UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

MAESTRÍA EN INFORMÁTICA

TESIS

ANÁLISIS DE RIESGO Y POLÍTICAS DE SEGURIDAD DE INFORMACIÓN DE LA OFICINA DE TECNOLOGÍAS DE INFORMACIÓN (OTI) – UNA PUNO 2018

PRESENTADA POR:

SAULO GUSTAVO MACHICAO MOLLOCONDO

PARA OPTAR EL GRADO ACADÉMICO DE:

MAGISTER SCIENTIAE EN INFORMÁTICA
MENCIÓN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PUNO, PERÚ

2019

DEDICATORIA

A Dios, quien me proporciona todo, absolutamente todo.

A mi Madre, por haberme cuidado, guiado, y dado sus consejos para luchar y luchar.

A mi Esposa, a mi príncipe SM, que siempre están ahí, los amo.

A mi tía, gracias por todo.

AGRADECIMIENTOS

- A Dios, por quedarse a mi lado y a superar cualquier dificultad.
- A los docentes de la EPG – UNA por los conocimientos impartidos.
- A todo el personal de la OTI-UNA que me escucho, y me brindo sus sinceros aplausos.
- Al líder de gobierno digital por su apoyo incondicional.
- A todos Uds. Que siempre están ahí, aunque no lo estén, pero no lo saben, pero lo están.
- A toda mi familia, amigos, jurados y asesor de tesis por ayudarme a la conclusión en mi trabajo de investigación.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

Pág.

ÍNDICES DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

Pág.

RESUMEN

El análisis de riesgo es una herramienta que se adecua a todo tipo de organización, haciendo un énfasis en la seguridad de la información, siendo de manera interna y externa este análisis; para ello se han desarrollado diferentes metodologías de mayor flexibilidad y adaptabilidad, dando un soporte al proponer las políticas de seguridad de la información. La presente investigación se realizó en la Oficina de Tecnologías de Información, de la Universidad Nacional del Altiplano – Puno, el cual no cuenta con políticas de seguridad de la información que pueda garantizar la información que almacena en diferentes medios, físicos o virtuales. Siendo necesario las políticas para el inicio de un sistema de gestión de seguridad de la información, según la NTP 27001:2014. El objetivo que se alcanzo fue analizar los riesgos existentes en la OTI usando la metodología MAAGTICSI, que fue acorde al propósito; por lo cual, se logró tener un conocimiento acerca de los riesgos existentes en la OTI y poder elaborar de esta manera las políticas de seguridad de la información. Para salvaguardar la información que es administrada por las tres sub áreas, gobierno electrónico, desarrollo de software, redes y telecomunicaciones, el cual tiene como objetivo individual de estas políticas, dar fortaleza a los tres principios de seguridad de la información: confidencialidad, integridad y disponibilidad, llegando a presentar la propuesta de políticas de seguridad de la información acorde a los objetivos de la OTI-UNA PUNO.

Palabras claves: Activo de información, análisis, gestión, seguridad de la información, riesgo.

ABSTRACT

Risk analysis is a tool that adapts to all types of organizations, with an emphasis on information security, this analysis being internally and externally; To this end, different methodologies of greater flexibility and adaptability have been developed, giving support in proposing information security policies. This research was conducted in the Office of Information Technology, of the National University of Altiplano - Puno, which does not have information security policies that can guarantee the information stored in different media, physical or virtual. Being necessary the policies for the beginning of an information security management system, according to NTP 27001: 2014. The objective was to analyze the risks existing in the OTI using the MAAGTICSI methodology, which was consistent with the purpose; Therefore, it was possible to have knowledge about the risks existing in the OTI and to be able to elaborate in this way the information security policies. To safeguard the information that is managed by the three sub-areas, electronic government, software development, networks and telecommunications, which has as an individual objective of these policies, to strengthen the three principles of information security: confidentiality, integrity and availability, coming to present the proposal of information security policies according to the objectives of the OTI-UNA PUNO.

Keywords: Analysis, information assets, information security, management, risk.

INTRODUCCION

En la actualidad la información es considerada un activo primordial, que es la base para tomar decisiones que permitan el fortalecimiento y la mejora de la institución, siendo necesario protegerla ante cualquier evento que pueda causar la alteración, manipulación, y/o modificación, no autorizada. Dada esta situación actual, la Secretaria de Gobierno Digital de la Presidencia del Consejo de Ministros – PCM, propone la adecuación de la NTP-ISO / IEC 27001: 2014, para salvaguardar la información y un uso adecuado de los activos en general.

El presente trabajo está orientado en el análisis de riesgos y proponer políticas de seguridad de la información para La Oficina de Tecnologías de Información de la Universidad Nacional del Altiplano Puno (organismo autónomo, obligado a la adecuación de la norma).

Capítulo I, en este capítulo se desarrolla el marco teórico, la información necesaria para poder dar a la estructura de políticas de seguridad de la información, según ISO 27001. Donde el principal objetivo es mantener los tres principios de seguridad de la información. Confidencialidad, Integridad, Disponibilidad.

Capítulo II, se ha considerado la problemática de investigación, permitiéndonos verificar los problemas que atraviesa la universidad en relación a la seguridad de la información, constatando que no tiene políticas de seguridad de la información por lo cual no ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI).

Capítulo III, se detalla los materiales y métodos utilizados para en análisis de riegos y propuesta de las políticas de seguridad de la información, el lugar de estudio y el método de investigación.

Capítulo IV, se presenta los resultados obtenidos luego de aplicar un análisis de riesgo y la propuesta de las políticas de seguridad de la información de la Oficina de Tecnologías de Información.

Las conclusiones y las recomendaciones, que se llegaron.

Finalmente, la bibliografía y anexos.

CAPÍTULO I

REVISIÓN DE LA LITERATURA

1.1. Marco teórico

1.1.1. Seguridad

La seguridad es un mecanismo por el cual se pretender proteger un activo, es considerado de suma importancia para la organización. Ya no siendo de una forma exclusiva solo para el gobierno u organismos militares o diplomáticas, a tener una gran variedad de aplicaciones de seguridad, en diferentes organizaciones, sean pequeñas, medianas o grandes. (Areitio, 2008). Estrategias y medidas se buscan la reducción del riesgo, así como sus efectos dañinos a cada individuo y la sociedad, incluyendo el temor de un delito informático, mediante la intervención para influir en sus múltiples causas. (Solórzano & Contreras, 2019)

La seguridad siempre ha buscado gestionar los riesgos, esto quiere decir que siempre busca formas o mecanismos que pretenden evitar o prevenirlo y que se pueda realizar acciones necesarias para evitar situaciones adversas de la mejor forma. (Romero et al., 2018) Definiéndose que la seguridad podría ser catalogada como la ausencia de riesgo, involucrando cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son:

- Prevención del riesgo.
- Transferir el riesgo.
- Mitigar el riesgo.
- Aceptar el riesgo.

1.1.2. Información

Como activo esencial de toda organización. Existiendo de diferentes formas. Siendo impresa, escrita en papel, o de una manera digital, transmitida por correo o almacenada en bits en servidores especializados, mostrada en películas o hablada en una conversación. (Definicion.pe, 2018)

En las universidades, la información a diferencia de los equipos informáticos (los cuales se deterioran con el pasar de los años), esta va teniendo un valor primordial para las personas su información (notas, exámenes, proyectos, datos sobre información personal, datos sobre su salud). Pudiendo ser en favor o en contra, al pasar los años si es accedida de manera ilícita a esta información. Por lo cual debe existir una calidad de la información, que no sea accedida sin autorización, ni modificada, ni borrada, y que exista un alto grado de confiabilidad, ya que la información con el pasar de los años a perdido este principio básico de seguridad. (Melchor, Lavín, & Pedraza, 2012)

1.1.3. Seguridad De La Información

Según Areitio (2008) la seguridad de la información, es darle mecanismos adecuados para salvaguardar la información, a diferencia de la seguridad informática que solo se basa en los equipos tecnológicos, esta abarca más, los activos primordiales que es la información los cuales no se desfasan a medida que pase los años como son los equipos informáticos, sino que incrementa el valor de la información. La seguridad es primordial para que la información no sea interceptada por nadie, ya que esta información en manos de un ente ajeno, puede dañar física y moralmente a una institución por lo cual siempre se debe dar prioridad a la seguridad.(Casla & Peréz, 2013) con el pasar esta continúa evolucionando, ya que desde la antigüedad la información siempre ha sido de vital importancia, y por ende a esta, se le debe dar una adecuada seguridad, permitiendo el cumplimiento de todos los objetivos de la organización. La seguridad informática cumple un papel muy importante para garantizar la disponibilidad, privacidad e integridad de la información, una de las técnicas que ayuda en ésta tarea es la criptografía, cuyo fundamento es transformar un mensaje de modo que sea inentendible salvo para los que posean la clave para descifrarlo.(Solís, Pinto, & Solís, 2017)

1.1.3.1. Principios Básicos De La Seguridad

El avance tecnológico siempre ha originado nuevos hábitos sociales y de consumo masivo que han conformado un contexto socioeconómico diametralmente diferente al de años anteriores, al que se deben adaptar las relaciones laborales (García, 2018). Los principios básicos de la seguridad son los siguiente:

a. Confidencialidad

Es uno de los primeros requisitos primordiales que intenta que la información privada o extremo secreta no sea revelada a individuos no autorizados o dicho de otra manera, personas que tengan acceso autorizado con controles o medidas de seguridad para salvaguardar la información. La protección de confidencialidad es aplicada a datos compartidos, almacenados, durante el procesamiento del mismo. Para todas las organizaciones la confidencialidad es de extrema importancia. (Areitio, 2008)

Así de esta manera evitando el plagio, robo, o manipulación a información confidencial, que pueda poner en riesgo a una organización.

b. Disponibilidad

La disponibilidad frecuentemente es uno de los objetivos principales de la seguridad. Y siempre teniendo el uso autorizado a la información. Siendo un requisito necesario para que se garantice que un sistema trabaje de manera adecuada y puntualmente, con prontitud y que no se deniegue el servicio a ningún usuario autorizado. La disponibilidad protege a todo sistema contra determinados problemas como los intentos delibrados o actuación de denegación de servicio a los datos y de los intentos de utilizar el sistema o los datos para propósito no autorizados. (Areitio, 2008)

c. Integridad

La integridad, normalmente, es el objetivo de seguridad más importante después de la disponibilidad. (Areitio, 2008)

Encargada de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la perdida de consistencia. Presentando dos facetas:

- Integridad de datos. Es la propiedad de que los datos no hayan sido alterados de forma no autorizada, mientras se almacenan, procesan o transmiten.
- Integridad del sistema. Es la cualidad que posee un sistema cuando realiza la función deseada, de manera no deteriorada y libre de manipulación no autorizada.

"La norma técnica peruana NTP-ISO/IEC 17799 ofrece todas las recomendaciones necesarias para poder gestionar un Sistema de Seguridad de la Información (SSI), al igual que la norma internacional ISO 27001, ofreciendo los requisitos necesarios para que los responsables del área en concreto puedan iniciar, implantar, mantener y mejorar la seguridad en las organizaciones."

1.1.3.2. Análisis de seguridad

Es el cual realiza una persona capacitada e independiente, totalmente ajeno, que no conoce el personal y desconoce el funcionamiento correcto de todos los procesos que se dan en diferentes áreas. Utilizando técnicas, métodos y procedimientos especializados. (Muñoz, 2002)

Cuando se realiza una revisión independiente de las actividades que pueden ser vistas desde el exterior, donde no conoce al personal, y al momento de dar un criterio los dará sin involucrar ningún prejuicio. Proporcionando procesos para un adecuado análisis de seguridad de la información que son de suma importancia para la adecuada toma de decisiones para un futura, optimo en la seguridad. (Diéguez & Cares, 2019)

Realizando:

- Revisiones
- Evaluar el cumplimiento de las políticas.

- Dictaminar de manera profesional e independiente.

1.1.3.3. Marco esquemático de sistemas computacionales

Para poder mitigar cualquier riesgo en la seguridad de la información siempre debe evaluar todo el entorno donde se administra, componentes en los cuales interactuaran tanto software, hardware, y personal, que velan por la información, que sea almacenada sin ningún riesgo. (Aguilar et al., 2018)

Evaluación a:

Hardware – tarjetas madre, procesadores, dispositivos periféricos, etc.

Software – sistema operativo, aplicaciones, programas, utilerías, software de telecomunicaciones

Gestión – actividad administrativa del área de sistemas, operación del sistema, planeación y control.

Información – administración, seguridad y control, salvaguardar, cumplimiento de las políticas, back up.

Diseño de los sistemas – Metodologías, estándares, documentación de sistemas.

Base de datos – administración de base de datos, diseño, metodología, seguridad.

Seguridad – física, lógica, instalaciones eléctricas, de datos y telecomunicaciones.

Redes de cómputo – plataformas y configuración de redes, protocolos de comunicación, administración de seguridad y base de datos.

1.1.3.4. Evaluación de riesgos, Vulnerabilidades y amenazas

Las dos metodologías de evaluación de sistemas por antonomasia son las de ANÁLISIS DE RIESGOS y propuesta de políticas, con dos enfoques distintos. El análisis informático sólo identifica el nivel de “exposición" por la falta de

controles, mientras el análisis de riesgos facilita la "evaluación" de k» riesgos y recomienda acciones en base al costo-beneficio de las mismas. (Piattini & Navarro, 2001). Entre las dificultades de recopilar datos, destacamos el veracidad de la información proporcionada por instituciones y empresas sobre ataques e intrusiones del sistema.(Cortez & Kubota, 2013).

Las metodologías de análisis de riesgos se utilizan desde los años setenta, en la industria del seguro basándose en grandes volúmenes de datos estadísticos agrupados en tablas actuarias. Se emplearon en la informática en los ochenta, y adolecen del problema de que los registros estadísticos de incidentes son escasos y por tanto, el rigor científico de los cálculos probabilísticos es pobre. Aunque existen bases de incidentes en varios países, estos dalos no son muy fiables por varios motivos: la tendencia a la ocultación de los afectados, la localización geográfica, las distintas mentalidades, la informática cambiante, el hecho de que los riesgos se presentan en un periodo de tiempo solamente (ventana de criticidad). etc. Siempre basándonos para la futura implementación de un SGSI, el cual dará el cumplimiento a la seguridad establecida por ISO 27001. (Martelo, Maderay, & Betín, 2015), pudiendo crear diferentes tipos de modalidades para dar un buen soporte a la seguridad, como también se puede crear software adecuado para la planeación, con la adecuada asignación de personal que pueda mitigar cada riesgo, debidamente capacitado para afrontar existentes problemas y futuras vulnerabilidades que pueden estar presentes estar presentes como amenazas para luego convertirse en riesgos, riesgos que generaran gran perdida a la universidad y o a la institución donde se puede evitar con una buena planeación de la alta gerencia, y hoy en día el gobierno digital, que se dispuso para la planeación de la creación de plan de gobierno digital del Perú.

Las dimensiones de inseguridad, individualmente no soy muy perjudiciales, pero cuando van juntos, puede ser gravemente afectado la seguridad de la información, estos son:

a. Riesgos

Los riesgos de una organización son aquellos que ponen en peligro la información y por ello, comprometiendo cualquier desarrollo de la organización. Sobre los riesgos habrá que calcular el impacto que dichos riesgos causen incidentes en la seguridad. (Gunea, 2018)

Tabla 1.

Riesgos de la Universidad

RIESGO	IMPACTO
Robo de información (proyectos, invenciones, y o propuestas)	Perdida de prestigio de la Universidad.
Intrusión y acceso a información sensible.	Exponer los datos personales de los estudiantes, docentes y personal administrativo de la UNA - PUNO
No realizar Backus	Al encontrarse con fallas en los sistemas, se ve gravemente afectados a la perdida de información y no poder recuperarlas.
Expuestos a ataques dirigidos o no dirigidos.	Perdida monetaria, ataques dirigidos para que dañen la infraestructura del sistema.
Expuestos a ataques cibernéticos de denegación de servicio	Perdida de información, cuando el alumno, docente o administrativo, pretende modificar alguna información cuando está conectado al sistema de la universidad.

Fuente: OTI – UNA PUNO – Riesgo Impacto.

Todas las metodologías existentes desarrolladas y utilizadas en el análisis y el control informático se pueden agrupar en dos grandes familias. Para que en un futuro puedan ser minimizadas que conlleven a afecciones importantes para la institución, (F. Muñoz, 2013). Éstas son:

Cuantitativas: Basadas en un modelo matemático numérico que ayuda a la realización del trabajo.

Cualitativas: Basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada.

Metodologías más comunes, se dan usando cuestionarios, identificar los riesgos, calcular el impacto, identificas las contramedidas y el coste, simulaciones, creaciones de los informes.

El riesgo es la probabilidad de que algo negativo suceda dañando los recursos tangibles o intangibles y por tanto impidiendo desarrollar la labor profesional. (Romero Castro et al., 2018)

Figura 1. Activos tangibles, Activos intangibles.

Fuente: 12manage (2019)

b. Vulnerabilidades

La vulnerabilidad es una debilidad, puede ser en hardware o software, que pone en peligro la información que este contenga, comprometiendo el buen desarrollo de la actividad profesional, (Gunea, 2018).

a. Tipos de vulnerabilidades

Existe tipos de vulnerabilidades por cada acción que se pueda efectuar.

- Error en la gestión de recursos: cuando lo recursos no están asignados debidamente, pueden consumir un exceso de recursos afectando a la disponibilidad de la información.
- Error de configuración: la configuración de software o servidores web, pueden provocar la inutilización de programación para la conexión al servidor y páginas web a través de ataques de denegación de servicio.
- Factor humano: Cuando el personal que labora o se conecta al servidor a través de un usuario o contraseña, no ha sido capacitado para la adecuada manipulación del sistema, puede perjudicar gravemente por el desconocimiento.
- Validación de usuario: pueden realizar ataques a través de otros usuarios, suplantándolos.
- Salto de directorio: Fallo en la depuración de programas, la validación de caracteres especiales que permite el acceso a directorios o subdirectorios no deseados.
- Permisos, privilegios y/o control de acceso: fallos de protección y permisos asignado que permiten el control de acceso.

Por ejemplo, si se usa el gestor de contenidos WordPress para desarrollar una página web, se puede buscar vulnerabilidades del CMS, de algunas de sus plantillas o de los plugins que se utilizarán para dar funcionalidad a la página web en https:// wpvulndb.com/, la Figura 2 muestra la página principal de este sitio de búsqueda de vulnerabilidades.

Figura 2. Vulnerabilidades del sistema

Fuente: Dewhurst (2019)

c. Amenazas

Es todo elemento que es aprovechado mediante una vulnerabilidad encontrada en los sistemas que utiliza una organización cansando daños, ocasionando incidentes en la seguridad del sistema y así comprometer directamente la seguridad de la información.

Cuando hablamos de seguridad, en la cabeza de la mayoría de las personas está la posibilidad de infectarse con un virus en el ámbito de su empresa. Sin embargo, este es sólo uno de los riesgos a los que puede verse expuesto.

De hecho, los mayores problemas en materia de seguridad están asociados con estos cuatro tipos de amenazas:

- Ataques de denegación de servicios: Degradar la calidad de servicio de un sistema, llegando a dejarlo no operativo o en un punto extremo, inaccesible.
- Acceso no autorizado a las bases de datos: es un ataque dirigido o no dirigido muy común.
- Fuga de información sensible: con el consiguiente daño a su imagen y reputación, la información que es almacenada en medios electrónicos.
- Robo de usuarios o contraseñas.

1.1.4. Análisis de riesgo de seguridad de la información

En principio debemos entender primero en qué consiste el análisis de riesgo, es importante comprender el valor estratégico de la información. (Herrera, 2003)

Toda actividad cotidiana requiere de información para su realización. Desde sus inicios la humanidad no se ha concebido sin información. Esta produce y maneja para propiciar el desarrollo de la actividad económica, política y social del mundo. Así, la generación y el intercambio de información es una necesidad primordial del quehacer humano.

Que es conocido que vivimos en la era de la información, muchas organizaciones gestionan informaciones a gran volumen, para ellas es un activo valioso como tal valor la información debe ser custodiada con el máximo cuidado porque, sin lugar a duda, será buscada por otros.

En otras palabras, al ser las diferentes informaciones elementos valiosos que son apetecidos por terceros, decidimos que la información está sometida a amenazas. (Gutiérrez 2003).

En base a los conceptos resaltados sobre la importancia de la información cabe destacar el concepto de seguridad de la información que según la (ISO/IEC 17799:2005):

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer,

implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

Gutiérrez (2003) Todo objetivo de seguridad siempre es de proteger los recursos (personal, información, material, instalaciones) y las actividades. Según sea el recurso a proteger, se utilizan distintos términos de seguridad del personal, seguridad de la información, seguridad del material, seguridad de las instalaciones, o seguridad de operaciones. Cuando la información es el mayor recurso que se debe proteger, hay que tener en cuenta que la información puede existir en la mente humana, en un documento, o en forma electrónica en un sistema de información y comunicaciones y, por tanto, hay que abordad el problema de la seguridad de la información bajo estos tres aspectos.

