UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

UNIVERSIDAD ANDINA DEL CUSCO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

FORMULACIÓN DE UN PLAN DE ACTIVIDADES DE LA CLÁUSULA GESTIÓN DE COMUNICACIONES Y OPERACIONES DE LA NTP-ISO/IEC 17799:2007, PARA SU IMPLEMENTACIÓN EN LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA ZONA REGISTRAL N°X SEDE CUSCO - SUNARP

Autores:

Bach. Claudia Lisseth Gamarra Zavaleta

Bach. Jorge Vargas Acosta

“PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS”

Asesor:

Mgt. Ing. Emilio Palomino Olivera

Cusco - Perú - 2015

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

DEDICATORIA

A mi madre, Maria Elsa, por confiar y creer siempre en mí, por su apoyo constante día a día, por su gran amor y calor de madre, por ser un gran ejemplo de mujer y por ser hoy lo que soy gracias a ella.

A mi padre, Carlos Antonio, por ser siempre mi modelo a seguir, por enseñarme que no hay problema alguno que no se pueda resolver si estamos todos juntos, por ser hoy lo que soy gracias a él y en especial porque sé que este gran paso en mi vida será también un triunfo para él.

A mis hermanos, Carlos Eduardo y Erika Lucia, por sacarme siempre una sonrisa cuando estamos juntos y por ser la felicidad constante que me motivó para la culminación de este proyecto.

A mis abuelos, Maria Lourdes y David Ángel y a mi tía Cristina, por brindarme siempre cariño sincero, apoyo incondicional y calor de familia.

.

Claudia Lisseth Gamarra Zavaleta

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

DEDICATORIA

A mi madre María Teresa:

Por ser el pilar más importante, por su apoyo incondicional en todo momento de mi vida, por sus consejos, comprensión, valores, esfuerzo, dedicación y motivación que me ha permitido ser una persona de bien, por ser mi confidente y por ser mi inspiración para lograr cada objetivo propuesto en mi vida, pero sobre todo por su amor puro y sincero.

A mi padre Jorge:

Por su amor y confianza que me brindo en cada momento de mi vida, dándome ejemplos dignos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por ser un ejemplo a seguir, por el valor mostrado para salir adelante, por su esfuerzo y sacrificio y por demostrarme que en todo momento cuento con él.

A mis hermanos Jimmy y Jackie:

Que con su amor me han enseñado y ayudado a salir adelante, por preocuparse por mí su hermano menor, por sus consejos, por encontrar en ustedes un respaldo incondicional, por brindarme grandes lotes de felicidad.

Jorge Vargas Acosta

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

AGRADECIMIENTOS

Ante todo agradecemos a Dios y a la Virgen del Carmen, quienes estuvieron presentes y nos guiaron espiritualmente en todo momento para la culminación de nuestra tesis.

A nuestros padres y hermanos por su total confianza y perseverancia, por ser el motivo, inspiración y el apoyo que nos anima a avanzar y a mejorar cada día.

Al Mgt. Ing. Emilio Palomino Olivera por su valiosa guía, experiencia y acertada dirección para la culminación de este proyecto.

Al Ing. Eduardo León Montoya, por su colaboración y apoyo para hacer posible el desarrollo del presente proyecto.

A nuestros amigos y compañeros, por la ayuda brindada y amistad incondicional.

Claudia Lisseth Gamarra Zavaleta
Jorge Vargas Acosta

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

RESUMEN

Este proyecto se enmarca en el desarrollo y formulación de un Plan de Actividades a ser implementados en la Unidad de Tecnologías de la Información de la Zona Registral N° X Sede Cusco - de la Superintendencia Nacional de los Registros Públicos (SUNARP), para poder brindar seguridad en los procesos que se realizan dentro de la Gestión de Comunicaciones y Operaciones, dicho plan está elaborado bajo normas y estándares de uso obligatorio.

Específicamente, la propuesta que se ofrece en el presente proyecto, es el de brindar lineamientos y establecer una nueva forma de trabajo, utilizando diagramas de actividades, diagramas de procesos y formularios que cumplan con lo sugerido en los códigos de buenas prácticas para la Gestión de Comunicaciones y Operaciones de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007, norma que, de acuerdo a la Resolución Ministerial N°246-2007-PCM de la Presidencia del Consejo de Ministros, es de uso obligatorio para todas las entidades públicas en el Estado Peruano, así y de ésta forma se propiciará y generará un mejor manejo y control de los procesos realizados en la Unidad de Tecnologías de la Información.

Finalmente, se ha desarrollado un Plan de Auditoría que permitirá evaluar y determinar si cada control implementado cumple con lo estipulado y sugerido en la cláusula de Gestión de Comunicaciones y Operaciones de la NTP-ISO/IEC 17799:2007.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ABSTRACT

This project is part of the development and formulation of a plan of activities to be implemented in the 'Unidad de Tecnologías de la Información' of the 'Zona Registral N° X Sede Cusco of the 'Superintendencia Nacional de los Registros Públicos (SUNARP)', in order to provide security in the processes performed within the Communications and Operations Management, this plan is prepared under mandatory standards.

Specifically, the proposal offered in this project, is to provide guidelines and establish a new way of working, using activity diagrams, process diagrams and forms complying with the suggested codes of good practice for the Management of Communications and Operations of the Peruvian Standard NTP-ISO / IEC 17799: 2007, which is, according to the Resolution Ministerial No. 246-2007-PCM of the Presidency of the Council of Ministers, is obligatory for all public entities in the Peruvian State, and thus it will encourage and generate better management and control of the processes performed in the 'Unidad de Tecnologías de la Información'

Finally, we have developed an audit plan that will assess and determine whether each implemented control complies with the requirements and suggested in the clause of Management of Communications and Operations of the NTP- ISO / IEC 17799: 2007.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

INTRODUCCIÓN

La Superintendencia Nacional de los Registros Públicos (SUNARP) es el organismo descentralizado del Sector Justicia y ente rector del Sistema Nacional de los Registros Públicos; dicho organismo dicta las políticas y normas técnico-registrales de los registros públicos, planifica y organiza, norma, dirige, coordina y supervisa la inscripción y publicidad de actos y contratos en los Registros que conforman el Sistema Nacional.[1]

La Unidad de Tecnologías de la Información (UTI) de la Zona Registral N° X - Sede Cusco, unidad a ser estudiada en el presente proyecto, es el órgano encargado de la sistematización, ejecución del procesamiento de la información, administración, mantenimiento y soporte técnico del Sistema Informático de la Zona.[2]

Actualmente, la UTI no cuenta con controles de seguridad que proporcionen una adecuada Gestión de Comunicaciones y Operaciones, ya que en dicha unidad, no existen actividades ni procesos correctamente definidos que estén documentados y vinculados a controlar: las operaciones que realizan día a día, la gestión de cambios, la aceptación de nuevos sistemas y/o actualizaciones y la arquitectura de los sistemas y la red.

