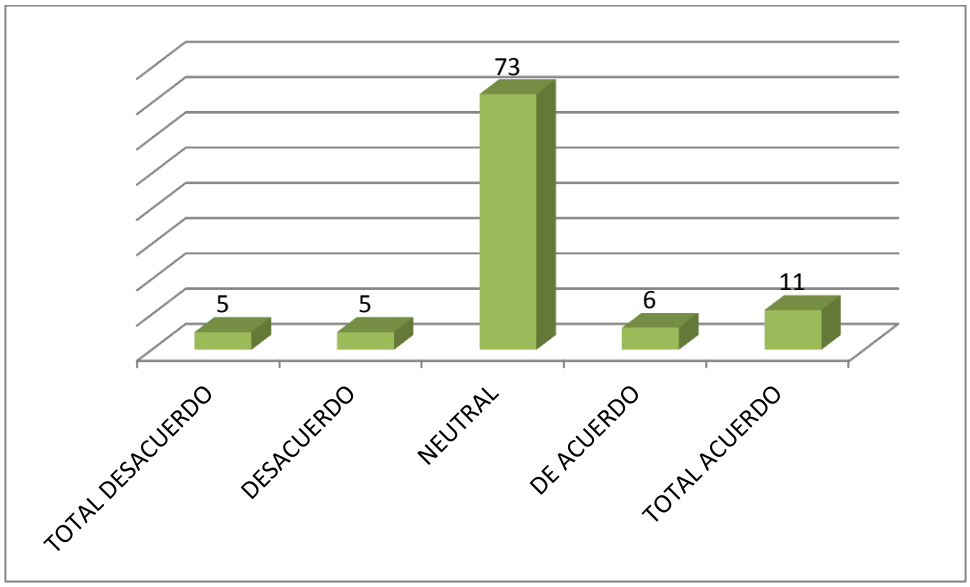
De la información anterior se puede deducir de que el 33% (15% total desacuerdo y 18% en desacuerdo) considera que no existen condiciones adecuadas para acceder correctamente la información, mientras de que el 77% (43% es neutral, 15% está de acuerdo y 10% totalmente de acuerdo) manifiesta que si existen dichas condiciones.

TABLA Nº 06: LA SELECCIÓN DE LOS CONTROLES DE LA SEGURIDAD DE LA INFORMACION MAS IMPORTANTES GARANTIZAN LA CONFIABILIDAD, INTEGRIDAD Y DISPONIBLIDAD DE LA INFORMACION.

	Frecuencia	Porcentaje
1.- En total Desacuerdo	4	5
2.- En Desacuerdo	4	5
3.- Neutral	58	73
4.- De Acuerdo	5	6
5.- Totalmente de Acuerdo	9	11
Total	80	100

Fuente: Datos obtenidos de la investigación

GRÁFICO Nº 06: LA SELECCIÓN DE LOS CONTROLES DE LA SEGURIDAD DE LA INFORMACIONMAS IMPORTANTES GARANTIZAN LACONFIABILIDAD, INTEGRIDAD Y DISPONIBLIDAD DE LAINFORMACION (%)



Fuente: Elaborado por el autor en base al cuadro Nº 06.

En la información anterior se puede notar que el 10% de los encuestados están en desacuerdo y el 90% señalan que los controles de seguridad de la información adoptados garantizan la confiablidad, integridad y disponibilidad de la información.

4.2.2. DESCRIPTIVAS – VARIABLE DEPENDIENTE: NORMA ISO/IEC 27001:2005.

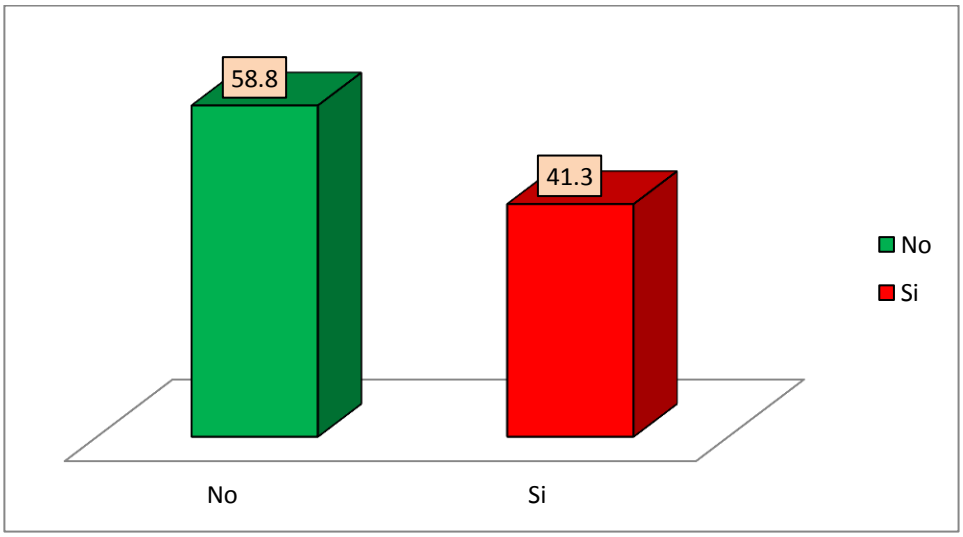
TABLA N° 07: SU ÁREA HA ESTABLECIDO NORMATIVAS PARA MANEJO DE LA INFORMACIÓN QUE PROCESA, RECIBE O GENERA

.

	Frecuencia	Porcentaje
No	47	58.8
Si	33	41.3
Total	80	100.0

Fuente: Datos obtenidos de la investigación

GRÁFICO N° 07: SU ÁREA HA ESTABLECIDO NORMATIVAS PARA MANEJO DE LA INFORMACIÓN QUE PROCESA, RECIBE O GENERA



Fuente: elaborado por el autor en base al cuadro Nº 07

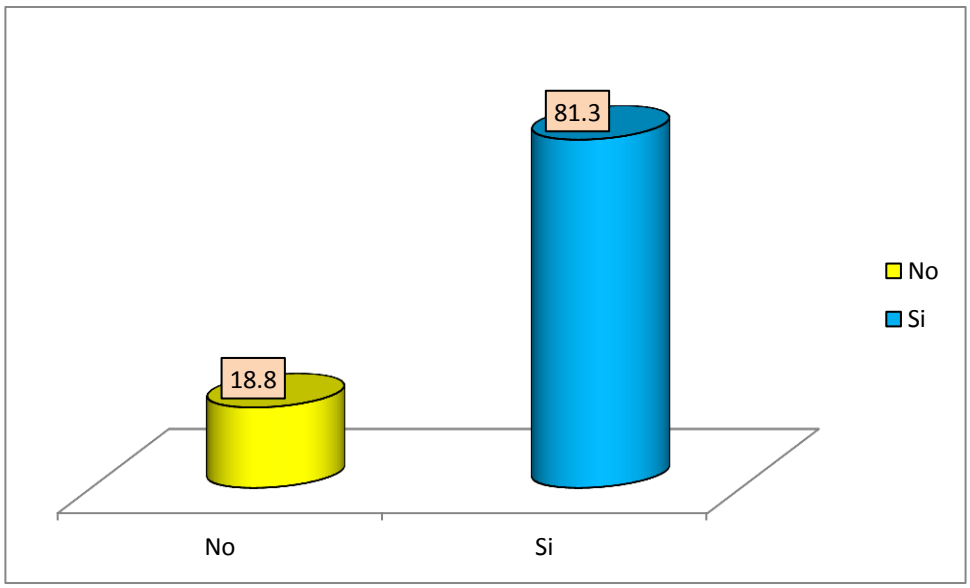
En la medición del item 1 ¿Su área ha establecido normativas para manejo de la información que procesa, recibe o genera? Apreciamos que el 58.8% de los encuestados expresan que no se han establecido y el 41% expresa que si se han establecido.

TABLA N° 08: EXISTEN PROCESOS DEFINIDOS DEL MANEJO (TRATAMIENTOS) DE LAINFORMACIÓN QUE SE GENERA EN SU ÁREA.

	Frecuencia	Porcentaje
No	15	18.8
Si	65	81.3
Total	80	100.0

Fuente: Datos obtenidos de la investigación.

GRÁFICO N° 08: EXISTEN PROCESOS DEFINIDOS DEL MANEJO (TRATAMIENTOS) DE LAINFORMACIÓN QUE SE GENERA EN SU ÁREA.



Fuente: Elaborado por el autor en base al cuadro Nº 08.

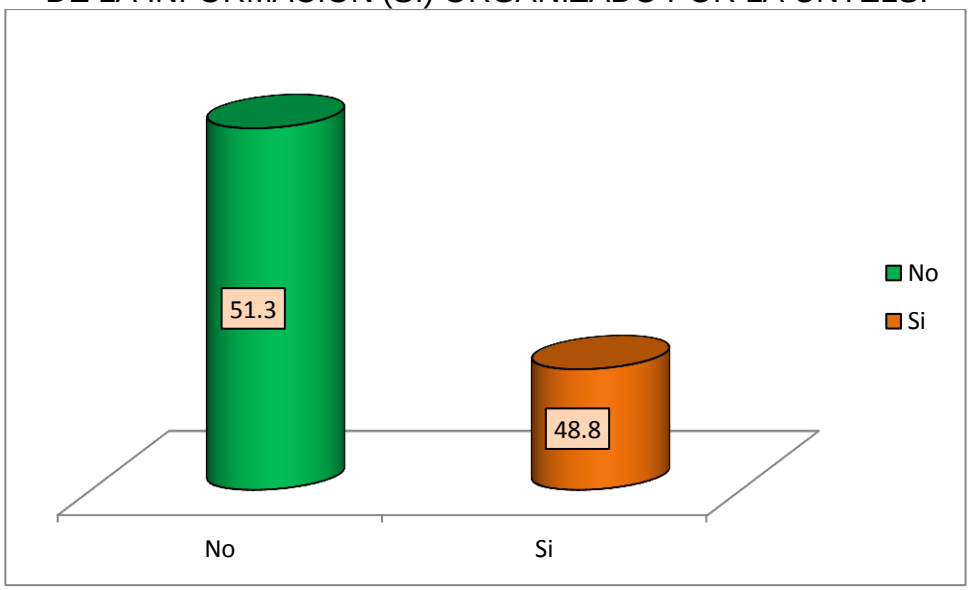
En la medición del ítem 2 ¿Existen procesos definidos del manejo (tratamientos) de la información que se genera en su área? Al respecto se observa que el 18.8% manifiesta que no existen proceso, mientras que el 81.3% dice que si existen dichos procesos.

TABLA N° 09: HA ASISTIDO A CAPACITACIONES SOBRE SEGURIDAD DE LA INFORMACIÓN (SI) ORGANIZADO POR LA UNTELS.

	Frecuencia	Porcentaje
No	41	51.3
Si	39	48.8
Total	80	100.0

Fuente: Datos obtenidos de la investigación.

GRÁFICO N° 09: HA ASISTIDO A CAPACITACIONES SOBRE SEGURIDAD DE LA INFORMACIÓN (SI) ORGANIZADO POR LA UNTELS.



Fuente: Elaborado por el autor en base al cuadro 09.

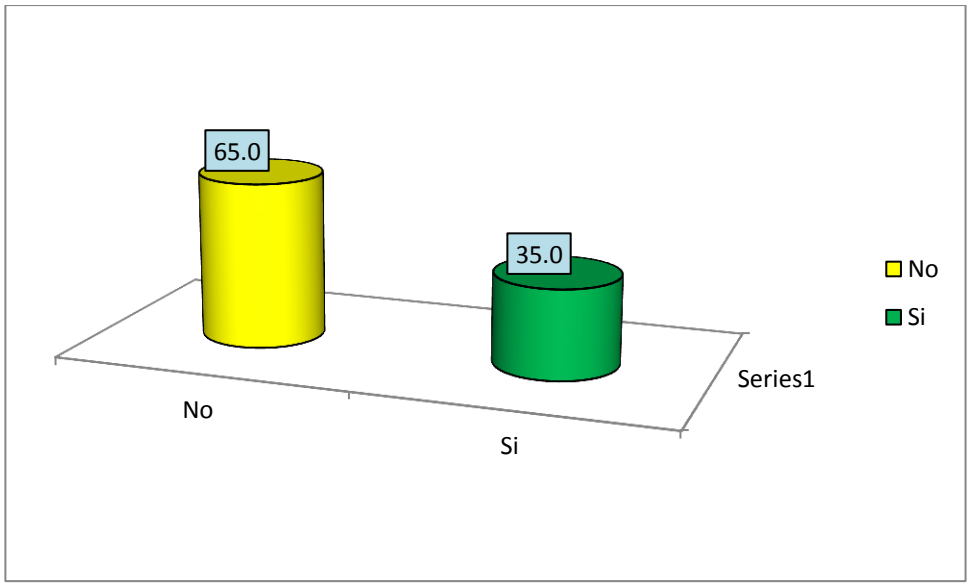
En la medición del ítem 3 ¿Ha asistido a capacitaciones sobre seguridad de la información (SI) organizado por la UNTELS? Al respecto se observan, que el 51.3% manifiesta que no han existido y el Si 48.8% dicen que si existieron capacitaciones.

TABLA N° 10: SE HACEN AUDITORIAS O CONTROLES PERIÓDICAS SOBREMANIPULACIÓN Y ALMACENAMIENTO DE LA INFORMACIÓN QUE SETRATA EN SU ÁREA

	Frecuencia	Porcentaje
No	52	65.0
Si	28	35.0
Total	80	100.0

Fuente: Datos obtenidos de la investigación.

GRÁFICO N° 10: SE HACEN AUDITORIAS O CONTROLES PERIÓDICAS SOBRE MANIPULACIÓN Y ALMACENAMIENTO DE LA INFORMACIÓN QUE SE TRATA EN SU ÁREA



Fuente: Elaborado por el autor en base al cuadro Nº 10.

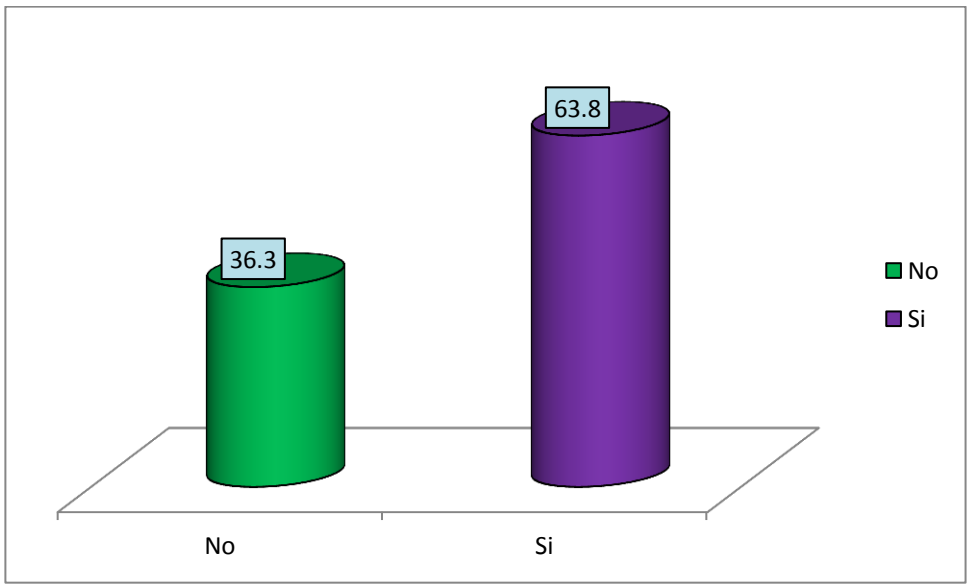
En la medición del ítem 4 ¿Se hacen auditorias o controles periódicas sobre manipulación y almacenamiento de la información que se trata en su área? Al respecto se observan: que el 65% manifiestan que no han existido, mientras que el Si 35 % dicen que si existieron.

TABLA N° 11:SI UN ENTE DE MAYOR JERARQUÍA A LA DE USTED SOLICITA INFORMACIÓN DE SU ÁREA ¿DEMORA MÁS DE 24 HORAS EN SER ATENDIDO?

	Frecuencia	Porcentaje
No	29	36.3
Si	51	63.8
Total	80	100.0

Fuente: Datos obtenidos de la investigación.

CUADRO N° 11: SI UN ENTE DE MAYOR JERARQUÍA A LA DE USTED SOLICITA INFORMACIÓN DE SU ÁREA ¿DEMORA MÁS DE 24 HORAS ENSER ATENDIDO?



Fuente: Elaborado por el autor en base al cuadro Nº 11.

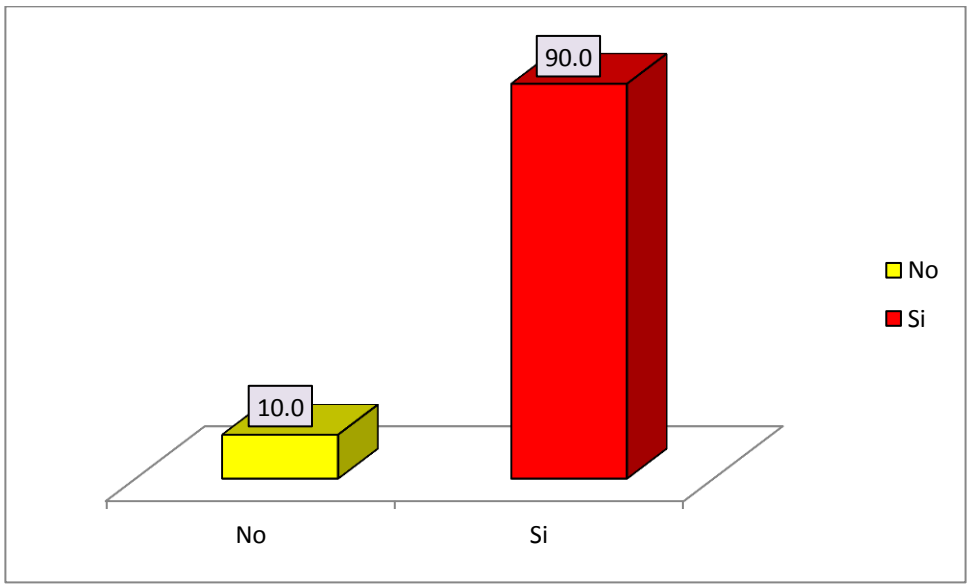
En la medición del ítem 5 Si un ente de mayor jerarquía a la de Usted solicita información de su área ¿Demora más de 24 horas en ser atendido? Al respecto se observan que el 36.3% dicen que no mientras que el 63.8% manifiestan de que si demoran más de 24 horas.

TABLA N° 12: HAY PRIORIDAD EN EL OTORGAMIENTO DE LOS RECURSOSMATERIALES QUE SE USA EN SU TRABAJO CON LOS SISTEMAS.

	Frecuencia	Porcentaje
No	8	10.0
Si	72	90.0
Total	80	100.0

Fuente: Datos obtenidos de la investigación

GRÁFICO N° 12: HAY PRIORIDAD EN EL OTORGAMIENTO DE LOS RECURSOSMATERIALES QUE SE USA EN SU TRABAJO CON LOS SISTEMAS.



Fuente: Elaborado por el autor en base al cuadro 12

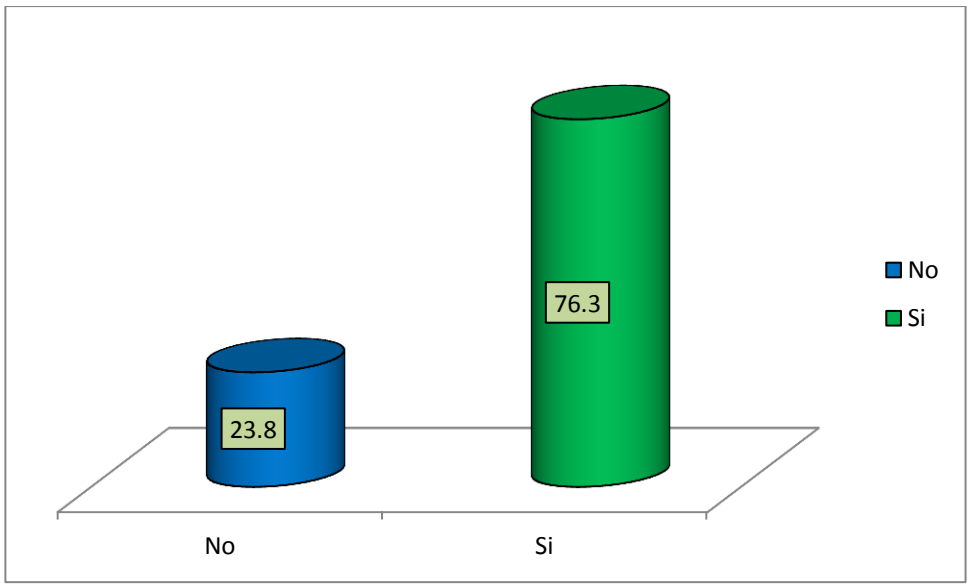
En la medición del ítem 6 ¿Siente que hay prioridad en el otorgamiento de los recursos materiales que se usa en su trabajo con los sistemas? Al respecto se observan que el 10% manifiesta que no, mientras que el 90%. Dice que si lo hubo.

TABLA N° 13: CONSIDERA QUE SU ENTORNO LABORAL ES ADECUADO PARA EL DESARROLLO DE SEGURIDAD EN LOS SISTEMAS.

	Frecuencia	Porcentaje
No	19	23.8
Si	61	76.3
Total	80	100.0

Fuente: Datos obtenidos de la investigación.

GRÁFICO N° 13:CONSIDERA QUE SU ENTORNO LABORAL ES ADECUADO PARA EL DESARROLLO DE SEGURIDAD EN LOS SISTEMAS.



Fuente: Elaborado por el autor en base al cuadro Nº 13

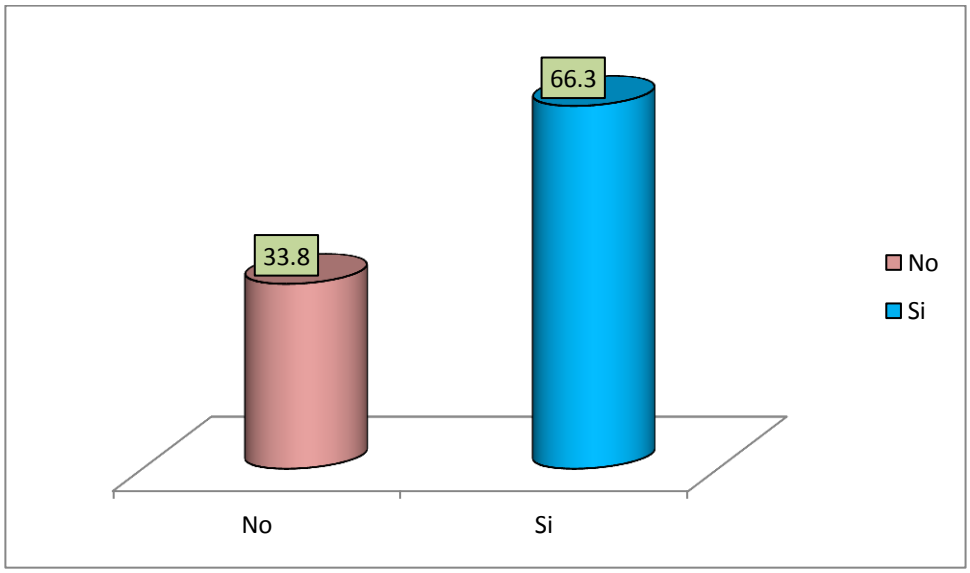
En la medición del ítem 7 ¿Considera que su entorno laboral es adecuado para el desarrollo de Seguridad en los Sistemas? Al respecto se observan que el 23.8% manifiestan que no, mientras que el 76.3% dice que si es el adecuado.

TABLA N° 14: EN GENERAL LA UNIVERSIDAD ESTÁ PREPARADA PARA IMPLEMENTAR LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN

	Frecuencia	Porcentaje
No	27	33.8
Si	53	66.3
Total	80	100.0

Fuente: Datos obtenidos de la investigación.

GRÁFICON°14:EN GENERAL LA UNIVERSIDAD ESTÁ PREPARADA PARA IMPLEMENTAR LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN.



Fuente: Elaborado por el autor en base al cuadro Nº 14.

En la medición del ítem 8 ¿En general la Universidad está preparada para implementar la seguridad en Sistemas de Información? Al respecto se observan que el No tiene el 38.8% y el Si 66.3 %.