1.1.4.1.Análisis de riesgo

Especifica que el primer paso en la seguridad de la información es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo. (Markus 2008)

1.1.4.1.1. Probabilidad de amenaza

Las consideraciones principales de la probabilidad de amenaza son:

a. Interés o la atracción por parte de individuos externos
b. Nivel de vulnerabilidad
c. Frecuencia en que ocurre los incidentes

Se habla de un Ataque, cuando una amenaza se convirtió en realidad, es decir cuando un evento se realizó. Pero el ataque no dice nada sobre el éxito del evento y sí o no, los datos e informaciones fueron perjudicado respecto a su confidencialidad, integridad, disponibilidad y autenticidad. Ya que todos los problemas siempre están presentes, aun cuando se trate de mitigar los mismos, ya que el avance de la seguridad, también viene de la mano la inseguridad de la información, por lo cual es siempre buscar la forma de mitigar problemas cualquier amenaza. (Aguilar et al., 2018)

Para estimar la Probabilidad de Amenaza nos podemos hacer algunas preguntas:

¿Cuál es el interés o la atracción por parte de individuos externos, de atacarnos? Algunas razones pueden ser que manejamos información que contiene novedades o inventos, información comprometedora etc., tal vez tenemos competidores en el trabajo, negocio o simplemente por el imagen o posición pública que tenemos.

¿Cuáles son nuestras vulnerabilidades? Es importante considerar todos los grupos de vulnerabilidades. También se recomienda incluir los expertos, especialistas de las diferentes áreas de trabajo para obtener una imagen más completa y más detallada sobre la situación interna y el entorno.

¿Cuántas veces ya han tratado de atacarnos? Ataques pasados nos sirven para identificar una amenaza y si su ocurrencia es frecuente, más grande es la probabilidad que pasará otra vez. En el caso de que ya tengamos implementadas medidas de protección es importante llevar un registro, que muestra los casos cuando la medida se aplicó exitosamente y cuando no. Porque de tal manera, sabemos en primer lugar si todavía existe la amenaza y segundo, cuál es su riesgo actual.

Considerando todos los puntos anteriores, nos permite clasificar la Probabilidad de Amenaza. Sin embargo, antes tenemos que definir el significado de cada condición de la probabilidad (Baja, Mediana, Alta). Se recomienda que cada institución defina sus propias condiciones. (Ibíd.)

1.1.4.1.2. Tipos de amenaza

La amenaza se puede definir todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. (Macen, 2014) presenta a continuación los tres tipos de amenazas con sus respectivas divisiones:

a. Actos originados por la criminalidad común y motivación política
   - Allanamiento (ilegal, legal)

- □ Persecución (civil, fiscal, penal)
- □ Orden de secuestro / Detención
- □ Sabotaje (ataque físico y electrónico)
- □ Daños por vandalismo
- □ Extorsión
- □ Fraude / Estafa
- □ Robo / Hurto (físico)
- □ Robo / Hurto de información electrónica
- □ Intrusión a Red interna
- □ Infiltración
- □ Virus / Ejecución no autorizado de programas
- □ Violación a derechos de autor

b. Suceso de origen físico

- □ Incendio
- □ Inundación / deslave
- □ Sismo
- □ Daños debidos al polvo
- □ Falta de ventilación
- □ Electromagnetismo
- □ Sobrecarga eléctrica
- □ Falla de corriente (apagones)
- □ Falla de sistema /Daño disco duro
- □ Valoración

c. Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

- □ Falta de inducción, capacitación y sensibilización sobre riesgos
- □ Mal manejo de sistemas y herramientas
- □ Utilización de programas no autorizados / software 'pirateado'
- □ Falta de pruebas de software nuevo con datos productivos (Ej.
- □ Instalación de nuevos programas sin respaldar los datos anteriormente)
- □ Pérdida de datos
- □ Infección de sistemas a través de unidades portables sin escaneo
- □ Manejo inadecuado de datos críticos (Ej. no cifrar datos, etc.)

- Unidades portables con información sin cifrado
- Transmisión no cifrada de datos críticos
- Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
- Compartir contraseñas o permisos a terceros no autorizados
- Transmisión de contraseñas por teléfono
- Exposición o extravío de equipo, unidades de almacenamiento, etc.
- Sobrepasar autoridades
- Falta de definición de perfil, privilegios y restricciones del personal
- Falta de mantenimiento físico (proceso, repuestos e insumos)
- Falta de actualización de software (proceso y recursos)
- Fallas en permisos de usuarios (acceso a archivos)
- Acceso electrónico no autorizado a sistemas externos
- Acceso electrónico no autorizado a sistemas internos
- Red cableada expuesta para el acceso no autorizado
- Red inalámbrica expuesta al acceso no autorizado
- Dependencia a servicio técnico externo
- Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
- Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
- Ausencia de documentación (Markus, 2008)

1.1.4.2. Magnitud de Daños

Se habla de un Impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones. Como ser:

- Perdida de información
- Acceso a la información por terceros
- Cambio de legitimación de la fuente información

Estimar la Magnitud de Daño generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que aparte del daño económico, también se considera otros valores como daños

materiales, imagen, emocionales, entre otros. Expresarlo de manera cuantitativa, es decir calcular todos los componentes en un solo daño económico, resulta en un ejercicio aún más complejo y extenso.

Aunque conozcamos bien el impacto de un ataque exitoso, sus consecuencias pueden ser múltiples, a veces son imprevisibles y dependen mucho del contexto donde manejamos la información, sea en una ONG (derechos humanos, centro de información etc.), en una empresa privada (banco, clínica, producción etc.), en una institución Estatal o en el ámbito privado. Otro factor decisivo, respecto a las consecuencias, es también el entorno donde nos ubicamos, es decir cuáles son las Leyes y prácticas comunes, culturales que se aplica para sancionar el incumplimiento de las normas.

Un punto muy esencial en el análisis de las consecuencias es la diferenciación entre los dos propósitos de protección de la Seguridad Informática, la Seguridad de la Información y la Protección de datos, porque nos permite determinar, quien va a sufrir el daño de un impacto, nosotros, otros o ambos. En todo caso, todos nuestros comportamientos y decisiones deben ser dirigidos por una conciencia responsable, de no causar daño a otros, aunque su realidad no tenga consecuencias negativas. (Gobierno, 2015)

Otras preguntas que podemos hacernos para identificar posibles consecuencias negativas causadas por un impacto son:

- ¿Existen condiciones de incumplimiento de confidencialidad (interna y externa)? Esto normalmente es el caso cuando personas non-autorizados tienen acceso a información y conocimiento ajeno que pondrá en peligro nuestra misión.
- ¿Existen condiciones de incumplimiento de obligación jurídicas, contratos y convenios? No cumplir con las normas legales fácilmente puede culminar en sanciones penales o económicas, que perjudican nuestra misión, existencia laboral y personal.
- ¿Cuál es el costo de recuperación? No solo hay que considerar los recursos económicos, tiempo, materiales, sino también el posible daño de la imagen pública y emocional.

Considerando todos los aspectos mencionados, nos permite clasificar la Magnitud del Daño. Sin embargo, otra vez tenemos que definir primero el

significado de cada nivel de daño (Baja, Mediana, Alta). Las definiciones mostradas en la imagen anterior solo son un ejemplo aproximado, pero no necesariamente refleja la realidad y la opinión común y por tanto se recomienda que cada institución defina sus propios niveles. Esos niveles pueden ser reflejados en las políticas de seguridad de la información (Ibíd.)

Clasificación y valoración de magnitud de daños son:

- Datos e información
- Sistema e infraestructura
- Personal

a. Datos e información

- Documentos institucionales (Proyectos, Planes,
- Evaluaciones, Informes, etc.)
- Finanzas
- Servicios bancarios
- RR. HH
- Directorio de Contactos
- Productos institucionales (Investigaciones,
- Folletos, Fotos, etc.)
- Correo electrónico
- Bases de datos internos
- Bases de datos externos
- Bases de datos colaborativos
- Página Web interna (Intranet)
- Página Web externa
- Respaldos
- Infraestructura (Planos, Documentación, etc.)
- Informática (Planos, Documentación, etc.)
- Base de datos de Contraseñas
- Datos e información no institucionales
- Navegación en Internet
- Chat interno
- Chat externo

- Llamadas telefónicas internas
- Llamadas telefónicas externas

Los tres campos de "Clasificación":

- Confidencial, Privado, Sensitivo
- Obligación por ley /Contrato /Convenio
- Costo de recuperación (tiempo, económico, material, imagen, emocional) (Ibíd.)

b. Sistemas E infraestructura

- Equipos de la red cableada (router, switch, etc.)
- Equipos de la red inalámbrica (router, punto de acceso, etc.)
- Cortafuego
- Servidores
- Computadoras
- Portátiles
- Programas de administración (contabilidad, manejo de personal, etc.)
- Programas de manejo de proyectos
- Programas de producción de datos
- Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)
- Impresoras
- Memorias portátiles
- PBX (Sistema de telefonía convencional)
- Celulares
- Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Depósitos, etc.)
- Vehículos
- Los tres campos de "Clasificación":
- Acceso exclusivo
- Acceso ilimitado
- Costo de recuperación (tiempo, económico, material, imagen, emocional)

c. Personal

- Junta Directiva
- Dirección / Coordinación
- Administración
- Personal técnico
- Recepción
- Piloto / conductor
- Informática / Soporte técnico interno
- Soporte técnico externo
- Servicio de limpieza de planta
- Servicio de limpieza externo
- Servicio de mensajería propio
- Servicio de mensajería externo
- Los tres campos de "Clasificación":
- Imagen pública de alto perfil, indispensable para funcionamiento institucional
- Perfil medio, experto en su área
- Perfil bajo, no indispensable para funcionamiento institucional. (Ibíd.)

d. Información

Ortega, (2014), La era de la información, donde la sociedad vive a través de esta información, se ha convertido en un bien mercantil, que tiene un valor, que puede ser comprada o vendida. Donde el conocimiento ya no es un secreto de estado, puede ser vulnerado fácilmente, si por medio ha sido valorado monetariamente, y vulnera cualquier medida de seguridad para acceder a esa información.

Formas de información que encontramos son: (Aguirre, 2014)

- Impresa o escrita en papel.
- Almacenada electrónicamente.
- Transmitida vía correo o e-mail.
- Mostrada en videos.
- Hablada en conversaciones [NTP ISO/IEC 17799].

1.1.5. Políticas de seguridad de la información

Las políticas de seguridad de la información son un conjunto de documentos de alto nivel (nivel estratégico) donde se definen las directrices a seguir por una organización en un aspecto en concreto para garantizar la confidencialidad, integridad y disponibilidad de la información. Siendo necesario para cualquier toma de decisiones adecuadas y una buena planeación de la seguridad de la información. (Anguiano & Trejo, 2013)

Es decir, estos documentos deben ser elaborados, revisados y mantenidos por el consejo directivo (preferiblemente) o la máxima autoridad de la organización, depende de cómo funcione la misma; la cuestión es que las políticas de seguridad de la información son una decisión y gestión estratégica, no táctica y mucho menos operativa. La intención de ellas es generar y/o confirmar el compromiso de la alta gerencia (de allí la importancia de la participación del consejo directivo) en materia de seguridad de la información. (Solís, 2014)

Considera que las políticas son directrices u orientaciones sobre una determinada materia en un entorno concreto. Se trata de fijar objetivos sin decir cómo conseguirlos y viene a representar el marco o filosofía de actuación de la entidad. No deben ser largas ni farragosas, una o dos páginas por política, a lo sumo. Tienen que ser fáciles de entender por todo el personal de la empresa. (Navarro, 2003)

1.1.5.1.Elaboración de la política

En el artículo publicado por Academia Latinoamericana de Seguridad informática (2013), menciona que la política es elaborada considerando el entorno en que se está trabajando como la tecnología de la seguridad de la información, para que los criterios establecidos estén de acuerdo con las prácticas internas más recomendadas de la organización, con las prácticas de seguridad actualmente adoptadas, para buscar una conformidad mayor con criterios actualizados y reconocidos en todo el mundo.

La política es elaborada tomando como base la cultura de la organización y el conocimiento especializado de seguridad de los profesionales involucrados con su aplicación y comprometimiento. Es importante considerar que para la

elaboración de una política de seguridad institucional se debe Integrar el Comité de Seguridad responsable de definir la política conformado por un equipo multidisciplinario que represente gran parte de los aspectos culturales y técnicos de la organización y que se reúnan periódicamente dentro de un cronograma establecido por el Comité de Seguridad. Este comité es formado por un grupo definido de personas responsables por actividades referentes a la creación y aprobación de nuevas normas de seguridad en la organización. En las reuniones se definen los criterios de seguridad adoptados en cada área y el esfuerzo común necesario para que la seguridad alcance un nivel más elevado.

Se debe tener en mente que los equipos involucrados necesitan tiempo libre para analizar y escribir todas las normas discutidas durante las reuniones. En síntesis, el comité:

Evalúa las normas y pautas de seguridad, así como los procedimientos de notificación de incidentes de seguridad.

Informa sobre los riesgos de seguridad en los activos TIC.

Vela por que la seguridad de la información sea parte del proceso de planificación de las Tics de la organización.

Tabla 2

Referencias de políticas implementadas y propuesta de políticas de seguridad de la información

INSTITUCIONES				Propuesta de políticas de seguridad de la información para la Oficina de Tecnología de Información de la Universidad Nacional del Altiplano - Puno
institución 1	institución 2	institución 3	institución 4	
Política de Seguridad de Información Política de Activos TI (Tecnologías de Información) Política de Control de Acceso Política de Control de Contraseñas Política de Correo Electrónico Política de Internet Política de Antivirus Política de Acceso Remoto Política de Subcontratación	Política de seguridad de la información Organización de la seguridad de la información Gestiones de activos de información Seguridad de los recursos humanos Seguridad física y ambiental Gestión de comunicaciones y las operaciones Control de acceso Adquisición, desarrollo y mantenimiento de sistemas de información Gestión de incidentes de seguridad de la información Gestión de la continuidad de negocio y operativa Cumplimiento de las normas legales y técnicas	Respóndales Propietario de la información Custodio de la información Propiedad de la información Requisitos de documentación Disposiciones específicas Control de documentos Control de registros Control de acceso a los sistemas de información Auditorías internas del sistema de gestión de seguridad de la información Seguridad física y ambiental Seguridad de personal Contratos con terceros Administración de activos de información Seguridad de las comunicaciones Desarrollo, adquisición y mantenimiento de sistemas de información. Continuidad de servicios de	POLÍTICAS política de Seguridad Seguridad Organizacional Oficial de Seguridad de la Información Comité de Seguridad Grupo de Seguridad Interdisciplinario Coordinación de la seguridad Seguridad con Terceros Acuerdos de Seguridad Responsabilidad por la información Segregación de Funciones Administración de Activos de Información Inventario de Activos Clasificación de la información Seguridad del Recurso Humano Responsabilidades de los usuarios Entrenamiento Seguridad Física y Ambiental Controles de acceso perimetral Controles ambientales	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN INTRODUCCION ALCANCE BASE LEGAL GLOSARIO DE TERMINOS ORGANIZACIÓN DE LAS POLITICAS DE SEGURIDAD INFORMÁTICA POLÍTICAS GENERALES OBJETIVOS ALCANCE POLÍTICAS SOBRE SEGURIDAD DE LA INFORMACIÓN POLÍTICAS Y ORGANIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN POLÍTICAS SOBRE SEGURIDAD FÍSICA Y AMBIENTAL POLÍTICAS SOBRE SEGURIDAD LÓGICA POLÍTICAS DE GESTIÓN DE ACTIVOS POLÍTICA DE RESPALDO (BACK-UP) DE INFORMACIÓN POLÍTICAS DE SEGURIDAD EN LAS TELECOMUNICACIONES POLÍTICAS DE GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE INFORMACIÓN POLÍTICA DE ADMINISTRACIÓN DE RECURSOS POLÍTICAS DE

Fuente: Análisis y comparación PSI

1.1.5.2.Directrices estratégicas

Conjunto de reglas generales donde expresan de manera estratégica los valores de seguridad de la universidad. Es elaborada por el líder asignado por la alta gerencia de la organización, y tiene como base la visión y misión abarcando toda filosofía que salvaguarda la información. (Macen,2014)

Toda directriz corresponde a cada preocupación de la organización sobre la seguridad de la información, estableciendo sus propios objetivos, medios y responsabilidades.

Las directrices estratégicas, en el contexto de la seguridad, corresponden a todos los valores que deben ser seguidos, para que el principal patrimonio de la empresa, que es la información, tenga el nivel de seguridad exigido.

Como la información no está presente en un único entorno (microinformática, por ejemplo) o medio convencional (fax, papel, comunicación de voz, etc.), debe permitir que se aplique a cualquier ambiente existente y no contener términos técnicos de informática. Se compone de un texto, no técnico, con las reglas generales que guían a la elaboración de las normas de seguridad.

1.1.5.3.Fases para el desarrollo de la política

La realización de una política comprende básicamente cuatro fases primordiales:

a. Desarrollo

Previamente a esta fase, se tiene que verificar las directrices que sigue la seguridad de la información, para luego crear, revisar, y aprobar las políticas de seguridad, con la supervisión de la alta gerencia. La creación está conformada por la planificación, investigación, documentación y coordinación de la política. La revisión debe llevarla a cabo la persona designada para el análisis de riesgo y posterior desarrollo, previo a la aprobación final de la política. La aprobación de la política es obtener el apoyo de la del jefe inmediato superior, para el desarrollo de la misma sin perjuicio de otras políticas ya implementadas. (Pacheco, 2015)

b. Implementación

En esta fase, se llevan a cabo la comunicación, el cumplimiento y las excepciones de la política. La comunicación es la difusión de la política a los involucrados directamente en la seguridad de la información, en diferentes sub áreas. (Pacheco, 2015) Posteriormente para su cumplimiento y la ejecución de política, un trabajo en conjunto con las partes involucradas y así asegurar que la misma sea entendida por los involucrados.

Las excepciones se refieren a las situaciones donde la implementación de la política no es posible por diversos factores que deben ser contemplados.

c. Mantenimiento

Comprende las etapas de concientización, monitorización, garantía de cumplimiento y mantenimiento de la política (lo recomendable cada año). Ya que la tecnología avanza y las amenas y riesgos son cada vez mayores, y se tiene que actualizar cada cambio en la información como en la informática. Pacheco (2015) La concientización comprende los esfuerzos para garantizar que las personas están conscientes de la política y así de esta manera se busca el cumplimiento adecuado. La monitorización constante, es seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política que ayudan a mejorar la seguridad de la información.

Se exige una garantía de cumplimiento que refiere a las respuestas de la administración a actos u omisiones que resulten en contravenciones de la política con el fin de prevenir que sigan ocurriendo y a la vez sea sancionado con el reglamento interno de la institución. El mantenimiento garantiza el proceso de vigencia e integridad de la política.

d. Eliminación

Esta fase se refiere al retiro y significa que cuando la política ha cumplido con su finalidad y ya no es necesaria (por cambios de tecnología o nuevas políticas generales de la institución), entonces debe ser retirada, archivarla para futuras

referencias y documentar la información sobre la decisión del retiro de la misma. (Pacheco, 2015)

1.1.5.4.Documento de la política

Al iniciar el proceso de elaboración sobre una política de seguridad, es necesario recopilar cierta información con los usuarios de activos y realizar estudios de los documentos existentes. El objetivo de esa tarea es definir qué tipo de adaptación debe ser hecha en el modelo de estandarización existente para atender las características de la empresa (con relación a trazado, identificación, numeración y lenguaje utilizado). Si ya existen esos estándares definidos, los documentos de la política de seguridad deben adaptarse a ellos para garantizar una proximidad entre la práctica gerencial existente y la política sugerida.

1.1.6. ISO 27001:2014 NTP

Indecopi, (2014) La norma ISO 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información.

Esta Norma Técnica Peruana ha sido preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. Por lo cual debe promoverse para su implementación de la sistema de gestión de seguridad de la información, para proteger la información que la institución está orientado a proteger y velar, (Arévalo, Bayona, & Rico, 2015) que es la información de los alumnos, docentes y administrativos, por lo cual tienen derecho a que su información personal, se mantenga en privacidad y de forma segura.

Esta Norma Técnica Peruana también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización.

Requisitos donde principalmente nos dice habla de las políticas de seguridad de la información

La alta dirección debe establecer una política de seguridad de la información que:

- Es apropiada al propósito de la organización;
- Incluye objetivos de seguridad de la información (véase 6.2) o proporciona el marco de referencia para fijar los objetivos de seguridad de la información;
- Incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información; e
- Incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información.

La política de seguridad de la información debe:

- Estar disponible como información documentada;
- Estar comunicada dentro de la organización;
- Estar disponible a las partes interesadas, según sea apropiado.

1.1.7. Propuesta de las políticas de seguridad de la información

Una persona capacitada que conoce todo el funcionamiento de la empresa. Pertenecer a un colegio oficial capacitado. Con supervisión necesariamente de alta gerencia un trabajador interno de la organización, cuando sea una propuesta externa. Que tiene una gran ventaja de ser preciso para poder realizar el análisis, sin embargo, una desventaja que puede incurrir muchas veces en el error. Siendo necesario que toda organización implemente de manera inmediata las políticas, conjuntamente con sus documentos complementarios que darán un mayor soporte de resguardo a la información.(Altamirano & Bayona, 2017)

1.1.7.1.Análisis de riesgos

Cuando usted crea una política de seguridad de red, es importante que comprenda que la razón para crear una política es, en primer lugar, asegurar que los esfuerzos dedicados a la seguridad impliquen un costo razonable. Esto significa que usted debe conocer cuales recursos vale la pena proteger, y cuales son más importantes que otros. También debe identificar la fuente de amenazas de la que usted está protegiendo a los recursos de la red. A pesar de toda la publicidad acerca de los intrusos que irrumpen en una red, muchos estudios indican que, en el caso de la mayoría de las organizaciones, las verdaderas pérdidas causadas por los usuarios internos son mucho mayores. (Alvarez, 2005)

El análisis de riesgo implica determinar lo siguiente:

- ¿Qué necesita proteger?
- ¿De qué necesita protegerlo?
- ¿Cómo protegerlo?