Además, la UTI cuenta con un control de accesos a su oficina e instalaciones, pero éste no está documentado ni es usado correctamente en todas sus instalaciones.

En cuestión de Infraestructura se suelen generar muchos problemas e incomodidades ya que no cuentan con una separación adecuada entre los ambientes de desarrollo, soporte y operación.

[1] www.sunarp.gob.pe
[2] Manual de Organización y Funciones (MOF) de la Zona Registral N°X

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

En ese entender, se hace necesaria la adopción y formulación de actividades que respondan y estén vinculadas a una norma que proporcione control, seguridad y gestión de las Comunicaciones y Operaciones, dichas actividades serán propuestas en el presente proyecto, con el fin de minimizar los riesgos y preservar la confidencialidad, integridad y disponibilidad de la información dentro de la Unidad de Tecnologías de la Información.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ÍNDICE GENERAL

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ÍNDICE DE TABLAS

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ÍNDICE DE GRÁFICOS

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ÍNDICE DE DIAGRAMAS DE ACTIVIDAD

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ÍNDICE DE DIAGRAMAS DE PROCESO

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ÍNDICE DE FORMULARIOS

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

1.1. Identificación del problema.-

La presente investigación y estudio se lleva a cabo en la Unidad de Tecnologías de la Información (UTI) de la Zona Registral N° X - Sede Cusco de la Superintendencia Nacional de los Registros Públicos.

La UTI es el órgano encargado de la sistematización, ejecución del procesamiento de la información, administración, mantenimiento y soporte técnico del Sistema Informático de la Zona Registral, mediante Sistemas de Procesamiento automático de datos, metodologías modernas de desarrollo de Sistemas, en concordancia a los lineamientos que sobre el particular, establezca la Superintendencia Nacionales de los Registros Públicos. [3]

Actualmente, la UTI no cuenta con controles de seguridad que proporcionen una adecuada Gestión de Comunicaciones y Operaciones, ya que en dicha unidad, no existen actividades ni procesos que trabajen correctamente y que estén debidamente documentados.

La falta de uso de controles que la norma sugiere y que están estipulados en la cláusula Gestión de Comunicaciones y Operaciones, pone en peligro y riesgo la información de la UTI, afectando así a la preservación de la confidencialidad, integridad y disponibilidad de la misma.

[3] Manual de Organización y Funciones (MOF) de la Zona Registral N°X.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

1.1.1. Descripción del problema.-

La Unidad de Tecnologías de la Información al no contar con mecanismos de control y de seguridad en la Gestión de Comunicaciones y Operaciones, cuenta con los siguientes problemas:

- No existen instalaciones de procesamiento lo suficientemente seguros para proteger la información generada en ellas.
- No existe un plan de recuperación ni de continuidad de sistemas antes alguna falla existente.
- La información manejada dentro de la oficina (lógica-física), no está protegida debidamente.
- Existen sistemas y software que no han sido revisados minuciosamente y no están aprobados para su uso en la institución.
- No se conserva la integridad ni la disponibilidad del procesamiento y/o transferencia de la información en su totalidad.
- No se garantiza que la información en las redes esté protegida totalmente.
- Existen algunos daños y caídas de los sistemas de información, que originan interrupciones en las actividades de la institución, pudiendo así, existir pérdida de paquetes de información.
- Algunos perfiles y accesos a la información necesitan ser revisados, reestructurados y documentados.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

1.1.1.1. Situación actual.-

(Ver Anexo A.1)

De acuerdo a la encuesta realizada a los trabajadores de la UTI, a continuación se detalla la información obtenida por cada objetivo de control de la cláusula de Gestión de Comunicaciones y Operaciones:

- **Responsabilidad y Procedimientos Operacionales:**
  - El 39.25% del Personal de la UTI indica que los controles se aplican en un 61.33%.
  - El 57.25% del Personal de la UTI, indica que los controles se aplican parcialmente en un 55.75%.
  - El 3.5% del Personal de la UTI, indica que los controles no se aplican en un 5%.

- **Gestión de Servicios por Terceras partes:**
  - El 29% del Personal de la UTI indica que los controles se aplican en un 81.67%.
  - El 57% del Personal de la UTI, indica que los controles se aplican parcialmente en un 56.33%.
  - El 14% del Personal de la UTI, indica que los controles no se aplican en un 6.67%.

- **Planificación y Aceptación del Sistema:**
  - El 43% del Personal de la UTI indica que los controles se aplican en un 80%.
  - El 43% del Personal de la UTI, indica que los controles se aplican parcialmente en un 51.65%.
  - El 14% del Personal de la UTI, indica que los controles no se aplican en un 15%.

DERECHOS DE AUTOR RESERVADOS

- **Protección contra código móvil y malicioso:**
  - El 21.5% del Personal de la UTI indica que los controles se aplican en un 40%.
  - El 35.5% del Personal de la UTI, indica que los controles se aplican parcialmente en un 56.25%.
  - El 36% del Personal de la UTI, indica que los controles no se aplican en un 12%
  - El 7% del Personal de la UTI, indica que los controles no se deberían aplicar.

- **Copia de Respaldo de Información:**
  - El 57% del Personal de la UTI indica que los controles se aplican en un 85%.
  - El 29% del Personal de la UTI, indica que los controles se aplican parcialmente en un 50%.
  - El 14% del Personal de la UTI, indica que los controles no se aplican en un 20%.

- **Gestión de Seguridad en la Red:**
  - El 43% del Personal de la UTI indica que los controles se aplican en un 86.25%.
  - El 57% del Personal de la UTI, indica que los controles se aplican parcialmente en un 52.65%.

- **Gestión de Soportes:**
  - El 50% del Personal de la UTI indica que los controles se aplican en un 83.65%.
  - El 46.5% del Personal de la UTI, indica que los controles se aplican parcialmente en un 53.33%.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

- El 3.5% del Personal de la UTI, indica que los controles no se aplican en un 5%.

- **Intercambio de Información:**
  - El 54.20% del Personal de la UTI indica que los controles se aplican en un 82.38%.
  - El 37% del Personal de la UTI, indica que los controles se aplican parcialmente en un 53.32%.
  - El 8.8% del Personal de la UTI, indica que los controles no se aplican en un 7%.

- **Servicios de Comercio Electrónico**:
  - El 62% del Personal de la UTI indica que los controles se aplican en un 85.17%.
  - El 9.33% del Personal de la UTI, indica que los controles se aplican parcialmente en un 36.67%.
  - El 28.67% del Personal de la UTI, que los controles no deberían aplicarse

- **Monitoreo**
  - El 57.33% del Personal de la UTI indica que los controles se aplican en un 85.17%.
  - El 35.67% del Personal de la UTI, indica que los controles se aplican parcialmente en un 53.18%.
  - El 7% del Personal de la UTI, indica que los controles no se aplican en un 11.67%.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

Luego de realizar el análisis de toda la información brindada por el personal de la UTI, se pudo determinar lo siguiente:

- El 47.41% de Trabajadores indica que los controles de la cláusula se aplican en un 83.26 %
- El 41.03% de Trabajadores indica que los controles se aplican de manera parcial, 53.94%
- El 8.44% de Trabajadores indica que los controles no se aplican en un 20%
- El 3.13 % de Trabajadores indica que algunos controles no deben ser aplicados.