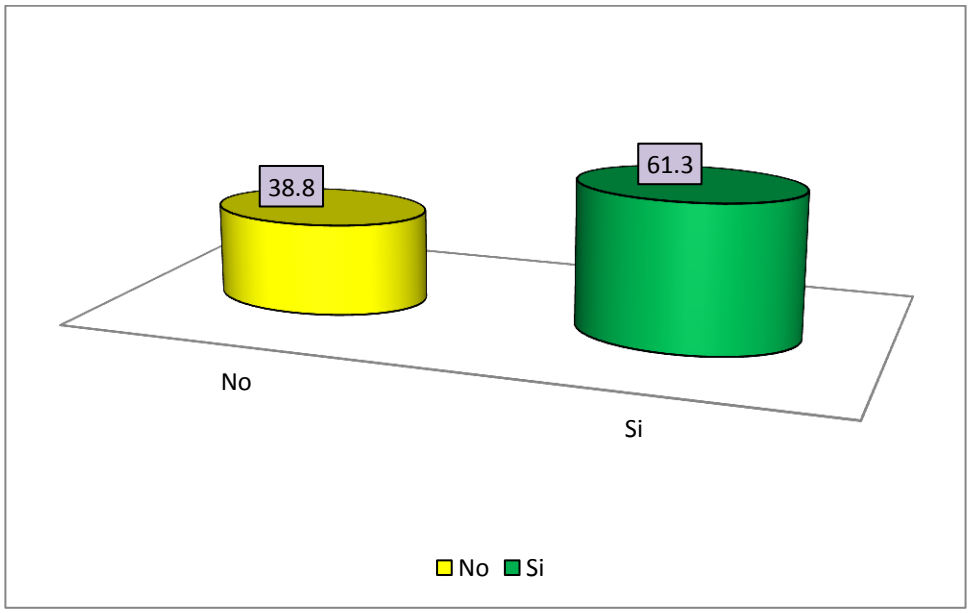
TABLA N° 15: MIS COMPAÑEROS DE TRABAJO PIENSAN QUE SE DEBE IMPLEMENTARLA SEGURIDAD EN SISTEMAS DE INFORMACIÓN

.

	Frecuencia	Porcentaje
No	31	38.8
Si	49	61.3
Total	80	100.0

Fuente: Datos obtenidos de la investigación.

GRÁFICO N° 15:MIS COMPAÑEROS DE TRABAJO PIENSAN QUE SE DEBE IMPLEMENTARLA SEGURIDAD EN SISTEMAS DE INFORMACIÓN.



Fuente: Elaborad por el autor en base al cuadro Nº 15

En la medición del ítem 9 ¿Mis compañeros de trabajo piensan que se debe implementar la seguridad en Sistemas de Información? Al respecto se observan que el 38.8% dicen que no, mientras que el 61.3 % manifiestan que Sí.

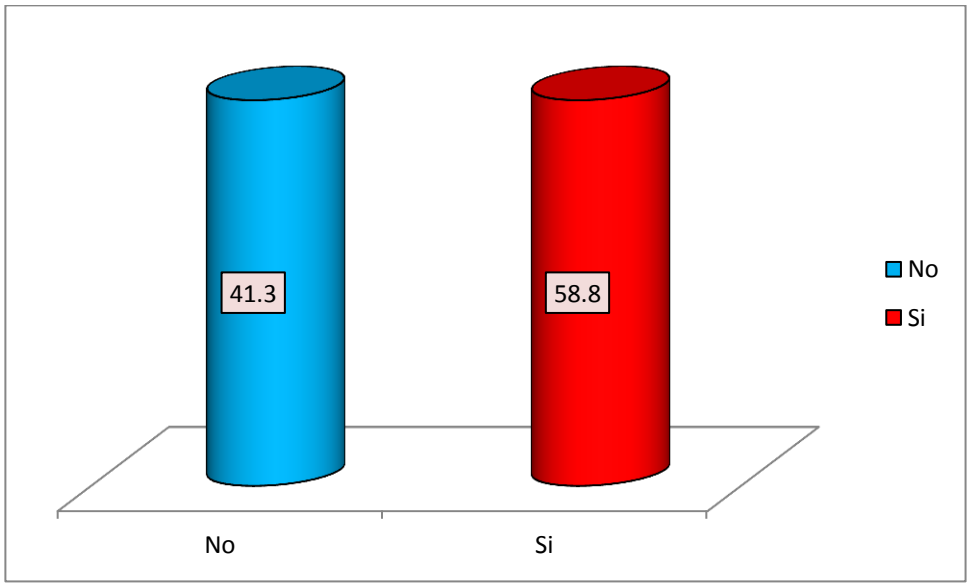
TABLA N° 16:MI JEFE INMEDIATO PIENSA QUE SE DEBE IMPLEMENTAR LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN

.

	Frecuencia	Porcentaje
No	33	41.3
Si	47	58.8
Total	80	100.0

Fuente: Datos obtenidos de la investigación.

GRÁFICO N° 16:MI JEFE INMEDIATO PIENSA QUE SE DEBE IMPLEMENTAR LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN.



Fuente: Elaborado por el autor en base al cuadro Nº 16

En la medición del ítem 10 ¿Mi jefe inmediato piensa que se debe implementar la seguridad en Sistemas de Información? Al respecto se observan que el 41.3% dicen que No, mientras que el 58.8 % manifiesta que Sí.

4.3 CONTRASTACIÓN DE LOS RESULTADOS

Prueba de hipótesis

Hipótesis General: El plan de seguridad de la información se relaciona significativamente con la norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur.

Hipótesis Nula Ho: El plan de seguridad de la información no se relaciona significativamente con la norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur

Hipótesis Alterna Ha: El plan de seguridad de la información si se relaciona significativamente con la norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur

Prueba Estadística.

Se aplicó la prueba No Paramétrica del Chi cuadrado:

$$x^2 = \sum \frac{(O-E)^2}{E}$$

O = Frecuencia observada en cada celda

E = Frecuencia esperada en cada celda

∑ =Sumatoria

X2 = Chi cuadrado calculada

Determinación de la zona de rechazo de la hipótesis nula

Nivel de confianza al 95%

Valor de significancia: $\alpha = 0.05$

Grados de Libertad = (k-1)(r-1) = (2-1)(5-1) = 4(k: es número de filas, r es número de columnas)

Zona de rechazo de Hipótesis nula: $x_c^{\,2} > x_t^{\,2}$

TABLA N° 17:
CONTINGENCIA (2 X 5) DE PLAN DE SEGURIDAD DE LA INFORMACIÓN CON LA NORMA ISO/IEC 27001:2005.

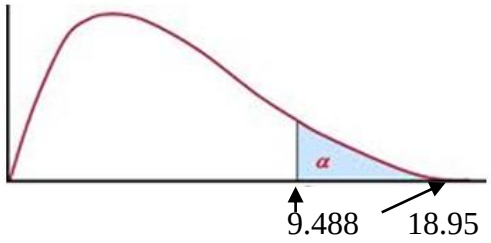
		Plan de seguridad de la información					
		En total Desacuerdo	En Desacuerdo	Neutral	De Acuerdo	Totalmente de Acuerdo	Total
Norma ISO/IEC 27001:2005	No	8	8	24	3	1	44
	Si	1	3	14	10	8	36
Total		9	11	38	13	9	80

Fuente: Datos obtenidos de la investigación

Prueba de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	18.95[a]	4	,003
Razón de verosimilitud	13,322	4	,149
Asociación lineal por lineal	3,876	1	,049
N de casos válidos	5		

a. 16 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,20.



X^2_t Crítico = 9.488

X^2_ccalculado = 18.95

como $T_c > T_t$ ⟶ se rechaza Ho

Interpretación: El valor calculado del Chi cuadrado de la prueba estadística de hipótesis es 18.95; que resulta ser superior al valor de la tabla en un nivel de confianza de 95% (13.30> 9.488). Por lo tanto se acepta la hipótesis alternativa (Ha) y se rechaza la hipótesis nula de investigación (Ho), lo que nos indica efectivamente que el plan de seguridad de la información se relaciona significativamente con la Norma ISO/IEC 27001:2005 en la UNTELS.

4.4 HIPÓTESIS ESPECÍFICAS

Hipótesis específica 1: Existe una relación directa y significativa entre la situación actual de la seguridad de la información (Diagnostico) con lo establecido por la norma ISO/IEC 27001:2005, respecto del personal administrativo de la UNTELS en el 2017.

Ho. El diagnóstico del plan de seguridad de la información no se relaciona significativamente con la norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur,respecto del personal administrativo

Ha.El diagnóstico del plan de seguridad de la información si se relaciona significativamente con la norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur, respecto del personal administrativo.

Prueba Estadística.

Prueba estadística : Chi cuadrada

$$x^2 = \sum \frac{(O-E)^2}{E}$$

O = Frecuencia observada en cada celda

E = Frecuencia esperada en cada celda

∑ =Sumatoria

X2 = Chi cuadrado obtenida u observada

Nivel de significancia : α = 0.05

Grado de libertad : 4

Punto crítico según tabla : X2(4) (0.95) = 9.844

gl	0.05
4	9.844

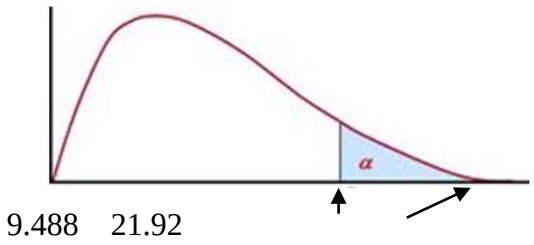
TABLA N° 18:
CONTINGENCIA (2 X 5) EL DIAGNÓSTICO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN Y NORMA ISO/IEC 27001:2005.

		El diagnóstico del plan de seguridad de la información					
		En total Desacuerdo	En Desacuerdo	Neutral	De Acuerdo	Totalmente de Acuerdo	Total
Norma ISO/IEC 27001:2005	No	4	8	24	7	1	44
	Si	1	7	6	10	12	36
Total		5	15	30	17	13	80

Prueba chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	21.920[a]	4	,241
Razón de verosimilitud	13,322	4	,346
Asociación lineal por lineal	3,283	1	,070
N de casos válidos	5		

a. 20 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,20.



X^2_t Crítico = 9.488

X^2_ccalculado = 21.92

como $T_c > T_t$ ⟶ se rechaza Ho

Interpretación:

El valor calculado del Chi cuadrado de la prueba de hipótesis es 21.92; que resulta ser superior al valor de la tabla en un nivel de confianza del 95% (21.92>9.488); Por lo tanto se acepta la hipótesis alternativa (Ha) y se rechaza la hipótesis nula de investigación (Ho), lo cual nos indica que efectivamente el diagnóstico del plan de seguridad de la información se relaciona significativamente con la Norma ISO/IEC 27001:2005 en la UNTELS.

Hipótesis Específica 2: Existe una relación directa y significativa entre la seguridad de la información (respecto del cuidado y distribución de la información) con lo establecido por la norma ISO/IEC 27001:2005 en el personal administrativo de la UNTELS en el 2017.

Ho. La evaluación del cuidadoy distribución de la información, no se relacionan significativamente con la norma ISO/IEC 27001:2005, en el personal administrativo de la UNTELS.

Ha. La evaluación del cuidado y distribución de la información, si se relacionan significativamente con la norma ISO/IEC 27001:2005, en el personal administrativo de la UNTELS.

Prueba Estadística.

Prueba estadística : Chi cuadrada

$$x^2 = \sum \frac{(O-E)^2}{E}$$

O = Frecuencia observada en cada celda

E = Frecuencia esperada en cada celda

∑ =Sumatoria

X2 = Chi cuadrado obtenida u observada

Nivel de significancia : α = 0.05

Grado de libertad : 4

Punto crítico según tabla : X2(4) (0.95) = 9.844

gl	**0.05**
4	**9.844**

TABLA N° 19:
CONTINGENCIA (2 X 5) DE EVALUACIÓN DE ÁREAS ENCARGADAS (CUIDADO Y DISTRIBUCIÓN) Y NORMA ISO/IEC 27001:2005.

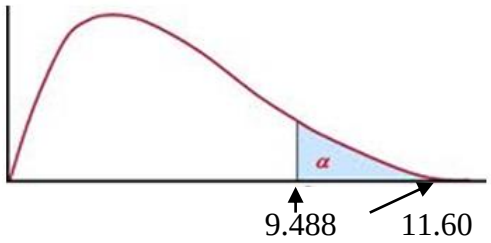
		Evaluación de las áreas encargadas (cuidado y distribución)					
		En total Desacuerdo	En Desacuerdo	Neutral	De Acuerdo	Totalmente de Acuerdo	Total
Norma ISO/IEC 27001:2005	No	5	6	26	5	2	44
	Si	1	3	15	7	10	36
Total		6	9	41	12	12	80

Fuente: Datos obtenidos de la investigación

PRUEBA CHI-CUADRADO

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	11,60[a]	4	,259
Razón de verosimilitud	10,549	4	,308
Asociación lineal por lineal	3,716	1	,054
N de casos válidos	5		

a. 16 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,20.



X^2_t Crítico = 9.488

X^2_ccalculado = 11.60

como $T_c > T_t$ ⟶ se rechaza Ho

Interpretación: El valor calculado del Chi cuadrado de la prueba estadística de hipótesis es 11.60; que resulta ser superior al valor de la tabla en un nivel de confianza del 95% (11.60>9.488). Por lo tanto se acepta la hipótesis alternativa (Ha) y se rechaza la hipótesis nula de investigación (Ho), y se concluye que efectivamente la evaluación del cuidado y distribución de la información, se relacionan significativamente con la norma ISO/IEC 27001:2005 en la UNTELS.

Hipótesis Específica 3: Existe una relación directa y significativa entre el cumplimiento del plan de seguridad de la información establecido mediante la identificación de los puntos fuertes y débiles de los sistemas de información (riesgo) y lo establecido por la norma ISO/IEC 27001:2005 respecto del personal administrativo que manejan dichos sistemas en la UNTELS en el 2017.

Ho. La identificación a través del análisis de riesgo los puntos fuertes y débiles de los sistemas de información según norma no se relacionan significativamente con la norma ISO/IEC 27001:2005.

Ha. La identificación a través del análisis de riesgo los puntos fuertes y débiles de los sistemas de información según norma si se relacionan significativamente con la norma ISO/IEC 27001:2005.

Prueba Estadística.

Prueba estadística : Chi cuadrada

$$x^2 = \sum \frac{(O-E)^2}{E}$$

O = Frecuencia observada en cada celda

E = Frecuencia esperada en cada celda

∑ =Sumatoria

X2 = Chi cuadrado obtenida u observada

Nivel de significancia : α = 0.05

Grado de libertad : 4

Punto crítico según tabla : X2(4) (0.95) = 9.844

gl	0.05
4	9.844

TABLA N° 20:
CONTINGENCIA (2 X 5) DEL ANÁLISIS DE RIESGO LOS PUNTOS FUERTES Y DÉBILES DE LOS SISTEMAS DE INFORMACIÓN Y NORMA ISO/IEC 27001:2005

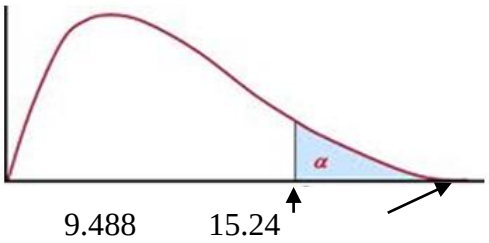
		Análisis de riesgo los puntos fuertes y débiles de los sistemas de información.					
		En total Desacuerdo	En Desacuerdo	Neutral	De Acuerdo	Totalmente de Acuerdo	Total
Norma ISO/IEC 27001:2005	No	3	8	30	2	1	44
	Si	1	7	13	8	7	36
Total		4	15	43	10	8	80

Fuente: Datos obtenidos de la investigación

Prueba chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	15,240[a]	4	,241
Razón de verosimilitud	13,322	4	,346
Asociación lineal por lineal	3,964	1	,046
N de casos válidos	5		

a. 20 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,20.



X^2_t Crítico = 9.488

X^2_c calculado = 15.24

como $T_c > T_t \longrightarrow$ se rechaza Ho

Interpretación: El valor calculado del Chi cuadrado de la prueba estadística de hipótesis es 15.24; que resulta ser superior al valor de la tabla en un nivel de confianza del 95% (15.24>9.488); por lo tanto se acepta la hipótesis alterna (Ha) y se rechaza la hipótesis nula de investigación (Ho), y se concluye que efectivamente la identificación a través del análisis de riesgo los puntos fuertes y débiles de los sistemas de información según norma se relacionan significativamente con la norma ISO/IEC 27001:2005 en la UNTELS.

Hipótesis Específica 4: Existe una relación directa y significativa entre el conocimiento de los accesos a la información, internos y externos (condiciones [de acceso]), con lo establecido por la norma ISO/IEC 27001:2005 en lo referente al personal administrativo de la UNTELS en el 2017.

Ho. El conocimiento de las diferentes condiciones de acceso a la información, tanto externo como interno, no se relacionan significativamente con la norma ISO/IEC 27001:2005.

Ha. El conocimiento de las diferentes condiciones de acceso a la información, tanto externo como interno, si se relacionan significativamente con la norma ISO/IEC 27001:2005.

Prueba Estadística.

Prueba estadística : Chi cuadrada

$$x^2 = \sum \frac{(O-E)^2}{E}$$

O = Frecuencia observada en cada celda

E = Frecuencia esperada en cada celda

∑ =Sumatoria

X2 = Chi cuadrado obtenida u observada

Nivel de significancia : α = 0.05

Grado de libertad : 4

Punto crítico según tabla : X2(4) (0.95) = 9.844

gl	0.05
4	9.844

TABLA N° 21:
CONTINGENCIA (2 X 5) DEL CONOCIMIENTO DE ASPECTOS NORMADOS POR ISO 27000 PARA LOS SISTEMAS DE INFORMACIÓN Y NORMA ISO/IEC 27001:2005

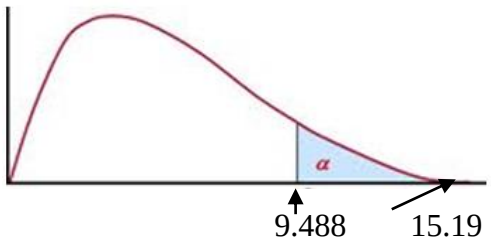
		Conocimiento aspectos normados por ISO 27000para los sistemas de información.					
		En total Desacuerdo	En Desacuerdo	Neutral	De Acuerdo	Totalmente de Acuerdo	Total
Norma ISO/IEC 27001:2005	No	7	5	26	5	1	44
	Si	5	9	8	7	7	36
Total		12	14	34	12	8	80

Fuente: Datos obtenidos de la investigación

Prueba chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	15,190[a]	4	,259
Razón de verosimilitud	10,549	4	,308
Asociación lineal por lineal	3,914	1	,048
N de casos válidos	5		

a. 16 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,20.



X^2_t Crítico = 9.488

X^2_ccalculado = 15.19

como $T_c > T_t$ se rechaza Ho

Interpretación: El valor calculado del Chi cuadrado de la prueba estadística de hipótesis es 15.19; que resulta sersuperior al valor de la tabla en un nivel de confianza del 95% (15.19>9.488); por lo tanto se acepta la hipótesis alternativa (Ha) y se rechaza la hipótesis nula de investigación (Ho), y se concluye que efectivamente el conocimiento de las diferentes condiciones de acceso a la información, tanto externo como interno, se relacionan significativamente con la norma ISO/IEC 27001:2005.en la UNTELS.

Hipótesis Específica 5: Existe una relación directa y significativa entre la seguridad de información (controles que garanticen la confidencialidad, integridad y disponibilidad de la información) con lo establecido por la norma ISO/IEC 27001:2005, respecto de su manejo por el personal administrativo de la UNTELS en el 2017.

Ho. Los controles de seguridad de información (que garanticen la confidencialidad, integridad y disponibilidad de la información), no se relacionan significativamente con la norma ISO/IEC 27001:2005.

Ha. Los controles de seguridad de información (que garanticen la confidencialidad, integridad y disponibilidad de la información), si se relacionan significativamente con la norma ISO/IEC 27001:2005.

Prueba Estadística.

Prueba estadística : Chi cuadrada

$$x^2 = \sum \frac{(O-E)^2}{E}$$

O = Frecuencia observada en cada celda

E = Frecuencia esperada en cada celda

∑ =Sumatoria

X2 = Chi cuadrado obtenida u observada

Nivel de significancia : α = 0.05

Grado de libertad : 4

Punto crítico según tabla : X2(4) (0.95) = 9.844

gl	0.05
4	9.844

TABLA N° 22:
CONTINGENCIA (2 X 5) DE LA SELECCIÓN DE LOS CONTROLES DE SEGURIDAD DE INFORMACIÓN MÁS IMPORTANTES Y NORMA ISO/IEC 27001:2005

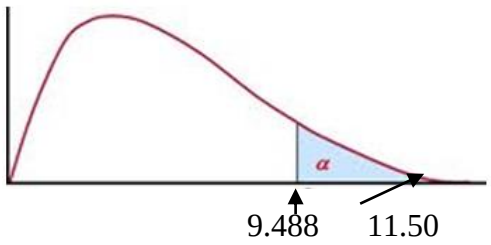
		La selección de los controles de seguridad de información más importantes					
		En total Desacuerdo	En Desacuerdo	Neutral	De Acuerdo	Totalmente de Acuerdo	Total
Norma ISO/IEC 27001:2005	No	1	3	27	4	1	44
	Si	3	1	31	1	8	36
Total		4	4	58	5	9	80

Fuente: Datos obtenidos de la investigación

Prueba chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	11,500[a]	4	,259
Razón de verosimilitud	10,549	4	,308
Asociación lineal por lineal	3,722	1	,054
N de casos válidos	5		

a. 16 casillas (100,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,20.



X^2_t Crítico = 9.488

X^2_ccalculado = 11.50

como $T_c > T_t$ ⟶ se rechaza Ho

Interpretación: El valor calculado del Chi cuadrado de la prueba estadística de hipótesis es 11.50; que resulta ser superior al valor de la tabla en un nivel de confianza del 95% (11.5>9.488); por lo tanto se acepta la hipótesis alternativa (Ha) y se rechaza la hipótesis nula de investigación (Ho), y se concluye que efectivamente los controles de seguridad de información que garanticen la confidencialidad, integridad y disponibilidad de la información, se relacionan significativamente con la norma ISO/IEC 27001:2005 en la UNTELS.

CAPÍTULO V

DISCUSIÓN DE RESULTADOS

En el trabajo de campo se ha verificado, de manera precisa, los objetivos planteados en nuestra investigación, cuyo propósito fue determinar la relación que existe entre el plan de seguridad de información y la norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur, estableciendo la correlación entre dichas variables. Así se ha cuantificado la relación que existe entre las variables planteadas en los objetivos a través del Coeficiente de Pearson, obteniéndose los resultados siguientes:

1.- Se ha determinado que existe una relación directa entre el cumplimientodel plan de seguridad de la información con la norma ISO/IEC 27001:2005enla Universidad Nacional Tecnológica de Lima Sur, al cuantificar estarelación se encontró un Coeficiente de Pearson de 0.984, lo que nos indicaque la relación entre las variables esdirecta y fuerte.

2.- Se encontró que la relación entre el diagnóstico del plan de seguridad de la información conla norma ISO/IEC 27000: 2005, es positiva con un Coeficiente dePearson de 0.906, lo que indica una fuerte relación entre las variablesen estudio.

3.- Se encontró que la relación entre las áreas encargadas del cuidado ydistribución de la información con la norma ISO/IEC 27001:2005, es directa con un Coeficiente de Pearson de 0.964, lo cual nosdice que la relación es fuerte y directa.

4.- La relación que existe entreel análisis de riesgo los puntos fuertes ydébiles de los sistemas de información según la norma ISO/IEC 27001:2005, es positiva y asciende a 0.995, lo cual indica una fuerterelación directa entre las variables en estudio.

5.- La relación entre las diferentes condiciones de acceso a la información,tanto externo como interno según la norma ISO/IEC 27001:2005, es directay asciende a 0.989, lo cual indica una fuerte relación directa entre lasvariables en estudio.

6.- La relación entre los controles de seguridad de información másimportantes que garanticen la confidencialidad, integridad y disponibilidadde la información de acuerdo con la norma ISO/IEC 27001:2005, es directay asciende a 0.965, lo cual indica una relación directa entre las variables enestudio.