Los riesgos deben clasificarse por nivel de importancia y gravedad de la perdida. Y a la vez por el impacto que estos pueden causar, de una amenaza que puede materializarse, produciendo un impacto y la privacidad de riesgo, (Angarita, Tabares, & Rios, 2015). No debe terminar en una situación en la que gaste más en proteger algo que es de menor valor para usted. En el análisis de riesgo hay que determinar los siguientes dos factores:

- Estimación del riesgo de perder el recurso.
- Estimación de la importancia del recurso.

1.1.7.2. Políticas y su composición

La norma ISO 27001 no dice mucho sobre la política de seguridad, pero sí dice lo siguiente:

La política tiene que adaptarse a la empresa, esto significa que no puede simplemente copiar la política de una gran organización y utilizarlo en una pequeña organización de TI. (Web, 2019),

Es necesario definir un marco para establecer todos los objetivos de seguridad de la información, la política debe definir cómo se proponen los objetivos, la forma en la que se encuentran aprobados y la manera en la que se revisan.

La política tiene que mostrar el compromiso de la alta dirección para cumplir con los requisitos de todas las partes interesadas y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, eso se hace normalmente mediante un tipo de declaración dentro de la política.

La política se debe comunicar dentro de la organización y a todas las partes interesadas, la mejor práctica es definir quién es el responsable de tal

comunicación, y entonces esa persona es responsable de hacerlo de forma continua.

La política debe ser revisada de forma continua por parte del propietario de una política que debe ser definida. Dicha persona será la responsable de mantener la política hasta la fecha. Siendo unos de los recursos esenciales la información, la cual puede ser resguarda cuando se implementa políticas de seguridad, que darán el cumplimiento para la implementación futura de un sistema de gestión de seguridad de la información. (Casla & Peréz, 2013)

1.1.7.3. Seguridad de la información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. (Web Seguridad, 2019), Para que la información sea considerada confiable para la organización ya que sus estrategias de negocio dependerán del almacenamiento, procesamiento y presentación de la misma, (Guzmán, 2015) esta deberá cubrir los tres fundamentos básicos de seguridad para la información que son:

- Confidencialidad: Se define como la capacidad de proporcionar acceso a usuarios autorizados, y negarlo a no autorizados
- Integridad: Se define como la capacidad de garantizar que una información o mensaje no han sido manipulados.
- Disponibilidad: Se define como la capacidad de acceder a información o utilizar un servicio siempre que lo necesitemos.

Figura 3. Triangulo de la Seguridad de la Información

Fuente: Cubas (2018)

1.1.7.4.Sistema de gestión de seguridad de la información

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. (Iso27000, 2010)

El sistema de gestión de la seguridad de la información consiste en garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (Rayme, 2007)

La base de un SGSI reside en, conociendo el contexto de la organización, evaluar los riesgos y fijar los niveles determinados como adecuados por parte de la Dirección de la organización para la aceptación de un nivel de riesgo de modo que se puedan tratar y gestionar los riesgos con eficacia.

El análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para garantizar la protección de estos

activos de información, según sea necesario, contribuye a la exitosa implementación de un SGSI.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos. (Iso27000, 2010)

Figura 4. Análisis de Riesgos

Fuente: Iso27000 (2018)

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:

Figura 5. Pirámide de un SGSI

Fuente: Iso27000 (2018)

1.1.7.5.Seguridad física y ambiental

Controles y medidas de seguridad, alrededor y dentro de la ubicación física de los sistemas informáticos, así como los medios de acceso al mismo, implementados para proteger el HW y medios de almacenamiento de datos. (Leal, 2019)

Medidas:

CPD y centro de respaldo: Lugar donde se ubican los recursos necesarios para el procesamiento de la información. Puede ser una sala de gran tamaño o incluso un edificio, que albergará gran cantidad de equipamiento informático y, en general, electrónico. Prácticamente todas las compañías medianas o grandes tienen algún tipo de CPD. Las más grandes llegan a tener varios interconectados con distintos centros de respaldo.

Ubicación y acondicionamiento físico: Tener en cuenta las condiciones atmosféricas adversa al decidir la ubicación y posterior construcción de los data centers.

Factores ambientales: Incendios, inundaciones, Terremotos, Humedad. Etc.

Aspectos a considerar	Precauciones y/o medidas
Incendios	✓ Ubicación en área no combustible o inflamable ✓ Disponer de un sistema antiincendios
Temperatura y humedad	✓ Sistema de aire acondicionado
Inundaciones	✓ Ubicación estanca de agua
Terremotos	✓ Conocer la actividad sísmica de la zona ✓ Construcciones antisísmicas
Rayos e interferencias electromagnéticas	✓ Salas protegidas mediante jaula de Faraday

Figura 6 condiciones atmosféricas

Fuente: slideplayer (2019)

Control de acceso físico: Uso de credenciales de identificación y acceso para apertura/cierre de puertas, entrada/salida a los distintos sectores de una empresa.

- A una persona se le puede identificar por:
- Algo que posee: llave, tarjeta de identificación, tarjeta inteligente.
- Algo que se sabe: PIN (Personal Identificación Number), password.
- Algo que es (señas de identidad: manos, ojos, huellas digitales, voz) o saber hacer (firma escrita). Biometría.

Los identificadores se almacenan en una base de datos que debe controlar un servicio de vigilancia.

1.1.7.6. Seguridad lógica

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.1.7.7. Gestión de activos

La gestión activos ayuda a que las empresas y organizaciones de planificación de mantenimiento a lograr dar respuesta confiable a las necesidades del negocio. Además, no se enfoca tanto en hacer acciones sobre los activos, sino en generar valor a través de los activos, es decir, se enfoca en el Negocio. (Iso, 27001),

En este sentido la norma ISO 55000, define a la gestión de activos como: "La coordinación de las actividades de una organización para crear valor a través de sus activos", y la definición de activo es: "algo que tiene valor o potencial valor para una organización". Esto sería el QUÉ…

El POR QUÉ está asociado a cómo lograr que la empresa tenga sustentabilidad, y qué se pueda demostrar cómo las acciones llevadas a cabo realmente están generando valor al negocio.

Los objetivos de gestión de activos, derivados como parte del Plan Estratégico de Gestión de Activos, proporcionan el vínculo esencial entre los objetivos de la organización y el plan(es) de gestión de activos que describe cómo estos

objetivos se van a alcanzar. Estos objetivos deben transforman los resultados requeridos (producto o servicio) que deben ser proporcionados por los activos, en actividades típicamente descritas en el plan(es) de gestión de activos.

Los objetivos de gestión de activos deben encajar en cada una de las necesidades de la organización, que pueden incluir abordar subconjuntos de objetivos (por ejemplo, para el sistema de gestión de activos, la cartera de activos, el sistema de activos y a nivel de activos), y pueden variar para diferentes funciones llevadas a cabo para cumplir con los requisitos de las partes interesadas. . La organización debería considerar la información o los datos de fuentes internas y externas a la organización, incluyendo contratistas, proveedores clave, reguladores y otras partes interesadas.

Los objetivos de gestión de activos deben ser específicos, medibles, alcanzables, realistas y de duración determinada (es decir, los objetivos "SMART"). Pueden ser tanto mediciones cuantitativas (por ejemplo, tiempo medio entre fallos) como mediciones cualitativas (por ejemplo, la satisfacción del cliente).

1.1.7.8. Respaldo (back-up) de información

Es necesario que la organización desarrolle una política que defina el alcance y la frecuencia en la que deben realizarse copias de seguridad de la información. También, hay que verificar que las copias se han realizado correctamente y se debe realizar un registro de la ubicación de cada copia, la cual debe ser distinta de la original, para evitar que sea afectada por el mismo problema. Todas las copias de seguridad deben disponer de controles de acceso, además, en el caso de que posea un alto grado de confidencialidad, hay que aplicarlas técnicas de cifrado para una mayor seguridad. Cualquier información que pueda ser afectada debe poder ser recuperada en caso de que se haya producido algún desastre. Para tener la certeza de que la información va a poder ser recuperada, se realiza el proceso de restauración desde la copia de seguridad y, de esta manera, se comprueba su efectividad. Es decir, que para mantener la disponibilidad y la integridad de los sistemas de información y de la información misma, una organización debe: Tener copias regularmente de los

activos de la información. Verificar que las copias son correctas. Comprobar la efectividad de la restauración de la información desde la copia. Otorgar a las copias el nivel adecuado de protección física.

1.1.7.9. Seguridad en las telecomunicaciones

La norma facilita modernos controles, además de una orientación para la implementación en las empresas de telecomunicaciones. Consolida la privacidad, disponibilidad e integridad de las infraestructuras y servicios de estas empresas. antenna-233349_640La información para las organizaciones de telecomunicaciones es un activo esencial y por ello le resuelta necesario conservarlo debido a que es también objeto de muchas amenazas. Por todo ello, los objetivos que proporciona están norma son: Seguridad de la información a través de prácticas que den confianza en las actividades realizadas por las organizaciones. Retos globales de la seguridad de la información acondicionados exclusivamente para estas empresas. La norma ISO27011 nos garantiza la seguridad de la información de las empresas a través de unos controles apropiados. Estos controles han de ser implementados, controlados, especificados y deben de ir evolucionando a lo largo del tiempo para que se lleve a cabo el cumplimento de los objetivos de seguridad fijados previamente por estas entidades. Previo a la selección de controles, las organizaciones de telecomunicaciones deben identificar los requisitos y la evaluación continua de los posibles riesgos de seguridad. La elección de estos controles va a depender de la aceptación del riesgo que tenga esta organización con el requisito, además, de estar sujetas a la normativa legales internacionales o no pertinentes. Con la implementación de la norma ISO-27011, las organizaciones dedicadas a las telecomunicaciones tendrán que llevar a cabo las siguientes pautas: Proteger la integridad, confidencialidad y disponibilidad de las infraestructuras y servicios. Asegurar la disminución de los riesgos de los servicios que las empresas de telecomunicaciones prestan mediante procesos de cooperación fiables. Han de saber reordenar los recursos para que las actividades llevadas a cabo sean más eficientes. Acoger un principio global relacionado con la seguridad de la información. Tener la capacidad de hacer que la moralidad de las personas y la confianza de las mismas mejoren. ISOTools, es una

Plataforma Tecnológica que ayuda a las organizaciones a la implementación de la norma ISO 27011. Además, pone a su disposición una serie de aplicaciones para el diagnóstico de la seguridad de la información, como por ejemplo el control sobre el riesgo o la eficacia de los mismos.

1.1.7.10. Gestión de incidentes de la seguridad de información

La gestión de los incidentes de seguridad es un aspecto muy importante para lograr el mejoramiento continuo de la seguridad de la información de cualquier compañía, el principal inconveniente es que muchas organizaciones no lo utilizan adecuadamente. A pesar que la norma ISO 27001, hace mención de este tema como uno de los dominios fundamentales.

Evento de Seguridad informática: Un evento de seguridad informática es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de medidas de seguridad (safeguards), o una situación previamente desconocida que pueda ser relevante para la seguridad. (Galeano, 2019)

Un Evento de Seguridad Informática no es necesariamente una ocurrencia maliciosa o adversa.

Incidente de seguridad informática: Un incidente de seguridad informática es la violación o amenaza inminente a la violación de una política de seguridad de la información implícita o explícita. También es un incidente de seguridad un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad). Un incidente puede ser denunciado por los involucrados, o indicado por un único o una serie de eventos de seguridad informática.

Se entienden por incidentes de seguridad las violaciones de acceso, intento de acceso, uso inadecuado, divulgación, modificación o destrucción no autorizada de información, cambios no controlados en el sistema, errores humanos, incumplimiento de las políticas de seguridad, pérdida o robo de información o recurso tecnológico, mal funcionamiento, manipulación, sabotaje, virus,

códigos maliciosos, negación del servicio, violaciones de confidencialidad, entre otros.

1.1.7.11. Administración de recursos

La administración de recursos humanos es la técnica de organizar el personal que integra una empresa con el fin de reclutarlo, ordenarlo, motivarlo, redistribuirlo y capacitarlo, para mejorar su eficiencia sintiéndose parte del emprendimiento que integra, y que a través de la empresa que es un poco suya, hallará la satisfacción de sus metas personales.

En general existe en las empresas un área dedicada a la administración de los recursos humanos o gestión de recursos humanos, integrada por personal idóneo, que comienzan su función con la selección del personal, previo planeamiento de lo requerido según las necesidades empresariales. Se deben diseñar los puestos de trabajo para luego realizar el reclutamiento, identificando los candidatos más adecuados y calificados para el cargo en cuestión.

1.1.7.12. Seguridad para aplicaciones en la nube

La seguridad de los datos en las aplicaciones en la nube es una de las mayores preocupaciones tanto de aquellos que nos dedicamos a proveer servicios como de aquellos potenciales clientes que piensan en contratar los servicios. Cuando la información solo se tiene en forma física o virtual, pero en un solo acceso, esto puede conllevar a perdidas no deseadas de información se por diferentes tipos de incidencias, cuando el personal quiere malintencionadamente borrar, alterar la información contenida en los servidores, (Oramas & Figueroa del Valle, 2014) que la información se almacenada en la nube para evitar este tipo de amenazas directas del personal.

Si nos remontamos sólo 3 años atrás, una gran mayoría de las pequeñas empresas indicaban que sus preocupaciones de seguridad se basaban en el acceso a la información y las políticas de backup de la empresa.

Los datos están en la nube y han viajado allí para quedarse, así, las empresas y sus gerentes ahora nos preocupamos por quién y desde dónde se va a acceder a

la información ya que tenemos contratos de servicio con proveedores de soluciones en la nube (SaaS, PaaS, etc..) que nos garantizan la integridad de los datos y nos dejan sólo con la responsabilidad del acceso a la información a las personas correctas de nuestro lado.

Seguridad de los datos en Aplicaciones SaaS, aplicaciones SaaS (software como servicio) como Flowsme, que tratan datos confidenciales tanto de contactos y empresas como de oportunidades y estrategias de negociación, deben contar con certificados de seguridad SSL que permiten encriptar los datos mientras viajan por Internet de forma que nadie puede acceder a la información sin tener un usuario válido de la aplicación.

El certificado SSL es un método de protección de los datos que viajan por internet. A modo de resumen, en la siguiente imagen podemos ver cómo se comunica nuestro navegador con los servidores de la aplicación a la que queremos acceder, por ejemplo, cuando accedemos a Gmail:

La seguridad de las aplicaciones en la nube para Pymes, por otro lado, la seguridad de los datos en las aplicaciones web se eleva a niveles muy complicados de conseguir por las pequeñas empresas que se ven beneficiadas por las economías de escala que aplican los proveedores de servicios cloud.

En resumidas cuentas, olvidarse de los backups y las tareas de mantenimiento de servidores es una muy buena noticia que cada vez más empresas están empezando a disfrutar gracias a contar con aplicaciones de negocio seguras y fiables como Flowsme.

1.1.7.13. Política de cumplimiento

La Constitución del Perú de 1993, en el Art. 200, num. 6º, consagró la acción de cumplimiento, en términos similares a los del Art. 87 de la Constitución Colombiana. El texto de la norma es el siguiente:

“La acción de cumplimiento procede contra cualquier autoridad o funcionario renuente a acatar una norma legal o un acto administrativo, sin perjuicio de las responsabilidades de ley”.

1º) Orígenes:

Según el constitucionalista peruano CESAR LANDA ARROYO, esta acción siguió el modelo brasileño del mandado de injuncao.

2º) Concepto y características:

El citado tratadista LANDA ARROYO define esta acción como "(…) una garantía constitucional (…)", cuyas características son las siguientes:

"a) Procede contra cualquier autoridad o funcionario, sin distinción de jerarquías.

"b) En cuanto al nivel de la norma no acatada, debe interpretarse que no importa la jerarquía de la misma, por lo que están comprendidas las leyes en sentido formal y material.

Significa, entonces, que se intentará esta acción frente al incumplimiento de lo dispuesto en una Ley Orgánica, Ley, Decretos Legislativos, Decreto-Leyes, Decretos Supremos, Reglamentos, normas emanadas de los Gobiernos locales, así como de los regionales".

"(…). Esta acción significa que el Estado de Derecho, (…), no sea meramente declarativo, al reconocer la existencia de un sistema de fuentes del derecho - Constitución, ley, reglamento y contratos, entre otros-, sino que sea eficaz mediante la justicia constitucional en caso de su incumplimiento.

1.1.7.14. Sanciones previstas por incumplimiento

Un documento de seguridad válido es aquel que incluye políticas, procedimientos, medidas de seguridad –organizativas, jurídicas y técnicas–, así como controles de seguridad de nivel técnico, físico y administrativo. Definitivamente, para establecer estos controles es muy útil la implementación de la norma internacional ISO 27001 de Sistemas de Gestión Seguridad Informática.

Crear, modificar, cancelar o mantener BDP sin cumplir con los requisitos legales es una infracción muy grave, con multas de entre 50 UIT y 100 UIT.

- "R" de redacción de cláusulas de protección de datos personales: La ley obliga a que las empresas obtengan el consentimiento para el tratamiento de los datos, el cual debe ser brindado en forma libre, con carácter previo, en forma expresa, inequívoca, escrita y autenticada (estas dos últimas solo para datos sensibles) y además informada. Es imprescindible realizar un buen mapeo de los puntos de interacción entre el cliente y la organización para asegurar de que el consentimiento se realiza conforme a ley. Estas sanciones recaerán directamente

1.2. Antecedentes

Los estudios previos que dieron origen a esta investigación son los siguientes:

Según Alvarez (2005) realizo una auditoria usando la metodología COBIT y concluyeron. La sociedad de la información y nuevas tecnologías de comunicación plantean la necesidad de mantener la usabilidad y confidencialidad de la información que soportan los sistemas en las organizaciones; para ello, es especialmente importante elegir e implantar los sistemas y métodos de seguridad más idóneos, que protejan las redes y sistemas ante eventuales amenazas, ya sean presentes o futuras. Los servicios de auditoría comprenden el estudio de los sistemas para gestionar las vulnerabilidades que pudieran estar presentes en los sistemas. Una vez localizadas, las anomalías se documentan, se informa de los resultados a los responsables y se establecen medidas proactivas de refuerzo, siguiendo siempre un proceso secuencial que permita que los sistemas mejoren su seguridad aprendiendo de los errores pasados. Las auditorías de los sistemas permiten conocer en el momento de su realización cual es la situación exacta de los activos de información, en cuanto a protección, control y medidas de seguridad. Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido, cobra especial importancia el hecho de que puedan contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas.

Según Rayme (2007) realizó un análisis de Gestión y concluye. La seguridad de la información ha sido siempre considerada como un problema de ingeniería, donde la

responsabilidad debe recaer en el personal de Tecnología de Información y Comunicaciones, de tal forma que las organizaciones han tratado de resolverlo utilizando tecnología como controles de acceso, pero este enfoque es incorrecto porque la gestión de la seguridad de la información requiere la participación de todos los empleados de una organización. Los resultados de la investigación demuestran que la estrategia de desarrollar políticas de seguridad de la información es de prioridad en las Universidades: UNMSM 37%, UNFV 19% y UPSJB 24%. Las autoridades no consideran a la seguridad como una prioridad alineada con la estrategia universitaria. Ello se refleja en las encuestas realizadas al personal de TIC donde se les formuló la pregunta si habían asistido a eventos o programas de capacitación de seguridad de la información, la cual reportó que la mayoría nunca asistió a programas de capacitación: UNMSM 20%, UNFV 100% y UPSJB 70%. De tal manera que la estrategia de capacitación es de mucho interés por el personal: UNMSM el 60%, UNFV el 70% y UPSJB el 70%.

Según Albanese Et. all…(2010) un sistema de control interno basado en estructuras tales como los modelos COSO Y COSO ERM colabora con la gestión de cualquier tipo de organización independientemente si persigue fines de lucro o no, de la naturaleza de su actividad, su tamaño o si se trata de un ente público o privado. Tanto el ambiente de control como la evaluación, análisis y gestión de riesgos son componentes claves en el cumplimiento de los objetivos definidos. Herramientas tales como elaboración de manuales de procesos y funciones, análisis FODA y la definición de una matriz de riesgos colaboran en la implementación del modelo.

Según Molina, Gascón, Blanco, & R.Antigüedad (2010) desde sus orígenes la informática ha venido experimentando notables cambios no solo en su arquitectura sino en la forma en la que las personas interactuamos con ella. Atrás quedan esos ordenadores que únicamente realizaban operaciones matemáticas y que estaban situados en grandes salas con personal dedicado en exclusiva a su mantenimiento.

Según Barrantes & Hugo (2012) proponen un diseño e implementación de un SGSI, y concluyeron. El implementar una política de seguridad y que los colaboradores la conozcan e interiorizan, es de gran utilidad cuando se quiere implementar cualquier sistema de gestión en una organización, ya que les da una visión clara de cómo sus labores cotidianas aportan para el mantenimiento y mejora de un sistema de gestión empresarial.