Cabe indicar, que según la encuesta realizada al personal de la UTI, el porcentaje de controles establecido tiene un nivel considerable de aplicación, pero sin embargo ninguno de ellos se rigen a lo establecido en los estándares ofrecidos en la cláusula 10: Gestión de Comunicaciones y Operaciones de la NTP ISO/IEC 17799:2007.

1.1.2. Formulación del problema.-

¿Cómo se pueden aplicar e implementar los controles de la cláusula de Gestión de Comunicaciones y Operaciones de la NTP-ISO/IEC 17799:2007 para que influyan positivamente en la gestión de la seguridad de la información de los procesos realizados en la Unidad de Tecnologías de la Información de la Zona Registral N°X - Sede Cusco - SUNARP?

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

1.2. Justificación e importancia del problema.-

Debido a la problemática presente, y a la necesidad de la Unidad de Tecnologías de la Información, con contar con procesos y controles que brinden seguridad a la Gestión de Comunicaciones y Operaciones, se hace necesaria la presente investigación, la cual tiene como finalidad el de plantear, formular e implementar una lista de actividades que respondan adecuadamente y estén vinculadas a la cláusula de la NTP ISO/IEC 17799:2007 nombrada líneas arriba.

Además, mediante Resolución Ministerial N° 246-2007 -PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "*NTP ISO/IEC 17799:2007 Tecnologías de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da edición*", en todas las instituciones públicas desde agosto del 2007, estandarizando de esta forma los diversos proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad de la información. La supervisión de su cumplimiento está a cargo de la Oficina Nacional del Gobierno Electrónico e Informática - ONGEI. [4]

1.3. Limitaciones de la Investigación.-

Las limitaciones encontradas en la presente investigación son las siguientes:

- Existen políticas emitidas por la Jefatura Zonal de la Zona Registral N°X – Sede Cusco, que restringen el acceso total a las instalaciones de sus oficinas, incluida la Unidad de Tecnologías de la Información.

- Los trabajadores de la Unidad de Tecnologías de la Información podrán brindarnos su apoyo y ayuda para la recolección de información sólo en días establecidos y en horarios definidos previamente. Asimismo, la gran

[4] Resolución Ministerial N° 246-2007-PCM

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

mayoría de personal no posee conocimiento sobre la seguridad de la información basada en la NTP-ISO/IEC 17799:2007

- La poca cantidad de bibliografía existente referentes al tema.
- En nuestra localidad, no contamos con muchos expertos profesionales certificados en la materia.

1.4. Objetivos de la Investigación.-

1.4.1. Objetivo General.-

Formular un plan de actividades que contengan la aplicación e implementación de los controles de la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO/IEC 17799:2007, para brindar una mejora en la gestión de la seguridad de la información de los procesos realizados en la Unidad de Tecnologías de la Información de la Zona registral N° X - Sede Cusco - SUNARP.

1.4.2. Objetivos Específicos.-

1. Identificar y desarrollar diagramas de actividades correspondientes a las guías de implementación de la cláusula de Gestión de Operaciones y Comunicaciones de la NTP ISO/IEC 17799:2007 necesarias para la Unidad de Tecnologías de la Información, las cuales ayudarán a identificar los roles del recurso humano que participará en la misma.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

2. Desarrollar diagramas de procesos, tomando como base lo elaborado en los diagramas de actividades para la cláusula de Gestión de Operaciones y Comunicaciones de la NTP ISO/IEC 17799:2007.

3. Elaborar formularios y/o formatos para todos los controles de la Cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO/IEC 17799:2007, que permitan ser usados durante la implementación.

4. Desarrollar un plan de auditoría, elaborando formatos para que evalúen que todos los controles estén implementados según los diagramas de actividades/procesos ya realizados y lo sugerido en la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO/IEC 17799:2007.

5. Contribuir al buen uso y a la buena práctica de ejecutar los procedimientos de la UTI siempre bajo un mismo estándar, utilizando normas/políticas que ya han sido revisadas y aprobadas para cumplir dicho fin.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

CAPÍTULO II

MARCO TEÓRICO

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

2.1 Aspectos teóricos pertinentes.-

2.1.1. Superintendencia Nacional de los Registros Públicos.-

La SUNARP es un organismo descentralizado del Sector Justicia y ente rector del Sistema Nacional de los Registros Públicos; sus principales funciones y atribuciones es el de dictar las políticas y normas técnico-registrales de los registros públicos que integran el Sistema Nacional, el de planificar y organizar, normar, dirigir, coordinar y supervisar la inscripción y publicidad de actos y contratos en los Registros que conforman el Sistema [5]

Imagen N°1 - *Logo actual de la SUNARP*

Fuente: *Página Web Institucional de la SUNARP (www.sunarp.gob.pe)*

Misión.- Otorgar seguridad jurídica al ciudadano a través del registro y publicidad de derechos y titularidades en forma eficiente y transparente.

Visión.- Ser una institución referente a nivel internacional, altamente tecnificada, proactiva, confiable y con presencia efectiva en todo el territorio nacional, brindando servicios registrales de calidad a satisfacción del ciudadano.

[5] Página Web Institucional de la SUNARP (www.sunarp.gob.pe)

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

Zonas Registrales.- La SUNARP está comprendida por la Sede Central ubicada en el departamento de Lima y las siguientes 13 Zonas Registrales:

Zona Registral N°I – Sede Piura	Zona Registral N° VIII – Sede Huancayo
Zona Registral N°II – Sede Chiclayo	Zona Registral N°IX – Sede Lima
Zona Registral N°III – Sede Moyobamba	Zona Registr al N°X – Sede Cusco
Zona Registral N°IV – Sede Iquitos	Zona Registral N°XI – Sede Ica
Zona Registral N°V – Sede Trujillo	Zona Registral N°XII – Sede Arequipa
Zona Registral N°VI – Sede Pucallpa	Zona Registral N°XIII – Sede Tacna
Zona Registral N°VII – Sede Huaraz	

Imagen N°2 - *Mapa del Perú con la distribución de las 13 Zonas Registrales de SUNARP*