CONCLUSIONES

1.- Se llegó a determinar que existe una relación directa significativa entre el plan de seguridad de la información con la norma ISO/IEC 27001:2005, en la Universidad Nacional Tecnológica de Lima Sur, ya quepor medio de la prueba Chi cuadrado se acepta la hipótesis alterna (Ha), indica que existe una relación significativa entre dichas variables, ya que lavariable Chi cuadrado calculada 18.95 es mayor que el valor de tabla 9.488

2.- Se determinó que existe una relación directa y significativa entre eldiagnóstico de la situación actual de la seguridad de información en laorganización y la norma ISO/IEC 27001:200, en la UNTELS, ya que elvalor de la variable Chi cuadrado calculada 21.92 es mayor que el valor detabla que es 9.488

3.- Existe una relación directa y significativa entre la evaluación del cuidado y distribución de la información con la norma ISO/IEC 27001:2005,en la UNTELS, ya que al realizar laprueba Chi cuadrado se encontró que el valor calculado de la variable 11.60es mayor que el valor de tabla 9.488

4.- hay una relación directa y significativa entre la identificación a través delanálisis de riesgo los puntos fuertes y débiles de los sistemas deinformación con la norma ISO/IEC 27001:2005, en la UNTELS, esto debidoa que la prueba de Chi cuadrado respectiva nos indica que hay que el valorcalculado 15.24 es mayor que el valor de tabla 9.488.

5.- Existe una relación directa y significativa entre el conocimiento de lasdiferentes condiciones de acceso a la información, tanto externo comointerno, con la norma ISO/IEC 27001:2005, en la UNTELS, por que el valorcalculado de la variable Chi cuadrado es de 15.19 frente al valor de tablaque es de 9.488

6.- Existe una relación directa y significativa entre los controles de seguridad de información que garantizan laconfidencialidad, integridad y disponibilidad de la información, con la normaISO/IEC 27001:2005, en la UNTELS, ya que la variable Chi cuadradocalculado 11.50 es mayor que el valor de tabla 9.48.

SUGERENCIAS

1. Se recomienda a la Universidad Nacional Tecnológica de Lima Sur realizar investigaciones de diseño experimental que conlleven desarrollar instrumentos de medición que permitan conocer los niveles de logro del plan de seguridad de la información y la norma ISO/IEC 27001:2005.

2. Se sugiere adecuarse al modelo de plan de seguridad de la información propuesto (anexo 6) a fin de reducir los riesgos y amenazas actualmente existentes.

3. Se sugiere a las universidades que incluyan en los programas capacitación las estrategias metodológicas sobre el plan de seguridad de la información y la norma ISO/IEC 27001:2005.

4. Se recomienda desarrollar investigaciones que permitan generar un estándar en la aplicación de la norma ISO 27000, en instituciones semejantes a la mencionada en el presente estudio

5. Su sugiere desarrollar proyectos de investigación y desarrollo que generen productos tecnológicos que aseguren la implementación de la seguridad de la información, tales como sistemas de información, procesos de información, etc.

6. Se recomienda al público en general y al personal administrativo de las universidades para garantizar el plan de seguridad de la información y la Norma ISO/IEC 27001:2005.

BIBLIOGRAFÍA

1. Alexander, A. (2007). Diseño De Un Sistema de Gestión de Seguridad de Información/Óptica ISO/ IEC 27001:2005. Primera edición. Bogotá: Alfaomega Colombiana S.A.
2. Alexander, A. (2005). Análisis Del Riesgo Y El Sistema De Gestión De Seguridad De Información: El Enfoque ISO 27001:2005. Lima.
3. Chiavenato, I. (2005). Introducción a la Teoría General de la Administración. México: McGraw-Hill.
4. Condori, h. (2012). Repositorio Concytec. Modelo De Evaluación De Factores Críticos De Éxito En La Implementación De La Seguridad En Sistemas De Información Para Determinar Su Influencia En La Intención Del Usuario. Recuperado el 15 de noviembre de 2015: http://repositorio.concytec.gob.pe/bitstream/CONCYTEC/115/1/condori_ah.pdf
5. Cortés, R., Marcela, D., Guzmán, A., & Victoria, A. (2012). Biblioteca Digital Minerva. Recuperado:http://hdl.handle.net/10882/2779
6. De la Cruz, C., Vásquez, J. (2008). Elaboración Y Aplicación De Un Sistema De Gestión De La Seguridad De La Información (SGSI) Para La Realidad Tecnológica De La USAT. (Proyecto de tesis para optar el título de Ingeniero de Sistemas y Computación). Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú.
7. Drucker, P. (2002). Los Desafíos De La Gerencia Del Siglo XXI. Bogotá : Norma.

8. Echeverry, C., & Trujillo, M. I. (2009). Modelos De Desarrollo Para Gobierno TI. Scientia et Technica. 41.
9. Espinoza, H. (2013). Análisis Y Diseño De Un Sistema De Gestión De Seguridad De Información Basado En La Norma ISO/IEC 27001:2005 Para Una Empresa De Producción Y Comercialización De Productos De Consumo Masivo. (Proyecto de tesis de fin de carrera, Pontificia Universidad Católica del Perú). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/4957
10. ETICOM, Asociación De Empresarios De Tecnologías De La Información Y Comunicaciones De Andalucía. Proyecto PYMETICA. (2002). Andalucía, España.
11. Fitzgerald, T. (2012). Information Security Governance Simplified. New York: CRC Press.
12. FONCODES. Seguridad De La Información. Recuperado: http://aulavirtual.foncodes.gob.pe/extranet/index.php/2013-05-07-17-21-24/seguridad-de-informacion?download=46:seguridad-de-informacion
13. Harris, S. (2013). CISSP Certification: All in One Exam Guide . New York: Mc Graw Hill.
14. Huamán, F. (2014). Diseño De Procedimientos De Auditoría De Cumplimiento De La Norma NTP-ISO/IEC 17799:2007 Como Parte Del Proceso De Implantación De La Norma Técnica NTP-ISO/IEC 27001:2008 En Instituciones Del Estado Peruano. (Tesis para optar por el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/5582.

15. IEC- ISO. (2015). ISO27000. Recuperado: http://www.iso27000.es
16. INDECOPI. (2007). Norma Técnica Peruana “NTP-ISO/ IEC. Lima: Comisión De Reglamentos Técnicos Y Comerciales.
17. López E. Universidad Nacional Autónoma de México. Esquemas De Seguridad Informática. Recuperado de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php
18. Llorens, J. (2005). Gerencia De Proyectos De Tecnología De Información. Venezuela: Editorial CEC, SA.
19. Maiwald, E. (2005). Fundamentos De Seguridad En Redes. Mexico: Mc Graw-Hill.
20. Palacios, D. Repositorio Institucional UNAD. (2015). Recuperado: http://repository.unad.edu.co/handle/10596/3817
21. Perafán, J., & Caicedo, M. (2014). Repositorio UNAD. Análisis De Riesgos De La Seguridad De La Información Para La Institución Universitaria Colegio Mayor Del Cauca.Recuperado:http://repository.unad.edu.co/bitstream/10596/2655/3.
22. Peter, N. (1996). Seguridad De La Información. Madrid: Nueva España.
23. Rodriguez, L. A. (1995). Seguridad De La Información En Sistemas De Cómputo. México: Ventura Ediciones.
24. Santos, L. (2010). Guía Para La Evaluación De Un Sistema De Información. Universidad De Pamplona .
25. Stoneburner, G. (2001). NIST Special Publication 800-33: Underlying Technical Models Forinformation Technology Security, Recommendations Of The National Institute Of Standards And Technology. Washington DC: NationalInstituteOf Standards And Technology.

26. Talavera, V. (2015). Diseño De Un Sistema De Gestión De Seguridad De La Información Para Una Entidad Estatal De Salud De Acuerdo A La ISO/IEC 27001:2013. (Tesis para optar por el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/6092
27. Tipton, H., & Krause, M. (2007). Information Security Management Handbook. New York: AuerbachPublications.
28. Tupia, M. (2011). Principios De Auditoría Y Control De Sistemas De Información. Segunda Edición. Lima: Tupia Consultores Y Auditores

ANEXOS

ANEXO 0: NOMBRES DE VARIABLES

V1: La información que reporta según el diagnóstico de la situación actual de la seguridad de información en la Universidad es totalmente confiable y se orienta a una toma de decisiones correcta u óptima.

V2: Conoce aspectos normados por ISO 27000, para la manipulación correcta de información.

V3: Con absoluta seguridad de su parte, considera usted que se maneja adecuadamente las consultas, la generación, las actualizaciones de datos en su área.

V4: El manejo del cuidado y distribución de la información.

V5: El manejo de información en su área en la captura, almacenamiento, distribución y consulta es pertinente.

V6: La identificación a través del análisis de riesgo los puntos fuertes y débiles de los sistemas de información. Sintió que los directivos participaron activamente y con responsabilidad.

V7: Los controles de seguridad de información que garantice la confidencialidad, integridad y disponibilidad de la información.

V8: Considera que existen factores políticos internos que afectan a usted en su trabajo y a la implementación de proyectos de Sistemas

V9: Considera que su entorno laboral es adecuado para el desarrollo de seguridad en los sistemas.

V10: Considera usted que el plan de sistemas de información en UNTELS implementado bajo ISO 27000 favorecería la implementación de Seguridad en los Sistemas.

V11. Plan de seguridad de la Información.

V12. Conocimiento de las diferentes condiciones de acceso a la información, tanto externo como interno.

VALORES DE LAS VARIABLES

V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12
5	10	4	6	28	4	4	13	11	6	9	12
15	15	11	9	4	15	4	25	3	9	11	14
30	33	59	41	9	43	58	36	32	34	38	34
17	12	3	12	34	10	5	4	20	17	13	12
13	10	3	12	5	8	9	2	14	14	9	8
80	80	80	80	80	80	80	80	80	80	80	80

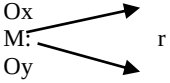
ANEXO 1: Matriz de consistencia

TÍTULO: ADECUACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN A LA NORMA ISO 27000 EN LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	CONCEPTOS
Problema General ¿De qué manera el plan de seguridad de la información se relaciona según norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur? **Problemas Específicos** 1.- ¿De qué manera el diagnóstico de la situación actual de la seguridad de información en la organización se relaciona con la norma ISO/IEC 27001:2005? 2. ¿De qué manera la evaluación de las áreas encargadas del cuidado y distribución de la información a través de una metodología de trabajo con encuestas, cuestionarios, entrevistas y otros se relaciona con la norma ISO/IEC 27001:2005? 3.- ¿De qué manera la identificación a través del análisis de riesgo los puntos fuertes y débiles de los sistemas de información se relaciona con la norma ISO/IEC 27001:2005? 4.- ¿De qué manera el conocimiento de las diferentes condiciones de acceso a la información, tanto externo como interno se relaciona con la norma ISO/IEC 27001:2005? 5.- ¿De qué manera la seleccionar de los controles de seguridad de información más importantes que garanticen la confidencialidad, integridad y disponibilidad de la información se relaciona con la norma ISO/IEC 27001:2005?	**Objetivo General**. Determinar la relación del plan de seguridad de la información con la norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur **Objetivos específicos** 1. Determinar la relación del diagnóstico de la situación actual de la seguridad de información en la organización con la norma ISO/IEC 27001:2005 2. Evaluar la relación de las áreas encargadas del cuidado y distribución de la información a través de una metodología de trabajo con encuestas, cuestionarios, entrevistas y otros con la norma ISO/IEC 27001:2005. 3. Identificar la relación a través del análisis de riesgo los puntos fuertes y débiles de los sistemas de información según norma. Con la norma ISO/IEC 27001:2005. 4. Conocer la relación de las diferentes condiciones de acceso a la información, tanto externo como interno con la norma ISO/IEC 27001:2005. 5. Determinar la relación de los controles de seguridad de información más importantes que garanticen la confidencialidad, integridad y disponibilidad de la información con la norma ISO/IEC 27001:2005.	**Hipótesis General:** El plan de seguridad de la información se relaciona significativamente con la norma ISO/IEC 27001:2005 en la Universidad Nacional Tecnológica de Lima Sur **Hipótesis específicas:** H1. El diagnóstico de la situación actual de la seguridad de información en la organización se relaciona significativamente con la norma ISO/IEC 27001:2005. H2. La evaluación de las áreas encargadas del cuidado y distribución de la información a través de una metodología de trabajo con encuestas, cuestionarios, entrevistas y otros, se relacionan significativamente con la norma ISO/IEC 27001:2005. H3. La identificación a través del análisis de riesgo los puntos fuertes y débiles de los sistemas de información según norma se relacionan significativamente con la norma ISO/IEC 27001:2005. H4.El conocimiento de las diferentes condiciones de acceso a la información, tanto externo como interno, se relacionan significativamente con la norma ISO/IEC 27001:2005. H5. La selección de los controles de seguridad de información más importantes que garanticen la confidencialidad, integridad y disponibilidad de la información, se relacionan significativamente con la norma ISO/IEC 27001:2005.	**Variable 1** Implementación del plan de seguridad **Variable 2** Norma ISO/IEC 27001:2005 **Variable Interviniente** Comunidad UNTELS	**PLAN DE SEGURIDAD DE LA INFORMACIÓN.** Se centra en un Sistema de Seguridad Informática que es un conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados en la UNTELS. NORMA **ISO/IEC 27001:2005** Es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International OrganizationforStandardization) e IEC (International ElectrotechnicalCommission), que proporcionan un marco de gestión de la seguridad de la información utilizable en la UNTELS.

<table>
<tr><th>TIPO Y DISEÑO DE ESTUDIO</th><th>POBLACIÓN Y MUESTRA</th><th>TÉCNICAS E INSTRUMENTOS</th><th>ESTADISTICA DE ANALISIS</th></tr>
<tr>
<td>3.3.1. Tipo de Investigación
Investigación Básica
Siguiendo a Hernández, Fernández & Baptista (2006) el presente trabajo de investigación es de tipo básica sustantiva de nivel descriptivo, correlacional

3.3.2. Diseño de Investigación
Siguiendo a Hernández, Fernández & Baptista (2006) el presente estudio asume el diseño no experimental - transversal – correlacional

Cuyo esquema es el siguiente:
 

Donde:
M: Muestra de estudiantes y docentes
Ox: Plan de seguridad
Oy: Norma ISO/IEC 27001:2005
r: Relación de las variables</td>
<td>La población de estudio está conformada por los administrativos de la Universidad Nacional Tecnológica de Lima Sur – UNTELS, 2015.

La población N = 100 Administrativos

$$n = \frac{Z^2 p * qN}{e^2(N-1) + Z^2 p * q}$$

<table>
<tr><th>Institución</th><th>UNTELS
Población</th><th>Muestra total</th></tr>
<tr><td>Administrativos</td><td>100</td><td>80</td></tr>
<tr><td>Total</td><td>100</td><td>80</td></tr>
</table>

La muestra de investigación es de n = 80 administrativos.</td>
<td>En tanto la implementación del plan de seguridad es atribución de los directivos de la UNTELS, se considera pertinente recabar la información sobre ésta, en forma simultánea de una muestra relativamente amplia de directivos y docentes; al igual que la apreciación que se requiere de los estudiantes, con respecto a su percepción de la conducción institucional

Instrumentos de recolección de datos
Se emplearan como instrumentos, para recoger los datos referidos a la implementación del plan de seguridad un cuestionario que se aplicó a los integrantes de la muestra. Igualmente para recoger la información sobre Norma ISO/IEC 27001:2005 se empleó un segundo cuestionario.
-La validez de estas encuestas se ve reflejada en que el total de los cuestionarios fueron llenados correctamente y sin errores que puedan llevar a dudar de la veracidad de los datos.
- Técnica de procesamiento de datos y su instrumento tablas de resultados de la encuesta.
- Técnica del Fichaje y su instrumento las fichas bibliográficas, para registrar datos de indagación bibliográfica</td>
<td>El análisis de los datos recolectados siguió ciertos procedimientos estadísticos descriptivos e inferencia les. En la estadística descriptiva se hizo la construcción de la base de datos, el ordenamiento de los datos y la organización de las frecuencias descriptivas basadas en contenidos y porcentajes.

El grado de correlación se establecerá mediante el Índice de correlación medido por el Coeficiente de Contingencia dados que los datos de ambas variables nos permiten realizar esto. El tratamiento estadístico, descriptivo e inferencial, se apoyará en el uso de los software EXCEL 2010 y SPSS 20.

Prueba de Hipótesis
Prueba de Correlación
En estadística, el coeficiente de correlación de Contingencia, C es una medida de la correlación (la asociación o interdependencia) entre dos variables aleatorias cualitativas y por lo menos una de ellas está clasificada en más de 2 categorías. Para calcular C se usa la expresión siguiente:

$C = \sqrt{X^2/(N+X^2)}$

Donde N es el número de datos</td>
</tr>
</table>

ANEXO 2: Matriz de la operacionalización de las variables

ESTUDIO DE CASO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR BASADO EN LA NORMA ISO/IEC 27001:2005.

VARIABLE	DIMENSIONES	INDICADORES	PUNTAJE O VALORACIÓN	TIPO DE INSTRUMENTO
Plan de seguridad de información	Diagnostico	Cobertura de servicios Promedios Calidad Índices Promedios	Escala Likert: 6. Totalmente en desacuerdo 7. En desacuerdo 8. Neutral 9. De acuerdo 10. Totalmente de acuerdo	Test para medir sobre el plan de seguridad de la información
	Cuidado y distribución	Actividades desarrolladas		
	Riesgos	Aspectos críticos		
	Condiciones	Contexto actual		
	Controles	Resultados		

VARIABLES	DIMENSIONES	INDICADORES	PUNTAJE O VALORACIÓN	TIPO DE INSTRUMENTO
V. 2 Norma ISO/IEC 27001:2005	Normativa	Funcionalidad. Confiabilidad. Usabilidad. Eficiencia. Mantenibilidad. Portabilidad	Escala dicotómico: 0 = No 1 = Si	Test para medir la Norma ISO/IEC 27001:2005
	Valorativa	Selección. Determinación. Revisión y atestación		

ANEXO 3: instrumentos

Cuestionario sobre el plan de seguridad de información

Estimado encuestado:

El presente cuestionario es parte de una del trabajo de investigación, que tiene por finalidad la recolección de datos para conocer sobre la seguridad de información.

Instrucciones: Lea minuciosamente las preguntas, y marque con un (X) la respuesta que crea conveniente.

En total Desacuerdo	En Desacuerdo	Neutral	De Acuerdo	Totalmente de Acuerdo
1	2	3	4	5

N°	PLAN DE SEGURIDAD DE INFORMACIÓN	1	2	3	4	5
1	La información que reporta según el diagnóstico de la situación actual de la seguridad de información en la Universidad es totalmente confiable y se orienta a una toma de decisiones correcta u óptima.					
2	Conoce aspectos normados por ISO 27000, para la manipulación correcta de información.					
3	Con absoluta seguridad de su parte, considera usted que se maneja adecuadamente las consultas, la generación, las actualizaciones de datos en su área.					
4	Según la evaluación de las áreas encargadas del cuidado y distribución de la información. Tiene acceso a todo tipo de información en su organización o área.					
5	El manejo de información en su área en la captura, almacenamiento, distribución y consulta es pertinente.					
6	La identificación a través del análisis de riesgo los puntos fuertes y débiles de los sistemas de información. Sintió que los directivos participaron activamente y con responsabilidad.					
7	La selección de los controles de seguridad de información más importantes garantice la confidencialidad, integridad y disponibilidad de la información.					
8	Considera que existen factores políticos internos que afectan a usted en su trabajo y a la implementación de proyectos de Sistemas					
9	Considera que su entorno laboral es adecuado para el desarrollo de Seguridad en los Sistemas					
10	Considera usted que el plan de sistemas de información en UNTELS implementado bajo ISO 27000 favorecería la implementación de Seguridad en los Sistemas					

Muchas gracias.

ANEXO 4:
Cuestionario sobre norma ISO/IEC 27001:2005

SI	NO
1	0

N°	ITEMS	SI	N0
	NORMATIVA Y VALORATIVA		
1	¿Su área ha establecido normativas para manejo de la información que procesa, recibe o genera?		
2	¿Existen procesos definidos del manejo (tratamientos) de la información que se genera en su área?		
3	¿Ha asistido a capacitaciones sobre seguridad de la información (SI) organizado por la UNTELS?		
4	¿Se hacen auditorias o controles periódicas sobre manipulación y almacenamiento de la información que se trata en su área?		
5	Si un ente de mayor jerarquía a la de Usted solicita información de su área ¿Demora más de 24 horas en ser atendido?		
6	¿Siente que hay prioridad en el otorgamiento de los recursos materiales que se usa en su trabajo con los sistemas?		
7	¿Considera que su entorno laboral es adecuado para el desarrollo de Seguridad en los Sistemas?		
8	¿En general la Universidad está preparada para implementar la seguridad en Sistemas de Información según norma ISO/IEC 27001:2005?		
9	¿Mis compañeros de trabajo piensan que se debe implementar la seguridad en Sistemas de Información?		
10	¿Mi jefe inmediato piensa que se debe implementar la seguridad en Sistemas de Información?		

ANEXO 5: Resolución Ministerial N°187-2010-PCM

Autorizan ejecución de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010"

RESOLUCIÓN MINISTERIAL N°187-2010-PCM

15 de junio de 2010

CONSIDERANDO:

Que, el artículo 2° del Decreto Supremo N°066-2003-PCM y el numeral 4.8 del artículo 4° y artículo 49° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Decreto Supremo N° 063-2007- PCM, disponen que la Presidencia del Consejo de Ministros, a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), actúa como ente rector del Sistema Nacional de Informática, encargándose de normar, coordinar integrar y promover el desarrollo de la actividad informática en la Administración Pública, impulsando el uso de las nuevas tecnologías de la información para la modernización y desarrollo del Estado;

Que, de acuerdo con los numerales 50.1 y 50.3 del artículo 50° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 063-2007-PCM, son funciones de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), proponer la Estrategia Nacional de Gobierno Electrónico, así como coordinar y supervisar su implementación, realizando acciones orientadas a la consolidación y desarrollo del Sistema Nacional de Informática y supervisar el cumplimiento de la normativa correspondiente;

Que, mediante Resolución Ministerial N° 246-2007-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información, 2ª Edición" en las entidades integrantes del Sistema Nacional de Informática;

Que, la Oficina Nacional de Gobierno Electrónico e Informática ha propuesto ejecutar el Reporte de Seguridad de la Información en la Administración Pública -2010, para obtener y mantener actualizada la información técnica relacionada con la seguridad de la información de las entidades del Sistema Nacional de Informática;

De conformidad con lo dispuesto en la Ley N° 29158 - Ley Orgánica del Poder Ejecutivo y el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 063-2007-PCM y sus modificatorias;

SE RESUELVE:

Artículo 1°.-Autoriza la realización de la "Encuesta ele Seguridad de la Información en la Administración Pública-2010"

Autorizar la ejecución de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010" en todas la entidades de la Administración Pública pertenecientes al Sistema Nacional de Informática.

Artículo 2°.- Aprueba de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010"

Aprobar la "Encuesta de Seguridad de la Información en la Administración Pública - 2010", que como anexo forma parte integrante de la presente Resolución Ministerial.

Artículo 3°,- Publicación

La presente Resolución Ministerial será publicada en el Diario Oficial El Peruano.

La "Encuesta de Seguridad de la Información en la Administración Pública -2010" será publicada en el Portal Institucional de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y el Portal Institucional de la Oficina Nacional de Gobierno Electrónico e

Informática (ONGEI) (www.ongei.gob.pe), al día siguiente de la publicación de la presente norma en el Diario Oficial "El Peruano".

Artículo 4°.- Plazo

Las entidades de la Administración Pública deberán remitir la Encuesta a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) hasta el 30 de Julio del 2010, de acuerdo a las indicaciones y a la información solicitada en el documento aprobado por el artículo 2° de la presente Resolución Ministerial.

Regístrese, comuníquese y publíquese.

JAVIER VELASQUEZ QUESQUÉN
Presidente del Consejo de Ministros

ANEXO 6: MODELO SUGERIDO PARA LA IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNTELS AJUSTADO A LA NORMA ISO 27:000:2005

DESCRIPCIÓN

La implementación del Plan de Seguridad de la Información tiene como propósito brindar la seguridad de la Información y tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, disrupción o destrucción no autorizada de la Universidad Nacional Tecnológica de Lima Sur - UNTELS.

Los términos Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información. Sin embargo, entre ellos existen algunas diferencias sutiles.

Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma que los datos puedan tener: electrónicos, impresos, audio u otras formas.

En la UNTELS se acumulan una gran cantidad de información confidencial sobre sus directivos, docentes, administrativos, equipos de laboratorios y herramientas, la investigación y la situación financiera y otros. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en computadoras y transmitida a través de las redes a otras computadoras.