Aún después de implementar un buen sistema de gestión de seguridad de información, en el futuro se presentan más activos de información, más amenazas, vulnerabilidades y por lo tanto, mayores riesgos. Este escenario no se puede evitar; es por ello que se concluye, que se debe estar preparado para actuar de manera inmediata ante cualquier nueva vulnerabilidad que se identifique. Diseñando e implementando una buena metodología para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables gran porcentaje de riesgos que afecten a los activos de información.

Según Aliaga (2013) en conjunto con las personas, la información es el activo más importante que tiene cualquier organización. La falta de controles y políticas enfocadas a su seguridad puede traer consecuencias graves para el cumplimiento de los objetivos de negocio e incluso, pérdidas más graves de lo que la organización supone. No hay un interés adecuado con respecto a la seguridad de información dentro de las instituciones educativas, partiendo desde la alta gerencia hasta los mismos departamentos de TI. Dicha falta de interés se muestra claramente en la falta de políticas, normas y controles dentro del instituto educativo y en la falta de concientización del personal del mismo con respecto a la seguridad de la información. Un Sistema de Gestión de Seguridad de Información (SGSI) establecido en una institución educativa se muestra como la solución para que el flujo de información que se da entre los procesos críticos y los activos involucrados dentro de dichos procesos, logren el nivel de seguridad adecuado para garantizar el cumplimiento de los objetivos de TI y, en consecuencia, los objetivos organizacionales.

Según Ortega (2014) las dimensiones del concepto información son múltiples y cada una de ellas ha repercutido, desde varios frentes y de un modo u otro, en la disciplina bibliotecológica. Lo anterior se explica porque el concepto información ha sido esencial en diversas teorías de la propia información, sociológicas y cognoscitivas–, y aunque su uso ha sido fundamentalmente ficcional y meta científico, se aprecia que su utilidad intratómica ha sido avasalladora. Desde su origen en la teoría de la información, este término permitió, como en el caso de la bibliotecología, introducir niveles de análisis más abstractos o substanciales. En consecuencia, se incorporó como un progreso conceptual y aportó modelos explicativos que enriquecieron la perspectiva marcadamente normativa que durante varias décadas ha predominado en la disciplina. No obstante, se ha llegado al

extremo de reducir o subsumir las entidades fundamentales de la bibliotecología a dicho término, lo cual también se ha visto favorecido por el empleo de las tecnologías de información y procesamiento de la misma. Afortunadamente, tal subsunción ha comenzado a difuminarse.

Según Aguirre (2014) el apoyo de la alta gerencia para el diseño de este sistema de gestión fue imprescindible, debido a que fue necesaria su intervención para ayudar a concientizar a los jefes de área y dueños de los procesos a participar de las entrevistas de levantamiento de información y ayudó a que entendieran que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga. Es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas. Existe una clara necesidad en la organización de contratar personal especializado para dar soporte a los procesos involucrados en el SGSI, debido a que los recursos actuales no se dan abasto para atender los requerimientos de los usuarios lo cual en muchos casos se ha utilizado como excusa para realizar actos que afectan la seguridad de la información como el préstamo de credenciales de usuarios, uso de un correo para varias personas o la dejadez en la generación de respaldos de información del área. Es necesario mejorar la comunicación con el área de logística para acelerar los procesos de compra de aquellos activos que nos ayudaran en el tratamiento de riesgos detectados, especialmente, si estos riesgos son considerados altos o graves por la organización.

Según Macen (2014) conocer el Análisis de riesgo de la seguridad de la información en la UTIC, para la construcción de políticas de seguridad de la información. En cuanto al primer objetivo específico el análisis de riesgo desde la percepción de la Dirección de Tecnología Informática arrojó un promedio que no supera el umbral de medio riesgo que está entre el 7,4 y 7.6 del rango 8-9 y no llega al umbral de alto riesgo que representa el rango de 12-16. Conocer los aspectos culturales y técnicos en el manejo de la información en la UTIC. En cuanto a los aspectos culturales en el manejo de la información se pudo evidenciar el manejo de la información en las Sedes de la UTIC, arrojando una proporción

global con respecto al manejo de la información de manera insegura con p=47/84= 55,95 % y una proporción de manera segura con p =37/84= 44,05 %. En los aspectos técnicos en el manejo de la información, se pudo demostrar que 28 puntos de la seguridad de la información cumplen con el manejo seguro de la información y 24 de manera inseguro, desde un análisis e interpretación teórica en base a la ISO/IEC 17799.

Según Bermudez & Bailon (2015) el análisis realizado demuestra que los activos de información de las áreas consideradas críticas y la situación actual de la empresa con respecto a la seguridad de la información, refleja potenciales índices de riesgos, los cuales exponen a la información a daños, robo o modificaciones que pueden causar un impacto negativo dentro de las actividades del negocio.

Según García (2015) si bien no ha sido recogido de forma específica en nuestra legislación, sí que tiene cabida en ella a través de las especialidades que las distintas normas procesales y, en menor medida, también sustantivas, han establecido acerca de las fuentes de prueba que son utilizadas como base material del peritaje informático, es decir, las denominadas evidencias digitales. Pero estas especialidades muestran algunas connotaciones que es conveniente resaltar a modo de conclusión de este informe.

Según Guzmán (2015) para definir el modelo de metodología de seguridad en tecnologías de información y comunicaciones se realizó el análisis de riesgo que permitió detectar las amenazas a los que son sometidos los activos de la información y los requerimientos de seguridad que se presentaron, han permitido delimitar el ámbito del modelo y su estructura. El modelo de seguridad propuesto consta de varias áreas en las que se han logrado implementar controles de seguridad para cada uno. De esta manera se logró la mejora del nivel de seguridad que es medido a través de la asignación de valores, obteniéndose un valor inicial de 16 y final de 50. Para el desarrollo del modelo de seguridad de tecnologías de información y comunicaciones se tuvo en cuenta Normas técnicas y las recomendaciones del modelo ISO además, se realizó la evaluación económica del mismo el cual ha sido tomado como referencia para considerar que el proyecto metodologías de seguridad de tecnologías de información y comunicaciones es económicamente factibles...

Según Tarazona (2015) la información ha sido uno de los elementos claves en el desarrollo y éxito de los negocios y en el desarrollo de la gran mayoría de actividades

diarias para cada individuo. Por tal razón, todas las organizaciones por no decirlo en su mayoría son cada vez más consientes al momento de proteger su información, el cual es el activo primordial, y no permitiendo que sea vulnerado por diferentes amenazas a las que están expuestas desde el momento en el que se conectan a la red mas grande del mundo. INTERNET.

Según Pacheco (2015) toda política implementada de seguridad de la información debe de divulgarse en todo el personal involucrado y ponerse a disposición de todos los que laboran en el ambiento, dando seguridad a cada proceso de información, que serán definidos en la política de seguridad, así como, clientes interno y externos, que tengan alguna participación directa o indirecta, accediendo a las aplicaciones existentes, a los servidores, a redes públicas, y privadas, así como, equipos que puedan ser objeto de ataques que comprometan la información que se resguarda.

Según Tarazona (2015) la información siempre va a ser un elemento clave en el desarrollo y existo de toda organización, por lo cual la gran mayoría, elabora procedimiento de actividades diarias para el personal externo e interno. Por tal razón, una organización debe ser mucho más consciente de la necesidad de proteger información de diferentes tipos de amenazas a las que están expuestas.

Según Tibaquira (2015) comenzando como base las normas ISO27035:2011 E ISO 27005:2008 se logra elaborar un modelo integro que abarca una gestión de incidentes y la gestión de riesgos asociada a estos incidentes, el cual permitió inicialmente la identificación y análisis de los componentes que hacen parte del establecimiento del contexto bajo el cual se implementaron las normas. Encontrando diferentes beneficios al implementar modelos basados en un estándar, de una estructura adecuada, y lograr controlar cada una de las actividades definidas dentro del proceso.

Según Santos (2016) la única referencia directa es la de la ISO 31000:2009 [07], que es referenciada como marco para el contexto y la gestión de riesgos (en la versión anterior de la norma era la ISO ISO/IEC 27005:2008 [06]). Para el tratamiento de riesgos, aunque no es referenciada, la ISO/IEC 27002:2013 [03] se debe considerar, ya que es una versión mucho más detallada del anexo A del estándar 27001 y puede permitir un mejor entendimiento para el diseño de los controles. Sobre las auditorías, la ISO 27001 indica algunos requisitos puntuales. Sin embargo, no detallan o dan lineamientos específicos

para realizar esta acción. Para estos casos, se debe tomar en cuenta la "ISO 27007:2011 Guía para auditorías de SGSI" [24], que a su vez referencia a la "ISO 19011:2011 Directrices para la auditoría de Sistemas de Gestión" [25], las cuales cuentan con lineamientos para más específicos para auditorías internas. Respecto a las métricas, el estándar ISO/IEC 27004:2009 [05] brinda lineamientos y nociones necesarias para la adecuada elaboración, análisis y evaluación de las mediciones sobre el sistema y sus controles.

Según Mercado (2016) se elaboró un modelo de gestión de seguridad de la información para el gobierno electrónico resultado de la revisión y análisis de 11 modelos de seguridad de la información, en los que se identificaron los elementos más relevantes que forman parte del modelo propuesto. Se ha definido una estructura organizacional con funciones definidas que contempla los procesos estratégicos, fundamentales y de soporte, la cual permite gestionar la seguridad de la información y garantizar una mejor experiencia al cliente cuando requiera interactuar con los procesos o servicios de la organización. Se han identificado 05 niveles de madurez para la implementación y operación del modelo de seguridad de la información en los procesos que brindan servicio de gobierno electrónico, permitiendo la gestión de la seguridad en dichos procesos y conocer el nivel de seguridad con que se cuenta.

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

2.1. Identificación del problema

2.1.1. Planteamiento del problema

La seguridad de la información siempre ha sido uno de los problemas en el mundo, por las diferentes técnicas que existen y que aparecen diariamente para vulnerar los sistemas y poder manipular la información.

La Universidad Nacional del Altiplano Puno, es un organismo autónomo, perteneciente al sistema nacional de informática, donde los objetivos son: normar, coordinar, integrar, racionalizar, promover la capacitación, investigación y desarrollo de las actividades de informática oficiales.

Como parte de una propuesta de la secretaria de gobierno digital, ser el Perú un impulsor cero papeles, y se digitalice toda la información que se procesa en documentos físicos. Es por lo cual se incentiva a un gobierno digital a nivel nacional.

Por ende, al sistematizar toda la información, se debe asegurar la información, mediante un sistema de gestión de seguridad de la información, según la norma técnica peruana, ISO/IEC 27001:2014, y uso obligatorio de esta norma según RESOLUCIÓN MINISTERIAL N.º 004-2016-PCM y la RESOLUCION MINISTERIAL Nº 087-2019 – PCM- APROBACION Y CONFORMACION DE FUNCIONES DE COMITÉ DE GOBIERNO DIGITAL.

Y como primera disposición en la Norma ISO 27001, en el inicio de los objetivos. A.5. POLITICAS DE SEGURIDAD DE LA INFORMACION. Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la

gerencia, publicado y comunicado a los empleados y a las partes externas relevantes. Y el uso obligatorio y la implementación de ISO 27001, recae directamente sobre la OFICINA DE TECNOLOGÍAS DE INFORMACIÓN (OTI).

Sin embargo, se evidencia que no se ha iniciado con un Sistema de Gestión de Seguridad de la Información (SGSI), ni mucho menos con implementar, POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, el cual es la base del SGSI según la NTP ISO IEC 27001:2014. Y como activo principal es la información que administra la OTI, de docentes, alumnos y personal administrativo de la Universidad Nacional del Altiplano – Puno. Esta información no está asegurada. Y hasta la fecha no se ha realizado una auditoria de sistemas a la institución.

Es por ello que se propone la implementación de políticas de seguridad de la información, que ayudaran al inicio para una implementación de un SGSI, que ha sido requerido por segunda vez en la RM. Nº 087-2019-PCM, para un gobierno digital seguro.

a. Problema general

- ¿El análisis de riegos y la propuesta de políticas de seguridad de la información lograra reducir los riesgos y optimizar la seguridad de información de la Oficina de Tecnologías de Información (OTI) UNA PUNO?

b. Problemas específicos

- ¿El análisis de riesgo de la seguridad de la información optimizara la seguridad de la información de la Oficina de tecnologías de Información (OTI)?
- ¿Al proponer políticas de seguridad de la información se logrará reducir los riesgos de información de la Oficina de Tecnologías de Información (OTI)?

2.2. Justificación

Para implementar políticas de seguridad de la información, primero debemos verificar que sea un requisito a través de una ley, u obligación para su implementación de un Sistema de Gestión de Seguridad de la Información. Según RM-004-2016-PCM, LO ES,

debido a es un requerimiento indispensable. Y el ultimo requerimiento que es dado por la última Resolución Ministerial N.º 087-2019-PCM, donde se solicita ya toda documentación generada para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Viendo las Resoluciones Ministeriales, la Universidad Nacional del Altiplano Puno, ya está fuera de plazo en el inicio de implementación de Políticas de Seguridad de la Información. Por lo cual es primordial darle mucho mayor énfasis en la publicación de la presente propuesta.

Por lo cual es primordial su implementación de la presente propuesta de **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.** Para un gobierno digital seguro, donde la información que es sistematizada, manteniendo los tres principios de seguridad de la información: confidencial, integro y disponible. Estando siempre en concordancia a todos los activos de la institución.

2.3.Objetivos

2.3.1. Objetivo general

- Analizar los riegos y proponer políticas de seguridad de la información de la Oficina de tecnologías de Información (OTI) UNA - PUNO

2.3.2. Objetivos específicos

- Analizar los riegos de la seguridad de la información.
- Proponer políticas de seguridad de la información.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1.Lugar de estudio

La información recogida se dio en el área de la Oficina de Tecnologías de Información (OTI) y la tres sub áreas, “Desarrollo y sistemas informáticos”, “gobierno Electrónico”, “Redes y Telecomunicaciones”, en conjunto forman la OTI de la Universidad Nacional del Altiplano Puno. Encargados de administrar la información por los diferentes medios digitales que hoy en día existen.

Figura 7. Ubicación geografía de la OTI dentro de la UNA – PUNO

Fuente: Google Maps (2019)

3.2.Población y tamaño de muestra

3.2.1. Población

La población se compuso de todos los trabajadores de la Oficina de Tecnologías de Información (OTI), siendo 12 personas divididas en cada sub área, incluyendo a la jefa de la OTI.

3.3.Método de investigación

Es de corte positivista, teniendo mayor preocupación en procedimientos analíticos, es decir, por la fragmentación y el estudio de las partes que constituyen el todo social. De una manera experimental donde se analiza los riesgos y se propone políticas de seguridad de la información para la Oficina de Tecnologías de Información. De la Universidad Nacional del Altiplano Puno.

Experimental: Solamente se describe la variable y se manipula para proponer políticas de seguridad de la información.

Siendo de manera ontológica proponiendo nuevos conocimientos.

3.4.Descripción detallada de métodos por objetivos específicos

Para desarrollar el alcance y los objetivos propuestos en el proyecto, la metodología a implementar enmarca las fases de inicio, análisis y propuesta, donde cada etapa establece una serie de actividades encaminadas a lograr los resultados del proyecto, las cuales se describen a continuación.

3.5.Análisis de los datos

Para el análisis de riesgo de la seguridad de la información en la Oficina de tecnología de la información de la UNA - PUNO, se aplicó el método de análisis de riesgo, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información:

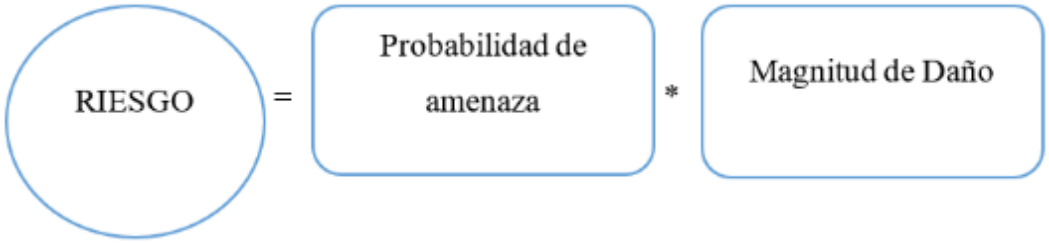


Figura 8. Fórmula para la obtención de riesgo.

Fuente: MAAGTICSI

Para el análisis e interpretación de los datos recogidos de la entrevista realizada con un cuestionario con preguntas al Personal de la OTI de la UNA PUNO.

3.6.Metodología para el análisis de riesgo

MAAGTICSI (Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información).

El Manual contiene, en tres grupos, los nueve procesos necesarios para propiciar la operación ágil y oportuna de las actividades de TIC de las Instituciones.

Para cada área de conocimiento se utilizan los principales estándares y mejores prácticas relacionadas y 9 procesos.

Gobernanza

PE - Proceso de Planeación Estratégica

Mantener la operación de un modelo de gobierno de TIC en la Institución.

APCT - Administración del Presupuesto y las Contrataciones

Coordinar las acciones para el ejercicio del presupuesto destinado a las TIC, a fin de maximizar su aplicación en las contrataciones de TIC requeridas por la Institución.

Organización

ADS - Proceso de Administración de Servicios

Definir los compromisos y costos de los servicios de TIC necesarios para mantener el adecuado funcionamiento de la Institución.

ACNF - Proceso de Administración de la Configuración

Establecer y actualizar un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas.

ASI - Proceso de Administración de la Seguridad de la Información

Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución.

Entrega

ADP - Proceso de Administración de Proyectos

Administrar la cartera operativa de proyectos de TIC, a fin de optimizar la aplicación de los recursos y obtener mayores beneficios para la Institución.

APRO - Proceso de Administración de Proveedores

Establecer un mecanismo que permita verificar el cumplimiento de las obligaciones derivadas de los contratos celebrados para la adquisición, arrendamiento o servicios de TIC.

AOP - Proceso de Administración de la Operación

Entregar a los usuarios los servicios de TIC, conforme a los niveles de servicio acordados y con los controles de seguridad definidos.

OPEC - Operación de Controles de Seguridad de la Información

Implementar y operar los controles de seguridad de la información de acuerdo al programa de implementación del SGSI, así como los correspondientes a la capacidad de respuesta a incidentes.

VALORACIÓN DE LAS MATRICES DE INFRAESTRUCTURAS ESENCIALES DE INFORMACIÓN Y, EN SU CASO, CRÍTICAS, ASÍ COMO DE ACTIVOS CLAVE.

CAPÍTULO IV

RESULTADOS Y DISCUSIONES

4.1. Resultados

Los resultados en la presente investigación se dan mediante el uso del análisis de riesgo de la metodología según ISO 27001:2013, y referencia a MAAGTICSI (Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información), donde surge a la necesidad de la seguridad, y al crecimiento del uso de la tecnología, hoy en día es parte de nuestra vida diaria, y esto no es la excepción la OTI-UNA PUNO.

La OTI, cuenta con 3 sub áreas que son:

- Desarrollo y sistemas informáticos.
- Gobierno digital.
- Redes y telecomunicaciones.

Las cuales en conjunto operan todos los activos tecnológicos de la Universidad Nacional del Altiplano Puno.

Según el primer objetivo específico planteado: Analizar los riegos de la seguridad de la información.

4.1.1. Aplicación de metodología análisis de riesgos

Se establece las 3 dimensiones esenciales de seguridad la seguridad de la información que son:

- Confidencialidad
- Integridad
- Disponibilidad

Valoración de las matrices esenciales de la seguridad de la información, se debe considerar la valoración de los activos e identificar aquellos que resultan críticos para la institución, se muestra en la siguiente tabla.

Tabla 3

Valoración de Activos

Valor	Descripción
1	La brecha puede resultar en poca o nula pérdida o daño.
2	La brecha puede resultar en una pérdida o daño menor.
3	La brecha puede resultar en una pérdida o daño serio, y los procesos del negocio pueden verse afectados negativamente.
4	La brecha puede resultar en una pérdida o daño serio, y los procesos del negocio pueden fallar o interrumpirse.
5	La brecha puede resultar en altas pérdidas. Los procesos del negocio fallarán.

Fuente: MAAGTICSI.

La valoración total, será la suma de los tres principios básicos de seguridad de la información, confidencialidad, integridad y disponibilidad. Los rangos se muestran en la siguiente tabla.

Tabla 4

Rango

*Rango	Valor
3-5	Bajo (1)
6-10	Medio (2)
11-15	Alto (3)

Fuente: MAAGTICSI.

a. Activos

De acuerdo a los criterios definidos por MAAGTICSI, se analizó cada uno de los activos de la Oficina de Tecnología de Información de la Universidad Nacional del Altiplano – Puno. El total final de cada amenaza, es obtenido un valor1 promedio de forma alfabética y un valor2 promedio en forma numérica, con cada dimensión que es afectado, tomando este junto con la frecuencia para calcular el nivel de riesgo asociado a la amenaza como se muestra en las siguientes tablas, individualmente.