Fuente: *Página Web Institucional de la SUNARP (www.sunarp.gob.pe)*

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

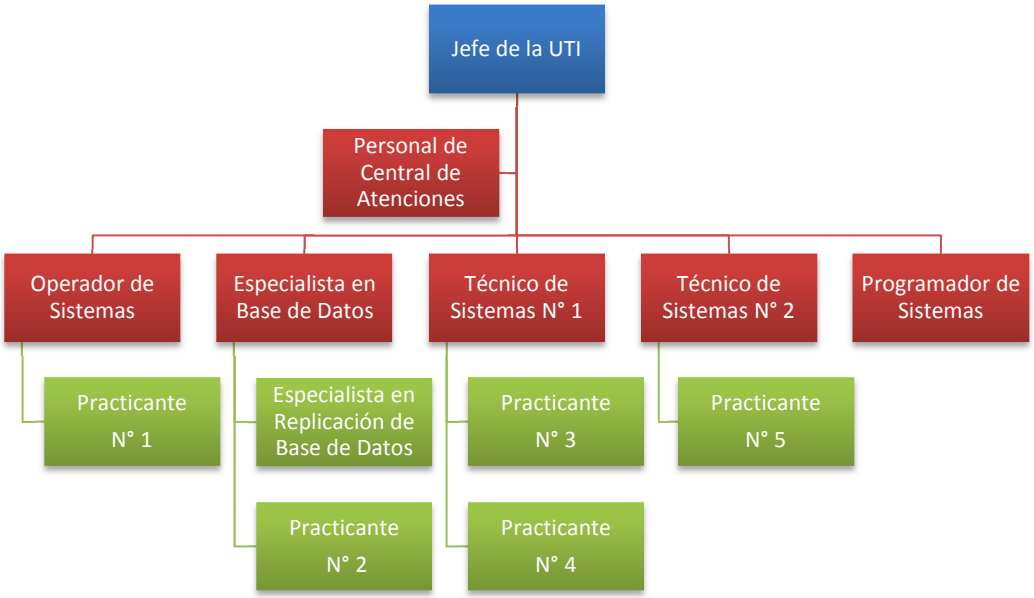
Zona Registral N°X - Sede Cusco.-

La Zona Registral N°X - Sede Cusco, zona a ser estu diada en la presente investigación, tiene a su cargo la inscripción y la publicidad de los hechos, actos y contratos que han cumplido los requisitos de ley en las ciudades de Cusco, Apurímac, Madre de Dios, Quillabamba y Sicuani.

Unidad de Tecnologías de la Información (UTI).-

La UTI es el órgano encargado de la sistematización, ejecución del procesamiento de la información, administración, mantenimiento y soporte técnico del Sistema Informático de la Zona Registral, mediante Sistemas de Procesamiento automático de datos, metodologías modernas de desarrollo de Sistemas, en concordancia a los lineamientos que sobre el particular, establezca la Superintendencia Nacionales de los Registros Públicos.

Imagen N°3 - *Organigrama de la Unidad de Tecnologías de la Información*



Fuente: *Manual de Organización y Funciones (MOF) de la Zona Registral N°X*

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

2.1.2. Plan.-

Un plan es una intención o un proyecto, se trata de un modelo sistemático que se elabora antes de realizar una acción, con el objetivo de dirigirla y encauzarla. Es un programa en el que se detalla el modo y conjunto de medios necesarios para llevar a cabo una idea o actividad.

2.1.3. Actividad.-

Es el conjunto de acciones que se llevan a cabo para cumplir las metas de un programa o subprograma de operación. Conjunto de tareas o acciones realizadas por un ser vivo, que las desarrolla impulsado por el instinto, la razón, la emoción, o la voluntad, hacia un objetivo.

2.1.4. Activo de Información.-

Es todo aquello que es o contiene información. La información es un activo importante para el negocio y necesita ser protegida de forma adecuada. Todo activo que procesa, contiene y transmite la información se debe de inventariar para el SGSI. [6]

2.1.5. Seguridad de la Información.-

Protege la información de un amplio rango de amenazas para garantizar la continuidad del negocio, minimizar los riesgos y maximizar el retorno de las inversiones en las oportunidades del negocio. Preserva la Triada de la Información. [7]

[6] Norma Técnica Peruana NTP-ISO/IEC 17799 ‘Términos y Definiciones‘
[7] Norma Técnica Peruana NTP-ISO/IEC 17799 ‘Introducción ‘

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

2.1.5.1. Triada de la Seguridad de la Información.-

- **Confidencialidad:** Que la información sea accedida por personas autorizadas y que sea usada sólo para los fines para los cuales se le fue entregada.
- **Integridad:** Que la información y su procesamiento sea exacta y completa.
- **Disponibilidad:** Que la información se encuentre disponible en su punto de uso y pueda ser accedida por los entes autorizados en el momento que se requiera.

Otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas.

2.1.6. Control.-

Proceso, dispositivo, o procedimiento que reduce o previene el efecto pernicioso. Reduce la probabilidad de ocurrencia de una amenaza, mitiga el impacto de una amenaza. Si un riesgo no se puede eliminar, entonces se debe de controlar el mismo. [8]

2.1.7. Amenaza.-

Causa potencial de un incidente no deseado que puede resultar en daño a la organización o a sus activos.

[8] Norma Técnica Peruana NTP-ISO/IEC 17799 ‘Términos y Definiciones‘

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

2.1.8. Vulnerabilidad.-

Es una debilidad o ausencia de control en la seguridad de la información, sola no causa daños pero expone a los activos a posibles amenazas.

2.1.9. ISO/IEC

La Organización Internacional para la Estandarización cuyo nombre en inglés es *International Organization for Standardization*, es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional. Las normas desarrolladas por ISO son voluntarias, ya que ISO no tiene autoridad para imponer sus normas en ningún país por ser un organismo no gubernamental. [9]

2.1.10. ISO/IEC 27000.-

Familia de normas para la gestión de la seguridad de la información. [10]

2.1.10.1. Serie 27001.-

Norma principal de la serie, contiene los requisitos del sistema de gestión de seguridad de la información. Su origen es la BS 7799-2:2002 y es la norma con la cual, los SGSI de las organizaciones se certifican por auditores externos.

[9] Página web 'ISO' (http://www.iso.org/iso/home.html)
[10] Página web 'El Portal de ISO 27001 en español' (http://www.iso27000.es/iso27000.html)

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

2.1.10.2. Serie 27002.-

Nuevo nombre de ISO 17799:2005. Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información. No es certificable.

2.1.10.3. Serie 27003.-

Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de sus requerimientos.

2.1.10.4. Serie 27004.-

Especificará las métricas y las técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados.

2.1.10.5. Serie 27005.-

Consistirá en una guía para la gestión del riesgo de la seguridad de la información y servirá de apoyo a la ISO 27001 y a la implantación de un SGSI.

2.1.10.6. Serie 27006.-

Especificará el proceso de acreditación de entidades de certificación y el registro de SGSIs.

2.1.10.7. Serie 27007.-

Guía para auditar al SGSI

2.1.11. Norma Técnica Peruana NTP ISO/IEC 17799:2007.-

Documento titulado “Código de buenas prácticas para la gestión de la seguridad de la información”. Norma equivalente del estándar ISO/IEC

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

17799:2000 en el Perú el cual es de uso obligatorio en todas las instituciones públicas desde agosto del 2004, estandarizando los diversos proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad. La supervisión de su cumplimiento está a cargo de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI (www.ongei.gob.pe). [11]

2.1.12. Estructura de la NTP ISO/IEC 17799:2007.-

Este estándar contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento de riesgos.