En caso de que la información confidencial de la UNTELS, sus usuarios, sus decisiones, su estado financiero o las nuevas decisiones de gestión no caigan en manos de un competidor o se vuelva pública en forma no autorizada, podría causar la pérdida de credibilidad de los usuarios, pérdida de información académica, demandas legales u otros. Por lo que proteger la información confidencial es un requisito de la universidad, y en muchos casos también un imperativo ético y una obligación legal.

Para el individuo común, la Seguridad de la Información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad: La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Integridad: Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas.

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.

4.3.1 ELECCIÓN Y APLICACIÓN DEL MÉTODO

Implantación del método

Planificación de la gestión de servicios (Planificar)

Objetivo: Planificar la implementación y la prestación de la gestión de servicios. El alcance se debe definir como parte del plan de gestión de servicios. Por ejemplo, puede definirse según:

- la organización;
- la ubicación;
- el servicio

La gestión de servicios se debe planificar. Como mínimo, las planificaciones deberán definir lo siguiente:

- el alcance de la gestión de servicios en la organización;
- los objetivos y los requisitos que debe cumplir la gestión de servicios; los procesos que se deben ejecutar;
- la infraestructura de funciones y responsabilidades de gestión, incluido el propietario del proceso y la gestión de proveedores externos;
- las interfaces entre los procesos de gestión de servicios y el modo en que se deben coordinar las actividades;
- el enfoque que se debe realizar para la identificación, la evaluación y la gestión de problemas y riesgos para la consecución de los objetivos definidos;
- el enfoque para el intercambio de información con proyectos que estén creando o modificando servicios;
- los recursos, las instalaciones y el presupuesto necesario para alcanzar los objetivos definidos; las herramientas adecuadas para dar soporte a los procesos; y
- cómo se gestionará, auditará y mejorará la calidad del servicio.

Deberá haber una dirección de gestión clara y responsabilidades documentadas para revisar, autorizar, comunicar, implementar y mantener los planes. Cualquier plan específico de un proceso que se elabore deberá ser compatible con este plan de gestión de servicios. Un plan de gestión de servicios debe incluir:

- la implementación de la gestión de servicios (o de parte de la gestión de servicios);
- la facilitación de procesos de gestión de servicios;
- los cambios de los procesos de gestión de servicios;
- las mejoras de los procesos de gestión de servicios;
- los nuevos servicios (hasta el punto que afectan a los procesos incluidos en el alcance acordado de la gestión de servicios).

4.3.2 PROPUESTA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNTELS.

I. OBJETIVO

Establecer las políticas y procedimientos necesarios para administrar la seguridad de la información asegurando además que se cumplan los criterios de ***confidencialidad, integridad y disponibilidad de la información*** producida en la universidad, y de esa forma contribuir a asegurar la permanencia de la institución en el tiempo.

Establecer estrategias y controles adecuados que garanticen una gestión segura de los procesos de la organización y mantener un nivel de exposición de la información menor al nivel de riesgo que la universidad decida asumir.

II. ALCANCE

Considerando que el objetivo principal del Plan de Seguridad de la Información (PSI) es asegurar la confidencialidad, integridad y disponibilidad, elementos que son parte integrante de las Tecnologías de Información y sus riesgos inherentes, el alcance está orientado a todas las unidades organizativas de la universidad y compromete los procesos actuales y los que se implementen.

III. NORMATIVIDAD

- Ley 23733 – Ley Universitaria
- Norma ISO/IEC 27001:2005 Sistema de Gestión de la seguridad de la información.
- Norma NTP-ISO/IEC 17799:2007 EDI
- Resolución ministerial Nº 187-2010-PCM
- Estatuto de la universidad

IV. CLASIFICACIÓN DE SEGURIDAD

Información Interna - confidencial

V. GLOSARIO DE TÉRMINOS

Para la aplicación del presente documento deberá considerarse las siguientes definiciones:

1. **Activo:** Es algo a lo que una organización le asigna un valor y por lo tanto la organización debe proteger. También es definido como el conjunto de los bienes y derechos tangibles e intangibles de propiedad de una institución y son generadores de renta o fuente de beneficios como; bienes, inversiones, cuentas por cobrar, inmuebles, instalaciones, maquinarías, etc.
2. **Administración de riesgos:** Son las actividades coordinadas para guiar y controlar una organización con respecto al riesgo. Incluye valoración, tratamiento, aceptación y comunicación de riesgos.
3. **Amenaza:** Se define como una causa potencial de un incidente no deseado, podría resultar dañino para un sistema u organización.
4. **Análisis de riesgo:** Es el sistemático uso de información para identificar fuentes de riesgo y estimar el mismo.
5. **Control de riesgo:** Es el proceso que busca asegurar que las políticas, estándares, límites y procedimientos para el tratamiento de riesgos son apropiadamente tomados y/o ejecutados. Las actividades de control están preferentemente incorporadas en los procesos organizacionales y las actividades de apoyo. Incluye los controles generales así como los de aplicación a los sistemas de información, además de la tecnología de información relacionada. Buscan la eficacia y efectividad de las operaciones de la universidad, la confiabilidad de la información administrativa o académica, interna y externa, así como el cumplimiento de las disposiciones legales que le sean aplicables.
6. **Evaluación de riesgo:** Se define como el proceso de comparar el riesgo estimado contra criterio de riesgo dado para determinar el significado del riesgo.
7. **Incidente de la seguridad de la información:** Es un evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene probabilidad significativa de comprometer procesos y amenazar la seguridad de la información.
8. **Identificación de riesgo:** Es un proceso por el que se determinan los eventos internos y externos que pueden tener un impacto negativo sobre los objetivos de la organización. Entre otros aspectos, considera la posible interdependencia entre eventos, así como los factores influyentes que los determinan.

9. **Información:** Es definida como cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.
10. **Gestión de Riesgos:** Es un conjunto de procesos efectuados por la dirección, las jefaturas, el personal administrativo y docente de la universidad, destinados a proveer una seguridad razonable sobre el logro de los objetivos de la institución. La gestión de riesgos está diseñada para contar con el entorno interno apropiado; desarrollar una adecuada determinación de objetivos; implementar una oportuna identificación, evaluación, tratamiento y control de riesgos; elaborar los reportes pertinentes; y efectuar un adecuado monitoreo.
11. **Monitoreo de riesgo:** Es un proceso que consiste en la evaluación de la existencia y el adecuado funcionamiento del sistema de gestión integral de riesgos. El monitoreo puede llevarse a cabo en el curso normal de las actividades de la organización. Incluye el reporte de las deficiencias o desviaciones encontradas y su corrección.
12. **La Entidad, la organización, la institución, la universidad:** Universidad Nacional Tecnológica de Lima Sur.
13. **Objetivo de control:** Es una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de tecnología de información particular.
14. **Proceso crítico:** Es el proceso considerado indispensable para la continuidad de las actividades y servicios de la organización, y cuya falta o ejecución deficiente puede tener impactos significativos (económico, académico, operacional o de imagen) para la universidad.
15. **Riesgo:** Se constituye como la condición en que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la entidad.
16. **Riesgos de operación:** Entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos.
17. **Riesgo de tecnología de información:** Son los riesgos de operación asociados a los sistemas informáticos y a la tecnología relacionada a dichos sistemas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la entidad al atentar contra la confidencialidad, integridad y disponibilidad de la información, entre otros criterios.
18. **Seguridad de la información:** Es la característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.
19. **Servicios críticos provistos por terceros:** Son los servicios relacionados a procesos críticos provistos por terceros, cuya realización podría ser razonablemente desarrollada por la universidad.
20. **Tecnología de la información:** Incluye los sistemas informáticos y la tecnología asociada a dichos sistemas.
21. **Tercera persona:** Es la persona o grupo que es reconocida como independiente de las partes involucradas, como concierne al asunto en cuestión
22. **Tratamiento de riesgo:** Es el proceso de selección e implementación de medidas para modificar el riesgo.
23. **Vulnerabilidad:** Es una debilidad de una ventaja o un grupo de ventajas que pueden ser explotadas por una o más amenazas.

VI. ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN

1. La Información

La información es un activo relevante e imprescindible en cualquier organización; es por este motivo que existe la necesidad de establecer normas organizacionales, tecnológicas y jurídicas para su protección.

La información en la universidad se encuentra en diversas formas y es vulnerable, pues existen múltiples amenazas y riesgos, ya sea por ataques externos, ataques internos y en la mayoría de casos errores humanos, esto supone un obstáculo para la continuidad de la organización por no contar con medidas de seguridad adecuadas que permitan la detección del ataque de personas no autorizadas a acceder a los bancos de información, la recuperación o reparación de la información afectada, es decir, no se dispone una eficaz gestión de Sistema de Información (SI).

2. Seguridad de la Información

a) ***Definición:*** La información es un recurso que, como el resto de los activos, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad de la organización, minimizar el daño y maximizar el retorno sobre las inversiones y las oportunidades.

La información puede existir en muchas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación.

Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Toda información en propiedad o custodia de la universidad debe estar clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización, facilitando la gestión del riesgo asociado a cada sistema de información, se clasificarán de acuerdo a la información que procesen o almacenen.

a.1. Confidencialidad: La confidencialidad se refiere a la protección de información frente a posibles accesos no autorizados, independientemente del lugar en que este almacenada la información o la manera en que se almacena.

Es por eso, que la información organizacional y toda aquella información sensible, crítica o valiosa que custodia o maneja la universidad, necesita ser protegida mediante estrictas normas de control, para garantizar que la misma solo podrá ser conocida y ser accedida por el personal autorizado.

a.2. Integridad: La integridad consiste en garantizar que la información sea y permanezca confiable, completa y exacta, dado que la misma no ha sido alterada, borrada, o reorganizada. Su relevancia radica en la necesidad de asegurar que la información refleja la realidad que la genera, ya que la tendencia hacia la automatización de los procesos conlleva a que en muchos procesos organizativos, la única evidencia de una transacción será la información que se haya generado de esta.

a.3. Disponibilidad: La disponibilidad abarca no solo a la información, sino a los procesos que sustenta su generación y uso; esto debe cumplir con las características de oportunidad, es decir, la recuperación de la información en el momento que se necesite, evitar la pérdida o bloqueo por algún acto inapropiado, no autorizado, mala operación accidental o causas fortuitas, para, de esta manera, garantizar su accesibilidad.

La seguridad de la información consiste en establecer un conjunto adecuado de controles, que abarcan políticas, prácticas, procedimientos, estructuras organizacionales y funciones de la organización y de los sistemas de información.

3. Seguridad Informática

La seguridad informática es el área de conocimiento que se encarga de establecer los procedimientos, herramientas y protocolos necesarios para garantizar el correcto, seguro y continuo funcionamiento de los diferentes elementos que componen un sistema o red informática.

El campo de la seguridad informática se puede dividir en varias áreas diferenciadas:

- **Seguridad de Sistemas Operativos:** Se refiere a la seguridad intrínseca del propio sistema operativo empleado (Windows y Linux).
- **Seguridad de Aplicaciones o Servicios:** Se refieren a los programas empleados tanto para acceder como para entregar datos. (Servidores Web, gestores de correo electrónico, etc.).
- **Seguridad de Redes:** Trata la seguridad de los datos transmitidos de un computador a otro, así como de la seguridad de todos los dispositivos que conforman la red.
- **Seguridad de Datos:** Compone las normas necesarias para una adecuada protección de los datos de un sistema.
- **Seguridad de Física:** Aunque de forma bastante tangencial, se asocian ciertos parámetros de seguridad física a la seguridad informática.

4. Criterios para el inventario de activos de la información

En los procesos del análisis de los activos de información se establecerá, en primer lugar, la clasificación de la seguridad de la información.

En segundo lugar, se establecerán medidas de protección mínimas a establecer, así como la asignación de un propietario. Se establecerán procedimientos de archivo de dicha clasificación que permitan consultar la sensibilidad del activo en términos de su valor, requerimientos legales y grado crítico para la organización. Razón por la cual, la universidad incidirá en el tratamiento de la confidencialidad.

4.1. Tratamiento de la confidencialidad

4.1.1. Tratamiento General:

a. Información pública: Información que no requiere de protección especial por el deseo expreso de su publicación por parte de la universidad, la exigencia de su publicación por parte de la normativa vigente o porque su divulgación, intencionada o accidental, no supondrá ningún tipo de riesgo para la universidad. La información clasificada pública será accesible por personal de la universidad o ajenas a la institución. (v.g. lo publicado en el portal de transparencia institucional)

b. Información interna: Información necesaria para el correcto desempeño de las funciones del personal administrativo y docente de la universidad; cuya divulgación, intencionada o accidental, puede suponer problemas leves a la organización, no deteriorará significativamente la imagen institucional, ni atentará contra los derechos de las personas. La información clasificada interna será accesible por el personal de la universidad o personal ligado a esta, de ***manera contractual***, esta información no deberá transmitirse ni comunicarse a nadie fuera de los mencionados en este párrafo, sin la autorización respectiva de las autoridades universitarias.(v.g. El cronograma de pagos)

c. Información restringida: Información de uso interno exclusivo de grupos de usuarios o áreas específicas que no debe transmitirse libremente dentro de la universidad. La información clasificada restringida será accesible únicamente por un grupo limitado de personas que necesita dicha información para el desempeño de sus actividades laborales. (v.g. La configuración de servidores, mapeo de IP, teléfonos de docentes)

d. Información confidencial: Información cuya divulgación, alteración o pérdida puede suponer un problema grave para la organización, un deterioro significativo de su imagen pública, atentar directamente contra el derecho a la intimidad de las personas o puede afectar significativamente a su posición en el mercado o el incumplimiento de la normativa vigente. No se transmitirá o divulgará a

terceras personas, con excepción de que exista autorización explícita y por escrito de las autoridades universitarias. (v.g. citaciones judiciales)

e. Información secreta: Información que debe ser conocida únicamente por el propietario de la misma, tales como: contraseñas de usuario, claves criptográficas, etc.

4.1.2 Tratamiento específico de información confidencial:

a. Datos Personales: Los datos personales del personal docente, administrativo y alumnos de la universidad, a los que se tenga acceso por motivos profesionales deberán ser tratados siempre de manera confidencial y siguiendo en todo caso los procedimientos establecidos para dicho tipo de datos según la legislación vigente; no se transmitirán o divulgarán a terceras partes si no nos consta que existe autorización de la universidad.

b. Datos secretos: Los datos que permitan accesos u operaciones en la Oficina de Informática y Estadística tales como las claves criptográficas ,claves criptográficas asociadas a aplicaciones, claves o contraseñas de acceso u operación, se consideran secretos . No se deben divulgar los propios ni solicitar los ajenos. Excepcionalmente, y bajo los procedimientos de seguridad y registro establecidos, el personal de soporte técnico puede establecer claves iníciales o de desbloqueo que deberán ser cambiadas por el titular en el primer acceso.

c. Archivos temporales: Los usuarios que por motivos de trabajo y de acuerdo con los procedimientos establecidos, organizativamente, necesiten trabajar en archivos temporales con datos personales o sujetos a confidencialidad, deberán proceder al borrado de los mismos una vez finalizado el tratamiento de los mismos y consolidados los resultados finales obtenidos.

4.2 Tratamiento de la integridad

4.2.1 Clasificación general:

La información se clasificará por sus requerimientos de mantenimiento de integridad en función del impacto que su modificación no autorizada pueda dañar a la universidad. Siguiendo criterios similares a los establecidos para riesgo operacional, los riesgos derivados de la no integridad pueden ser legales/regulatorios y de referencia a la buena imagen organizacional.

Se analizarán los posibles riesgos derivados de la manipulación o alteración de la información procesada por los sistemas de información atendiendo a las pérdidas directas, indirectas (debidas a los procesos de cuadre y conciliación), regulatorias y de imagen organizacional.

a. Información de operaciones del área de economía: La información sobre operaciones del área económica cuya alteración suponga una pérdida patrimonial cierta y no recuperable mediante procesos posteriores de cuadre o conciliación deberá estar especialmente protegida.

Para las posibles pérdidas recuperables mediante procesos de conciliación se evaluará la conveniencia de establecer el mismo tipo de controles. La modificación de la información almacenada que soporte operaciones financieras se efectuará siempre a través de aplicaciones que garanticen que siempre existe la contrapartida correspondiente, cualquier otro tipo de acceso extraordinario para cuadres manuales deberá estar restringido y estrictamente auditado.

Las comunicaciones de información cuya modificación en tránsito estén sujetas al tipo de riesgo antedicho deberán estar protegidas mediante mecanismos de control de integridad (mediante claves de acceso). Si la comunicación es con terceros los mecanismos de integridad deberán incluir adicionalmente la posibilidad de no repudio.

b. Información para la elaboración de reportes económicos: La información para la elaboración y consolidación de los reportes económicos de la universidad, estará sometida a procesos rigurosos para el control de su integridad, a fin de dar adecuado cumplimiento a las regulaciones y al compromiso de la

organización de ofrecer información veraz a los entes superiores en general que están registrados en su sistema de Gobierno.

c. Información expuesta a redes públicas: La información accesible directamente por terceros a través de la Internet (Web institucional) deberá estar especialmente protegida contra su alteración no autorizada mediante la aplicación de las Normas de

Seguridad perimetral, segmentación de redes, sistemas software de seguridad, sistemas operativos, controles de acceso, análisis periódico de vulnerabilidades, detección de intrusión y aquellas específicas de control de integridad de contenidos públicos.

d. Credenciales y perfiles de acceso: Por su capacidad de dar o modificar privilegios de acceso, se protegerán especialmente la integridad de las credenciales (incluso en su almacenamiento cifrado) y de los perfiles asignados a los usuarios de los Sistemas de Información. El acceso a las bases de datos de autenticación y autorización de usuarios estará estrictamente limitado al personal de la Oficina de Informática y Estadística, los accesos a cualquier sistema de la universidad siempre serán auditados

4.3 Tratamiento de la disponibilidad

La clasificación de los activos de información, de los procesos y sistemas que los soportan, en cuanto a su disponibilidad frente a contingencias y las correspondientes medidas a adoptar se desarrollarán, de acuerdo al nivel crítico asignado por las diferente área de la universidad a los mismos, en el marco de los planes de recuperación de sistemas.

5. Evaluación de Riesgos

La evaluación de riesgos identifica, cuantifica y documenta las amenazas a la seguridad de la institución, evalúa el nivel de exposición en el que queda la universidad por cada riesgo asumido y determina el grado de importancia para la eliminación de cada uno de ellos. La evaluación del riesgo provee la base para desarrollar políticas de seguridad.

Es necesario realizar un análisis formal para identificar los riesgos específicos asociados con los activos críticos de información.

El resultado más importante del proceso de evaluación de riesgo, es la información que se utiliza para desarrollar e implantar las políticas de seguridad.

Se debe identificar en cada unidad organizacional de la UNTELS con una frecuencia anual para asegurar tanto la integridad como la disponibilidad y confidencialidad de la información.

6. Política de Seguridad

Las políticas de seguridad informática surgen como una herramienta organizacional para sensibilizar a la comunidad de la UNTECS sobre la importancia de la información y servicios críticos que permiten a la universidad crecer y mantenerse competitiva.

Todo el personal de la universidad debe seguir las políticas y estándares de seguridad para controlar y proteger la Información, esto también alcanza a empleados no regulares tales como temporales, contratistas, vendedores y consultores. Este estándar se refiere a toda la información sin tomar en cuenta la forma ni formato.

7. Selección de Controles

Una vez identificados los requerimientos de seguridad, se debe implementar los controles para garantizar que los riesgos sean reducidos a un nivel aceptable.

Los controles se seleccionarán sobre la base de este documento o según nuevos controles que se pueden diseñar para satisfacer necesidades específicas según corresponda.

Los controles serán seleccionados teniendo en cuenta el costo de implementación en relación con los riesgos a reducir y las pérdidas que podrían producirse de tener lugar una violación de la seguridad.

También se tendrá en cuenta los factores no monetarios, como el daño en la reputación institucional.

VII. EVALUACION DE RIESGOS

Implica la identificación, análisis y documentación de las amenazas a la seguridad de la organización, evalúa el nivel de exposición en el que queda la institución por cada riesgo asumido y determina el grado de importancia para la eliminación de cada uno de ellos.

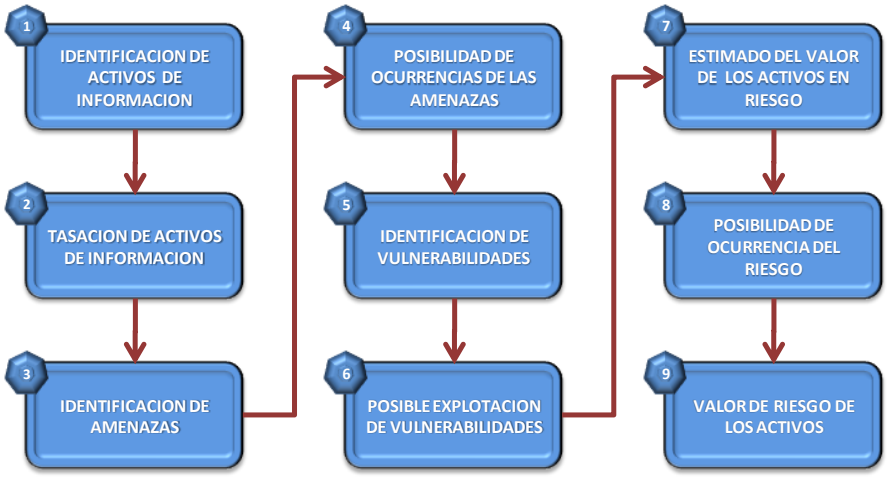
Ayuda a identificar a los propietarios de la información de la universidad (entendemos por propietario al personal responsable por el origen de la información). La evaluación del riesgo provee la base para desarrollar políticas de seguridad.

Es necesario realizar un análisis formal para identificar los riesgos específicos asociados con los activos críticos de información.

El resultado más importante del proceso de evaluación de riesgo es la información que se utiliza para desarrollar e implantar las políticas y controles de seguridad.

El proceso de evaluación de riesgo que permitirá a la UNTECS a gestionar el riesgo y estar de acuerdo con los requerimientos normativos, se ejecutará a través de un proceso de análisis metodológico de nueve fases.

Figura 1: Análisis de riesgo – proceso metodológico



1. Identificación de activos de la Información

- Se identifican a los propietarios funcionales para todos los activos importantes y se asigna la responsabilidad por el mantenimiento de los controles apropiados.
- La responsabilidad por la implementación de los controles puede ser delegada.
- En último término, el propietario designado del activo debe rendir cuentas por el mismo.

Tabla 1: Ejemplo de activos de información y propietarios funcionales

Nº	ACTIVO DE INFORMACIÓN HARDWARE Y SOFTWARE	PROPIETARIO FUNCIONAL
1	Programa fuente del SIGU – escritorio	**Jefe de la OIE**
2	Programa fuente SIGUNET	**Jefe de la OIE**
3	Microsoft SQL-SERVER 2003	**Jefe de la OIE**
4	Microsoft Windows Server 2003	**Jefe de la OIE**
5	Linux Debian	**Jefe de la OIE**
6	Linux Centos	**Jefe de la OIE**
7	Microsoft Windows Seven	**Jefe de la OIE**
8	Microsoft Windows XP	**Jefe de la OIE**
9	Microsoft Windows Vista	**Jefe de la OIE**

10	Antivirus Karpesky 6	**Jefe de la OIE**
11	Microsoft Office 2007	**Jefe de la OIE**

Tabla 2: Ejemplo de la clasificación de la Información por unidades organizativas y funcionales.