Tabla 5

Base de datos riesgo

*Rango	Valor	resultado
3-5	Bajo (1)	3
6-10	Medio (2)	4
11-15	Alto (3)	3
	Total	10

Fuente: análisis de riesgo de la OTI

Activo	Amenaza	C	I	D	Total1	Valor1	Valor2
Base de datos	Errores del administrador	1	1	1	3	Bajo	1
	Alteración accidental de la información	2	2	2	6	Medio	2
	Destrucción de información		2		2	Bajo	1
	Fugas de información	2			2	Bajo	1
	Suplantación de la identidad del usuario	1			1	Bajo	1
	Abuso de privilegios de acceso	5	1	5	11	Alto	3
	Acceso no autorizado	3	2	1	6	Medio	2
	Modificación deliberada de la información	5	5	5	15	Alto	3
	Destrucción de información	5	1	3	9	Medio	2
	Revelación de información	5	5	5	15	Alto	3

Figura 9. Análisis de activo de Base de datos

Fuente: análisis de riesgo de la OTI

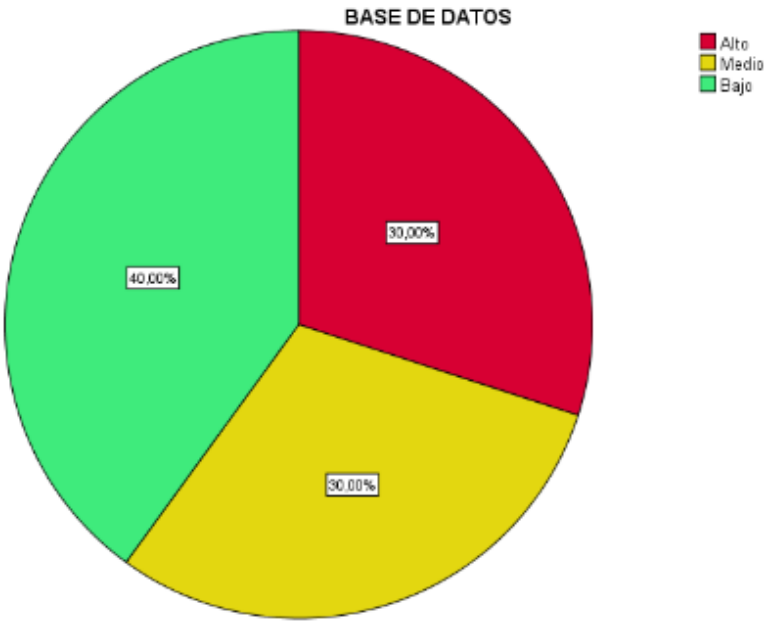


Figura 10. Base de datos

Fuente: análisis de riesgo de la OTI

En la figura 10 siendo un 40% respecto al activo de base de datos, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo.

Siendo un 30% respecto al activo de base de datos, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo medio.

Siendo un 30 % respecto al activo de base de datos, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo alto.

Discusión

Según Aguirre (2014), menciona que cuando existe un riesgo bajo, la amenaza se puede dar con una probabilidad de un ataque y vulnerar en promedio no menor de 2 años. Sin embargo, un activo que es la base de datos, donde se almacena toda la información de la Universidad, este si sufre un ataque así, y al no tener ningún backup, puede ser vulnerado en menos tiempo de lo indicado, 6 meses.

Tabla 6

Análisis de activo de software

*Rango	Valor	resultado
3-5	Bajo (1)	6
6-10	Medio (2)	6
11-15	Alto (3)	6
	Total	12

Fuente: análisis de riesgo de la OTI

ACTIVO	AMENAZA	C	I	D	Total1	Valor1	Valor2
SOFTWARE	Avería de origen fisico o lógico	5			5	Bajo	1
	Errores de los usuarios	1	1	1	3	Bajo	1
	Errores del administrador	1	4	3	8	Medio	2
	Difusión de software dañino	2	1	1	4	Bajo	1
	Alteración accidental de la información		1		1	Bajo	1
	Destrucción de información	2	4	5	11	Alto	3
	Fugas de información	4	5	2	11	Alto	3
	Vulnerabilidades de los programas	3	4	5	12	Alto	3
	Errores de mantenimiento / actualización de programas	5	5	5	15	Alto	3
	Suplantación de la identidad del usuario	5	5	5	15	Alto	3
	Abuso de privilegios de acceso	4	2	4	10	Medio	2
	Uso no previsto	1	2	4	7	Medio	2
	Difusión de software dañino	1	1	1	3	Bajo	1
	Acceso no autorizado	2	3	5	10	Medio	2
	Modificación deliberada de la información	5	5	5	15	Alto	3
	Destrucción de información			5	5	Bajo	1
	Revelación de información	4		4	8	Medio	2
	Manipulación de programas	1	5	1	7	Medio	2

Figura 11. Análisis de activo de software

Fuente: análisis de riesgo de la OTI

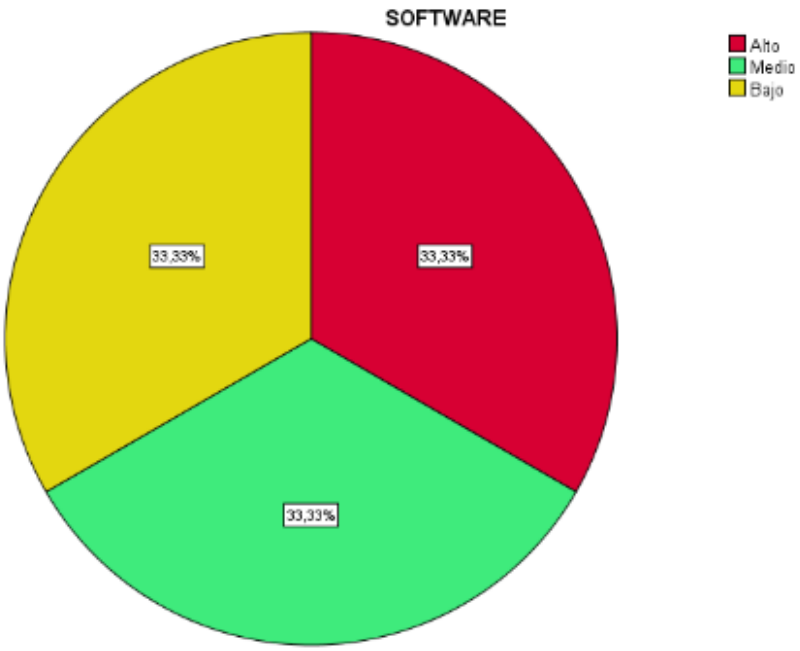


Figura 12. Software

Fuente: análisis de riesgo de la OTI.

En la figura 12 siendo un 33.33% respecto al activo de software, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo.

Siendo un 33.33% respecto al activo de software, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo medio.

Siendo un 33.33 % respecto al activo de software, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo alto.

Discusión

Según Aguirre (2014), menciona que cuando existe un riesgo alto, estas amenazas se deben mitigar a la brevedad posible, para que no pueda afectar la funcionalidad de un sistema. Pero lo cual implica cambios a gran escala, y nuevamente desarrollar los programas basado en principios. Sin embargo, día a día se crean mecanismos para vulnerar los softwares, por lo cual es recomendable realizar procesos de monitoreo a cada inestabilidad o perdida de conexión.

Tabla 7

Análisis de activo de Hardware

*Rango	Valor	resultado
3-5	Bajo (1)	1
6-10	Medio (2)	16
11-15	Alto (3)	4
	Total	21

Fuente: análisis de riesgo de la OTI.

Activo	Amenazas	C	I	D	Total1	Valor1	Valor2
Hardware	Fuego			5	5	Bajo	1
	Daños por agua			4	4	Bajo	1
	Desastres naturales			5	5	Bajo	1
	Desastres industriales			5	5	Bajo	1
	Contaminación medioambiental			4	4	Bajo	1
	Contaminación electromagnética			5	5	Bajo	1
	Avería de origen fisico o lógico			3	3	Bajo	1
	Corte de suministro eléctrico			2	2	Bajo	1
	Condiciones inadecuadas de temperatura o humedad			5	5	Bajo	1
	Emanaciones electromagnéticas			5	5	Bajo	1
	Errores del administrador del sistema / de la seguridad	5	4	5	14	Alto	3
	Errores de mantenimiento / actualización de equipos			1	1	Bajo	1
	Caída del sistema por agotamiento de recursos			3	3	Bajo	1
	Perdida de equipos	1		2	3	Bajo	1
	Abuso de privilegios de acceso	2	2	4	8	Medio	2
	Uso no previsto	5	1	2	8	Medio	2
	Acceso no autorizado	5	1	1	7	Medio	2
	Manipulación del hardware	4		3	7	Medio	2
	Denegación de servicio			5	5	Bajo	1
	Robo de equipos	1		1	2	Bajo	1
	Ataque destructivo	5			5	Bajo	1

Figura 13. Análisis de riesgo hardware

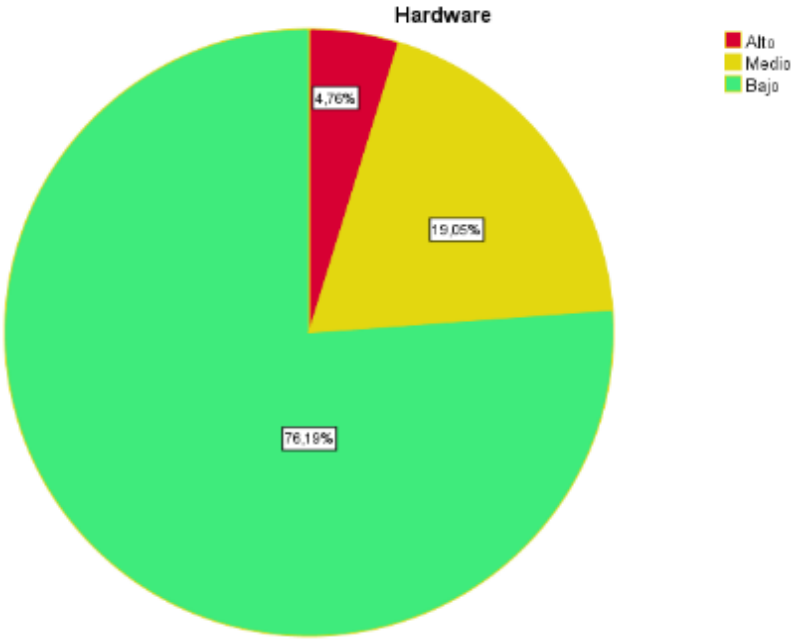


Figura 14. Hardware riesgo

Fuente: Análisis de riesgo de la OTI.

En la figura 14 siendo un 76.19% respecto al activo hardware, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo.

Siendo un 19.5% respecto al activo de base de datos, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo medio.

Siendo un 4.76 % respecto al activo de base de datos, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo alto.

Discusión

Según Santos (2016), menciona que solo con poner controles de seguridad física se puede mitigar los problemas respecto a la parte física (hardware), y a la vez poner personal de seguridad para resguardar los mismos. Sin embargo, no se tiene previsto en la OTI, medidas de seguridad que respalden el hardware de la universidad. Lo cual puede a llegar a ser en un futuro un riesgo alto.

Tabla 8

Análisis de activo de Servidores

*Rango	Valor	resultado
3-5	Bajo (1)	14
6-10	Medio (2)	6
11-15	Alto (3)	1
	Total	21

Fuente: análisis de riesgo de la OTI.

Activo	Amenazas	C	I	D	Total1	Valor1	Valor2
Servidores	Fuego			4	4	Bajo	1
	Daños por agua			3	3	Bajo	1
	Desastres naturales			4	4	Bajo	1
	Desastres industriales			3	3	Bajo	1
	Contaminación medioambiental			4	4	Bajo	1
	Contaminación electromagnética			2	2	Bajo	1
	Avería de origen físico o lógico			4	4	Bajo	1
	Corte de suministro eléctrico			4	4	Bajo	1
	Condiciones inadecuadas de temperatura o humedad			5	5	Bajo	1
	Emanaciones electromagnéticas	1			1	Bajo	1
	Errores del administrador del sistema / de la seguridad	3	3	3	9	Medio	2
	Errores de mantenimiento / actualización de equipos			1	1	Bajo	1
	Caída del sistema por agotamiento de recursos			4	4	Bajo	1
	Perdida de equipos	5		5	10	Medio	2
	Abuso de privilegios de acceso	5	4	1	10	Medio	2
	Uso no previsto	5	2	1	8	Medio	2
	Acceso no autorizado	5	5	1	11	Alto	3
	Manipulación de hardware	3		1	4	Bajo	1
	Denegación de servicio		1	5	6	Medio	2
	Robo de equipos	5		5	10	Medio	2
	Ataque destructivo	5			5	Bajo	1

Figura 15. Análisis de activo de Servidores.

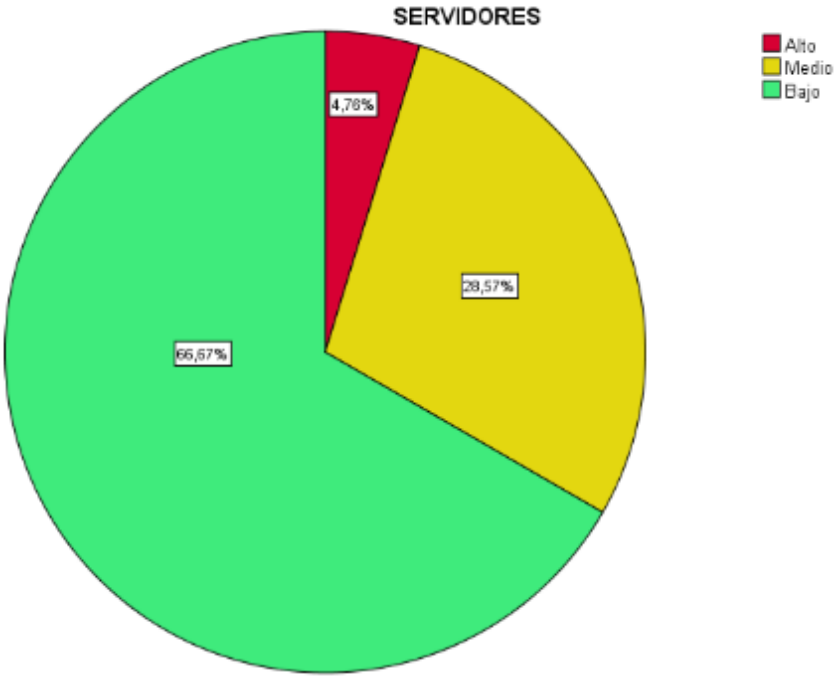


Figura 16. servidores.

Fuente: Análisis de riesgo OTI.

En la figura 16 siendo un 68.67 % respecto al activo servidores, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo.

Siendo un 28.57 % respecto al activo de servidores, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo medio.

Siendo un 4.76 % respecto al activo de servidores, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo alto.

Discusión

Según Gobierno (2015), menciona que el encargado de monitorear toda actividad es el de seguridad de la información. Sin embargo, por iniciativa propia el encargado del área de administración de los servidores red, también debe proteger o proponer medidas de seguridad física.

Tabla 9

Análisis de activos de Switch

*Rango	Valor	resultado
3-5	Bajo (1)	33
6-10	Medio (2)	1
11-15	Alto (3)	0
	Total	34

Fuente: análisis de riesgo de la OTI.

ACTIVOS	Amenazas	C	I	D	Total1	Valor1	Valor2
Switch	Fuego			4	4	Bajo	1
	Daños por agua			4	4	Bajo	1
	Desastres naturales			3	3	Bajo	1
	Desastres industriales			3	3	Bajo	1
	Contaminación medioambiental			3	3	Bajo	1
	Contaminación electromagnética			1	1	Bajo	1
	Avería de origen físico o lógico			4	4	Bajo	1
	Corte del suministro eléctrico			4	4	Bajo	1
	Condiciones inadecuadas de temperatura o humedad			3	3	Bajo	1
	Fallo de servicios de comunicaciones			4	4	Bajo	1
	Emanaciones electromagnéticas	1			1	Bajo	1
	Errores del administrador del sistema / de la seguridad	1	1	1	3	Bajo	1
	Errores de [re-]encaminamiento	1			1	Bajo	1
	Errores de secuencia		1		1	Bajo	1
	Alteración de la información		1		1	Bajo	1
	Fugas de información	1			1	Bajo	1
	Errores de mantenimiento / actualización de equipos (hardware)			1	1	Bajo	1
	Caída del sistema por agotamiento de recursos			1	1	Bajo	1
	Pérdida de equipos	1	1	1	3	Bajo	1
	Suplantación de la identidad	1	1	1	3	Bajo	1
	Abuso de privilegios de acceso	1	1	1	3	Bajo	1
	Uso no previsto	1			1	Bajo	1
	[Re-]encaminamiento de mensajes	1			1	Bajo	1
	Alteración de secuencia		1		1	Bajo	1
	Acceso no autorizado	1	1	2	4	Bajo	1
	Análisis de tráfico	1			1	Bajo	1
	Interceptación de información (escucha)	1			1	Bajo	1
	Modificación de la información		1		1	Bajo	1
	Destrucción de la información			3	3	Bajo	1
	Revelación de información			5	5	Bajo	1
	Manipulación del hardware	1		5	6	Medio	2
	Denegación de servicio			5	5	Bajo	1
	Robo de equipos	1		2	3	Bajo	1
	Ataque destructivo			5	5	Bajo	1

Figura 17. Análisis de riesgo Switch.

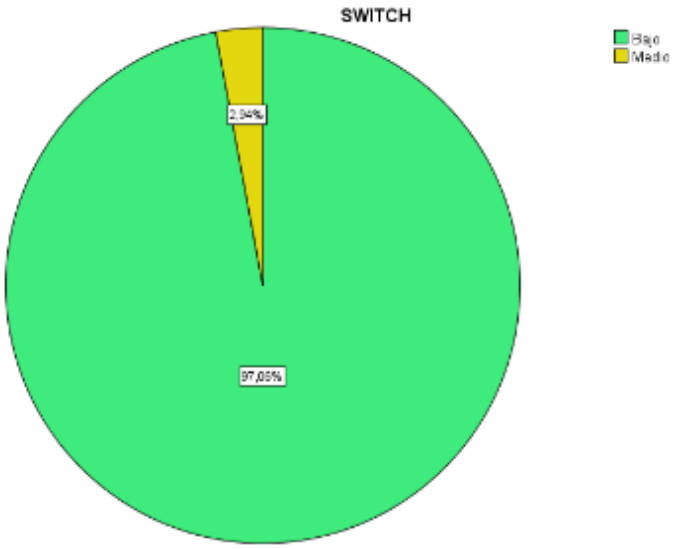


Figura 18. Switch

Fuente: Análisis de riesgo de la OTI

En la figura 18 siendo un 68.67 % respecto al activo switch, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo.

Siendo un 28.57 % respecto al activo de switch, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo medio.

Discusión

Según Ortega (2014), menciona que la información hoy en día es imprescindible, por lo cual, si es compartida o enviada por una red, la conexión debe ser constante. Sin embargo, si hubiera una amenaza física no existiera un mecanismo de respaldo u otro igual.

Tabla 10

Análisis de activos de Patch Panel

*Rango	Valor	resultado
3-5	Bajo (1)	19
6-10	Medio (2)	2
11-15	Alto (3)	0
	Total	21

Fuente: análisis de riesgo de la OTI.

Activo	amenazas	C	I	D	Total1	Valor1	Valor2
Patch panel	Fuego			4	4	Bajo	1
	Daños por agua			5	5	Bajo	1
	Desastres naturales			3	3	Bajo	1
	Desastres industriales			4	4	Bajo	1
	Contaminación medioambiental			3	3	Bajo	1
	Contaminación electromagnética			5	5	Bajo	1
	Avería de origen físico o lógico			4	4	Bajo	1
	Corte de suministro eléctrico			5	5	Bajo	1
	Condiciones inadecuadas de temperatura o humedad			4	4	Bajo	1
	Emanaciones electromagnéticas	2			2	Bajo	1
	Errores del administrado del sistema / de la seguridad	1	1	1	3	Bajo	1
	Errores de mantenimiento / actualización de equipos			1	1	Bajo	1
	Caída del sistema por agotamiento de recursos			4	4	Bajo	1
	Perdida de equipos	1		1	2	Bajo	1
	Abuso de privilegios de acceso	1	1	1	3	Bajo	1
	Uso no previsto	1	1	1	3	Bajo	1
	Acceso no autorizado	1	1	1	3	Bajo	1
	Manipulación del hardware	2		5	7	Medio	2
	Denegación de servicio	1		2	3	Bajo	1
	Robo de equipos	1		5	6	Medio	2
	Ataque destructivo	1		3	4	Bajo	1

Figura 19. Análisis de riesgo patch panel.

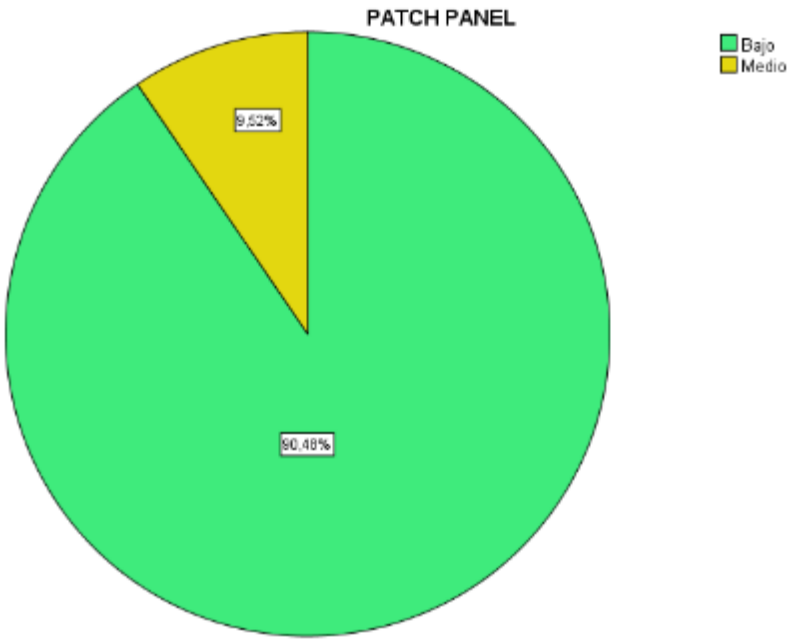


Figura 20. Patch panel

Fuente: Análisis de riesgo de la OTI.