Cada cláusula contiene un número de categorías principales de seguridad. Las 11 cláusulas (acompañadas por el número de categorías principales de seguridad incluidas en cláusula) son [12] :

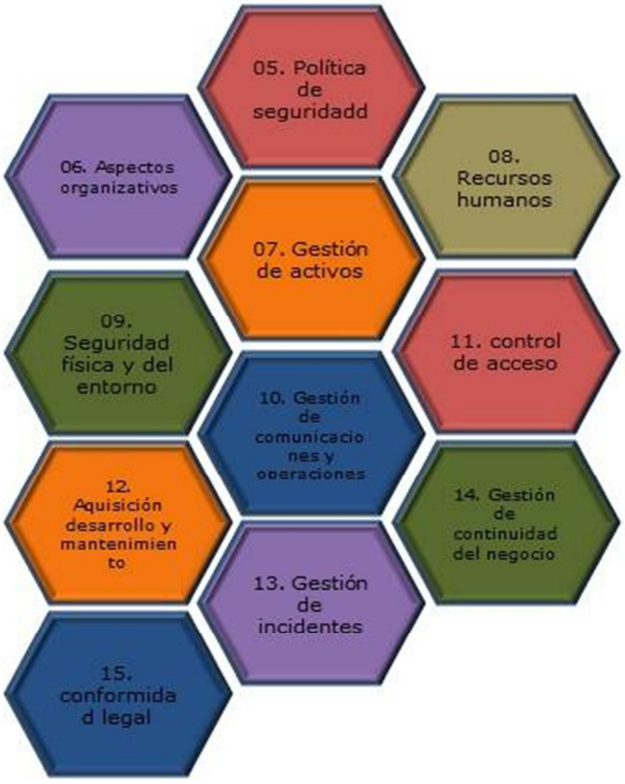
A5. Política de Seguridad (1)
A6. Aspectos organizativos de la Seguridad (2)
A7. Gestión de Activos (2)
A8. Seguridad en recursos humanos (3)
A9. Seguridad física y del entorno (2)
A10. Gestión de comunicaciones y operaciones (10)
A11. Control de Acceso (7)
A12. Adquisición, desarrollo y mantenimiento (6)
A13. Gestión de Incidentes en la Seguridad de la Información (2)
A14. Gestión de Continuidad del Negocio (1)
A15. Cumplimiento (3)

[11] Norma Técnica Peruana NTP ISO/IEC 17799:2007 – 'Reseña Histórica'
[12] Norma Técnica Peruana NTP ISO/IEC 17799:2007 - Capítulo 3 'Estructura del Estándar'

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

Imagen N°4 - *Cláusulas de la NTP-ISO/IEC 17799:2007*



Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

2.1.12.1. (A10) Gestión de Comunicaciones y Operaciones.-

Cláusula que cuenta con los siguientes 10 Objetivos de control: [13]

- **A10.1 Procedimientos y responsabilidades de operación.-**

  Objetivo: Asegurar la operación correcta y segura de los recursos de tratamiento de información.

  Controles:

  A10.1.1 Documentación de procedimientos operativos.
  A10.1.2 Gestión de Cambios.

[13] Norma Técnica Peruana NTP ISO/IEC 17799:2007 - Capítulo 10 'Gestión de Comunicaciones y Operaciones'

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

A10.1.3 Segregación de tareas.
A10.1.4 Separación de los recursos para desarrollo y para producción.

- **A10.2 Gestión de servicios externos.-**

Objetivo: Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos con terceros.

Controles:
A10.2.1 Servicio de entrega.
A10.2.2 Monitoreo y Revisión de los servicios externos.
A10.2.3 Gestionando cambios para los servicios externos.

- **A10.3 Planificación y aceptación del sistema.-**

Objetivo: Minimizar el riesgo de fallos de los sistemas

Controles:
A10.3.1 Planificación de la capacidad
A10.3.2 Aceptación del sistema.

- **A10.4 Protección contra software malicioso.-**

Objetivo: Proteger la integridad del software y de la información.

Controles:
A10.4.1 Medidas y controles contra software malicioso.
A10.4.2 Medidas y controles contra código móvil.

- **A10.5 Gestión de respaldo y recuperación.-**

Objetivo: Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

Controles:

A10.5.1 Recuperación de la información.

- **A10.6 Gestión de seguridad en redes.-**

Objetivo: Apoyar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.

Controles:

A10.6.1 Controles de red.
A10.6.2 Seguridad en los servicios de redes.

- **A10.7 Utilización de medios de información.-**

Objetivo: Prevenir acceso no autorizado, modificaciones, evitar daños a los activos e interrupciones de las actividades de la organización.

Controles:

A10.7.1 Gestión de medios removibles
A10.7.2 Eliminación de medios
A10.7.3 Procedimientos de manipulación de la información.
A10.7.4 Seguridad de la documentación de sistemas.

- **A10.8 Intercambio de información.-**

Objetivo: Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

Controles:

A10.8.1 Políticas y procedimientos para el intercambio de información y software.
A10.8.2 Acuerdos de intercambio.
A10.8.3 Medios físicos en tránsito.
A10.8.4 Seguridad en la mensajería electrónica.
A10.8.5 Sistemas de Información de Negocios.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

- **A10.9 Servicios de comercio electrónico.-**

  Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.

  Controles:

A10.9.1	Comercio Electrónico.
A10.9.2	Transacciones en línea.
A10.9.3	Información pública disponible.

- **A10.10 Monitoreo.-**

  Objetivo: Detectar las actividades de procesamiento de información no autorizadas.

  Controles:

A10.10.1	Registro de la auditoría.
A10.10.2	Monitoreando el uso del sistema.
A10.10.3	Protección de la información de registro.
A10.10.4	Registro de administradores y operadores.
A10.10.5	Registro de la avería.
A10.10.6	Sincronización del reloj.

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

En inglés *"Information Security Management System (ISMS)"* se basa en un conjunto de políticas orientadas a conseguir y a mantener la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la Información, en todo el ciclo de una organización.