UNIDAD: INFORMATICA Y ESTADISTICA

ACTIVOS DE INFORMACIÓN	CLASIFICACIÖN	PROPIETARIO
plan de seguridad de la información	información interna	personal de OIE
manual de control de riesgos	información restringida	OIE
informes reportados a presidencia	información restringida	OIE
Contraseñas de usuarios del sistema	Información secreta	Jefe de OIE

2. Valoración de Activos de Información

La valoración es el atributo que hace valioso a un activo de información en términos de su importancia para la organización. Mediante su dimensionamiento permite valorar las consecuencias de la materialización de una amenaza. Para valorar los activos de información se emplea una escala cualitativa

Tabla 3: Valoración de los activos de información

VALOR		CRITERIO
MA	MUY ALTO	DAÑO MUY GRAVE A LA UNIVERSIDAD
A	ALTO	DAÑO GRAVE A LA UNIVERSIDAD
M	MEDIANO	DAÑO IMPORTANTE A LA UNIVERSIDAD
B	BAJO	DAÑO MENOR A LA UNIVERSIDAD
MB	MUY BAJO	SIN IMPORTANCIA

Esta tabla permite evaluar los activos de información mediante su relación a los conceptos claves de información:

- Confidencialidad
- Integridad
- Disponibilidad

Tabla 4: Ejemplo de la evaluación de los activos de información

Nº	ACTIVO DE INFORMACIÓN HARDWARE Y SOFTWARE	Confidencialidad	integridad	Disponibilidad	TOTAL
1	Programa fuente del SIGU – escritorio	**MA**	**MA**	**A**	**MA**
2	Programa fuente SIGUNET	**MA**	**MA**	**A**	**MA**
3	Microsoft SQL-SERVER 2008	**M**	**MA**	**MA**	**MA**
4	Microsoft Windows Server 2008	**A**	**MA**	**MA**	**MA**
5	Linux Debian	**M**	**MA**	**MA**	**MA**
6	Linux Centos	**M**	**MA**	**MA**	**MA**
7	Microsoft Windows Seven	**B**	**M**	**M**	**M**
8	Microsoft Windows XP	**B**	**M**	**M**	**M**
9	Microsoft Windows Vista	**B**	**M**	**M**	**M**
10	Antivirus Karpesky 6	**M**	**M**	**M**	**M**
11	Microsoft Office 2007	**B**	**M**	**M**	**M**

3. Identificación de Amenazas

Una amenaza es un evento o incidente provocado por un ente (humano, natural o artificial) hostil a la organización que aprovecha una o varias vulnerabilidades de un activo con el fin de agredir la confidencialidad, integridad o disponibilidad de ese mismo activo o de otros activos de la organización (la amenaza "explota" la vulnerabilidad del activo). Todas esas condiciones que pueden generar daño a la universidad serán definidas.

Las amenazas al explotar las vulnerabilidades pueden ocasionar riesgo que afecta las operaciones y las puede paralizar, esto es definido como "desastre". Un desastre es "un evento que altera los procesos críticos de la universidad que afectan su misión y degrada el servicio a un punto donde el impacto operativo se convierte en inaceptable.

Las amenazas tienen un origen externo o interno a la organización y pueden ser deliberadas o accidentales (por ejemplo en el caso de desastres naturales o negligencia sin intención de daño por parte de personal de la organización).

La gestión de riesgos abarca una gama amplia de actividades para identificar, controlar y atenuar riesgos del sistema de Información. Las actividades de la gestión de riesgos desde la perspectiva de planificación de contingencia identifican amenazas y vulnerabilidades para que, mediante, apropiados controles puedan ser ubicados en lugares estratégicos, a fin de prevenir incidentes que pueden suceder.

La universidad tomará decisiones sobre las opciones de tratamiento del riesgo, decidirá que amenazas se reducirán con controles, cuáles se aceptarán y se decidirá convivir con ellas, cuáles se transferirán (por ejemplo a una aseguradora.) y cuales se evitarán.

El resultado final de esta etapa es un listado de amenazas consideradas vitales y un listado de funciones organizacionales mostrando su dependencia con determinados recursos, así como la implementación de los controles apropiados para su tratamiento.

Los controles de seguridad protegerán al sistema de información contra los siguientes tipos de amenazas:

3.1 Amenazas Lógicas

- Suplantación de identidad por internos.
- Suplantación de identidad por proveedores.
- Suplantación de identidad por externos.
- Uso no autorizado de una aplicación informática.
- Software malicioso y virus.
- Abuso de los recursos de los sistemas.

3.2 Amenazas a las Comunicaciones

- Infiltración en las comunicaciones.
- Interceptación de las comunicaciones.
- Alteración de las comunicaciones.
- Repudio.
- Falla en las comunicaciones.
- Inclusión de código malicioso.
- Entrega incorrecta.

3.3 Amenazas físicas

- - Fuego.
- - Inundación.
- - Desastre natural
- - Robo por internos
- - Robo por externos.
- - Daño intencionado por internos.
- - Daño intencionado por externos.
- - Terrorismo

3.4 Fallos Técnicos

- Falla de Host, impresora o dispositivo de almacenamiento
- Falla de elemento de red, interfaz de red
- Falla de pasarela de red.
- Falla de gestión de red.
- Falla de servicios de red.
- Falla de electricidad.
- Falla de aire acondicionado
- Falla de software de sistema
- Falla de software de red
- Falla de aplicación.

3.5 Errores Humanos

- Error de operador.
- Error en el mantenimiento hardware.
- Error en el mantenimiento software.
- Error de usuario común

A fin de identificar de manera apropiada, las amenazas que afectan los activos de información, se ha agrupado los activos según su funcionalidad

Tabla Nº 5: Ejemplo de la identificación de amenazas a los activos de información

Nº	GRUPOS DE ACTIVOS DE INFORMACION	AMENAZAS
1	PROGRAMAS FUENTE	○ Control de cambios ○ Daño intencionado por internos ○ Error de usuario ○ Falla de código ○ Software malicioso
2	DATOS ACADEMICOS ALMACENADOS	○ Alteración ○ Error de operador ○ Falsificación ○ Plagio
3	SOFTWARE EMPLEADO EN LA UNIVERSIDAD	○ Uso no autorizado de aplicación ○ Abuso de los recursos de los sistemas ○ Error de usuario ○ Falla de electricidad ○ Falla de software de sistema ○ Software malicioso ○ Suplantación identidad por internos ○ Acceso no permitido
4	SERVIDORES	○ Daño intencionado por usuario interno ○ Error en el mantenimiento de hardware ○ Error de operador ○ Falla de aire acondicionado ○ Falla de equipo ○ Falla de electricidad ○ Falla de servicio de red ○ Falla de software de aplicación ○ Fuego ○ Repudio ○ Software malicioso

		○ **Suplantación identidad por internos** ○ **Suplantación identidad por externos** ○ Abuso de los recursos del sistema ○ Terrorismo ○ Uso no autorizado de aplicación
5	DISPOSITIVOS DE RED	○ Alteración en las comunicaciones ○ Infiltración en las comunicaciones ○ Interceptación de las comunicaciones ○ Repudio ○ Entrega incorrecta de datos ○ Error de operador ○ Falla en comunicaciones ○ Falla de electricidad ○ Falla de equipo ○ Inclusión de código malicioso
6	CABLEADO DE RED	○ Daño malintencionado por internos y externos ○ Fuego ○ Inundación
7	SERVICIOS DE TERCEROS (PROVEEDORES)	○ Alteración contractual ○ Desastre natural ○ Entrega incorrecta ○ Error de operador ○ Falla en aplicación ○ Falla en electricidad ○ Falla en la gestión de red ○ Falla de servicio de red ○ Falla de software de red ○ Fuego ○ Inclusión de código malicioso ○ Infiltración ○ Interceptación
8	ESTACIONES DE TRABAJO	○ Falla de electricidad ○ Falla de equipo ○ Suplantación de identidad ○ Error de usuario ○ Software malicioso y virus
9	EQUIPOS DE RESPALDO Y EN CUSTODIA	○ Error de operador ○ Error en el mantenimiento de hardware ○ Falla de equipo
10	BACKUP (COPIAS DE SEGURIDAD DE DATA ALMACENADA)	○ Falla en almacenamiento ○ Falla de operador ○ Falla en dispositivo de almacenamiento ○ Backup no autorizado

4. Posibilidad de ocurrencia de amenazas

Se han revisado las amenazas potenciales que pueden afectar a la universidad y se ha identificado exposiciones específicas que pueden requerir medidas protectoras para menguar la probabilidad de daño.

Este análisis ha permitido identificar los siguientes aspectos:

- ubicación de instalaciones
- seguridad interna y externa
- ambiente físico
- protección de activos
- protección del personal
- protección de información

También se ha identificado las interrupciones a las que las funciones organizacionales están expuestas por la pérdida de recursos esenciales tales como:

Instalaciones:

- sistemas de cómputo
- registros vitales
- sistemas telefónicos
- personal clave
- conectividad de la red
- equipo especializado.

A cada amenaza identificada se ha calculado la posibilidad de ocurrencia y el impacto que puede ocasionar en la universidad

Tabla Nº 6: Valoración de ocurrencias de amenazas a la universidad

VALOR		CRITERIO
A	ALTO	DAÑO GRAVE A LA UNIVERSIDAD
M	MEDIANO	DAÑO IMPORTANTE A LA UNIVERSIDAD
B	BAJO	DAÑO MENOR A LA UNIVERSIDAD

La universidad tomará decisiones sobre las opciones de tratamiento del riesgo además determinará que amenazas se reducirán con controles, cuáles se aceptarán y con cuáles convivir, cuáles se transferirán y cuales se evitarán.

Tabla Nº 7: Ejemplo del listado de amenazas consideradas vitales por la universidad y la posibilidad de ocurrencia

Nº	GRUPOS DE ACTIVOS DE INFORMACION	AMENAZAS	POSIBILIDAD DE OCURRENCIA
1	PROGRAMAS FUENTE	o Control de cambios	A
		o Daño intencionado por internos	B
		o Error de usuario	M
		o Falla de código	M
		o Software malicioso	M
2	DATOS ACADEMICOS ALMACENADOS	o Alteración	B
		o Error de operador	M
		o Falsificación	B
		o Plagio	B
3	SOFTWARE EMPLEADO EN LA UNIVERSIDAD	o Uso no autorizado de aplicación	B
		o Abuso de los recursos de los sistemas	B
		o Error de usuario	M
		o Falla de electricidad	A
		o Falla de software de sistema	M
		o Software malicioso	M
		o Suplantación identidad por internos	B
		o Acceso no permitido	B
4	SERVIDORES	o Daño intencionado por usuario interno	B
		o Error en el mantenimiento de hardware	M
		o Error de operador	M
		o Falla de aire acondicionado	A
		o Falla de equipo	M

		o Falla de electricidad	A
		o Falla de servicio de red	M
		o Falla de software de aplicación	B
		o Fuego	B
		o Repudio	B
		o Software malicioso	M
		o **Suplantación identidad por internos**	B
		o **Suplantación identidad por externos**	B
		o Abuso de los recursos del sistema	B
		o Terrorismo	B
		o Uso no autorizado de aplicación	B
5	DISPOSITIVOS DE RED	o Alteración en las comunicaciones	B
		o Infiltración en las comunicaciones	B
		o Interceptación de las comunicaciones	B
		o Repudio	B
		o Entrega incorrecta de datos	B
		o Error de operador	M
		o Falla en comunicaciones	M
		o Falla de electricidad	A
		o Falla de equipo	M
		o Inclusión de código malicioso	B
6	CABLEADO DE RED	o Daño malintencionado por internos y externos	M
		o Fuego	B
		o Inundación	B
7	SERVICIOS DE TERCEROS (PROVEEDORES)	o Alteración contractual	M
		o Desastre natural	M
		o Entrega incorrecta	B
		o Error de operador	M
		o Falla en aplicación	B
		o Falla en electricidad	M
		o Falla en la gestión de red	B
		o Falla de servicio de red	B
		o Falla de software de red	B
		o Fuego	B
		o Inclusión de código malicioso	B
		o Infiltración	B
		o Interceptación	B
8	ESTACIONES DE TRABAJO	o Falla de electricidad	A
		o Falla de equipo	M
		o Suplantación de identidad	M
		o Error de usuario	A
		o Software malicioso y virus	A
9	EQUIPOS DE RESPALDO Y EN CUSTODIA	o Error de operador	M
		o Error en el mantenimiento de hardware	B
		o Falla de equipo	B
10	BACKUP (COPIAS DE SEGURIDAD DE DATA ALMACENADA)	o Falla en almacenamiento	B
		o Falla de operador	M
		o Falla en dispositivo de almacenamiento	B
		o Backup no autorizado	B

5. Identificación de vulnerabilidades (debilidades)

La Vulnerabilidad se define como la materialización de una amenaza sobre un activo de información, una vulnerabilidad es una falla en la concepción, desarrollo o implantación de un sistema informático que puede permitir a un atacante eludir, mediante acciones dentro de los parámetros de uso del sistema (no se considera el uso de la fuerza bruta o cortar la alimentación de un equipo) el planteamiento de seguridad del sistema.

Una vulnerabilidad puede permitir ataques locales y/o remotos:

- **Local:** estos ataques son lanzados directamente en el sistema informático por un miembro de la organización que tiene algún tipo de acceso previo al sistema.
- **Remota:** Cuando el ataque proviene de una red contra el sistema informático en que el atacante no tiene un acceso previo, lo más habitual es acceder con un navegador web a páginas con código malicioso.

5.1 Tipos de vulnerabilidad: Dependiendo del origen de la vulnerabilidad, esta puede tener una o varias características:

5.1.1 Debilidad en el diseño de los protocolos en las redes

Los protocolos utilizados para ofrecer determinados servicios en redes como Internet han sido diseñados sin prever cómo reaccionar frente a situaciones anómalas o ante un mal comportamiento de una de las partes intervinientes en la comunicación.

Algunos protocolos de Internet no contemplaron la seguridad en su diseño inicial, al considerar sus inventores que iban a ser utilizados en redes fiables y con usuarios de confianza, como podría ser el escenario de Internet que conectaba a universidades y centros de investigación.

5.1.2 Errores de programación

- Fallos en el diseño y/o en la codificación de los programas (SIGUNET – SIGU escritorio).
- Comportamiento incorrecto de las aplicaciones informáticas frente a entradas no válidas, que pueden provocar situaciones indeseadas como el desbordamiento de una zona de la memoria utilizada, existen lenguajes de programación utilizados para construir aplicaciones para Internet, que no realizan comprobaciones de las zonas de memoria reservada a las distintas variables declaradas por un programa.

5.1.3 Configuración inadecuada de los sistemas informáticos

- Las opciones que traen por defecto (de fábrica) muchos dispositivos y programas suelen ser poco seguras. Esta situación puede ser motivada, en parte, por una deficiente documentación sobre la configuración del sistema o dispositivo.
- Ejecución de más servicios de los necesarios en los equipos, con cuentas de usuarios que tienen privilegios excesivos para su función.
- Mantenimiento adecuado del software, no se instalan o revisan los parches suministrados por el fabricante.
- Problemas de uso por parte del usuario final (usuario poco experimentado) que no es consciente de las opciones relacionadas con la seguridad.
- Contar con excesivas relaciones de confianza entre redes y servidores, que facilitan el acceso a servidores sin requerir de autenticación, como los dominios de confianza en sistemas Windows.

5.1.4 Políticas de Seguridad deficientes o inexistentes

- Política de contraseñas poco robustas.
- Deficiente control de los intentos de acceso al sistema.
- Escaso rigor en el control de acceso a los recursos.
- Procedimientos inadecuados para la gestión de soportes informáticos o en el control de equipos portátiles.
- Escaso control de las copias generadas en papel con información sensible.
- Deficiente o inexistente limitación del acceso físico a los equipos más sensibles, dispositivos de red y cableado.
- Información sensible que se guarda sin encriptar en el sistema.

5.1.5 Desconocimiento y falta de sensibilidad

Por parte de los usuarios, un principio básico desde el punto de vista de Seguridad Informática a tener en cuenta es que todas las soluciones tecnológicas implantadas por la entidad (cortafuegos, antivirus, etc.), pueden resultar inútiles ante la falta de normativas, falta de sensibilización, desinterés o ánimo de causar daño de algún empleado desleal.

5.1.6 Disponibilidad de herramientas que faciliten los ataques

Existencia en Internet de todo tipo de programas gratuitos o no, fáciles de usar, con detallada documentación sobre su instalación y manejo, que permiten explorar vulnerabilidades de seguridad o llevar a cabo ataques más sofisticados contra redes y sistemas informáticos.

5.1.7 Existencia de backdoors ("puertas traseras")

- Un backdoor se define como una vía de acceso no autorizado a un sistema informático, saltándose las medidas de protección previstas e implantadas por sus administradores. Tienen su origen en una serie de servicios que se utilizan durante las fases de desarrollo de un sistema informático y que por intención, error o descuido, se mantienen en la versión final distribuida a los clientes.
- Funciones indocumentadas o códigos secretos de servicios instalados para facilitar identificación de personas o la descodificación de documentos.

5.1.8 Descuido de los fabricantes

- Inclusión de código maligno (virus o programas dañinos) en los discos duros de sus equipos.
- Entrega de actualizaciones o controladores que contienen código maligno.

Por cada amenaza identificada se ha identificado sus vulnerabilidades.

Es importante recalcar, que una vulnerabilidad no causa daño, es simplemente una condición o conjunto de condiciones que pueden hacer que una amenaza afecte a un activo de información.

Una vez identificadas las distintas vulnerabilidades por cada amenaza, se define el grado en que la amenaza puede explotar cada vulnerabilidad.

Tabla Nº 8: Ejemplo de identificación de vulnerabilidades de los activos de información

Nº	GRUPOS DE ACTIVOS DE INFORMACION	VULNERABILIDAD
1	PROGRAMAS FUENTE	o Errores de programación o Políticas de seguridad deficientes o inexistentes o Error en el diseño de software o Control de cambios deficiente o Error en validación de entrada (límites o desbordamiento de buffers)
2	DATOS ACADEMICOS ALMACENADOS	o Políticas de seguridad deficientes o inexistentes o Acceso no autorizado o Difusa organización y cadena de mando o Falta de capacitación o Personal no calificado
3	SOFTWARE EMPLEADO EN LA UNIVERSIDAD	o Configuración inadecuada o Disponibilidad de herramientas que facilitan ataque o Políticas de seguridad deficientes o inexistentes o Descuido de fabricantes o de operadores o Falta de capacitación en los usuarios finales o Error en validación de entrada (límites o desbordamiento de buffers) o Error en validación de acceso o Errores en el software o Defectos de instalación
4	SERVIDORES	o Debilidad en el diseño de protocolos o Acceso no autorizado o Error en configuración en los servicios o Mal funcionamiento del servidor

		○ Políticas de seguridad deficientes o inexistentes ○ Falta de capacitación en operador ○ Ejecución de código remoto ○ Error en validación de entrada ○ Error en validación de acceso ○ Denegación de servicio (DoS) ○ Falsificación de identidad ○ Intrusión ○ Ingeniería social ○ Protocolos de administración permitidos en interfaces públicas ○ Existencia de backdoors
5	DISPOSITIVOS DE RED	○ Políticas de seguridad deficientes o inexistentes ○ Falta de capacitación de los operadores ○ Fallos en la autenticación ○ Inexistencia de sistemas contra incendios ○ Protocolos de red sin cifrar ○ No existe segmentación de red ni filtros ○ Políticas de seguridad deficientes o inexistentes ○ Desastres naturales
6	CABLEADO DE RED	○ Energía eléctrica ○ Errores de configuración ○ Falta de capacitación del operador ○ Desastres naturales ○ Políticas de seguridad deficientes o inexistentes
7	SERVICIOS DE TERCEROS (PROVEEDORES)	○ Desastres naturales ○ Políticas de seguridad deficientes o inexistentes ○ Falta de capacitación de los operadores por parte del proveedor ○ Inexistencia de sistemas contra incendios ○ Desconocimiento y falta de sensibilidad de usuarios ○ Alteraciones en contratos
8	ESTACIONES DE TRABAJO	○ Falla de electricidad ○ Falla de equipo ○ Suplantación de identidad ○ Error de usuario final
9	EQUIPOS DE RESPALDO Y EN CUSTODIA	○ Políticas de seguridad deficientes o inexistentes ○ Ingeniería social ○ Falla de electricidad
10	BACKUP (COPIAS DE SEGURIDAD DE DATA ALMACENADA)	○ Falla de dispositivo de almacenamiento ○ Falla de aplicación de backup ○ Falla de operador

6. Posible Explotación de Vulnerabilidades

Siendo las vulnerabilidades debilidades asociadas con los activos de información, éstas pueden ser explotadas causando incidentes no deseados que pudieran terminar causando desastres graves.

Recordemos que la vulnerabilidad como tal, no causa daño, es simplemente una condición o conjunto de condiciones que pueden permitir que una amenaza afecte un activo de información.

6.1 Valoración de vulnerabilidad

Tabla Nº 9: Tabla de valoración de la vulnerabilidad

VALOR		CRITERIO
A	ALTO	VULNERABILIDAD MUY DEFICIENTE
M	MEDIANO	VULNERABILIDAD DEFICIENTE
B	BAJO	VULNERABILIDAD CONTROLADA

Alto:

- Permite a un atacante remoto violar la protección de seguridad del sistema (por ejemplo conseguir acceso de algún usuario o de tipo 'root' o administrador)
- Permite a un atacante local tomar control completo del sistema

Mediano:

- Permite a un atacante remoto o local violar la protección de seguridad.
- No toma control competo del sistema.

Bajo:

- La vulnerabilidad no permite obtener información valiosa de por sí ni control del sistema, si no que da al atacante información que le puede ayudar a encontrar otras vulnerabilidades en el sistema.
- La vulnerabilidad resulta inocua.

Tabla Nº 10: Ejemplo de una posible evaluación de las vulnerabilidades

Nº	GRUPOS DE ACTIVOS DE INFORMACION	VULNERABILIDAD	POSIBILIDAD EXPLOTACIÓN
1	PROGRAMAS FUENTE	○ Errores de programación	A
		○ Políticas de seguridad deficientes o inexistentes	M
		○ Error en el diseño de software	A
		○ Control de cambios deficiente	B
		○ Error en validación de entrada (límites o desbordamiento de buffers)	A
2	DATOS ACADEMICOS ALMACENADOS	○ Políticas de seguridad deficientes o inexistentes	A
		○ Acceso no autorizado	B
		○ Difusa organización y cadena de mando	M
		○ Falta de capacitación	M
		○ Personal no calificado	B
3	SOFTWARE EMPLEADO EN LA UNIVERSIDAD	○ Configuración inadecuada	M
		○ Disponibilidad de herramientas que facilitan ataque	A
		○ Políticas de seguridad deficientes o inexistentes	A
		○ Descuido de fabricantes o de operadores	M
		○ Falta de capacitación en los usuarios finales	A
		○ Error en validación de entrada (límites o desbordamiento de buffers)	M
		○ Error en validación de acceso	B
		○ Errores en el software	M
		○ Defectos de instalación	M
4	SERVIDORES	○ Debilidad en el diseño de protocolos	M
		○ Acceso no autorizado	M
		○ Error en configuración en los servicios	M
		○ Mal funcionamiento del servidor	M
		○ Políticas de seguridad deficientes o inexistentes	A
		○ Falta de capacitación en operador	M
		○ Ejecución de código remoto	M
		○ Error en validación de entrada	M
		○ Error en validación de acceso	B
		○ Denegación de servicio (DoS)	M
		○ Falsificación de identidad	B
		○ Intrusión	B
		○ Ingeniería social	M

		○ Protocolos de administración permitidos en interfaces públicas	M
		○ Existencia de backdoors	A
5	DISPOSITIVOS DE RED	○ Políticas de seguridad deficientes o inexistentes	A
		○ Falta de capacitación de los operadores	M
		○ Fallos en la autenticación	M
		○ Inexistencia de sistemas contra incendios	B
		○ Protocolos de red sin cifrar	M
		○ No existe segmentación de red ni filtros	A
		○ Políticas de seguridad deficientes o inexistentes	A
		○ Desastres naturales	B
6	CABLEADO DE RED	○ Energía eléctrica	M
		○ Errores de configuración	M
		○ Falta de capacitación del operador	M
		○ Desastres naturales	B
		○ Políticas de seguridad deficientes o inexistentes	A
7	SERVICIOS DE TERCEROS (PROVEEDORES)	○ Desastres naturales	B
		○ Políticas de seguridad deficientes o inexistentes	A
		○ Falta de capacitación de los operadores por parte del proveedor	M
		○ Inexistencia de sistemas contra incendios	B
		○ Desconocimiento y falta de sensibilidad de usuarios	A
		○ Alteraciones en contratos	M
8	ESTACIONES DE TRABAJO	○ Falla de electricidad	M
		○ Falla de equipo	B
		○ Suplantación de identidad	M
		○ Error de usuario final	M
9	EQUIPOS DE RESPALDO Y EN CUSTODIA	○ Políticas de seguridad deficientes o inexistentes	A
		○ Ingeniería social	M
		○ Falla de electricidad	M
10	BACKUP (COPIAS DE SEGURIDAD DE DATA ALMACENADA)	○ Falla de dispositivo de almacenamiento	M
		○ Falla de aplicación de backup	M
		○ Falla de operador	B

7. Estimado del Valor de los Activos en Riesgo

La siguiente tabla muestra la evaluación del riesgo, a fin de determinar el daño cualitativo que el riesgo pudiera causar a los activos de información

Tabla Nº 11: Ejemplo de la evaluación del riesgo

Nº	GRUPOS DE ACTIVOS DE INFORMACION	AMENAZAS	POSIBILIDAD DE OCURRENCIA	POSIBILIDAD EXPLOTACIÓN	VALOR ACTIVO DE INFORMACIÓN
1	PROGRAMAS FUENTE	○ Control de cambios	A	A	AM
		○ Daño intencionado por internos	B	M	
		○ Error de usuario	M	A	
		○ Falla de código	M	B	
		○ Software malicioso	M	A	
2	DATOS	○ Alteración	B	A	MB