En la figura 20 siendo un 90.48 % respecto al activo Patch panel, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo.

Siendo un 9.52 % respecto al activo de Patch panel, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo medio.

Discusión

Según Muñoz (2002), siempre se tiene que observar, monitorear, informar, gestionar, sin dejar los elementos que en su mayoría son menos relevantes. Si bien es cierto, pero no se le puede dar prioridad aquellos que son considerados intermediarios de la comunicación.

Tabla 11

Análisis de activos de Acceso a internet

*Rango	Valor	resultado
3-5	Bajo (1)	19
6-10	Medio (2)	2
11-15	Alto (3)	0
	Total	21

Fuente: análisis de riesgo de la OTI.

Activo	Amenazas	C	I	D	Total1	Valor1	Valor2
Acceso a internet	Fallo de servicios de comunicaciones			5	5	Bajo	1
	Interrupción de otros servicios o suministros esenciales			5	5	Bajo	1
	Errores del administrador del sistema / de la seguridad	2	2	1	5	Bajo	1
	Errores de (re-)encaminamiento	1			1	Bajo	1
	Errores de secuencia		1		1	Bajo	1
	alteración de la información		1		1	Bajo	1
	Destrucción de información			1	1	Bajo	1
	Fugas de información	1			1	Bajo	1
	Caída del sistema por agotamiento de recursos			4	4	Bajo	1
	Suplantación de la identidad		1	2	3	Bajo	1
	Abuso de privilegios de acceso	1	1		2	Bajo	1
	Uso no previsto	1	1	1	3	Bajo	1
	(re-)encaminamiento de mensajes	1			1	Bajo	1
	alteración de secuencia		1		1	Bajo	1
	Acceso no autorizado		1	3	4	Bajo	1
	Análisis de trafico	1			1	Bajo	1
	Repudio (negación de actuaciones)		1	5	6	Medio	2
	Interceptación de información			1	1	Bajo	1
	Modificación de la información		1		1	Bajo	1
	Destrucción de información			4	4	Bajo	1
	Denegación de servicio	4			4	Bajo	1

Figura 21. análisis de riesgo acceso a internet

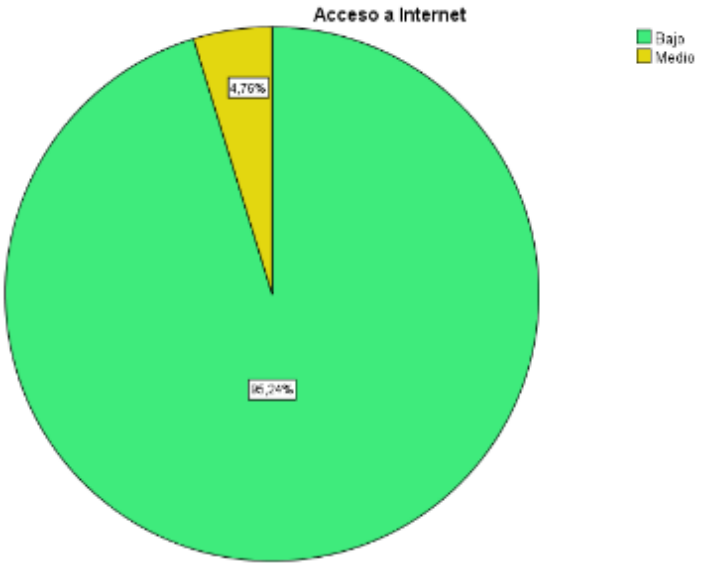


Figura 22. Acceso a internet

Fuente: Análisis de riesgo de la OTI.

En la figura 22 siendo un 95.24 % respecto al activo de acceso a internet, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo.

Siendo un 4.76 % respecto al activo de acceso a internet, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo medio.

Discusión

Según Muñoz (2002), siempre se tiene que observar, monitorear, informar, gestionar, sin dejar los elementos que en su mayoría son menos relevantes. Si bien es cierto, pero no se le puede dar prioridad aquellos que son considerados intermediarios de la comunicación.

Tabla 12

Análisis de activos de personal que labora

*Rango	Valor	resultado
3-5	Bajo (1)	8
6-10	Medio (2)	2
11-15	Alto (3)	0
	Total	10

Fuente: análisis de riesgo de la OTI.

Activo	Amenazas	C	I	D	Total1	Valor1	Valor2
Personal que labora	Alteración de la información		1		1	Bajo	1
	Destrucción de información	2			2	Bajo	1
	Fugas de información	1			1	Bajo	1
	Indisponibilidad de personal			1	1	Bajo	1
	Modificación de la información		5		5	Bajo	1
	Destrucción de información	1			1	Bajo	1
	Revelación de información			4	4	Bajo	1
	Indisponibilidad de personal	4			4	Bajo	1
	Extorsión	2	2	2	6	Medio	2
	Ingeniería social	2	2	2	6	Medio	2

Figura 23. Análisis de riesgo personal que labora.

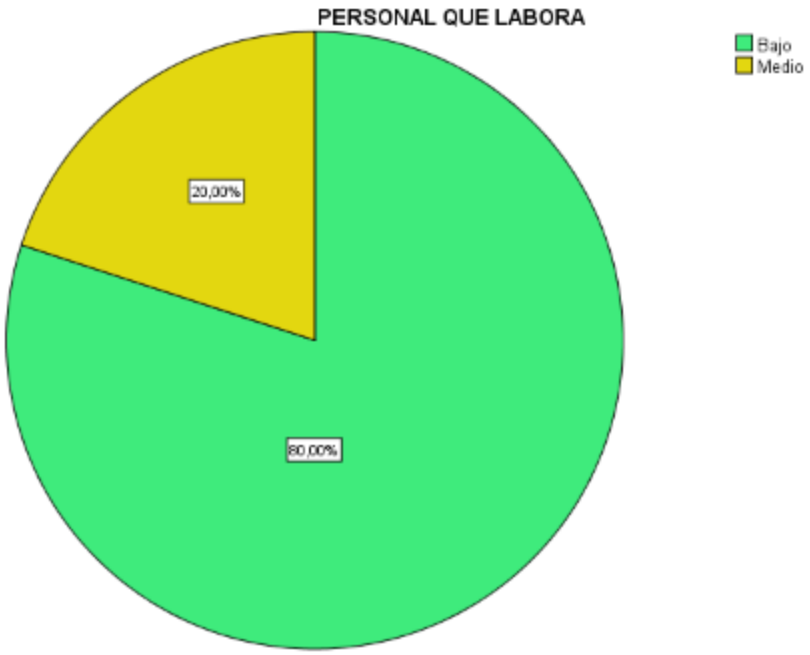


Figura 24. Personal que labora

Fuente: Análisis de riesgo de la OTI.

En la figura 24 siendo un 80 % respecto al activo de acceso a internet, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo.

Siendo un 20% respecto al activo de acceso a internet, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo medio.

Discusión

Según Muñoz (2002), una auditoría externa, es confiable porque lo realiza una persona externa y los datos siempre son verdaderos. Sin embargo, cuando se realiza encuestas a las personas, respecto a una auditoria, estos datos pueden ser inexactos porque los empleados mienten, por miedo a perder el trabajo o cometer un delito.

Tabla 13

Total, de Amenazas por Riesgo

*Rango	Valor	resultado
3-5	Bajo (1)	151
6-10	Medio (2)	28
11-15	Alto (3)	12
	Total	191

Fuente: análisis de riesgo de la OTI.

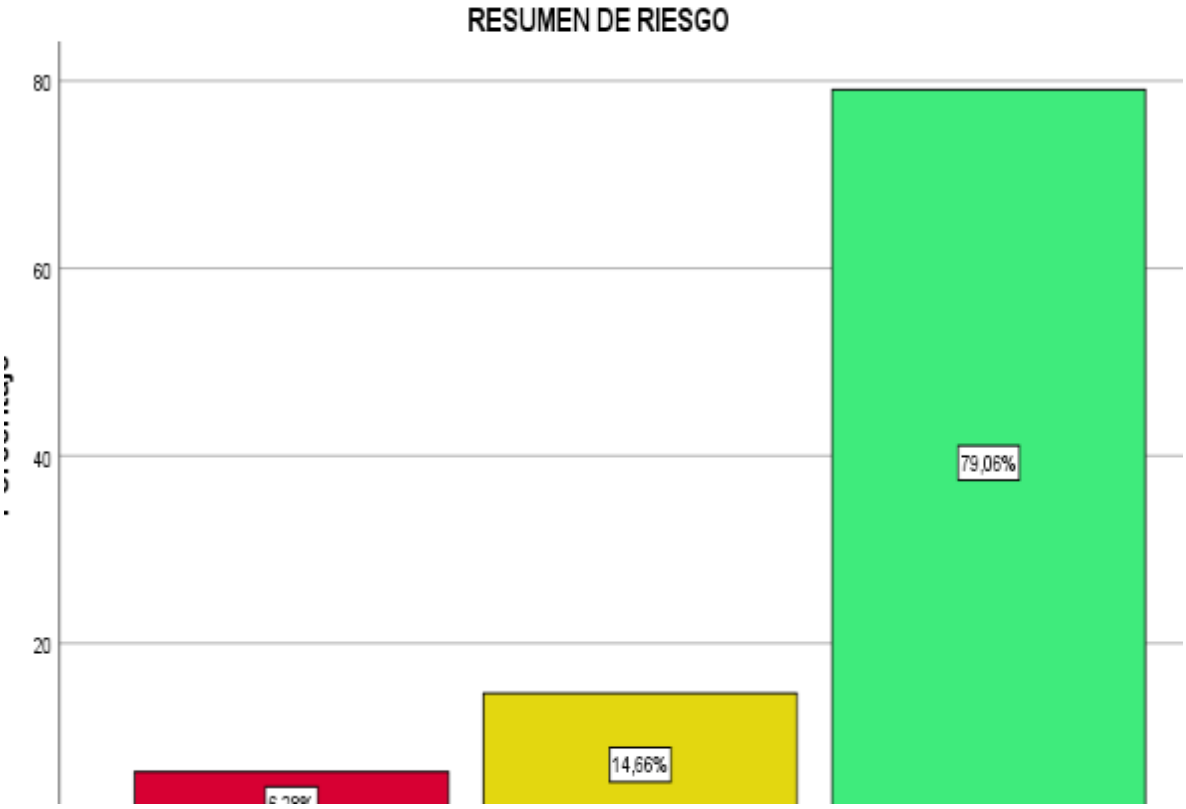


Figura 25. Resumen de global de riesgo

Fuente: Análisis de riesgo de la OTI

En la figura 25 siendo un 79.06 % respecto a todos los activos, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo bajo.

Siendo un 14.66% respecto a todos los activos, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo medio.

Siendo un 6.28% respecto a todos los activos, de las amenazas desde un rango de 3-5, de confidencialidad, integridad y disponibilidad, de la información se muestra que es un riesgo alto.

Discusión

Según Muñoz (2002), el número de elementos elegidos para una auditoria puede variar mientras el transcurso de la auditoria cambia. Sin embargo, en una auditoría externa. Esto se mantiene. Por lo que antes de hacer una auditoria por un consultor externo este debe haber realizado el análisis de riesgo y visualizar las políticas de seguridad de la información existente.

4.2. Análisis de la existencia de políticas de seguridad de la información - OTI

Antes de proponer las políticas de seguridad de la información se validó, si actualmente existe políticas de seguridad de la información basado en la norma técnica peruana 27001:2014. En la página 18 de esta norma, en la tabla A1. El objetivo de control y controles.

Según NTP ISO/IEC 27001, se debe verificar si existe políticas de seguridad de la información implementadas en el área.

A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

A.5.1. Dirección de la gerencia para la seguridad de la información.

NO EXISTE

A.5.1.1. Políticas para la seguridad de la información

Un conjunto de políticas para la seguridad de la información debe de ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes

Por lo cual se verifico, se consultó, no encontrando ninguna política de seguridad existente en la Oficina de Tecnologías de la Información.

4.2.1. Análisis de las encuestas realizadas a los trabajadores de la OTI

Para el segundo objetivo específico se realizó encuestas a los trabajares de la OTI, directa e indirectamente. Realizando técnicas de auditoria para la obtención de información exacta.

Lo cual se da en la siguiente tabla.

Tabla 14

Resultado de encuesta

PREGUNTAS	SI		NO		TOTAL	
	N.º	%	N.º	%	N.º	%
¿Existen políticas de seguridad de la información?	0	0%	12	100%	12	100%
¿Conoce Ud. La norma ISO/IEC 27001:2014 NTP?	3	25%	9	75%	12	100%
¿Existen lineamientos de seguridad de la información?	3	25%	9	75%	12	100%
¿Existe un área de seguridad de la información?	0	0%	12	100%	12	100%
¿Alguna vez sea divulgado información personal o privada?	2	17%	10	83%	12	100%
¿Existe un procedimiento o manual que ayude al manejo de información privada o restringida?	9	75%	3	25%	12	100%
Cuando está ausente en su puesto de trabajo, ¿Es de fácil acceso a personal no autorizado a su ordenador a cargo?	4	33%	8	67%	12	100%
¿Es monitoreado constantemente la información que manipula o modifica el usuario final (alumnos y estudiantes)?	11	92%	1	8%	12	100%
¿Realiza respaldos de la información al terminar sus labores diarias?	2	17%	10	83%	12	100%
¿Ha llevado archivos digitales para terminar en su casa por falta de tiempo?	0	0%	12	100%	12	100%
¿Constantemente actualiza los mecanismos de seguridad de la información?	7	58%	5	42%	12	100%
¿Los ordenadores a su cargo, tienen contraseñas?	8	67%	4	33%	12	100%
¿Realiza periódicamente cambio de contraseñas a los ordenadores, servidores, etc.?	2	17%	10	83%	12	100%
¿Utiliza mecanismo de cifrado para su memoria USB?	0	0%	12	100%	12	100%
¿Existe algún registro de fallas o ataques a través de la red?	11	92%	1	8%	12	100%
¿La infraestructura de gobierno electrónico está acorde a las normas o estándares establecidos por La secretaria de gobierno digital?	6	50%	6	50%	12	100%
¿La información que se transmite a través del área, tiene los 3 principios básicos de la seguridad de la información? – Confidencial – Integro – Disponible.	9	75%	3	25%	12	100%
¿Ha tenido alguna capacitación para mejorar la seguridad informática?	12	100%	0	0%	12	100%
¿Se hace teletrabajo?	0	0%	12	100%	12	100%
¿El usuario final conoce las normas o reglas existentes?	12	100%	0	0%	12	100%

Fuente: Resultado de encuesta.

En la tabla 14 respecto al conocimiento de la norma un 75% desconoce dicha norma. Y es primordial el conocimiento de esta.

Los lineamientos de seguridad un 75% respondieron que no existe lineamientos.

la seguridad de la información un 100% respondieron que no existe un área de la seguridad de la información.

Divulgación de la información un 17% afirma que se ha divulgado la información a terceros.

Procedimiento o manual para el manejo de la información un 25% respondieron que no existe procedimiento o manuales para el tratamiento de la información privada o restringida.

Ausencia en el trabajo un 33% afirmaron que es de fácil acceso a su área de trabajo.

Monitoreo de la información un 8% respondieron que no monitorean la información.

Respaldos de información un 83% respondieron que no realizan respaldos de información diaria.

Trabajo a casa un 100% afirma que no lleva archivos digitales para la casa.

Mecanismos de seguridad un 42% respondieron que no actualizan constantemente su firewall y antivirus

Contraseña en los ordenadores un 33% respondieron que no ponen contraseñas a los ordenadores a su cargo.

Realiza periódicamente cambios de contraseñas un 83% respondieron que no realizan cambios de contraseñas.

Cifrado en memorias USB. Un 100% respondieron que no usan ningún mecanismo de cifrado en sus memorias USB.

Registro de fallas un 8% respondieron que no existen un reporte de registro de fallas de seguridad

Gobierno electrónico un 50% afirmaron que si está acorde a las normas o estándares requeridos por la secretaria de gobierno digital.

Información trasmitida a través de la OTI, un 25% respondieron que no tiene los 3 principios básicos de seguridad.

Capacitación un 100% afirma que si se tuvo capacitaciones sobre seguridad informática.

Teletrabajo un 100% respondieron que no se realiza teletrabajo.

Usuarios finales, un 100% afirma que la población universitaria conoce las normas existentes en la OTI. Como se muestra en la tabla 6.

Discusión

Según Barrantes & Hugo (2012), nos menciona que cuando no se tiene implementado un Sistema de gestión de seguridad de la Información, aun si los empleados son capacitados de una manera eficiente, estos no están acordes para salvaguardar la información pertinente que manipulan durante un proceso. No está lejos esta situación los trabajadores de la OTI, que desconocen la normativa vigente, y mecanismos para salvaguardar la información.

Tabla 15

Análisis estadístico descriptivo

SI		***NO***		**TOTAL**
Media	5,65	Media	6,35	12
Mediana	5	Mediana	7	12
Moda	0	Moda	12	12
Desviación estándar	4,545385167	Desviación estándar	4,54539	9,0908
Varianza de la muestra	20,66052632	Varianza de la muestra	20,6605	41,321
Mínimo	0	Mínimo	0	0
Máximo	12	Máximo	12	24

Fuente: SPSS v.25

En la tabla 15 una *media* de conociendo respecto a la seguridad de la información menor al desconocimiento de la misma, esto nos evidencia claramente que si bien es cierto existe un conocimiento adecuado de los trabajadores de la OTI, pero sin embargo desconocen las políticas de seguridad de la información, por lo cual no ha sido implementado tales políticas que nos ayudan a un mayor control de la seguridad de la información.

4.2.2. Análisis para la propuesta de políticas de seguridad de la información.

Para lo cual se analizó otras políticas implementadas en otras instituciones pertenecientes al sistema nacional de informática, de las cuales no se mencionará el nombre, solo los parámetros en los cuales se pretende dar seguridad a la información, y poder estar apto para poder aplicar la norma técnica peruana ISO/IEC 27001.

El criterio de la valoración siempre es de forma individual, ya que no existe una normativa en la cual de un formato como debe de ser las políticas, sin embargo, menciona la NORMA TECNICA PERUANA, que debe ser acorde a las actividades de la organización.

Planteada por el encargado de la OTI, comunicada, y publicada para el usuario final.

Lo cual se realiza con la propuesta de políticas planteadas, al momento de la concientización realizada en la OFICINA DE TECNOLOGIAS DE INFORMACION DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO PUNO, ORGANISMO PERTENECIENTE AL SISTEMA NACIONAL DE INFORMATICA, de todo el personal que labora en la OTI, siendo un requisito indispensable para su posterior aprobación.

La propuesta de las políticas de seguridad de la información se encuentra en los anexos.

CONCLUSIONES

- De acuerdo al resultado de análisis de riego de la seguridad de la información respecto a los activos primordiales de la Oficina de Tecnologías de Información UNA PUNO, existen 12 riesgo de nivel alto, 28 riesgos de nivel medio y 151 riesgos de nivel bajo, siendo varios los criterios respecto a las amenazas que puedan vulnerar la información que administra la OTI, que permite delimitar el su estructura, siendo hoy en día la información en todas sus formas un activo primordial, al cual debe garantizarse su confidencialidad, integridad y disponibilidad.
- La propuesta de políticas de seguridad de la información coadyuvará con los controles de seguridad, a mejorar de una manera técnica, precisa, siendo un documento de gran jerarquía, con el cumplimiento adecuado de la misma. Promoviendo un alto grado de manejo de la información. Siendo acordes a las necesidades de la OTI, ya que se trabajó en conjunto de forma indirecta.

RECOMENDACIONES

- De acuerdo al análisis de riesgo, se debe mitigar las amenazas, para evitar que se vulnera la seguridad de la información, y se conviertan en riesgos existentes en la OTI, promoviendo estudios y capacitaciones de concientización acerca de los activos de la Universidad, en base a los principios básicos de seguridad, confidencialidad, disponibilidad e integridad, y a la vez podrá tomar diferentes criterios para una correcta administración de la información, mitigando futuras amenazas.
- La OTI debe Implementar las políticas de seguridad de la información, para el cumplimiento de la NTP ISO/IEC 27001, el cual permite la implementación de un Sistema de Gestión de Seguridad de la Información, que reduce riesgos asegurando la información, el activo primordial, dando el cumplimiento a lo establecido por la secretaria general de gobierno digital.

BIBLIOGRAFÍA

Aguilar, G. F. C., Peña, A. B., Ortiz, F. G. P., Lara, F. R. O., Villón, D. J. E., & Álvarez, D. M. L. (2018). Método para el aseguramiento de ingresos basado en análisis de riesgos y computación con palabras. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *27*(27), 126–140. https://doi.org/10.17013/risti.27.126-140

Aguirre, D. A. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del perú s.a.* (Tesis de pregrado). Pontificia Universidad Católica del Perú, Lima.