Un SGSI permite dotar y mantener seguridad, sobre la información que maneja la organización, además ofrece una ventaja competitiva a la organización si se certifica con el estándar ISO/IEC 27001. [14]

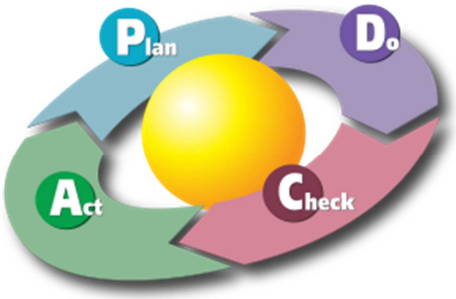
[14] Norma Técnica Peruana NTP ISO/IEC 27001:2008 - 'Sistema de Gestión de Seguridad de la Información'

DERECHOS DE AUTOR RESERVADOS

2.1.14. Ciclo de Deming.-

El estándar de seguridad de la información ISO/IEC 27001, detalla los requisitos para diseñar, implantar y mejorar un SGSI, basándose en el **Ciclo de Deming** (también conocido como PDCA) ***"Plan - Do - Check - Act"*** (Planificar - Desarrollar - Controlar - Actuar), orientado a la mejora continua, en este caso, aplicado a la seguridad. [15]

Imagen N°5 - *Diagrama del Ciclo de Deming (Planificar - Desarrollar - Controlar - Actuar)*



Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

Inicio del proyecto: Arranque del Proyecto en donde se obtiene el compromiso y apoyo de la Dirección de la organización. Se planifican fechas y responsables.

Imagen N°6 - *Inicio del Proyecto dentro del Ciclo de Deming (PDCA)*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

[15] Norma Técnica Peruana NTP-ISO/IEC 27001:2008 - 'Enfoque de Proceso'

DERECHOS DE AUTOR RESERVADOS

El ciclo de Deming lo componen 4 etapas cíclicas, de forma que una vez acabada la etapa final, se debe de volver a la primera y repetir el ciclo de nuevo, así las actividades (medidas de prevención, corrección y evaluación) son de nuevo evaluadas periódicamente para incorporar nuevas mejoras, las etapas son:

- **Planificar (Plan).-**

  En esta etapa se enmarca todo el proceso de análisis de la situación en que se encuentra la empresa respecto a los mecanismos de seguridad implementados.

Imagen N°7 - *Etapa de Planificación del Ciclo de Deming (PDCA)*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

- **Desarrollar (Do).-**

  En esta etapa se implementan todos los controles necesarios de acuerdo a una previa selección en la etapa de planeación. Aquí también se formula e implementa un plan de riesgo.

Imagen N°8 - *Etapa de Desarrollo del Ciclo de Deming (PDCA)*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

DERECHOS DE AUTOR RESERVADOS

- **Controlar o Verificar (Check):**

  Consiste en efectuar el control de todos los procedimientos implementados en el SGSI, realizando exámenes para asegurar la eficacia del SGSI, revisando los niveles de riesgos residuales.

Imagen N°9 - *Etapa de Control del Ciclo de Deming (PDCA)*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

- **Actuar (Act).-**

  Desarrollar y validar mejoras a los hallazgos identificados en el SGSI. Realizar las acciones correctivas y preventivas y mantener comunicación con el personal.

Imagen N°10 - *Etapa de Acción del Ciclo de Deming (PDCA)*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

2.1.15. Conceptos y Principios Fundamentales de Auditoría.-

2.1.15.1. Auditoría.-

Procesos sistemáticos, independientes y documentados para obtener evidencia de auditoría y evaluarla sistemáticamente para determinar el grado en el cuál los criterios de auditoría se cumplen.

Auditar significa preguntar al auditado que es lo que hace y revisar si en realidad lo está haciendo.

2.1.15.2. Tipos de Auditoría-

- **Auditoría Interna:** Primera parte de la auditoría, es una actividad independiente y objetiva que da a la organización un aseguramiento sobre el nivel de control de las operaciones.

- **Auditoría Externa:** Se divide en 2 partes:
  - Segunda parte de la auditoría, son conducidas por la parte que tienen un interés en la organización auditada.
  - Tercera parte de la auditoría, son conducidas por externos e independientes a la organización.

2.1.15.3. Objetivos de Auditoría.-

- Opinión de auditoría, recibe advertencias y recomendaciones.
- Pre evaluación de auditoría, que prepara para la certificación.
- Auditoría de certificación, recomienda o no la certificación.

2.1.15.4. Criterios de Auditoría.-

Son un conjunto de políticas, procedimientos o requerimientos usados como referencia para comparar contra una evidencia de auditoría.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

2.1.15.5. Principios de Auditoría.-

Los principios de auditoría son:

- Integridad
- Debido cuidado profesional
- Independencia
- Presentación razonable
- Confidencialidad
- Enfoque basado en evidencia

2.1.15.6. Evidencia de Auditoría.-

Son los registros, definiciones de actos u otra información relevante y verificable para el criterio de una auditoría. Debe de ser disponible y verificable. La naturaleza de la evidencia puede ser:

- Cualitativa (ejem: Entrevistas a personas).
- Cuantitativa (ejem: Estadísticas y Reportes de control)

2.1.15.7. Tipos de Evidencia de Auditoría.-

Existen 7 tipos de evidencia de auditoría las cuales explicaremos a continuación:

- **Física:** Es todo lo que puede ser contado, examinado, observado e inspeccionado. Por ejemplo: etiquetas de identificación de activos, sistema contra incendios, etc.

- **Matemática:** Consiste en calculaciones realizadas por el auditor. Por ejemplo: número de horas de entrenamiento recibido, licencias compradas, etc.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

- **Confirmativa:** Originada por entidades con una relación externa al auditado. Por ejemplo: eventos coleccionados y mantenidos por un tercero, cartas de abogado, etc.

- **Técnica:** Resultado de análisis de pruebas técnicas. Por ejemplo: test de penetración, configuración de firewall, etc.

- **Analítica:** Consiste en el resultado de análisis y la comparación de diferentes datos. Por ejemplo: datos estadísticos, incidentes de seguridad, etc.

- **Documentaria:** Es la evidencia de algún registro o documento. Por ejemplo: políticas, guías, reportes, procedimientos, etc.

- **Verbal:** Recolectada durante las interacciones entre el auditor y personal del auditado. Por ejemplo: discusiones, llamadas, etc.

2.2 Investigación Actual.-

2.2.1. Resoluciones de la Superintendencia Nacional de los Registros Públicos referidas a Seguridad de la Información.-

- **Resolución N° 321-2008-SUNARP/SN.-** Resolución en la cual se resuelve: "Constituir el Comité de Seguridad de Información encargado de gestionar la seguridad de información en la SUNARP, Sede Central y Órganos Desconcentrados" [16], así mismo se detallan los miembros del Comité y sus funciones.

[16] Artículo Primero de la Resolución N° 321-2008-SUNAR P/SN de fecha 01-12-2008

DERECHOS DE AUTOR RESERVADOS

- **Resolución N° 060-2010-SUNARP-SN.-** Resolución en la cual se resuelve: "Aprobar el Reglamento de Seguridad de la Información de la SUNARP, el mismo que forma parte de la Presente Resolución" [17], así mismo se solicita a la Gerencia de Informática la comunicación del Reglamento y encarga a la Gerencia de Imagen Institucional la publicación de la Resolución en el Portal Web.