	ACADEMICOS ALMACENADOS	○ Error de operador	M	B	
		○ Falsificación	B	M	
		○ Plagio	B	M	
3	SOFTWARE EMPLEADO EN LA UNIVERSIDAD	○ Uso no autorizado de aplicación	B	M	AM
		○ Abuso de los recursos de los sistemas	B	A	
		○ Error de usuario	M	A	
		○ Falla de electricidad	A	M	
		○ Falla de software de sistema	M	A	
		○ Software malicioso	M	M	
		○ Suplantación identidad por internos	B	B	
		○ Acceso no permitido	B	M	
4	SERVIDORES	○ Daño intencionado por usuario interno	B	M	M
		○ Error en el mantenimiento de hardware	M	M	
		○ Error de operador	M	M	
		○ Falla de aire acondicionado	A	M	
		○ Falla de equipo	M	M	
		○ Falla de electricidad	A	A	
		○ Falla de servicio de red	M	M	
		○ Falla de software de aplicación	B	M	
		○ Fuego	B	M	
		○ Repudio	B	B	
		○ Software malicioso	M	M	
		○ **Suplantación identidad por internos**	B	B	
		○ **Suplantación identidad por externos**	B	B	
		○ Abuso de los recursos del sistema	B	M	
		○ Terrorismo	B	M	
		○ Uso no autorizado de aplicación	B	A	
5	DISPOSITIVOS DE RED	○ Alteración en las comunicaciones	B	A	B
		○ Infiltración en las comunicaciones	B	M	
		○ Interceptación de las comunicaciones	B	M	
		○ Repudio	B	B	
		○ Entrega incorrecta de datos	B	M	
		○ Error de operador	M	A	
		○ Falla en comunicaciones	M	A	
		○ Falla de electricidad	A	B	
		○ Falla de equipo	M	M	
		○ Inclusión de código malicioso	B	M	
6	CABLEADO DE RED	○ Daño malintencionado por internos y externos	M	M	MB
		○ Fuego	B	B	
		○ Inundación	B	A	
7	SERVICIOS DE TERCEROS (PROVEEDORES)	○ Alteración contractual	M	B	MB
		○ Desastre natural	M	A	
		○ Entrega incorrecta	B	M	
		○ Error de operador	M	B	
		○ Falla en aplicación	B	A	
		○ Falla en electricidad	M	M	
		○ Falla en la gestión de red	B	M	

		○ Falla de servicio de red	B	B	
		○ Falla de software de red	B	M	
		○ Fuego	B	M	
		○ Inclusión de código malicioso	B	A	
		○ Infiltración	B	M	
		○ Interceptación	B	M	
8	ESTACIONES DE TRABAJO	○ Falla de electricidad	A	M	AM
		○ Falla de equipo	M	M	
		○ Suplantación de identidad	M	B	
		○ Error de usuario	A	A	
		○ Software malicioso y virus	A	A	
9	EQUIPOS DE RESPALDO Y EN CUSTODIA	○ Error de operador	M	A	MB
		○ Error en el mantenimiento de hardware	B	M	
		○ Falla de equipo	B	B	
10	BACKUP (COPIAS DE SEGURIDAD DE DATA ALMACENADA)	○ Falla en almacenamiento	B	B	MB
		○ Falla de operador	M	M	
		○ Falla en dispositivo de almacenamiento	B	M	
		○ Backup no autorizado	B	B	

8. Posibilidad de Ocurrencia del Riesgo

La posibilidad de ocurrencia del riesgo se obtiene analizando cada activo de información, con referencia a las amenazas que sufre y la posibilidad que ocurra, así como sus vulnerabilidades y la posibilidad que tiene de ser explotadas.

Tabla Nº 12: ejemplo del cálculo de la posibilidad de ocurrencia del riesgo de los activos de información

Nº	GRUPOS DE ACTIVOS DE INFORMACION	AMENAZAS	VULNERABILIDAD	VALOR ACTIVO DE INFORMACIÓN	POSIBLE OCURRENCIA
1	PROGRAMAS FUENTE	○ Control de cambios	○ Errores de programación	AM	A
		○ Daño intencionado por internos	○ Políticas de seguridad deficientes o inexistentes		
		○ Error de usuario	○ Error en el diseño de software		
		○ Falla de código	○ Control de cambios deficiente		
		○ Software malicioso	○ Error en validación de entrada (límites o desbordamiento de buffers)		
2	DATOS ACADEMICOS ALMACENADOS	○ Alteración	○ Políticas de seguridad deficientes o inexistentes	MB	M
		○ Error de operador	○ Acceso no autorizado		
		○ Falsificación	○ Difusa organización y cadena de mando		
		○ Plagio	○ Falta de capacitación		
		○ Privacidad	○ Personal no		

			calificado		
3	SOFTWARE EMPLEADO EN LA UNIVERSIDAD	○ Uso no autorizado de aplicación	○ Configuración inadecuada	AM	M
		○ Abuso de los recursos de los sistemas	○ Disponibilidad de herramientas que facilitan ataque		
		○ Error de usuario	○ Políticas de seguridad deficientes o inexistentes		
		○ Falla de electricidad	○ Descuido de fabricantes o de operadores		
		○ Falla de software de sistema	○ Falta de capacitación en los usuarios finales		
		○ Software malicioso	○ Error en validación de entrada (límites o desbordamiento de buffers)		
		○ Suplantación identidad por internos	○ Error en validación de acceso		
		○ Acceso no permitido	○ Errores en el software		
			○ Defectos de instalación		
4	SERVIDORES	○ Daño intencionado por usuario interno	○ Debilidad en el diseño de protocolos	M	M
		○ Error en el mantenimiento de hardware	○ Acceso no autorizado		
		○ Error de operador	○ Error en configuración en los servicios		
		○ Falla de aire acondicionado	○ Mal funcionamiento del servidor		
		○ Falla de equipo	○ Políticas de seguridad deficientes o inexistentes		
		○ Falla de electricidad	○ Falta de capacitación en operadora		
		○ Falla de servicio de red	○ Ejecución de código remoto		
		○ Falla de software de aplicación	○ Error en validación de entrada		
		○ Fuego	○ Error en validación de acceso		
		○ Repudio	○ Denegación de servicio (DoS)		
		○ Software malicioso	○ Falsificación de identidad		
		○ **Suplantación identidad por internos**	○ Intrusión		
		○ **Suplantación**	○ Ingeniería social		

		identidad por externos			
		○ Abuso de los recursos del sistema	○ Protocolos de administración permitidos en ○ interfaces públicas		
		○ Terrorismo	○ Existencia de backdoors		
		○ Uso no autorizado de aplicación			
5	DISPOSITIVOS DE RED	○ Alteración en las comunicaciones	○ Políticas de seguridad deficientes o inexistentes	B	A
		○ Infiltración en las comunicaciones	○ Falta de capacitación de los operadores		
		○ Interceptación de las comunicaciones	○ Fallos en la autenticación		
		○ Repudio	○ Inexistencia de sistemas contra incendios		
		○ Entrega incorrecta de datos	○ Protocolos de red sin cifrar		
		○ Error de operador	○ No existe segmentación de red ni filtros		
		○ Falla en comunicaciones	○ Políticas de seguridad deficientes o inexistentes		
		○ Falla de electricidad	○ Desastres naturales		
		○ Falla de equipo			
		○ Inclusión de código malicioso			
6	CABLEADO DE RED	○ Daño malintencionado por internos y externos	○ Energía eléctrica	MB	M
			○ Errores de configuración		
			○ Falta de capacitación del operador		
		○ Fuego	○ Desastres naturales		
		○ Inundación	○ Políticas de seguridad deficientes o inexistentes		
7	SERVICIOS DE TERCEROS (PROVEEDORES)	○ Alteración contractual	○ Desastres naturales	MB	M
		○ Desastre natural	○ Políticas de seguridad deficientes o inexistentes		
		○ Entrega incorrecta	○ Falta de capacitación de los operadores por parte del proveedor		
		○ Error de operador	○ Inexistencia de		

			sistemas contra incendios		
		○ Falla en aplicación	○ Desconocimiento y falta de sensibilidad de usuarios		
		○ Falla en electricidad	○ Alteraciones en contratos		
		○ Falla en la gestión de red			
		○ Falla de servicio de red			
		○ Falla de software de red			
		○ Fuego			
		○ Inclusión de código malicioso			
		○ Infiltración			
		○ Interceptación			
8	ESTACIONES DE TRABAJO	○ Falla de electricidad	○ Falla de electricidad	AM	M
		○ Falla de equipo	○ Falla de equipo		
		○ Suplantación de identidad	○ Suplantación de identidad		
		○ Error de usuario	○ Error de usuario final		
		○ Software malicioso y virus			
9	EQUIPOS DE RESPALDO Y EN CUSTODIA	○ Error de operador	○ Políticas de seguridad deficientes o inexistentes	MB	M
		○ Error en el mantenimiento de hardware	○ Ingeniería social		
		○ Falla de equipo	○ Falla de electricidad		
10	BACKUP (COPIAS DE SEGURIDAD DE DATA ALMACENADA)	○ Falla en almacenamiento	○ Falla de dispositivo de almacenamiento	MB	M
		○ Falla de operador	○ Falla de aplicación de backup		
		○ Falla en dispositivo de almacenamiento	○ Falla de operador		
		○ Backup no autorizado			

9. Valor del Riesgo de los Activos.

La estimación de la exposición al riesgo se basa en la evaluación de dos factores, probabilidad y nivel de impacto.

La probabilidad con la que las amenazas consideradas podrían materializarse (estimando la probabilidad de que las amenazas consideradas puedan explotar las vulnerabilidades de los activos)

El Impacto hace referencia a la magnitud de las consecuencias, que tiene para la organización. el hecho de que uno o varios activos de información hayan visto comprometido su confidencialidad, integridad o disponibilidad debido a que una o varias amenazas en las que se hayan explotado sus vulnerabilidades. Al estimar un determinado nivel de impacto es necesario considerar la criticidad de los activos de información afectados. La exposición al riesgo, también es evaluada desde un análisis cuantitativo y cualitativo del riesgo.

9.1 Análisis cuantitativo: Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en cifras concretas de forma objetiva.

Un modelo cuantitativo habitual es aquel en el que las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de la estimación del costo económico que suponen para la organización

9.2 Análisis cualitativo: Las métricas asociadas con el impacto causado por la materialización de las amenazas se valoran en términos subjetivos (Impacto Muy Alto, Alto, Medio, Bajo o Muy Bajo). Las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de multitud de factores (pérdidas económicas efectivas, pérdida de conocimiento, pérdida de competitividad, interrupción de negocio, pérdida de imagen, etc.).

Tabla Nº 13: Valoración de la probabilidad de ocurrencia

VALOR			CRITERIO
5	**MA**	PROBABLE	POSIBILIDAD DE INCIDENTES REPETITIVOS
4	**A**	POSIBLE	POSIBLIDAD DE INCIDENTES AISLADOS
3	**M**	POCO PROBABLE	POSIBILIDAD DE OCURRENCIA MUY MODERADA
2	**B**	RARO	NO ES PROBABLE QUE OCURRA
1	**MB**	IMPERCEPTIBLE	POSIBILIDAD DE OCURRENCIA MUY ESCASA

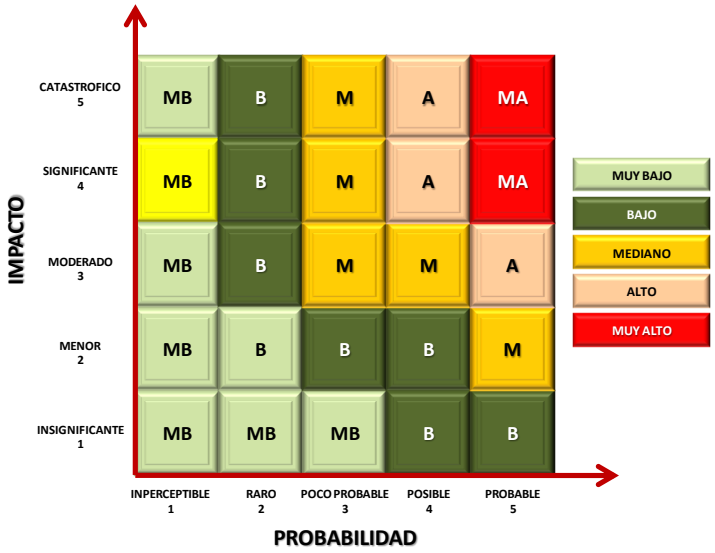
Tabla Nº 14: Valoración del impacto

VALOR			CRITERIO
5	**MA**	CATASTROFICO	Deficiencia detectada, implica cambios en los procedimientos para su corrección (reingeniería de procesos).
4	**A**	SIGNIFICATIVO	Deficiencia detectada, implica más de un procedimiento para su corrección
3	**M**	MODERADO	Deficiencia detectada, implica un Procedimiento para su corrección.
2	**B**	MENOR	Riesgo controlado el cual revierte la mínima complicación posible para el sistema de información, el cual no requiere ninguna contingencia.
1	**MB**	INSIGNIFICANTE	Este punto se obtiene como producto de la revisión y verificación de las actividades, que resultado tienen luego de ser ejecutadas, si el resultado es satisfactorio o de pleno cumplimiento.

Tabla Nº 15: Ejemplo de la valoración del riesgo de los activos de información

Nº	ACTIVO DE INFORMACIÓN HARDWARE Y SOFTWARE	PROBABILIDAD DE OCURRENCIA	IMPACTO
1	Programa fuente del SIGU – escritorio	**MA**	**MA**
2	Programa fuente SIGUNET	**MA**	**MA**
3	Microsoft SQL-SERVER 2008	**MA**	**MA**
4	Microsoft Windows Server 2008	**MA**	**MA**
5	Linux Debian	**MA**	**A**
6	Linux Centos	**MA**	**A**
7	Microsoft Windows Seven	**M**	**A**
8	Microsoft Windows XP	**M**	**A**
9	Microsoft Windows Vista	**M**	**A**
10	Antivirus Karpesky 6	**M**	**M**
11	Microsoft Office 2007	**M**	**MB**

Figura Nº 2: Matriz de evaluación de riesgo en activos de información



VIII. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información se definen como los documentos que describen, la forma de empleo de los recursos de tecnología de información, las responsabilidades y derechos que los usuarios y los administradores tienen, que acción tomar cuando ocurre un incidente de seguridad y qué medidas a tomar para proteger la seguridad del sistema.

- Las políticas son parte fundamental de un esquema de seguridad de la información eficiente, permiten aminorar los riesgos
- actuar de manera rápida y acertada en caso de haber una emergencia.
- indican la manera adecuada de usar un sistema
- contribuyen a un uso adecuado del sistema de información.

Las políticas deben ser comunicadas a todos los usuarios de la organización de manera pertinente, accesible y comprensible.

Figura Nº 3: Ciclo procedimental para la generación de políticas de seguridad de la información

Las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes:

- aumento de personal
- cambios en la infraestructura informática
- rotación de personal
- desarrollo de nuevos servicios
- cambio o diversificación del área de negocios, etc.

Los principales elementos que contienen las políticas de seguridad son:

- **Ámbito de aplicación:** Clasificación y división de los grupos campos en los cuales se ha separado las políticas.
- **Análisis de Riesgos:** Tiene como objetivo el mantenimiento de la confidencialidad, integridad y disponibilidad de los sistemas de Información e identificar y controlar cualquier evento que pueda afectar negativamente a estos tres aspectos.
- **Enunciados de políticas:** Es el texto descriptivo de la política de seguridad.
- **Sanciones:** Es el castigo a imponer por violación a alguna política.
- **Sección de uso ético de los recursos informáticos:** Reglas emitidas para el buen uso de los equipos o programas que son de la institución.
- **Sección de procedimientos para el manejo de incidentes:** Descripción de cómo se debe controlar y proteger lo definido en las políticas de seguridad de la información.

Para diseñar el esquema de políticas de seguridad, se divide los enunciados en diferentes políticas específicas a un campo. El documento separa recursos, cuentas, contraseñas, control de acceso, uso adecuado de recursos de información, respaldos, correo electrónico, aplicaciones del sistema, seguridad física, etc.

1. Políticas Generales de Seguridad de la Información

Con el fin de optimizar el uso de la información, aplicaciones y sistemas de la universidad, se dan las siguientes políticas de observancia general y obligatoria:

1.1 Todo usuario con acceso a la información, aplicaciones o sistemas de la universidad tiene la obligación de adoptar todas las medidas de control establecidas por UNTELS, así como los ordenamientos legales aplicables para la protección de la información o sistemas a los que tenga acceso, preservando su naturaleza confidencial y evitando su transferencia, modificación, destrucción o divulgación a entidades no autorizadas.

1.2 Toda información que la infraestructura de sistemas, aplicaciones, programas transmiten o almacenan son propiedad de la universidad, por lo que ningún usuario puede copiar, duplicar, transmitir o divulgar dicha información. La información, propiedad de UNTELS, está disponible únicamente para los usuarios que lo requieran dentro del estricto desempeño de sus funciones.

1.3 Los nombres de usuario y contraseña secreta que son asignadas para el acceso a los sistemas, aplicaciones, y los recursos de cómputo e información de la UNTELS, son personales, intransferibles y estrictamente confidenciales

El titular de la misma es el responsable del uso que se haga de ellos, así como de la información y provecho que a través de ellos obtenga, para sí o para terceros y de los daños y perjuicios que se ocasionen sin menoscabo de las responsabilidades y sanciones de naturaleza organizacional, civil y penal que resulten.

1.4 El acceso a los sistemas de cómputo y aplicaciones de UNETCS mediante el nombre de usuario y contraseña de un ajeno, se considerara como un uso no autorizado de información confidencial, sancionable.

1.5 Es considerada como una falta grave el uso (ejecución) de programas, aplicaciones u otros mecanismos que puedan dañar, alterar o impactar en el desempeño de los componentes de software de una computadora, sistema de cómputo o comunicaciones propiedad de la universidad, o bien, con el fin de molestar a otros usuarios, infiltrarse en un sistema, y en general, intentar violar los estándares de seguridad definidos por UNETCS

1.6 El usuario tiene la obligación de reportar inmediatamente a la Oficina de Informática y Estadística cualquier violación a las políticas y estándares de seguridad de información de UNTELS.

1.7 La infraestructura de sistemas, aplicaciones y los recursos de computo e información de UNTELS deben ser utilizados únicamente para los fines de la organización, no deberá ser usada para provecho personal, tales como entretenimientos, grupos de conversación, juegos recreativos, etc.

1.8 La infraestructura de sistemas, aplicaciones y, los recursos de computo e información de UNTELS no deben ser usados para introducir o traficar con material obsceno, lujurioso o pornográfico, almacenar y/o solicitar mensajes o imágenes con orientación sexual, ni para provocar disgustos, ofensas y daño moral lo cual incluye hostigamiento a otros basado en raza, nacionalidad, sexo, orientación sexual, edad, religión, defecto físico o creencias políticas.

1.9 Es responsabilidad del usuario ejecutar las acciones necesarias para que los equipos de cómputo, aplicaciones y sistemas asignados a su responsabilidad cumplan con los procedimientos de detección de virus definidos por la Oficina de Informática y Estadística.

1.10 No está permitida la instalación o ejecución de software no autorizado o sin licencia en cualquiera de los equipos que forman parte de la infraestructura de tecnologías de información de UNETLS,

1.11 Por cuestiones de seguridad se mantendrá un log de operaciones transaccionales a nivel académico y administrativo como medida precautoria por un lapso no menor a 6 meses (rastreo de incidencias)

1.12 La custodia de los equipos contenedores de información (servidores, computadoras personales, equipos móviles, dispositivos de almacenamiento secundario) estará a cargo del personal asignado a su uso, debiendo estos informar a su inmediato superior si alguno de estos equipos sufriera algún daño.

1.13 Los requerimientos mínimos para la compra de equipos tecnológicos referidos a la comunicación e información serán definidos en coordinación con la Oficina de Informática y Estadística.

.1.14 Es responsabilidad de todo miembro de la UNETCS, asegurarse que el personal a su cargo (contratado o no) conozca la presente normativa y cumpla con las disposiciones que requieren aprobación o supervisión previa al inicio de su trabajo, especialmente aquellas relativas a conexión de equipos ajenos a las redes de la universidad.

1.15 La persona encargada de clasificar la información es la única que puede degradar su grado de confidencialidad.

2. Políticas Específicas de Seguridad de la Información

Todo el personal de la universidad deberá seguir las políticas y estándares de seguridad de la información, a fin de controlar y proteger la este activo; las presentes políticas son aplicables a todos los docentes (nombrados, contratados e invitados), empleados (nombrados y contratados), contratistas, vendedores y consultores que utilicen los sistemas e instalaciones de la UNTELS. Este estándar hace referencia a toda la información sin tomar en cuenta la forma ni formato.

2.1 Los sistemas, la red de comunicaciones y la Información de la UNTECS solamente serán utilizados para los fines propios de la organización aprobados por la dirección responsable.

- La información de la universidad (normas, actas, resoluciones, dictámenes, oficios, memorándums, cartas, bases de datos, listas de correo, software interno, documentación de computador, etc.), así como la red de comunicaciones y el acceso a los sistemas deberán ser empleados exclusivamente para propósitos de la organización aprobados por la alta dirección. Por lo tanto, su uso está sujeto en cualquier momento a revisión,

2.2 El uso de los equipos, propiedad de los docentes, administrativos y alumnos, en instalaciones de la universidad deben ser autorizados por su respectiva jefatura o decanatura.

- Los miembros de la universidad pueden utilizar sus propios computadores, dispositivos periféricos, o software en las instalaciones de UNTELS siempre y cuando cuenten con la autorización de su Jefatura o decanatura correspondiente.
- Los dispositivos de almacenamiento (memorias USB, discos externos, etc.) deberán ser revisados en la Oficina de Informática y Estadística, a fin de garantizar su limpieza de posible software malicioso y virus, antes de su empleo en las instalaciones de la universidad.
- Las computadoras portátiles, deberán ser revisadas en la Oficina de Informática y Estadística por el mismo motivo señalado en el punto anterior
- El incumplimiento de alguna de estas políticas será tomado como una violación del protocolo de seguridad y será motivo de sanción.

2.3 Todo software utilizado en UNTELS debe contar con licencia de uso:

- Todo el software cargado en las computadoras de UNTECS deben estar de acuerdo a los compromisos de licencias, las leyes de protección de reproducción y los acuerdos de compra.

2.4 Está absolutamente prohibido el uso de software de seguridad por parte de los usuarios del sistema:

- A menos que este específicamente autorizado por el la jefatura de la Oficina de Informática y Estadística, el personal de la universidad y los alumnos no deben poseer o emplear software o equipos que puedan romper mecanismos de seguridad.
- El incumplimiento de esta política será tomado como una violación del protocolo de seguridad y será motivo de sanción.

2.5 Políticas para el control de accesos:

a. Todo usuario de los sistemas debe contar con autorización explícita de uso:
    - Los individuos y programas deben estar explícitamente autorizados para usar los sistemas y espacios físicos de UNTELS. Este es un privilegio que solo será otorgado cuando sea necesario que un individuo realice una función específica de trabajo y se hayan documentado sus responsabilidades y su perfil de acceso.
b. Los terceros podrán usar de los sistemas e instalaciones de UNTELS solo si cuentan con autorización específica:
    - Personas que no sean personal ni alumnos de la UNTELS no tendrán acceso a los espacios físicos, excepto bajo circunstancias particulares, y tendrán acceso estrictamente a la mínima información que requieran conocer y deberán ser controlados todo el tiempo, salvo indicaciones de los órganos de dirección.

2.6 Políticas de seguridad de la información para la promoción, vacaciones, rotación y/o cese del personal docente y administrativo de la universidad.

- Los estándares relacionados al personal docente y administrativo, alumnos, deben ser aplicados para asegurar que estos sean seleccionados adecuadamente antes de ser reclutados a la organización; a fin de que puedan ser fácilmente identificados mientras formen parte de UNETCS y que el acceso sea reevaluado o revocado temporal o indefinidamente cuando un docente o administrativo es promocionado, goce de vacaciones, de licencia, sea despedido o transferido, esta política se aplica a toda la comunidad de la universidad (docentes, alumnos, administrativos, contratistas, proveedores, etc.)

2.7 Cada puesto que se desempeñe dentro de la institución debe estar completamente descrito y el personal que los desarrolla debe conocer las responsabilidades propias de su puesto.