Albaneses, D., Argañaraz, A. A., Fernández, M. A., Goenaga, A., & Rivera, C. (2010). Identificación y análisis de riesgos organizacionales. Aplicación de una matriz de riesgos a una organización académica de educación universitaria. *ResearchGate*, *2010*(21), 101–122. https://www.researchgate.net/publication/258508531.

Aliaga, L. C. (2013). *Diseño De Un Sistema De Gestión De Seguridad De La Información Para Un Instituto Educativo*. (Tesis de pregrado). Pontificia Universidad Católica del Perú, Lima.

Altamirano, J. R., & Bayona, S. (2017). Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2017*(25), 112–134. https://doi.org/10.17013/risti.25.112-134

Alvarez, L. D. (2005). *Seguridad en informática (Auditoría de sistemas)* (Tesis de posgrado). Universidad Iberoamericana, Distrito Federal.

Angarita, A. A., Tabares, C. A., & Rios, J. I. (2015). Definición de un modelo de medición de análisis de riesgos de la seguridad de la información aplicando lógica difusa y sistemas basados en el conocimiento TT - Definition of a model for measuring risk analysis of security information applying fuzzy logic. *Entre Ciencia e Ingeniería*, *9*(17), 71–80. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672015000100010&lang=es%0Ahttp://www.scielo.org.co/pdf/ecei/v9n17/v9n17a10.pdf

Anguiano, M. E., & Trejo, A. (2013). Políticas de seguridad fronteriza y nuevas rutas de movilidad de migrantes mexicanos y guatemaltecos. *LiminaR. Estudios Sociales y Humanísticos*, *5*(2), 47. https://doi.org/10.29043/liminar.v5i2.250

Areitio, J. (2008). Principios basicos de seguridad de la información. In P. in Spain (Ed.), *Seguridad de la Informacion* (Clara M. d, p. 527). Magallanes.

Arévalo, J. G., Bayona, R. A., & Rico, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Revista Tecnura*, *19*(46), 123. https://doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10

Barrantes, C. E., & Hugo, J. R. (2012). *Diseño E Implementación De Un Sistema De Gestión De Seguridad De Información En Procesos Tecnológicos* (Tesis de pregrado). Universidad San Martin de Porres, Lima.

Bermudez, K. G., & Bailon, E. R. (2015). *Análisis En Seguridad Informática Y Seguridad De La Información Basado En La Norma Iso/Iec 27001- Sistemas De Gestión De Seguridad De La Información Dirigido A Una Empresa De Servicios Financieros*. Universidad Politécnica Salesiana sede Guayaquil, Guayaquil.

Casla, P., & Peréz, B. (2013). Red Española de Seguridad y Salud en el Trabajo: una red de información fundamental en el ámbito de la prevención de riesgos. *Med Segur Trab*, *59*(230).

Cortez, I. S., & Kubota, L. C. (2013). Contramedidas de segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. *Revista de Administração*, *48*(4), 757–769. https://doi.org/10.5700/rausp1119

Diéguez, M., & Cares, C. (2019). Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (32), 113–128. https://doi.org/10.17013/risti.32.113-128

Galeano, D. (2019). *Gestion de Incidentes de seguridad* (p. 38). p. 38. Ibagué: Alcaldia Municipal Ibagué.

García, G. (2018). Fluid work and the prevention of occupational risks: a needed revisit of occupational health and safety in today's information society. *Archivos de Prevención de Riesgos Laborales*, *21*(1), 5–6. https://doi.org/10.12961/aprl.2018.21.01.1

García, J. L. (2015). *Informe sobre el Peritaje Informático*. (Tesis de posgrado). Universidad II de Madrid, Madrid

Gobierno, M. (2015). *Política de Seguridad de la Información de la Universidad de Castilla-La Mancha* (Tesis de posgrado) Universidad de Castilla - La macha, La Castilla.

Gunea. (2018). Ciberseguridad: Concienciación y buenas prácticas para proteger tu negocio. Retrieved from http://e-forma.kzgunea.eus/mod/book/view.php?id=9920&chapterid=16244

Guzman, F. G. (2015). *Metodología para la seguridad de tecnologías de información y comunicaciones en la Clínica Ortega* (Tesis de posgrado). Universidad Nacional del Centro del Perú, Huancayo.

INDECOPI, C. de N. y de F. de B. C. no A.-. (2014). *NORMA TECNICA PERUANA Ntp-Iso / Iec 27001 Tecnología De La Información* . Lima: Secretaria de Gobierno digital del Perú.

ISO27001. (2010). Sistema de Gestión de la Seguridad de la Información. *Www.Iso27000.Es*, *1*, 14.

Leal, M. (2019). *Seguridad física y ambiental*.

Macen, R. C. D. (2014). *Politicas de Seguridad de la Información* (Tesis de posgrado).

Universidad Tecnológica Intercontinental, Asunción.

Martelo, R. J., Maderay, J. E., & Betín, A. D. (2015). Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Informacion Tecnologica*, *26*(2), 129–134. https://doi.org/10.4067/S0718-07642015000200015

Melchor, J., Lavín, J., & Pedraza, N. A. (2012). Security in the data management and quality of accounting information systems for organizational performance. *Universidad Autónoma de Tamaulipas*, *57*(4), 11–34. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0186-10422012000400002&lang=pt

Mercado Rojas, J. E. (2016). *Modelo de gestión de seguridad de la información para el E-Gobierno* (Tesis de posgrado). Universidad Nacional Mayor de San Marcos, Lima.

Molina, C. D., Gascón, J. P., Blanco, J. J. P., & R.Antigüedad, M. A. (2010). *Ciber-terrorismo Definición de políticas de seguridad para proteger infraestructuras críticas frente a ciber-ataques terroristas* (Tesis posgrado). Universidad Europea de Madrid, Madrid.

Muñoz, F. (2013). Retos para el siglo XXI en la seguridad de procesos y análisis de riesgos. *Revista de Ingeniería Dossier*, (37), 48–49. https://doi.org/10.16924/riua.v0i37.118

Muñoz, R. C. (2002). Analisis de riesgos. In M. G. Trujano (Ed.), *Auditoria en Sistemas* (Primera Ed, p. 805). Mexico: Pearson Educacion.

Oramas, I., & Figueroa del Valle, D. (2014). Análisis de riesgos para el trabajo con un analizador de diagnóstico de cámaras gamma. *Ciencias Nucleares - Nucleos*, (55), 19–23.

Ortega, J. R. (2014). El concepto de información: dimensiones bibliotecológica, sociológica y cognoscitiva. *UNAM*, *28*, 143–179.

Pacheco, J. E. (2015). *Plan para elaborar Politicas de Seguridad de informacion para un*

departamente de Tecnologia de la Unviersidad de San Carlos de Guatemala. (Tesis de pregrado). Universidad de San Carlos de Guatemala, Guatemala.

Piattini, M. G., & Navarro, E. del P. (2001). Analisis de riesgos, vulnerabilidaddes. In V. M. G. Piattini (Ed.), *Auditoria Informática un enfoque practico* (2º edicion, p. 649). Castilla - La Mancha: Freelibros.

Rayme Serrano, R. A. (2007). *Gestión de seguridad de la información y los servicios críticos de las universidades : un estudio de tres casos en Lima Metropolitana* (Tesis de posgrado). Universidad Nacional Mayor de San Marcos, Lima.

Romero, M. I., Figueroa, G. L., Vera, D. S., Álava, J. E., Parrales, G. R., Álava, C. J., … Castillo, M. A. (2018). Mecanismo Correctivos en seguridad informática. In 17 - 03802 - ALCOY (ALICANTE) info@3ciencias.com C/ Els Alzamora (Ed.), *Introducción a la seguridad informática y el análisis de vulnerabilidades* (Ingeniería). https://doi.org/10.17993/ingytec.2018.46

Santos Llanos, D. E. (2016). Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la iso/iec 27001:2013, para una empresa de consultoría de software (Tesis pregrado). Pontificia Universidad Católica Del Perú, Lima.

Solís, F., Pinto, D., & Solís, S. (2017). Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema Android utilizando el método de encriptación RSA. *Enfoque UTE*, *8*(1), 160. https://doi.org/10.29019/enfoqueute.v8n1.123

Solórzano, P. M. A., & Contreras, A. R. (2019). Seguridad, tecnologías de la información y derechos humanos: impunidad gubernamental e inercia ciudadana. *Revista Ius*, *13*(44), 281–303. https://doi.org/10.35487/rius.v13i44.2019.452

Tarazona, C. H. (2015). Amenazas Informáticas y seguridad de la informacion. *Etek Internacional*. Retrieved from https://revistas.uexternado.edu.co/index.php/derpen/article/view/965

Tibaquira, C. A. Y. (2015). *Metodología De Gestión De Incidentes De Seguridad De La Información Y Gestión De Riesgos Para La Plataforma Siem De Una Entidad*

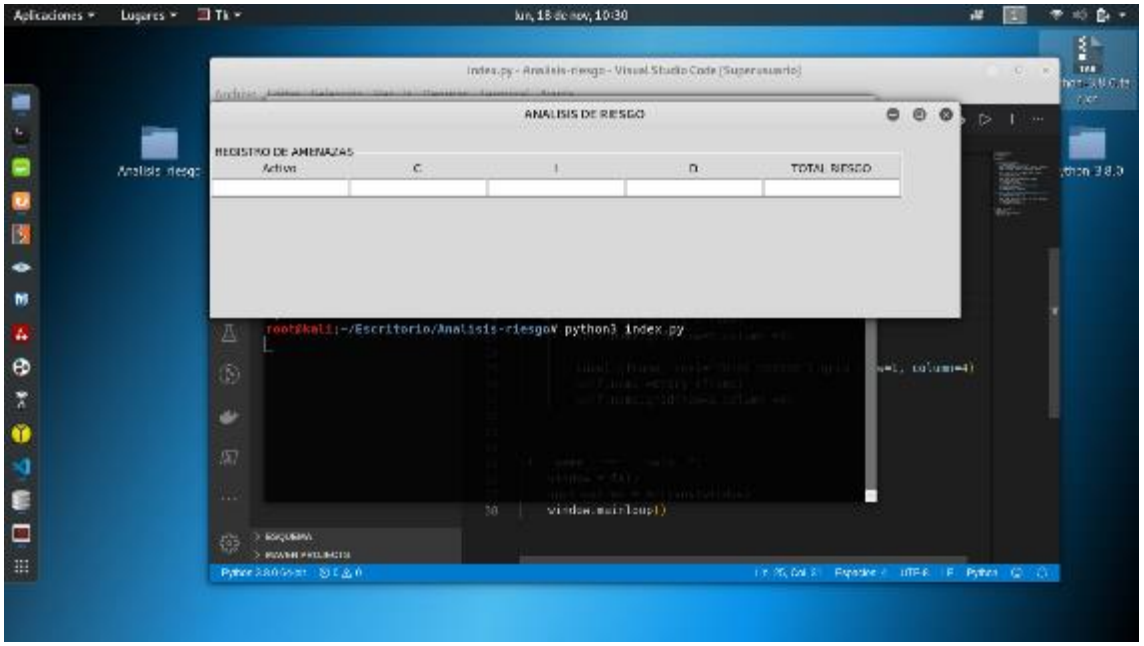
Financiera Basada En La Norma Iso/Iec 27035 E Iso/Iec 27005 (Tesis de especialidad) Universidad nacional abierta y a distancia escuela de ciencias básicas, Bogota.

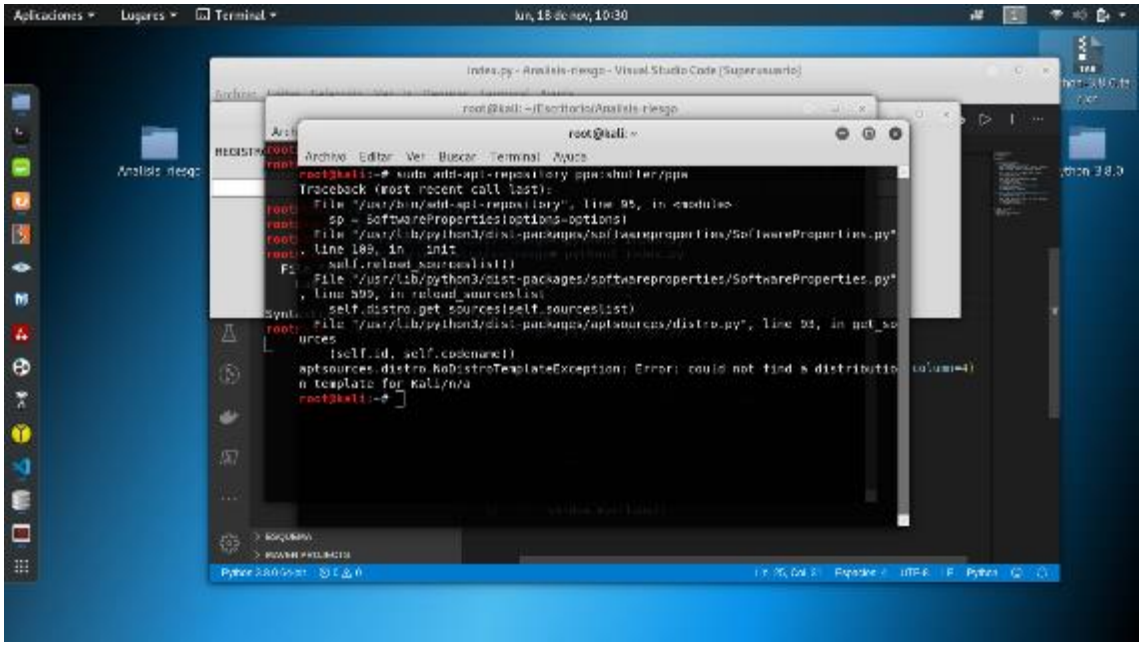
Web. (2018). politicas. Retrieved from https://www.pmg-ssi.com/2016/06/que-debe-incluir-en-su-politica-de-seguridad-de-la-informacion-basado-en-la-norma-iso-27001/

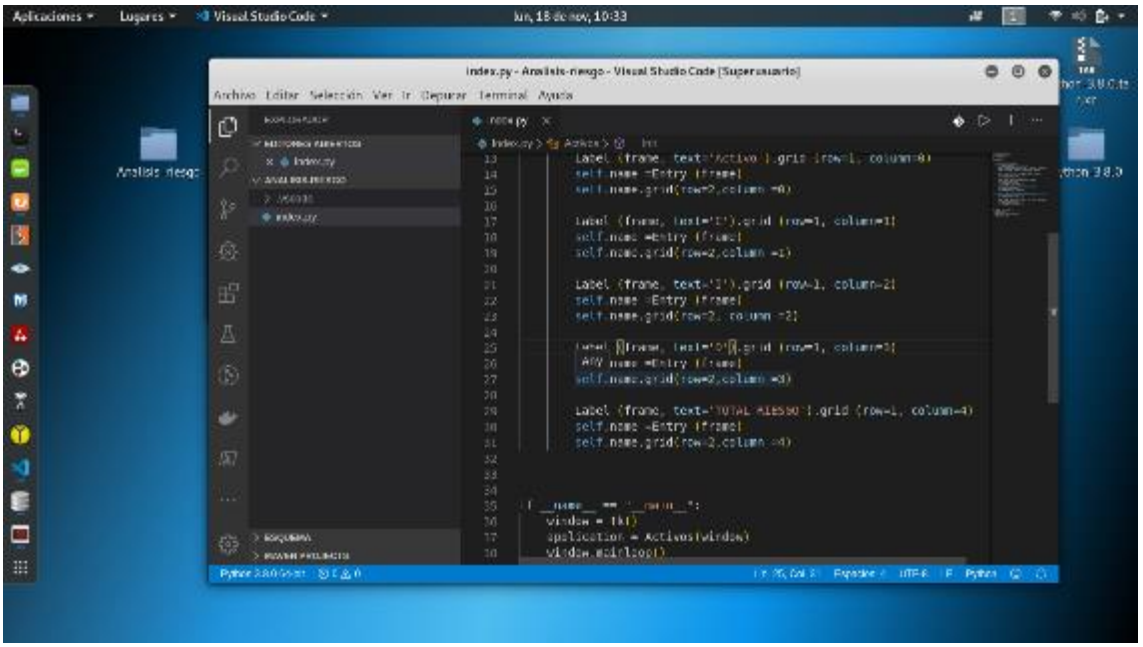
Web Seguridad. (2019). Seguridad De La Información. *Https://Www.Agro.Uba.Ar/Uti/Servicios/Seguridad_informacion*. https://doi.org/10.13128/ijae-9077

ANEXOS

Anexo 1. Programa para la recolección de información - registro de amenazas







Anexo 2. Encuesta – OTI

CON EL OBJETIVO DE EVALUAR, SI EXISTE POLITICAS DE SEGURIDAD INFORMATICA, Y A TRAVES DE ESTA IMPLEMENTAR A LA VEZ, DIRECTIVAS PARA UNA MEJOR GESTION DE LA SEGURIDAD DE LA INFORMACION.

DATOS GENERALES: FECHA DE AUDITORIA: DIA……MES……..AÑO……

NOMBRE A EVALUAR.

PERFIL: **FIRMA**

PREGUNTAS	**SI**	**NO**
1. ¿Existen políticas de seguridad de la información?		
2. ¿Conoce Ud. La norma ISO/IEC 27001:2014 NTP?		
3. ¿Existen lineamientos de seguridad de la información?		
4. ¿Existe un área de seguridad de la información?		
5. ¿Alguna vez sea divulgado información personal o privada?		
6. ¿Existe un procedimiento o manual que ayude al manejo de información privada o restringida?		
7. Cuando está ausente en su puesto de trabajo, ¿Es de fácil acceso a personal no autorizado a su ordenador a cargo?		
8. ¿Es monitoreado constantemente la información que manipula o modifica el usuario final (alumnos y estudiantes)?		
9. ¿Realiza respaldos de la información al terminar sus labores diarias?		
10. ¿Ha llevado archivos digitales para terminar en su casa por falta de tiempo?		

11. ¿Constantemente actualiza los mecanismos de seguridad de la información?		
12. ¿Los ordenadores a su cargo, tienen contraseñas?		
13. ¿Realiza periódicamente cambio de contraseñas a los ordenadores, servidores, etc.?		
14. ¿Utiliza mecanismo de cifrado para su memoria USB?		
15. ¿Existe algún registro de fallas o ataques a través de la red?		
16. ¿La infraestructura de gobierno electrónico está acorde a las normas o estándares establecidos por La secretaria de gobierno digital?		
17. ¿La información que se transmite a través del área, tiene los 3 principios básicos de la seguridad de la información? – Confidencial – Integro – Disponible.		
18. ¿Ha tenido alguna capacitación para mejorar la seguridad informática?		
19. ¿Se hace teletrabajo?		
20. ¿El usuario final conoce las normas o reglas existentes? - No alterando los tres principios de la seguridad. - No Alterando la fiabilidad y veracidad de la información consultada, modificada por cualquier medio informático.		

Anexos 3. Propuesta de políticas de seguridad de la información

UNIVERSIDAD NACIONAL DEL ALTIPLANO PUNO

POLÍTICAS DE SEGURIDAD DE LA INFORMACION

OFICINA DE TECNOLOGIAS DE INFORMACION

ROL	NOMBRE	UNIDAD / CARGO	FECHA	FIRMA
Elaborado por:	ING. SAULO GUSTAVO MACHICAO MOLLOCONDO	EPG - MAESTRIA INFORMATICA / TESISTA	04/05/2019	
Aprobado por:	ING. RENE LEONIDAS ARAUJO COTACALLAPA	OTI - UGD / JEFE UGD	28/11/2019	

ÍNDICE

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCION

Las POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN son conjuntos de lineamientos que proporcionan dirección y apoyo, estableciendo un marco de referencia sustentado por normas técnicas y/o procedimientos internacionales aprobados por la secretaria de gobierno digital (Antes ONGEI). Por lo cual será el medio adecuado de actuar del personal a cargo de los recursos informáticos de la OTI – UNA PUNO.

La OTI es el órgano encargado de organizar, diseñar, dirigir y mantener renovado los sistemas de información automatizada; estos sistemas necesitan políticas de seguridad, para que la información sea reconocida como el principal de sus activos, para un mejor intercambio y desarrollo en el ámbito de sus funciones. Por lo cual estos procesos deben tener una infraestructura segura, y así salvaguardar la información minimizando riesgos preexistentes o futuros asociados a la seguridad y los costos de administración y operaciones.

La presente propuesta de POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, contiene los puntos mas importantes y acciones necesarias para normar en la prevención y contingencias futuras relacionadas a las TIC de la OTI. Siendo cuidadosamente estudiada, analizada y planteada, a fin de no topar con los Derechos Humanos y convirtiéndose en una traba para poder realizar las funciones, y mas bien muestra una forma adecuada de gestionar la seguridad de la información, respetando lineamientos y normas aprobadas vigentes.

La OTI, tiene que asegurar la información que maneja, o al menos prevenir en gran medida de lo posible, que la información o los servicios sean vulnerados por incidentes de seguridad. Para ello, se deberá conducir un sistema de gestión de seguridad de la información, en concordancia con las recomendaciones contenidas en NORMA TÉCNICA NTP-ISO/IEC 27001 PERUANA 2014.

El objetivo de la seguridad de la información es garantizar la calidad de la información y el normal funcionamiento de las TIC en la OTI, destinado a preservar la confidencialidad, la integridad y la disponibilidad de la información.

2. ALCANCE

El presente documento de gestión interna contiene; Políticas de seguridad de la información, de la Oficina de Tecnologías de Información, que tiene por establecer lineamientos de gestión para practicas seguras de manejo de la seguridad de la información, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad de la información y el fortalecimiento información.