- **Resolución N° 206-2011-SUNARP-SN.-** Resolución en la cual se resuelve: "Modificar el numeral 14) del artículo 33° del Reglamento de Seguridad de la Información de la SUNARP, aprobado por Resolución N° 060-2010-SUNARP/SN" [18], así mismo indican el texto a modificar.

- **Resolución N° 203-2012-SUNARP-SN.-** Resolución en la cual se resuelve: "Designa al Ingeniero Reyner Melchor Ricaldi Arauzo como Oficial de la Seguridad de la Información, de la SUNARP quien será responsable del Sistema de Gestión de la Seguridad de la Información de la SUNARP y de la coordinación con la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI)" [19], así mismo solicita poner conocimiento dicha Resolución a la ONGEI.

[17] Artículo Primero de la Resolución N° 0060-2010-SUNA RP/SN de fecha 17-03-2010
[18] Artículo Único de la Resolución N° 206-2011-SUNARP/ SN de fecha 09-08-2011
[19] Artículo Primero de la Resolución N° 203-2012-SUNAR P/SN de fecha 01-08-2012

DERECHOS DE AUTOR RESERVADOS

- **Resolución N° 270-2014-SUNARP-SN.-** Resolución en la cual se resuelve: "Aprobar el documento de gestión interna denominado 'Política del Sistema de Gestión de la Seguridad de la Información de la SUNARP' y el documento denominado 'Organización de la Seguridad de la Información'" [20], así mismo se dispone que lo indicado en el documento de la Política es de cumplimiento obligatorio, y solicita la correspondiente publicación del mismo.

- **Resolución N° 185-2015-SUNARP-SN.-** Resolución en la cual se resuelve: "Recomponer la conformidad del Comité de Seguridad de la Información establecida por Resolución N° 321-2008-SUNARP/SN" [21], así mismo se detalla los integrantes del nuevo Comité, se solicita a todas las áreas brindar el apoyo correspondiente para el cumplimiento de las funciones del Comité y dejar sin efecto la Resolución N° 321-2008-SUNARP/SN del 01 de diciembre de 2008.

2.2.2. Evolución de certificaciones ISO/IEC 27001 en el mundo.-

De acuerdo a la encuesta oficial realizada por la ISO a finales del año 2012, se han identificado al menos 19577 empresas en todo el mundo, certificadas en ISO/IEC 27001:2005. Comparando con la cifra de un año anterior (17355 empresas certificadas), hubo un crecimiento del 13%, en donde se incrementaron 2222 certificaciones.

Los tres principales países para el número total de certificados emitidos fueron Japón, el Reino Unido y la India, mientras que los tres primeros para el crecimiento en el número de certificados en 2012 eran Rumania, Japón y China.[22]

[20] Artículo Primero de la Resolución N° 270-2014-SUNAR P/SN de fecha 31-10-2014
[21] Artículo Primero de la Resolución N° 185-2015-SUNAR P/SN de fecha 22-07-2015
[22] Página web 'ISO' (http://www.iso.org/iso/home.html)

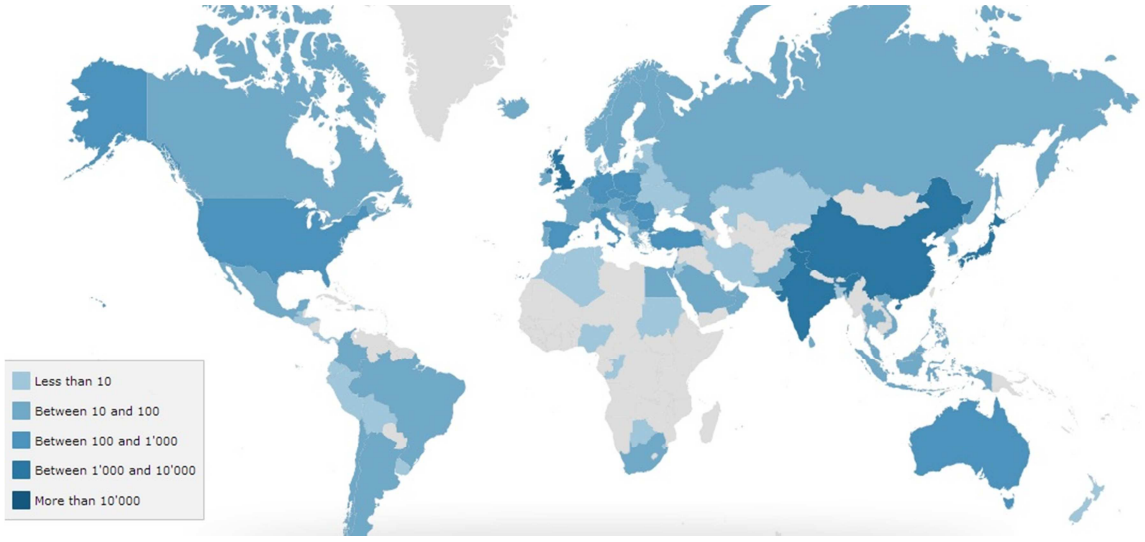
DERECHOS DE AUTOR RESERVADOS

Los 10 países con mayor número de empresas certificadas en ISO/IEC 27001:2005 en el 2012		
1	Japón	7199
2	Reino Unido	1701
3	India	1600
4	China	1490
5	Rumania	866
6	Taiwán	855
7	España	805
8	Italia	495
9	Alemania	488
10	Estados Unidos	415

Tabla N°1 - *Los 10 países con mayor número de empresas certificadas E0n ISO/IEC 27001:2005 en el 2012*

La distribución del total de certificaciones ISO/IEC 27001 en el mundo se puede apreciar en la Imagen N° 11, en la cual Perú aparece con un rango menor de 10 empresas certificadas.

Imagen N°11 - *Distribución de las certificaciones ISO/IEC 27001 en el mundo en el año 2012*



Fuente: *Página web de la ISO – Sección Certificaciones*

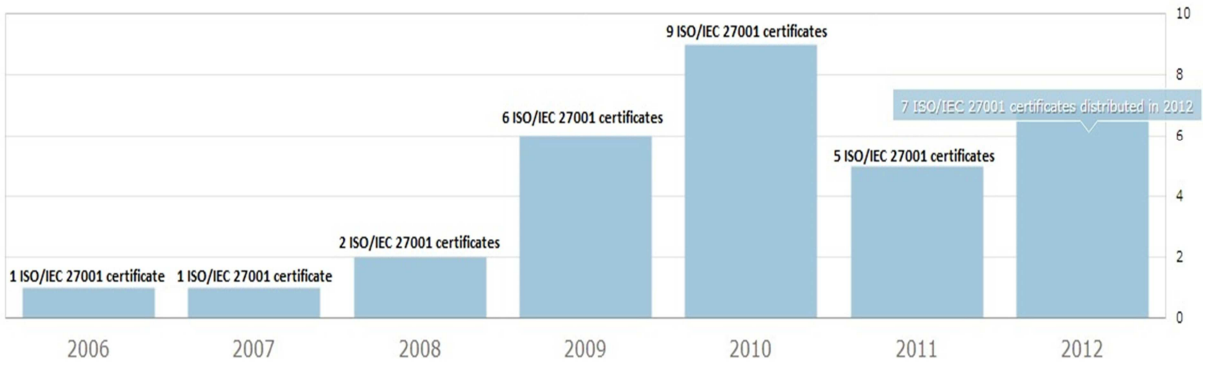
DERECHOS DE AUTOR RESERVADOS

2.2.3. Evolución de certificaciones ISO/IEC 27001 en Perú.-

El número de empresas peruanas con certificación ISO/IEC 27001 ha ido aumentando con el paso de los años. En el año 2006, Perú contaba con solo una empresa certificada, pero poco a poco dicha cantidad fue incrementando, y para el año 2012, año en que se realizó la correspondiente encuesta elaborada por la ISO, Perú contaba ya con 7 empresas certificadas. [23]