- La dirección, los jefes, decanos, deben conocer las responsabilidades del personal que está a su cargo, así también las funciones de cada empleado que desarrolla una función específica dentro

de la organización, se debe contar con una descripción formal del puesto y las responsabilidades asociadas (MOF).

2.8 Manejo adecuado de las pistas de auditoría.

- La Oficina de Informática y Estadística guarda un log de todas las operaciones que se realizan y registran, esto sirve como base para evaluar la seguridad del sistema y el acatamiento de las políticas; asimismo, proporciona pistas que permitan realizar un seguimiento a las actividades del sistema, en caso de una auditoria

IX. SELECCIÓN E IMPLEMENTACION DE CONTROLES PARA MITIGAR LOS RIESGOS

De acuerdo a los requerimientos de seguridad, se han de implementar controles que garanticen que los riesgos sean reducidos a un nivel aceptable.

Los controles a implementar:

1. Seguridad Lógica
2. Seguridad Personal
3. Seguridad física y ambiental
4. Inventario de activos y clasificación de la información
5. Administración de las operaciones y comunicaciones
6. Adquisición, desarrollo y mantenimiento de sistemas informáticos
7. Procedimiento de respaldo
8. Gestión de incidentes de seguridad
9. Cumplimiento normativo
10. Privacidad de la información

Los controles antes mencionados se consideran principios rectores para la administración de la seguridad de la información en la organización.

Para cada riesgo identificado existe una decisión de tratamiento de riesgo. Las opciones posibles para el tratamiento de riesgo incluyen:

- Aplicación de controles (reducción del riesgo) aceptando los riesgos, proporcionándolos claramente, a fin de satisfacer la política de la universidad y los criterios para la aceptación de riesgo.
- Transfiriendo los riesgos asociados a un procesos a otras partes (aseguradoras)

Los controles asegurarán que los riesgos se reduzcan a un nivel aceptable, tomando en cuenta:

- Requerimientos y restricciones de legislación nacional e internacional y regulaciones.
- Objetivos de la organización.
- Exigencias operacionales y restricciones.
- El costo de implementación y operación en relación con los riesgos siendo reducidos y restando proporcionalmente a la organización requerimientos y restricciones.
- La necesidad de equilibrar la inversión en implementación y operación de controles contra el daño probable ante una violación o falla de los protocolos de seguridad

Se debe considerar que ningún juego de controles puede alcanzar completamente la seguridad y que la acción adicional de la dirección debe ser puesta en práctica para supervisar, evaluar, y mejorar la eficiencia y la eficacia de dichos controles de seguridad

1. Seguridad Lógica

Objetivo: Controlar adecuadamente los accesos a la información mediante la aplicación de mecanismos de seguridad establecidos para evitar la modificación, destrucción inconsistencia de los archivos y datos, especificando cuando estos se implementan a nivel de un sistema operativo.

Los procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios se mencionan a continuación:

a) Los usuarios del sistema informático tienen un firme compromiso de mantener en secreto sus contraseñas personales y las compartidas por un grupo al cual pertenece, este compromiso está contemplado en los términos y condiciones del contrato o resolución. **Responsable: Jefe de la Oficina de Personal**

b) Cada usuario pertenecerá a un grupo de trabajo definido y poseerá un determinado perfil, el que permitirá accesos a los mismos recursos y servicios informáticos, de acuerdo a las funciones del área o unidad a la que pertenecen y de acuerdo al rol correspondiente a su cargo. Los accesos personalizados deberán contar con la autorización y aprobación del Jefe Inmediato. **Responsable: Jefe de la Oficina de Informática y Estadística**

c) Todo acceso a la red y al sistema, deberá pedir el nombre de usuario (username) y la contraseña (password) .**Responsable: Jefe de la Oficina de Informática y Estadística**

d) El número máximo de intentos de acceso al sistema informático, será de 3 veces, luego de lo cual el sistema bloqueará automáticamente la cuenta. **Responsable: Jefe de la Oficina de Informática y Estadística**

e) Cada usuario de la entidad tendrá una sola clave de acceso, válida para el ingreso al sistema informático. Responsable. **Responsable: Jefe de la Oficina de Informática y Estadística**

f) La Oficina de Informática y Estadística activará el pedido de cambio de contraseña, después de creada la cuenta. **Responsable: Jefe de la Oficina de Informática y Estadística**.

g) El usuario y contraseña asignada al trabajador es personal e intransferible. **Responsable: Jefe de la Oficina de Informática y Estadística**.

h) Los accesos a la Internet, serán bloqueados desde las 5::00 p.m. hasta las 7:30 a.m. para oficinas administrativas y de 11:00 p.m. a 7:30 a.m. para el área académica de lunes a sábado, y los domingos todo el día. Solo las oficinas de la alta dirección y unidades críticas contarán con el servicio ininterrumpido, salvo indicación contraria de las mismas. Cualquier excepción será autorizada por la alta dirección de la universidad. **Responsable: Jefe de la Oficina de Informática y Estadística**

i) Los usuarios tendrán acceso a Internet limitado solo a las páginas definidas por las políticas de la universidad, el acceso a otras páginas de Internet o acceso total, serán autorizadas por la alta dirección de la universidad mediante oficio, están excluidas de esta política las oficinas de la alta dirección y jefaturas de las área críticas de UNTECS. **Responsable: Jefe de la Oficina de Informática y Estadística.**

j) Los usuarios que tengan acceso a Internet deben usar del mismo sólo para conseguir información o informarse sobre temas afines a las labores o funciones que realiza dentro de la universidad. **Responsable: Jefes de Área y Jefe de la Oficina de Informática y Estadística.**

k) Está prohibido el uso de Internet para descargar programas ejecutables, archivos de video, de imagen o de audio que no estén permitidos o aprobados por las políticas de la universidad ni se orienten a los objetivos de la institución. **Responsable: Jefes de Área y Jefe de la Oficina de Informática y Estadística.**

Revisiones periódicas sobre los derechos concedidos a los usuarios.

a) La Oficina de Personal comunicará a la Oficina de Informática y Estadística, mediante oficio, el cambio de cargo de los trabajadores, por rotación, promoción o encargatura, a fin de conceder los permisos respectivos en el sistema. **Responsable: Jefe de la Oficina de Personal.**

Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades referidas a la manipulación de información puedan ser seguidas e identificadas.

a) Todos los usuarios del sistema informático en UNETCS tienen asignado un nombre de usuario o userid, el cuál es único e invariable durante el tiempo que dure su relación con la institución, para acceder a los sistemas de información, los usuarios deberán identificarse con el userid que tienen asignado y con

una contraseña de su exclusivo conocimiento. **Responsable: usuario del sistema informático de UNTELS**.

b) El usuario/administrador es el único responsable de mantener la confidencialidad de su contraseña.

Deben existir controles especiales sobre utilidades del sistema y herramientas de auditoría.

a) Las utilidades del sistema deben ser usadas sólo por personal autorizado, se debe de tener un registro de las utilidades del sistema y el personal que tiene acceso a ellas. **Responsable: Jefe de la Oficina de Informática y Estadística.**

b) Las herramientas de auditoría, deben ser usadas sólo por personal autorizado, se debe de tener un registro de las herramientas de auditoría y el personal que tiene acceso a ellas. **Responsable: Jefe de la Oficina de Informática y Estadística.**

Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.

a) El jefe de la Oficina de Informática y Estadística o un sub jefe de la oficina en coordinación con el DBA (Data Base Administrador) deben mantener un registro adecuado de las pistas de auditoría que permitan verificar el cumplimiento de las normas en la universidad.

Controles especiales sobre usuarios remotos y computación móvil.

a) Todos los puestos remotos que vayan a acceder a la infraestructura de UNTELS llevarán instalado y configurado el antivirus homologado por la entidad. Dicho antivirus deberá poder ser monitoreado (verificación del estado, de versiones) por personal técnico de la Oficina de Informática y Estadística. **Responsable: Jefe de la Oficina de Informática y Estadística.**

b) Las empresas proveedoras que realicen accesos remotos deben comprometerse por contrato al cumplimiento del requerimiento estipulado en el acápite anterior. **Responsable: Jefe de la Oficina de Informática y Estadística.**

c) Las empresas proveedoras de la universidad que acedan a la red deben:

- Poseer un antivirus actualizado
- Realizar control de vulnerabilidades e informar a UNTECS (Fortalecimiento de control de acceso)

d) El mecanismo de control de acceso utilizado en los accesos remotos deberá ser robusto, de forma que aumenten las garantías de que el código de usuario utilizado en el acceso corresponde con la persona que está accediendo. **Responsable: Jefe de la Oficina de Informática y Estadística.**

e) UNTELS trasladará la responsabilidad de los accesos remotos realizados a las empresas que realizan dichos accesos. Para ello, en dichas empresas deberá existir un Agente de Seguridad que será el responsable de gestionar los mecanismos de seguridad utilizados y sus usuarios con

f) correspondientes. **Responsable: Jefe de la Oficina de Economía.**

2. Seguridad Personal

Objetivo: Asegurar que todo el personal de la universidad, alumnos y las empresas proveedoras entiendan y acepten sus responsabilidades en cuanto a seguridad de la información.

A continuación se muestra la definición de roles y responsabilidades establecidos sobre la seguridad de información.

a) La seguridad es responsabilidad de todo el personal, alumnos y proveedores de UNTELS, por ende, todos los mencionados son personas con acceso a las instalaciones e información de la institución y deben acatar los estándares documentados en la política de seguridad de información e incluirla como una de sus responsabilidades principales. **Responsables: Jefes de área**

b) Todos los dispositivos personales de información (computadoras de propiedad de los empleados, asistentes digitales personales PDA [Personal Digital Assistant]) que interactúen con los sistemas

de UNTECS, deben estar autorizados por la oficina de informática y estadística. **Responsable: Jefe de la Oficina de Informática y Estadística.**

c) Cuando se contrate al personal, se debe de entregar la política de seguridad así como las normas y procedimientos para el uso de las aplicaciones y los sistemas de información de la universidad. Asimismo, se debe entregar un resumen escrito de las medidas básicas de seguridad de la información, una copia firmada de la política de seguridad de información debe de ser guardada en el archivo del empleado. **Responsable: Jefe de la Oficina de Personal**

d) Las empresas proveedoras que interactúen con la información de UNTELS deberán recibir una copia del acuerdo de no divulgación, este debe estar firmado por UNTELS y por el proveedor de servicios. **Responsable: Jefe de Economía**, **Comité permanente de adquisiciones**

Verificación de antecedentes.

a) Todo personal que labora en UNTELS deberá mantener en ella su hoja de vida documentada y actualizada. **Responsable: Jefe de la Oficina de Personal.**

b) Todo personal que labora en UNTELS deberá comunicar obligatoriamente a la Oficina de Personal los cambios ocurridos en la información proporcionada inicialmente, tales como domicilio, estado civil, estudios entre otros. **Responsable: Jefe de la Oficina de Personal.**

c) Todo participante en el proceso de selección se someterá a la revisión de su documentación original. **Responsable: Jefe de la Oficina de Personal.**

Concientización y entrenamiento.

a) Es responsabilidad de la Oficina de Informática y Estadística promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información. El programa de concientización en seguridad debe de contener continuas capacitaciones y charlas, adicionalmente se puede emplear diversos métodos como afiches, llaveros, mensajes de LOG-IN (acceso), etc., los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información. **Responsable: Jefe de la Oficina de Informática y Estadística.**

b) Los usuarios de los sistemas de información de UNTELS deberán de ser informados (capacitados) anualmente sobre la importancia de la seguridad de la información. Un resumen escrito de la información básica debe de ser entregada nuevamente a cada empleado y una copia firmada debe de ser guardada en sus archivos. **Responsable: Jefe de la Oficina de Personal**, **Jefe de la Oficina de Informática y Estadística.**

c) Es responsabilidad de los tutores y/o entrenadores proveer de material escrito al personal en el proceso de capacitación, los materiales pueden ser manuales, guías, separatas, entre otros. Responsables: Responsable**: Jefe de la Oficina de Personal**, **Jefe de la Oficina de Informática y Estadística.**

d) Los entrenadores deberán ser elegidos de acuerdo a la experiencia y al conocimiento de un tema específico. Responsables: **Responsable: Jefe de la Oficina de Personal**, **Jefe de la Oficina de Informática y Estadística.**

Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad.

a) El incumplimiento por parte del empleado a lo establecido en las políticas de seguridad de la información, da causa a:

- Que UNTELS aplique las medidas disciplinarias correspondientes, incluyendo en su caso, la baja de la(s) clave(s) de acceso a los sistemas y/o aplicaciones involucradas o de la Institución
- Si el caso lo amerita la baja de la institución.
- Resarcir de manera económica los daños y perjuicios que le ocasione a UNTELS el problema ocasionado, independientemente a que se ejecuten las acciones legales de carácter civil, laboral y penal. **Responsable: Jefe de la Oficina de Personal**

Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos

a) La Oficina de Personal, solicitará a la Oficina de Informática y Estadística, la des habilitación de cuenta de usuario, mediante oficio; esto se debe dar por: goce vacacional, licencia, suspensión o al cese del trabajador. **Responsable: Jefe de la Oficina de Personal**, **Jefe de la Oficina de Informática y Estadística.**
b) Es responsabilidad de la Oficina de Informática y Estadística proceder en caso de cese, deshabilitando el código de usuario y todos los accesos asignados al personal cesante, en forma definitiva y registrar la fecha de cese. En caso de goce vacacional, permiso por licencia o suspensión, bloquear temporalmente el código de usuario del personal. Cualquier excepción a lo establecido, será autorizada por el por la alta dirección de la universidad.

3. **Seguridad Física y Ambiental**

Objetivo: Evitar accesos no autorizados, daños e interferencias contra los ambientes y la información de la organización.

Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.

a) Se debe establecer un registro de control de entrada y salida de visitas a las Oficinas administrativas. **Responsable: Jefe de Seguridad.**
b) Implementar un sistema de vigilancia con cámaras de seguridad en lugares estratégicos, a fin de mantener un mejor control del movimiento de las personal dentro de la universidad. **Responsable: Jefe de Seguridad.**

Controles para prevenir pérdidas, daños o robos de los activos. Esto incluye la protección de los equipos frente a amenazas físicas y ambientales.

a) Cuando el personal se aleje de su estación de trabajo momentáneamente, deberá asegurarse de activar el "protector de pantalla" protegido con una contraseña personal.
b) Bajo ningún motivo, ninguna persona deberá retirar un equipo o componente de cómputo propiedad de la universidad sin una guía de salida previamente autorizada por la dependencia en cuestión. **Responsable: personal de la universidad, Jefes de área.**
c) Apagar los equipos de cómputo cuando se dejen de usar por un prolongado tiempo, en especial cuando se disponga de feriados largos. **Responsable: personal de la universidad, Jefes de área.**
d) Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados. **Responsable: Jefe de Patrimonio.**
e) La Oficina de Informática y Estadística es la responsable de asegurar que el usuario no pueda modificar la configuración de hardware y software establecida.
f) La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente. **Responsable: Jefes de área, agentes de seguridad interna.**

Controles para establecer medidas de seguridad en la Oficina de Informática y Estadística.

a) La Oficina de Informática y Estadística es un ambiente de acceso restringido en el cuál se encuentran los ambientes de desarrollo, producción y soporte, el ingresó al mismo sólo debe estar disponible al personal autorizado, el mismo que debe estar debidamente identificado. **Responsable: Jefe de la Oficina de Informática y Estadística.**
b) Se debe establecer un registro de control de entrada y salida de visitas a la Oficina de Informática y Estadística, el cual debe ser custodiado en todo momento (horario de labor) por un personal de Informática y un agente de seguridad (horario fuera de labor). **Responsable: Jefe de la Oficina de Informática y Estadística, personal de informática**

c) Las autorizaciones de ingreso al Data Center deberá hacer la Jefatura de la Oficina de Informática y Estadística o por el responsable que este designe.

d) El Data Center y los equipos de cómputo de la Oficina de Informática y Estadística no deben estar expuestos al personal en general. . **Responsable: Jefe de la Oficina de Informática y Estadística.**

e) La puerta del centro de cómputo deberá permanecer con cerrada permanente, tanto de día como de noche. **Responsable: Jefe de la Oficina de Informática y Estadística.**

f) La limpieza del centro de cómputo, deberá realizarse en presencia de algún trabajador encargado de la Oficina de Informática y Estadística. **Responsable: Jefe de la Oficina de Informática y Estadística.**

g) Todo el personal deberá conocer las zonas de seguridad identificando las señalizaciones convenientemente. **Responsable: Jefe de Seguridad, Jefe de la Oficina de Bienestar Universitario**

h) El personal deberá informar la existencia de cualquier obstáculo que se encuentre en las rutas señaladas como salida, informando a la jefatura de seguridad, sobre las condiciones inseguras encontradas, con la finalidad que esta unidad realice la reubicación o retiro de la zona. **Responsable: Jefe de Seguridad, Jefe de la Oficina de Bienestar Universitario.**

i) La Oficina de Informática y Estadística es una zona en que está terminantemente prohibido fumar, así como el ingreso o transporte de material inflamable. **Responsable: Jefe de Seguridad, Jefe de la Oficina de Informática y Estadística.**

j) Los archivos de información deberán estar debidamente señalizados en prioridad para su evacuación (prioridad de 1 a 3), y el brigadista de turno deberá mantener una relación nominal de estos documentos. **Responsables: Jefes de Área y Jefe de Seguridad**

4. Inventario de los activos y clasificación de la información

Objetivo: Asegurar que la información reciba un nivel de protección adecuado.

4.1. Realizar y mantener un inventario de activos asociados a la tecnología de información.

a) Todo documento o contenedor de información debe ser etiquetado como "Restringido", "Confidencial", de "Uso interno" o de "Acceso General", dependiendo de la clasificación asignada. **Responsable: Jefes de área**

b) Todo documento que presente información clasificada como "Confidencial" o "Restringida", debe ser etiquetado en la parte superior e inferior de cada página con la clasificación correspondiente. **Responsable: Jefes de área.**

c) Todo documento clasificado como "Confidencial" o "Restringido" debe contar con una carátula en la cual se muestre la clasificación de la información que contiene. **Responsable: Jefes de área**

d) El ambiente donde se almacena la información clasificada como "Restringida", debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado. El personal de limpieza debe ingresar al ambiente acompañado por personal autorizado. **Responsable: Jefe de Seguridad.**

e) Solo el personal formalmente autorizado debe tener acceso a información clasificada como "Restringida" o "Confidencial". **Responsable: Jefes de área.**

f) Brindar un esquema normativo a la Oficina de Informática y Estadística para actualizar en forma oportuna los recursos informáticos, así como para la distribución a las diferentes áreas usuarias de la universidad. **Responsable: Jefe de la Oficina de Informática y Estadística**

g) Reportar inmediatamente al Jefe de la Oficina de Informática y Estadística los cambios ocurridos en el Inventario actual de activos tecnológicos (disminución de memorias RAM, capacidad de disco, cambio de discos, conflictos de IP, cambio de teclado, cambio de mouse, rotación o traslado de activos, entre otros). **Responsable: Jefes de área, jefatura de control patrimonial**

h) la Oficina de Informática y Estadística a través del responsable designado deberá mantener actualizada la relación de software base, necesario para cada grupo de usuarios.

i) La Unidad de Tecnología de la Información a través del responsable deberá mantener actualizado el inventario de los equipos de cómputo, periféricos, equipos de comunicación y redes, UPS, a nivel de la institución y por grupos de usuarios.

j) La Oficina de Informática y Estadística a través de uno o más responsables deberá mantener una relación actualizada de los archivos de configuración que deben ser protegidos en forma permanente (*.INI, *.CNF, *.SYS, *.DLL, *.EXE, *.BAT, otros) en las máquinas de la red informática de la entidad.

k) La Oficina de Informática y Estadística a través de un responsable designado deberá mantener actualizada la relación de productos de software o aplicaciones desarrolladas o adquiridos por la universidad.

4.2 Realizar una clasificación de la información.

a) Todo contenedor de información en medio digital (CD, DVD, memorias USB, cintas de backup, diskettes, etc.) deben presentar una etiqueta con la clasificación correspondiente. **Responsable: Jefe de la Oficina de Informática y Estadística**.

b) La información en formato digital clasificada como de acceso "público", puede ser almacenada en cualquier sistema de la universidad, sin embargo, se deben tomar las medidas necesarias para no mezclar información pública con información correspondiente a otra clasificación. **Responsable: Jefe de la Oficina de Informática y Estadística**

c) Todo usuario, antes de transmitir información clasificada como "Restringida o Confidencial", debe asegurarse que el destinatario de la información esté autorizado a recibir dicha información. **Responsable: Jefes de área.**

d) Todo usuario que requiere acceso a información clasificada como "Restringida" o "Confidencial", debe ser autorizado por el propietario de la misma. Las autorizaciones de acceso a este tipo de información deben ser documentadas. **Responsable: Jefes de área.**

e) La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación. **Responsable: Jefes de área.**

f) La información en formato digital, clasificada como "Restringida", debe ser encriptada con un método aprobado por los encargados de la administración de seguridad de la información de la Oficina de Informática y Estadística, cuando es almacenada en cualquier medio (disco duro, CD, DVD, memorias USB, disquetes, cintas, CDs, etc.). **Responsable: Jefes de área.**

g) No tirar documentos confidenciales a las papeleras. Destruir dichos documentos con un picador de papel o de manera tal que se impida su reconstrucción. **Responsable: Jefes de área.**

h) No dejar documentos confidenciales sobre el escritorio, durante las horas de ausencia del usuario responsable. **Responsable: Jefes de área.**

i) Al retirarse de las oficinas, dejar con llave los escritorios y estantes que contienen documentos confidenciales. **Responsable: Jefes de área.**

j) A la hora de entrada, verificar que los escritorios y estantes permanezcan con llave y que no hayan sido manipulados, de no ser así se deberá informar a la jefatura de seguridad con copia a la alta dirección de la universidad. **Responsable: Jefes de área.**

k) No deben dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la universidad. **Responsable: Jefes de área.**

5. Administración de las operaciones y comunicaciones

Objetivo: Asegurar un adecuado nivel de servicio a los clientes, los requerimientos de seguridad deben ser desarrollados e implementados para mantener el control sobre las comunicaciones y las operaciones.