La OTI, va a evitar o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidencias de seguridad. Para ello debe implementar medidas mínimas de seguridad determinadas por la secretaria de gobierno digital.

3. BASE LEGAL

Las normas legales relacionadas con el tema de políticas de seguridad de la información, que rigen para el sector público, se consideran:

- Constitución Política del Estado.
- Ley Nº 30096 Ley de delitos informáticos.
- Secretaria técnica, de conformidad con el decreto legislativo 1030, el decreto legislativo 1033, el decreto supremo 081-2008-PCM y la resolución 048-2008/CNB-INDECOPI, la comisión con el acuerdo unánime de sus miembros, APROBAR, NTP-ISO/IEC 27001:2014 TECNOLOGIA DE LA INFORMACION, técnicas de seguridad de la información, requisitos 2ª Edición Reemplaza a la NTP-ISO/IEC 27001:2008 (REVISADA EL 2013).
- R.M. N° 004-2016-PCM y sus modificatorias.
- Código Penal – Delitos Informáticos.

4. GLOSARIO DE TERMINOS

Acceso: Provee medios para controlar la información que los usuarios pueden utilizar, los programas que pueden ejecutar y las modificaciones que pueden hacer. Los controles pueden estar en el sistema operativo, aplicaciones, bases de datos, dispositivos de red y utilerías.

Activos: Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Administrador: Es la actividad que realiza una persona que presta el servicio a través de control de los medios electrónicos, manteniendo al mismo tiempo, los niveles adecuados de seguridad y procurando la mejora de la calidad de los servicios.

Back-up: Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Confiabilidad: Un sistema en el cual la información que se comparte es confiable y viaje por un medio seguro, sin sufrir ninguna alteración.

Confidencialidad: Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

Contingencia: Una estrategia constituida por un conjunto de recursos de respaldo de toda la información frente a una emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información.

Custodia: Conserva la integridad física y lógica de una prueba. Identificación donde se realizó un ataque y recolectando la prueba, pasando a su registro y almacenamiento, y posterior traslado para un análisis final.

Delitos: Son los cometidos a través de cualquier medio electrónico, con el fin de perjudicar el sistema, y la integridad de la información.

Disponibilidad: Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados

cuando éstos lo requieran. Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.

Divulgación: Es la tarea de procesar y difundir el conocimiento científico (POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN) de un modo que resulte accesible para el público general.

Electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

Fortalecimiento: Es asegurad la información previniendo antes que ocurra, detectando la presencia de agentes no deseados y correctivos para actuar luego de lo ocurrido.

Fuga de Información: La fuga de información o la fuga de datos, es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

Gestión: Es todo lo que tiene que ver con obtener la información correcta, en la forma adecuada, para la persona indicada, al costo correcto, en el momento oportuno, en el lugar indicado para tomar la acción precisa.

Integridad: La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

Legalidad: Cuando se habla de legalidad se hace referencia a la presencia de un sistema de leyes que debe ser cumplido y que otorga la aprobación a determinadas acciones, actos o circunstancias, y como contrapartida desaprueba a otras tantas que afectan las normas establecidas y vigentes.

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

OTI: Oficina de Tecnologías de Información.

Política: es aquella que tiene medidas y acciones que indican los puntos principales en el ámbito de sistemas, para la protección y seguridad de los datos y medios de información

SGSI: Sistema de Gestión de Seguridad de la Información, parte de un sistema global de gestión, basado en el análisis de riesgos, establece, implementa, opera y monitoriza, revisa, mantiene y mejora la seguridad de la información.

Vulnerabilidad: Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos.

5. ORGANIZACIÓN DE LAS POLITICAS DE SEGURIDAD INFORMÁTICA

Se ha organizado en grupos de políticas, según se aprecia a continuación:

- Políticas generales
- Políticas sobre seguridad de la información
- Políticas y organización del sistema de gestión de seguridad de la información (SGSI).
- Políticas sobre seguridad física y ambiental.
- Políticas sobre seguridad lógica.
- Políticas de gestión de activos.
- Política de respaldo (back-up) de información.
- Políticas de seguridad en las telecomunicaciones.
- Políticas de gestión de incidentes de la seguridad de información.
- Política de administración de recursos.
- Políticas de seguridad para aplicaciones en la nube.
- Políticas de cumplimiento.

5.1. POLÍTICAS GENERALES

La OTI, es el órgano encargado de organizar, diseñar, dirigir y mantener renovado los sistemas de información automatizada; así como desarrollar y administrar los recursos informáticos de la Universidad Nacional del Altiplano de acuerdo a los lineamientos del gobierno electrónico. Donde se propone implementar POLÍTICAS

DE SEGURIDAD DE LA INFORMACIÓN, para la prevención de fuga de información y al fraude informático, buscando la razonable gestión de incidentes de Seguridad de Información en los activos de información dentro del alcance del sistema.

Las políticas consideradas en este grupo son aquellas que están relacionadas a la propiedad, conocimiento, sanciones y responsabilidades de toda política, norma y procedimiento sobre seguridad informática establecida por la OTI.

OBJETIVOS

- Asegurar la implementación del Sistema de Gestión de Seguridad de la Información, capacitando al personal que labora en la OTI.
- Asegurar los controles implementados, y su coherencia con la estructura de la información y riesgos administrados por la OTI.
- Asegurar los servicios y subcontrataciones vinculadas a tecnologías de información cumplan con requisitos de seguridad para asegurar la calidad del servicio brindado (capacitaciones dirigidas por la OTI).
- Asegurar que los servicios brindados cumplan con las buenas practicas y controles mínimos exigidos por la regulación.
- Definir el propietario de las políticas, normas y procedimientos de seguridad informática emitidas por la OTI, estableciendo privilegios de acceso y restricciones sobre su divulgación por parte del personal que labora.

ALCANCE

- El alcance del SGSI de la OTI comprende la implementación de controles generales a nivel de toda la universidad y luego concentrarse en procesos cuyo manejo de información resultan altamente sensible para la universidad. Estos procesos son:
  - Proceso de admisión a la universidad (registro de alumnos usuario y contraseña).
  - Proceso de registro y control de notas (docentes).
  - Proceso de registro y control de coordinaciones académicas (personal administrativo).

5.2. POLÍTICAS SOBRE SEGURIDAD DE LA INFORMACIÓN

- La información es uno de los activos mas importantes para el desarrollo de la gestión universitaria. Es responsabilidad de la OTI, velar por el cumplimiento de las políticas, lineamientos y procedimientos de seguridad de la información.
- La OTI debe establecer un programa de capacitación con el fin de crear una cultura de seguridad de la información.
- Los usuarios finales que tengan acceso, a la consulta o modificación, de la información (alumnos, docentes y administrativo) deben desarrollar sus funciones dentro de la normativa establecida por la universidad para así cumplir los lineamientos de la seguridad de la información y manteniendo una actitud proactiva en la gestión de los mismos.
- El nivel de seguridad de la información a implementarse debe considerar el nivel de riesgo y el valor de la información, siguiendo criterios de eficacia y eficiencia.
- La OTI definirá procedimientos en casos en que no se pueda cumplir con las políticas de Seguridad, siguiendo criterios de aceptación del riesgo.
- El incumplimiento de estas políticas de Seguridad de la Información estará sujeto a sanciones de acuerdo a los indicado en el reglamento interno de trabajo de la OTI.
- La OTI debe implementar un contrato de confidencialidad de la información que maneja el personal que labora.

5.3. POLÍTICAS Y ORGANIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- Se debe contar con un manual de procesos de seguridad de información que establezca los mecanismos para definir y revisar las políticas de sistema de gestión de seguridad de la información en la OTI, los roles y responsabilidades dentro de la oficina respecto a la seguridad de la información.
- Con un periodo no mayor de 2 años se debe realizar una revisión y actualización de las políticas de seguridad de la información, así como la gestión de la seguridad de la información en la OTI.

5.4. POLÍTICAS SOBRE SEGURIDAD FÍSICA Y AMBIENTAL

- El área de la OTI y cada unidad (desarrollo y sistemas informáticos, gobierno electrónico, redes y telecomunicaciones) es responsable que los equipos de

cómputo central a su cargo cuenten con los controles físicos y ambientales necesarios para un adecuado funcionamiento.

- La OTI en concordancia con cada unidad, establecerá los requerimientos técnicos necesarios y se formalizará en un documento estándar de seguridad física y ambiental para su implementación por cada área responsable.
- La OTI debe establecer que todo lugar donde se instalen o se almacene recursos informáticos, debe contar con las medidas de seguridad necesaria y cumplir con los requerimientos técnicos especificados y recomendados por el proveedor de recursos informáticos, a fin de garantizar su integridad y seguridad.
- La OTI debe establecer un programa de monitoreo de cumplimiento de los controles de acceso.
- Toda instalación de recursos informáticos es función exclusiva de la OTI. Por lo cual está prohibida la instalación de equipos informáticos por personal no autorizado por dicha unidad.

5.5. POLÍTICAS SOBRE SEGURIDAD LÓGICA

- La asignación de accesos en los sistemas de información e infraestructura se debe realizar bajo un concepto de perfiles basados en roles.
- La OTI debe establecer los estándares para la creación de usuarios y contraseñas de todos los usuarios de la universidad, la cual comprende.
    - Identificador de usuario.
    - Longitud y formato de la contraseña.
    - Periodo en el cual se debe cambiar la contraseña.
    - Periodo para la reutilización de la clave.
    - Periodo de bloqueo de pantalla.
    - Periodo para el termino de sesión.
- La OTI es responsable de implementar procedimientos de creación de usuario y contraseña y de control de accesos para asegurar el uso de los sistemas y recursos de información a personal autorizado.
- Todo recurso informático que participe en forma directa en el intercambio de información de la red, debe tener una identificación o dirección electrónica única, con la finalidad de garantizar el correcto trafico de la información en la red.

- Todo el personal que labore en la OTI, bajo cualquier régimen o modalidad, de acuerdo a sus funciones asignadas por la universidad, deberá acceder a la información electrónica, lo hará mediante un identificador de usuario (USER-ID)
- La OTI es responsable de implementar procedimientos de control de accesos para asegurar el uso de los sistemas y recursos de información a personal autorizado.
    - Controles automáticos para prevenir accesos no autorizados en caso de equipos informáticos desatendidos.
    - Controles de accesos de usuarios remotos.
    - Controles de accesos físico y lógico a puertos de diagnóstico y de configuración de los equipos de cómputo.
    - Medidas que restrinjan la instalación de programas o utilitarios (como restricción de administrador local) que permitan eludir controles establecidos (firewall, antivirus, puertos usb, etc).
    - Uso de Tablets y smartphones.
- Todo uso indebido de los identificadores de usuario o de los privilegios de acceso otorgados por la OTI, son considerados "Delitos Informáticos", conforme lo establece Código Penal.
- Todo el personal que labora en la OTI, que se le haya asignado una identificación de usuario tiene derecho y la obligación de usar una contraseña personal, exclusiva y confidencial. Por este motivo, se considera que todo acceso o alteración de información electrónica efectuada con una identificación de usuario es realizado por dicho usuario.
- Todo acceso no autorizado a los servicios informáticos que administra la OTI, es considerado un "Delito Informático".

5.6. POLÍTICAS DE GESTIÓN DE ACTIVOS

- La OTI debe establecer normas y procedimientos relativos a la gestión de activos en donde se defina.
    - Establecer propietarios y custodios de los activos de información.
    - Las responsabilidades sobre los activos de información.
    - Los mecanismos para la clasificación de la información.
    - Recomendaciones para un manejo de la información en la universidad, la cual incluye los soportes de almacenamiento.

- La OTI debe elaborar y mantener un inventario de sus activos de información, asociados a cada proceso, sus propietarios y ubicación. El inventario será actualizado una vez al año o ante cualquier modificación de la información registrada; lo que suceda primero.
- La responsabilidad de uso de los activos de información recae en el administrador de la información (OTI) y de los procesos que manipula, sean estos manuales o electrónicos. Aunque tenga autoridad formal, no significa que tenga derechos de propiedad el activo.

5.7. POLÍTICA DE RESPALDO (BACK-UP) DE INFORMACIÓN

- La OTI debe establecer las normas con el diseño de los controles, estándares y procedimientos para:
  - Alcance de los sistemas que deben contar con copias de respaldo.
  - El mecanismo de respaldo (incremental o full) que tendrá cada sistema.
  - Condiciones de almacenamiento para un adecuado funcionamiento del respaldo.
  - Periodo de almacenamiento.
  - Ubicación de la segunda copia de respaldo.
  - La frecuencia de las pruebas de restauración.
- La OTI debe implementar los controles en base a las normas y estándares definidos, para este fin debe presentar un plan de trabajo para la adecuación de dichas normas.
- La OTI debe establecer un programa de seguimiento de cumplimiento del plan de trabajo para la implementación de los controles definidos.
- La OTI debe establecer un programa de monitoreo de cumplimiento de los controles de acceso.

5.8. POLÍTICAS DE SEGURIDAD EN LAS TELECOMUNICACIONES

- La OTI debe establecer las normas, estándares y procedimientos para:
  - Los controles para la administración de la seguridad de las redes.
  - Los mecanismos de seguridad asociados a los servidores de red.
  - Segmentación y segregación de redes.
  - Intercambio de información con entidades externas.

- La OTI debe implementar los controles en base a las normas y estándares definidos, para este fin deben presentar un plan de trabajo para la adecuación de dichas normas.
- La OTI debe establecer un programa de seguimiento de plan de trabajo para la implementación de los controles definidos.
- La OTI debe establecer un programa de monitoreo de cumplimiento de los controles de acceso.

5.9. POLÍTICAS DE GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE INFORMACIÓN

- La gestión de incidentes de seguridad será definida en un procedimiento específico para este fin.
- La OTI debe capacitar a todo el personal que tenga acceso legítimo a los sistemas de información y recursos informáticos, con el fin de proteger la integridad, confidencialidad y disponibilidad de la información. La política aplica a todo el personal que labora y toda persona que tengan contacto con la infraestructura tecnológica de forma física, lógica, remota.
- La OTI revisará periódicamente los incidentes ocurridos y se generará un "archivo de incidentes" para su posterior almacenamiento.
- La OTI designara a un personal para poder analizar el "archivo de incidentes" con el fin de determinar las causas y analizar el comportamiento del evento (Recurrencia, impacto, relación con otros eventos).
- En caso de que los incidentes determinen un evento de interrupción significativa de operaciones, se debe incluir un reporte basado en los procedimientos de operaciones específicos para el servicio impactado.

5.10. POLÍTICA DE ADMINISTRACIÓN DE RECURSOS

Las políticas sobre la administración de los recursos informáticos, buscan evitar posibles riesgos que afecten la operación de los sistemas informáticos, a causa de manipulaciones indebidas o por desconocimiento.

- La OTI es el ente encargado de administrar los equipos informáticos de propiedad o en alquiler de la universidad, para lo cual debe realizar actividades como el registro, traslado, instalación, asignación, mantenimiento, configuración

y custodia de los equipos informáticos de propiedad de la Universidad Nacional del Altiplano.

- Está prohibido que el personal no autorizado por la OTI, realice alguna actividad de traslado o instalación o mantenimiento o configuración de equipos informáticos, siendo excepciones a esta prohibición el traslado de los equipos portátiles y la custodia de equipos informáticos que estén asignados a los usuarios finales.
- La OTI es el ente encargado de la administración de software, para lo cual realiza acciones, de registro, instalación, actualización y configuración del mismo en los equipos informáticos de la universidad, respetando los derechos de autor, el numero de licencia y la propiedad intelectual del software.
- Esta prohibido que el personal no autorizado por la OTI, realice alguna actividad de instalación o actualización o configuración de software, en los equipos informáticos de la universidad. Categorías de software no autorizadas por la OTI, incluyen programas tales como: juegos, protectores de pantalla, aplicativos particulares, aplicativos recibidos por la red o a través de internet, aplicativos entregados en calidad de prueba, empaquetadores. Etc.
- La OTI, también está encargada de aprobar los requerimientos, las evaluaciones de proveedores, la recepción y los servicios, que estén relacionados en forma directa o indirectamente con el software de la Universidad.
- La OTI, es el encargado de la administración de correo electrónico, para lo cual debe asegurar su operación continua, mantener actualizadas las cuentas, tomar medidas de seguridad contra virus y controlar el uso debido del correo por parte de los usuarios finales.
- La OTI, es el encargado de administrar las copias de respaldo (back-up), concerniente a la información sensible de los activos de la universidad y que son compartidos a través de la red. Para esta función debe realizar estudios sobre información sensible, como la identificación, que tan critico resulta para la universidad, que tanto cambia en el tiempo, volumen de la información, etc. Con estas actividades determina la importancia de la información, la periodicidad, tiempo de retención y cantidad de las copias de respaldo.
- La OTI debe verificar que las copias de respaldo cumplan su objetivo, para lo cual debe realizar pruebas de recuperación de la información sensible, a fin de garantizar que los procesos y los medios de respaldo funcionen correctamente.

- La OTI debe establecer un plan de contingencia que responda eficazmente a las necesidades de continuidad del servicio informático. Con el siguiente nombre. Plan de emergencia que tiene como objetivo el contener el daño causado por un desastre, Plan de respaldo que tiene como objetivo mantener los servicios críticos de la operación y el plan de recuperación tiene el objetivo de restaurar temporal o permanentemente la capacidad de los servicios informáticos. Estos planes para garantizar la efectividad deben ser probados en su totalidad.
- La OTI es el órgano encargado de administrar todos los desarrollos de proyectos informáticos de la universidad, por lo cual debe registrar desde el requerimiento inicial del usuario hasta el descarte o conclusión de los proyectos.
- La OTI es el órgano encargado de administrar todos los mantenimientos a las aplicaciones solicitadas por los usuarios, debiendo empezar desde el requerimiento inicial del usuario hasta el descarte o conclusión del mantenimiento.

La OTI debe contar con herramientas necesarias para el control de los mantenimientos de aplicaciones.

5.11. POLÍTICAS DE SEGURIDAD PARA APLICACIONES EN LA NUBE

La contratación y adopción de servicios en la nube como estrategia para soportar los procesos y servicios públicos de las entidades de la Administración Pública introduce un amplio número de beneficios para que estas puedan innovar, reducir costos en sus procesos y brindar soluciones ágiles; sin embargo, y, aun con los beneficios indicados, emergen riesgos que requieren ser controlados y gestionados adecuadamente. Más aun, es condición necesaria que la contratación y adopción de servicios en la nube se enmarque dentro de los requisitos exigibles por los marcos legales existentes y en la adopción de guías de buenas prácticas de dichos marcos, como los relativos a seguridad de la información y, en su caso, correspondiente del presente lineamiento, los vinculados con la protección de datos personales

- La OTI debe tener el control absoluto de todos los dispositivos que se conectan a través de la red propiedad de la universidad y dispositivos (portátiles, tables y móviles) que se conectan a través de aplicaciones web para el acceso de la información.
- La OTI debe verificar constantemente que dispositivos móviles se conectan a la red, el uso y tráfico, tiempo y que paginas están accediendo por este medio.

Registrar los usuarios frecuentes con el que accede por este medio a través de aplicaciones web.

- La OTI debe tener la capacidad de bloquear o permitir aplicaciones nativas en tiempo real.
- La OTI debe bloquear aplicaciones web móviles, para evitar perdida de información por las brechas de seguridad en las aplicaciones móviles existentes.
- La OTI debe aplicar políticas de seguridad en base a cada usuario, ubicación y tipo de dispositivo que se conecta a través de las aplicaciones web para acceder a la red.
- La OTI debe mantener la seguridad efectiva y controles de políticas ajustables a cada dispositivo electrónico de uso de tecnologías de la información. Utilizar herramientas de reportes para visualizar cual es el impacto de las políticas frente a los usuarios y la red e identificar y solucionar inconvenientes en tiempo real.

5.12. POLÍTICA DE CUMPLIMIENTO

- Lineamientos para asegurar el cumplimiento de las políticas y normativa de seguridad de información por la OFICINA DE TECNOLOGÍAS DE INFORMACIÓN.
- La OTI exigirá al personal y usuarios finales, de bienes y servicios se adhieran obligatoriamente a lo establecido en la presente POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. Regulado por el ISO 27001:2014 y código penal del Perú.
- La OTI tomara acciones, medidas administrativas y acciones legales, si fuera necesario en cualquier falta cometida conforme lo establece las POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

6. SANCIONES PREVISTAS POR INCUMPLIMIENTO

La OTI administrará todos los incidentes y propondrá las sanciones al personal y usuarios finales (docentes, coordinaciones académicas y estudiantes) a partir de una minuciosa investigación y comprobación fehaciente de los hechos, de acuerdo a los lineamientos y normas establecidas en la presente POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. Las sanciones serán públicas o reservadas, según sea el caso. Sin vulnerar los derechos humanos.

7. DISPOSICIONES FINALES

- La OTI propondrá un área de seguridad informática con el que actualizará el presente documento de acuerdo a las necesidades y requerimientos establecidos por la Secretaria de Gobierno Digital.
- La OTI difundirá el presente documento, para que así el personal que labora dentro de la misma pueda conocerlo.
- La OTI de acuerdo a las necesidades realizara una auditoria interna para verificar el cumplimiento de las POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN planteadas en el presente documento.
- Quedan sin efecto las disposiciones administrativas que se opongan o contravengan a lo dispuesto en el presente documento.