Procedimientos documentados para la operación de los sistemas.

a) Todos los procedimientos de operación de los sistemas deben ser documentados y los cambios realizados a dichos procedimientos deben ser autorizados por el la jefatura de la Oficina de Informática y Estadística.

b) Todos los procedimientos de encendido y apagado de los equipos deben ser documentados; dichos procedimientos deben incluir el detalle de personal clave a ser contactado en caso de fallas no contempladas en el procedimiento regular documentado. **Responsable: Jefe de la Oficina de Informática y Estadística**

c) Todas las tareas programadas en los sistemas para su realización periódica, deben ser documentados. Este documento debe incluir tiempo de inicio, tiempo de duración de la tarea, procedimientos en caso de falla, entre otros. **Responsable: Jefe de la Oficina de Informática y Estadística**

d) Los procedimientos para resolución de errores deben ser documentados, entre ellos se debe incluir: Errores en la ejecución de procesos por lotes, Fallas o apagado de los sistemas, Códigos de error en la ejecución de procesos por lotes, Información de los contactos que podrían colaborar con la resolución de errores, **Responsable: Jefe de la Oficina de Informática y Estadística**

Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.

a) La Oficina de Informática y Estadística es la única unidad encargada y autorizada para realizar las configuraciones de software de aplicación, a través del personal especializado.

b) Los responsables de realizar dichas configuraciones deberán seguir el estándar y lineamientos según grupo y perfil de usuario, al mismo tiempo de realizar las adecuaciones necesarias para el buen funcionamiento del mismo. **Responsable: Jefe de la Oficina de Informática y Estadística**

c) Es responsabilidad del personal de la Oficina de Informática y Estadística la verificación de programas y software licenciados a instalar y/o configurarse.

d) Las configuraciones de las aplicaciones deben estar estandarizadas y formalizadas en documentos visados por el encargado de la administración de la red. **Responsable: Jefe de la Oficina de Informática y Estadística**

e) Cada vez que existan variaciones en las configuraciones del servidor, del software base (sistema operativo), del número de licencias, en los dispositivos, se deben afinar las configuraciones y mantener actualizada la documentación respectiva. La configuración actual debe estar reflejada en los documentos de soporte para el área de administración de red. **Responsable: Jefe de la Oficina de Informática y Estadística**

f) Es responsabilidad y autoridad única del DBA realizar las funciones de creación, instalación y configuración de la Base de Datos de la organización. **Responsable: Jefe de la Oficina de Informática y Estadística**

g) Se debe crear un documento que contenga los estándares y procedimientos detallados para la creación, instalación y configuración de la Base de Datos de la organización. Dicho documento deberá estar disponible para el DBA y la persona que se haya designado para su apoyo en caso de ausencia. **Responsable: Jefe de la Oficina de Informática y Estadística**

h) El DBA deberá reportar inmediatamente al Jefe de la Oficina de Informática y Estadística cualquier anomalía en los procedimientos de creación, instalación y configuración de la Base de Datos. **Responsable: Jefe de la Oficina de Informática y Estadística**

i) Es responsabilidad del DBA el mantenerse en continua investigación de nuevos métodos y procesos para las mejoras en dichas instalaciones y configuraciones. **Responsable: Jefe de la Oficina de Informática y Estadística**

j) Todos los equipos en donde se instalará la base de datos, deben estar referenciados en un documento actualizado y deberá formar parte de la documentación para la administración de la base de datos. **Responsable: Jefe de la Oficina de Informática y Estadística**

k) Se debe mantener una relación actualizada de los componentes que son necesarios instalar en la máquina del usuario que tendrá acceso a la base de datos. **Responsable: Jefe de la Oficina de Informática y Estadística**

l) El BDA llevará una bitácora actualizada de la creación, instalación y configuración de la base de datos. **Responsable: Jefe de la Oficina de Informática y Estadística**.

m) Antes de realizar una creación, instalación o configuración de la base de datos, es necesario obtener una copia de seguridad de la información existente previa al proceso. **Responsable: Jefe de la Oficina de Informática y Estadística**

n) Los parámetros de configuración de la base de datos deberán estar en un documento impreso que formará parte de la documentación de administración de la base de datos. **Responsable: Jefe de la Oficina de Informática y Estadística**

Separación de los ambientes de desarrollo, pruebas y producción.

a) El ambiente de servidores (DATA CENTER) debe de mantenerse siempre separado de los ambientes de producción, debiendo existir controles de acceso adecuados para cada uno de ellos. **Responsable: Jefe de la Oficina de Informática y Estadística**

b) Los ambientes de producción son aquellos en donde residen los programas ejecutables de producción y los datos necesarios para el funcionamiento de los mismos. Solo el personal autorizado a efectuar los cambios en los sistemas debe contar con privilegios de escritura en los mismos. **Responsable: Jefe de la Oficina de Informática y Estadística**

c) Los programas compiladores no deben ser instalados en los sistemas en producción, todo el código debe ser compilado antes de ser transferido al ambiente de producción. **Responsable: Jefe de la Oficina de Informática y Estadística**

d) Las pruebas deben de realizarse utilizando datos de prueba. Sin embargo, copias de datos de producción pueden ser usadas para las pruebas, siempre y cuando los datos sean autorizados por el propietario y manejados de manera confidencial. **Responsable: Jefe de la Oficina de Informática y Estadística**

e) El personal de desarrollo puede tener acceso de solo lectura a los datos. La actualización de los permisos de acceso a los datos de producción debe de ser autorizada por el propietario de información y otorgada por un periodo limitado. **Responsable: Jefe de la Oficina de Informática y Estadística**

f) El personal del área de desarrollo no debe modificar, o accesar a información de los ambientes de producción o de pruebas, el acceso a estos ambientes estarán bajo un estricto control por el responsable designado. **Responsable: Jefe de la Oficina de Informática y Estadística**

Monitoreo del servicio dado por terceras partes.

a) El proveedor de auditoría debe facilitar a la universidad toda la información y documentación propia de EL PROVEEDOR o de terceros relacionada con el servicio materia del contrato, incluyendo la revisión de la respectiva prestación, a satisfacción de las personas mencionadas. **Responsable: Jefe de Economía,Jefe de la Oficina de Informática y Estadística**

Administración de la capacidad de procesamiento

a) Es responsabilidad del DBA el cuidado y la integridad de la Información almacenada en la estructura de la misma. **Responsable: Jefe de la Oficina de Informática y Estadística.**

b) El DBA deberá garantizar los casos de acceso concurrentes a la base de datos de manera que no altere el funcionamiento del sistema o programa, **Responsable: Jefe de la Oficina de Informática y Estadística.**

c) El DBA deberá monitorear periódicamente el tamaño de la base de datos, el espacio en disco, entre otros aspectos que garanticen el funcionamiento continuo. **Responsable: Jefe de la Oficina de Informática y Estadística.**

d) Es responsabilidad del DBA realizar la gestión de la base de batos efectivamente, optimizándola periódicamente y determinado los puntos críticos de la misma. **Responsable: Jefe de la Oficina de Informática y Estadística.**

e) Los cambios o puntos de control determinados ya sea por el BDA o los desarrolladores deberán ser coordinados e informados a la jefatura de Informática y Estadística

f) Todos los objetos o elementos del modelo de datos, deberán obedecer a estándares de relaciones de integridad y normalización. **Responsable: Jefe de la Oficina de Informática y Estadística.**

g) El modelo físico debe contener las últimas actualizaciones del modelo lógico definido. **Responsable: Jefe de la Oficina de Informática y Estadística.**

Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.

a) La Oficina de Informática y Estadística debe asegurar que cualquier usuario no pueda instalar software o programa en los equipos propiedad de la universidad. **Responsable: Jefe de la Oficina de Informática y Estadística.**

b) Cuidar de que el antivirus instalado en el puesto de trabajo se encuentre siempre actualizado. En los puestos conectados a la red de la empresa este proceso se encuentra centralizado y automatizado al arrancar el PC todos los días, pero en los portátiles y en los puestos que no están conectados a la red, ese procedimiento de actualización es responsabilidad de cada usuario. **Responsable: personal de la universidad.**

c) La Oficina de Informática y Estadística, bloqueará los accesos de ingreso o salida de información a través de medios de almacenamiento, a excepción de las áreas y/o unidades autorizadas por la alta dirección de la universidad.

d) La Oficina de Informática y Estadística mantendrá una bitácora actualizada de los virus encontrados por PC y por tipo de archivo.

e) La Oficina de Informática y Estadística, deberá instruir al personal y hacerse cargo de eliminar la existencia de virus que se presenten en la organización con apoyo de las diferentes herramientas con que se dispone.

f) La Oficina de Informática y Estadística deberá mantener constantemente informado al personal de la organización sobre la aparición de nuevos virus informáticos y la forma como se transmiten y atacan

Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.

a) La Oficina de Informática y Estadística a través del responsable de procesos internos, determinará el impacto de la instalación de un componente, tal como un equipo de comunicaciones, en la red, también deberá tomar las precauciones debidas. Para tal fin, se deberá elaborar un plan de instalación, el cual debe prever posibles contingencias.

b) El responsable del Área de Procesos de la Oficina de Informática y Estadística antes de instalar un componente, tal como un equipo de comunicaciones (accespiont, switch, router, hub, etc) se deberá determinar su tipo, el lugar donde se instalará y las recomendaciones brindadas por el proveedor para la instalación.

c) El responsable del Área de Procesos de la Oficina de Informática y Estadística antes y después de la instalación deberá probar o "testear" el componente a instalar.

d) El responsable del Área de Procesos de la Oficina de Informática y Estadística deberá revisar constantemente el tráfico o flujo de información en la red. Revisar el nivel de congestión y las causas probables del mismo, también revisará periódicamente de manera integral el estado de los componentes y enlaces de comunicación.

e) El responsable del Área de Procesos de la Oficina de Informática y Estadística deberá revisar periódicamente la información contenida en las carpetas, principalmente las relacionadas al sistema operativo, correos y carpetas destinadas a determinadas áreas funcionales, a fin de depurarlas para mantener un buen estado y rendimiento de la red informática de la universidad.

f) Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PC's que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado por la alta dirección de la universidad. Todas las comunicaciones de datos deben efectuarse directamente a través de la LAN de la institución. **Responsable: Jefe de la Oficina de Informática y Estadística.**

g) Los servidores de red y los equipos de comunicación deben estar ubicados en lugares apropiados, protegidos contra daños y robo (DATA CENTER). Debe restringirse severamente el acceso a estos locales y a los ambientes de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso. **Responsable: Jefe de la Oficina de Informática y Estadística.**

Seguridad sobre el intercambio de la información, incluido el correo electrónico.

a) Cada usuario está obligado a utilizar la red corporativa sin incurrir en actividades que pueden ser consideradas ilícitas o ilegales (actividades que infrinjan los derechos de la universidad o de terceros). **Responsable: Jefes de área.**

b) El correo electrónico institucional, es una herramienta de comunicación e intercambio de información oficial entre personas, no es una herramienta de difusión indiscriminada de información. Responsables: **Responsable: Jefes de área, personal de la universidad.**

c) El uso reiterado del Correo Electrónico y su acceso a la red con fines particulares o de forma irregular, pueden constituir falta laboral y motiva sanción. **Responsable: Jefes de área, personal de la universidad.**

d) La Oficina de Informática y Estadística debe garantizar la privacidad de las cuentas de correo electrónico institucional de todos los usuarios.

e) Ante la existencia de indicios racionales de uso indebido del correo electrónico, UNTELS en el ejercicio regular de sus facultades de dirección, se reserva el derecho de adoptar medidas de control y supervisión, que garanticen el adecuado empleo del mismo, estableciendo los mecanismos técnicos necesarios que permitan verificar un uso correcto del correo electrónico y su acceso a la red, por parte de los trabajadores. **Responsable: Jefe de la Oficina de Informática y Estadística.**

f) El correo institucional asignado a la alta dirección y a los jefes de áreas críticas serán los únicos que podrán enviar y recibir información fuera del dominio de UNTELS. **Responsable: Jefe de la Oficina de Informática y Estadística.**

g) Se deben desactivar las opciones que permiten la ejecución de macros en aplicaciones ofimáticas sin pedir expresamente la autorización del usuario. Además, siempre que se autorice la ejecución de macros, se debe estar completamente seguro de la procedencia, fiabilidad e integridad de los contenidos del documento en que dichas macros se encuentran. **Responsable: Jefes de área, personal de la universidad, Jefe de la Oficina de Informática y Estadística.**

h) Nunca deben ejecutarse ni descargarse programas o archivos adjuntos (en correos electrónicos) cuya procedencia y fiabilidad no ofrezcan todas las garantías. **Responsable: Jefes de área, personal de la universidad.**

i) Si se recibe un mensaje de correo sospechoso, por sus contenidos o por incluir archivos adjuntos que se consideren extraños, aun en el caso de que proceda de personas conocidas, se deberá informar de forma inmediata a la Oficina de Informática y estadística para que se puedan tomar las medidas correspondientes. **Responsable: Jefes de área, personal de la universidad.**

Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.

a) Los archivos de bitácora (logs) y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de un año. **Responsable: Jefe de la Oficina de Informática y Estadística.**

b) Todos los intentos de conexión (logon), desconexión (logoff), cambios de contraseña, fallas en los cambios de contraseña, reinstalación de contraseñas, registro de usuarios, actualización de los registros de usuarios, y supresión de usuarios, serán registrados. **Responsable: Jefe de la Oficina de Informática y Estadística.**

6. Adquisición, desarrollo y mantenimiento de sistemas informáticos

Objetivo: Asegurar que la seguridad esté imbuida dentro de los sistemas de información.

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida. **Responsable: Jefe de la Oficina de Informática y Estadística.**

b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida. En UNTELS, la información confidencial esta rutinariamente encriptada, antes de que viaje a través de la red de comunicaciones. **Responsable: Jefe de la Oficina de Informática y Estadística.**

c) En UNTECS las llaves de encriptación son consideradas como un activo de información altamente crítico y confidencial, el propietario de su custodia recae en la Oficina de Informática y Estadística o por el responsable que esta designe. **Responsable: Jefe de la Oficina de Informática y Estadística.**

d) La información crítica debe ser encriptada cuando se vaya a respaldar o guardar. **Responsable: Jefe de la Oficina de Informática y Estadística.**

Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.

a) Los sistemas aplicativos deben ser probados en forma exhaustiva, antes de ser liberados a producción, en ambientes controlados de pruebas (Test y Calidad). El proceso de pruebas debe llevar un control estricto en los puntos que debe cumplir la nueva aplicación, y realizar un reporte a desarrollo del resultado de la prueba, se dará reporte con carácter de obligatorio al Jefe de la Oficina de Informática y Estadística. **Responsable: Sub jefaturas de la Oficina de Informática y Estadística.**

b) UNTECS deberá implantar mecanismos que permitan llevar controles de las modificaciones y accesos a las bibliotecas del sistema operativo y de programas producto y programas fuente con el objeto de mantener integridad sobre los ambientes de prueba y producción. **Responsable: Jefe de la Oficina de Informática y Estadística.**

c) Solo el jefe de la Oficina de Informática y Estadística es el responsable de mover código de los ambientes de prueba a los ambientes de producción. Debe existir un registro detallado de los cambios realizados utilizando el Proceso de Control de Cambios. **Responsable: Jefe de la Oficina de Informática y Estadística.**

Propiedad de los programas

a) Cualquier programa de computadora escrito por algún empleado de UNTELS dentro del alcance de su trabajo así como aquellos adquiridos por UNTELS son de propiedad de la organización. **Responsable: Jefe de la Oficina de Informática y Estadística.**

b) Los contratos para desarrollo externo deben acordarse por escrito y deben señalar claramente al propietario de los derechos del programa. En la mayoría de circunstancias, la universidad debería ser propietaria de todos los programas de cómputo desarrollados, debiendo pagar los costos **Responsable: Jefe de Economía, comité permanente de adquisidores**

c) Cada programa elaborado por desarrolladores propios de la universidad o por desarrolladores externos contratados por UNTELS, debe contener la información de derecho de autor correspondiente. Generalmente, el aviso debe aparecer en cuando el usuario inicie la aplicación. Un aviso

legible también debe estar anexado a las copias de los programas almacenados en dispositivos como CD, DVD, Memorias USB, cassettes, discos, disquetes, etc. **Responsable: Jefe de la Oficina de Informática y Estadística.**

d) Controlar las vulnerabilidades técnicas de los programas existentes en los sistemas de comunicación de la organización. **Responsable: Jefe de la Oficina de Informática y Estadística.**

7. Procedimientos de respaldo.

Objetivo: Establecer un conjunto de controles que permitan gestionar adecuadamente el respaldo de la información producida en UNTELS

Procedimientos de respaldos regulares y periódicamente validados.

a) La Oficina de Informática y Estadística mediante el responsable que designe, llevará una bitácora actualizada de la realización de backups de bases de datos detallando la fecha de backup, la hora, el tamaño, el responsable de la operación, el contenido, la fecha de registro, y observaciones en el caso que estas existieran.

b) La Oficina de Informática y Estadística mediante el responsable que designe llevará un kardex actualizado para el control de salidas e ingresos de copias de seguridad. El lugar que almacena las copias de seguridad (estante con llave asignado a la oficina bajo la custodia directa del jefe), debe ser administrada bajo la lógica de un almacén, y con los criterios de control dual.

c) El procedimiento de backup, debe ser difundido a todas las personas involucradas teniendo como responsable de tal difusión al Jefe de la Oficina de Informática y Estadística.

e) Las copias de seguridad de la base de datos de UNTELS abarcan, índices, tablas de validación y todo archivo requerido para la correcta ejecución de los aplicativos de la organización, los programas fuentes, programas objetos y cualquier software o procedimiento que trabaje con datos para producir resultados al usuario final. **Responsable: Jefe de la Oficina de Informática y Estadística.**

f) Todas las copias de seguridad se obtendrán por duplicado, una copia será almacenada en el lugar asignado por la Oficina de Informática y Estadística y la otra copia de seguridad (Tape Backup) debe ser remitida al despacho del secretario general de la universidad; remitiendo la documentación que respalde este proceso; cumplimiento con periodicidad mensual. **Responsable: Jefe de la Oficina de Informática y Estadística.**

g) El DBA, realizará comprobaciones puntuales para asegurar que las copias de seguridad se realicen correctamente, considerando lo siguiente:

- Organizar pruebas periódicas de hardware y software para la recuperación de la información.
- Establecer y ejecutar procedimientos para la restauración de la información de la universidad
- Participar en pruebas y simulacros de desastres en la entidad, donde se verifique el buen funcionamiento de los procedimientos de backups.

Responsable: Jefe de la Oficina de Informática y Estadística.

Conservar la información de respaldo en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro de procesamiento.

a) Los activos de información correspondiente a distintos niveles de clasificación, deben ser almacenados en distintos contenedores. La información etiquetada como "de uso interno" debe ser guardada de manera que sea inaccesible a personas ajenas a la universidad (tampoco accesible a alumnos). La información "Confidencial o "Restringida" debe ser asegurada para que esté sólo disponible a los individuos específicamente autorizados para acceder a ella. **Responsable: Jefe de la Oficina de Informática y Estadística.**

b) El ambiente donde se almacena la información clasificada como "Restringida", debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado. Personal de limpieza debe ingresar al

ambiente acompañado por personal autorizado. **Responsable: Jefe de la Oficina de Informática y Estadística.**

c) Los medios de almacenamiento, incluyendo discos duros de computadoras, que albergan información clasificada como "Restringida", deben ser ubicados en ambientes cerrados diseñados para el almacenamiento de dicho tipo de información. **Responsable: Jefes de área.**

8. Gestión de incidentes de seguridad de la información.

Objetivo: Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva a tiempo.

Procedimientos formales para el reporte de los eventos de seguridad de información y las vulnerabilidades asociadas con los sistemas de información.

a) Luego de reportado el incidente de seguridad, éste debe ser investigado por el personal técnico de la Oficina de Informática y Estadística en forma rápida y confidencial. Se debe identificar la severidad del incidente para la toma de medidas correctivas.

b) Se debe mantener una documentación de todos los incidentes de seguridad ocurridos en UNTELS.

d) Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida tanto por entes internos o externos, para su posterior utilización en procesos legales en caso de ser necesario. **Responsable: Jefes de área.**

Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

a) Luego de la investigación realizada por el personal designado para tal efecto, se elaborará un informe al Jefe de la Oficina de Informática y Estadística indicando la severidad del incidente, para que este tome las medidas del caso e informe a la alta dirección de la universidad en caso el incidente sea demasiado grave.

b) Jefe de la Oficina de Informática y Estadística reportará a la alta dirección las medidas de solución al incidente de seguridad ocurrido.

9. Cumplimiento Normativo y de Auditoria.

Objetivo: Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad.

a) Los jefes deben asegurarse que las responsabilidades de seguridad sean cumplidas y las funciones relacionadas se ejecuten apropiadamente. **Responsable: Jefe de planificación, Jefes de área.**

b) Es responsabilidad del personal encargado de la administración de la seguridad y de auditoría interna verificar el cumplimiento de las políticas de seguridad. Las excepciones deben ser reportadas a la jefatura de oficina apropiada. **Responsable: Jefes de área, jefe de planificación.**

c) Un proceso documentado asegurara que las violaciones a las políticas de seguridad y procedimientos no se den sin conllevar a un tipo de sanción por parte del usuario que comete dicha falta. **Responsable: Jefes de área.**

d) Los propietarios de la información deben participar en el proceso de auditoría, un proceso de revisión de la auditoria debe asegurar que: existan los informes de la misma, las alertas sean revisadas, se haya completado el análisis de auditoría, se obtenga la conclusión y sean tomadas las acciones establecidas durante el proceso. **Responsable: Jefes de área.**

e) Todos los registros de auditoría de sistemas, serán consolidados en una base de datos o archivo que facilite la generación de informes. **Responsable: jefe de planificación, Jefe de la Oficina de Informática y Estadística.**

f) Es necesario identificar y desarrollar modelos de informes de auditorías. **Responsable: Jefe de planificación.**

g) Habrá un solo punto de recolección y manejo de la información de auditoría del control de acceso. **Responsable: Jefe de la Oficina de Informática y Estadística.**

10. Privacidad de la información.

Objetivo: Asegurar niveles adecuados de privacidad en UNTELS

Para asegurar los niveles adecuados de privacidad se aplicarán los criterios de Inventario de Activos de la Información (Numeral 4. de los Aspectos Generales)

a) UNTELS debe adoptar prácticas óptimas que manejen cuidadosamente la información institucional. Todos los sistemas informáticos de UNTELS deben seguir una política de privacidad basada en principios de información, deben tomar medidas apropiadas para proveer seguridad adecuada. **Responsable: Jefes de área.**

b) UNTECS deberá definir responsabilidades con respecto a la aplicación de la clasificación de secreto institucional. **Responsable: Jefes de área.**

c) UNTELS deberá restringir el acceso a información en salvaguarda de su privacidad. **Responsable: Jefes de área.**

X. PLAN DE IMPLEMENTACIÓN DE LOS CONTROLES Y PROCEDIMIENTOS DE REVISIÓN PERIÓDICA.

PLAN DE IMPLEMENTACION DE CONTROLES DE SEGURIDAD DE LA INFORMACION

Nº	CONTROL	meses/semanas								Total semanas
		1	2	3	4	5	6	7	8	
1	Políticas de Seguridad	x x x x x								5
2	Seguridad Lógica		x x x x x x							6
3	Seguridad Física y Ambiental		x x x x x x x x							8
4	Seguridad Personal			x x x x x						5
5	Inventario de activos y clasificación de la información		x x x x x x x x x x x x x x x x							16
6	Administración de las operaciones y comunicaciones			x x x x x x x x						8
7	Adquisición, desarrollo y mantenimiento de sistemas informáticos		x x x x x x x x x x x x x x x x							16
8	Procedimiento de respaldo				x x x x x x x x x x x x x x					13
9	Gestión de incidentes de seguridad				x x x x x x x x x x x x x x x x					17
10	Cumplimiento normativo					x x x x x x x x x x x x x x				15
11	Privacidad de la información						x x x x x x x x x x x x			12

XI. RESPONSABILIDADES EN LA IMPLEMENTACION DEL PLAN

1. Alta dirección de la Universidad
2. Jefatura de la Oficina de Informática y Estadística
3. Personal informático asignado al área de seguridad de la información digital
4. Jefaturas de las diferentes áreas de UNTECS (por periodos)

a) Personal necesario para la implementación del Plan

- **Representante de la Alta dirección de la Universidad**
  - i. Algún profesional que determine la Alta dirección (preferencia con conocimientos de sistemas) con capacidad de toma de decisiones, en aspectos de seguridad de datos.
- **Coordinador del proyecto de seguridad de información**
  - i. Profesional de experiencia en gestión de TI, con capacidad de organización.
- **Ingeniero supervisor de seguridad de redes informáticas y de comunicación**
  - i. Ingeniero de sistemas o telecomunicaciones, con experiencia de 3 años como mínimo en trabajos similares
- **Ingeniero supervisor de procesos de mantenimiento y reparación de equipos informáticos**
  - i. Ingeniero de sistemas, con experiencia de 3 años como mínimo en trabajos similares

- **Ingeniero DBA**
    i. Ingeniero de sistemas, con experiencia de 3 años como mínimo como administrador de base de datos en ambiente Ms SQLSERVER
- **Técnico profesional en computación e informática (experiencia en manejo de base de datos)**
    i. Profesional técnico en informática o afines, con experiencia como operador de base de datos
- **Técnico profesional en computación e informática (experiencia en configuración de servidores y seguridad periférica)**
    i. Profesional técnico en telecomunicaciones, electrónica, informática o afines, con experiencia como operador servidores de datos y VoIP
- **Técnico profesional en computación e informática (experiencia mantenimiento y reparación de equipos informáticos)**
    i. Profesional técnico en informática o afines, especialista en reparación y mantenimiento de equipos informáticos y comunicaciones.
- **Asistente (secretaria con experiencia en ambientes informáticos)**

Costes de implementación:

Personal	Pago mensual	Pago total
Representante de la Alta dirección de la Universidad	4500	36000
Coordinador del proyecto de seguridad de información	4500	36000
Ingeniero supervisor de seguridad de redes informáticas y de comunicación	3500	28000
Ingeniero supervisor de procesos de mantenimiento y reparación de equipos informáticos	3500	28000
Ingeniero DBA	3500	28000
Técnico profesional en computación e informática (experiencia en manejo de base de datos)	1200	9600
Técnico profesional en computación e informática (experiencia en configuración de servidores y seguridad periférica)	1200	9600
Técnico profesional en computación e informática (experiencia mantenimiento y reparación de equipos informáticos)	1200	9600
Asistente (secretaria con experiencia en ambientes informáticos)	1100	8800
TOTAL EN RRHH		193600

Costes en hardware: (1 servidor firewall, 1 servidor base de datos de respaldo, 1 servidor proxy, router)

S/. 120000 (aproximado)

Costes en software: (antivirus, firewall, backup de base de datos, proxy)

S/. 90000 (aproximado)

Coste total aproximado de la implementación del plan (8 meses):

120000 (RRHH)

90000 (Hardware)

193600 (Software)

TOTAL **S/. 295600**