La Figura N° 12 muestra el crecimiento que hubo desde el año 2006 al 2012, en la cual podemos apreciar claramente una mejora en el aumento de empresas certificadas con ISO/IEC 27001.

Imagen N°12 - *Evolución de Certificaciones ISO/IEC 27001 en el Perú para el año 2012*



Fuente: *Página web de la ISO – Sección Certificaciones*

A continuación mencionaremos algunas de las empresas peruanas que cuentan con certificación ISO/IEC 27001:

[23] Página web 'ISO' (http://www.iso.org/iso/home.html)

DERECHOS DE AUTOR RESERVADOS

- **Hermes.-**

  Para febrero del 2012, Hermes se convirtió en la sexta empresa peruana y la única en el sector financiero, seguros y de servicios conexos en certificar este estándar. Al certificar la norma internacional ISO/IEC 27001:2005 (a través de SGS), Hermes afianza su misión de brindar soluciones seguras para procesos de riesgo. La certificación tiene como alcance sus servicios en Traslado de Valores, ATM, Procesamiento, Custodia y Seguridad.

  Los requisitos de la ISO 27001 tienen como objetivo eliminar o minimizar los riesgos de fraude, y robo (pérdida) de información clasificada. La adecuación a la norma tomó un año de trabajo e inversión en seguridad para redes, software y herramientas de control.[24]

- **Telefónica del Perú.-**

  Telefónica del Perú alcanzó la Certificación Internacional ISO/IEC 27001:2005, para su Data Center, que brinda servicios de Outsourcing de TI, Disaster Recovery/Business Continuity, Hosting, Housing a las empresas de mayor envergadura en el país, y para sus centros de gestión de móviles, de banda ancha y de redes empresariales, que han sido elevados a estándares de clase mundial Esta certificación posiciona a Telefónica del Perú como la operadora de Latinoamérica con la certificación ISO 27001 de mayor alcance y la única con la Gestión de los Servicios Móviles y de Gestión del Data Center certificada.[25]

[24] Página web de Noticias Perú.com (http://peru.com/2012/02/06/actualidad/economia-y-finanzas/hermes)
[25] Página web de noticias - Gestión.pe (http://gestion.pe/noticia/311271/telefonica-peru-obtiene-certificacion-iso-27001)

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

- **INDECOPI.-**

  El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), obtuvo la Certificación ISO 27001 el 17 de abril del 2013, con la cual garantiza que el sistema de gestión de seguridad de la información implementado funciona adecuadamente, aplicando buenas prácticas internacionales para proteger la información que el Estado, los consumidores, las autoridades y la sociedad en general le confía a la institución.

  El alcance de la certificación ISO 27001 del INDECOPI involucra los procesos que realiza el Servicio de Atención al Ciudadano, gestión de tecnologías de la información, gestión financiera, gestión humana, así como la gestión logística y de control patrimonial de la sede principal de la institución, ubicada en San Borja, Lima. [26]

- **Bolsa de Valores de Lima.-**

  Para diciembre del 2013 y luego de aproximadamente dos años de haber dado inicio a un proyecto con miras a mejorar sus procesos, la Bolsa de Valores de Lima (BVL) se convirtió oficialmente en la primera bolsa del mundo en obtener las certificaciones de calidad- ISO 9001, seguridad de la información- ISO27001 y continuidad de negocio – ISO 22301.

  La obtención de los mencionados certificados representa un avance cualitativo en los procesos implementados por la BVL, ya que garantiza la satisfacción de las expectativas de sus clientes, la

[26] Página web de noticias: http: (www.connuestroperu.com/consumidor/37084-indecopi-recibe-certificacion-iso-27001)

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

preservación de la confidencialidad, integridad y disponibilidad de los activos de información. [27]

- **PROMPERÚ.-**

  Es un organismo técnico especializado adscrito al Ministerio de Comercio Exterior y Turismo - MINCETUR, competente para formular, aprobar, ejecutar y evaluar los planes y estrategias de promoción de bienes y servicios exportables con valor agregado, del turismo interno y receptivo, promoviendo y difundiendo la imagen del Perú en materia turística y de exportaciones, de conformidad con las políticas, estrategias y objetivos sectoriales.

  En junio del año 2014, el SGSI de PROMPERÚ ha sido desarrollado teniendo en cuenta el concepto de procesos y busca garantizar la seguridad de la información, así como definir el funcionamiento del Sistema, bajo un enfoque de mejora continua.

2.2.4. Resolución Ministerial N°246-2007-PCM.-

Aprobación del uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición" en todas las entidades Integrantes del Sistema Nacional de Informática, publicada en fecha 22 de agosto de 2007. Firmada por Jorge Del Castillo Gálvez, Presidente del Consejo de Ministros en esa fecha. Dicha resolución resuelve: [28]

[27] Página web de noticias - Gestión.pe: (http://gestion.pe/mercados/bvl-se-convirtio-primera-plaza-bursatil-mundo-contar-iso-9001-27001-y-22301-2082934)
[28] Resolución Ministerial N° 246-2007-PCM Publicada por El Peruano el 22 de agosto de 2007

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

Artículo 1°.- Aprobar el uso obligatorio de la NTP-ISO/IEC 17799:2007 EDI, en todas las entidades Integrantes del Sistema Nacional de Informática, documento que será publicado en el portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe)

Artículo 2°.- La Norma Técnica Peruana señalada en el artículo precedente, se aplicará a partir del día siguiente de la publicación de la presente Resolución Ministerial, debiendo las Entidades antes mencionadas considerar las actividades necesarias en sus respectivos Planes Operativos Informáticos (POI), para su implantación.

Artículo 3°.- Dejar sin efecto la Resolución Ministerial N° 224- 2004-PCM del 23 de julio de 2004.

2.3 Hipótesis.-

El desarrollo de un plan de actividades ajustada a la cláusula Gestión de Comunicaciones y Operaciones de la Norma Técnica Peruana NTP ISO/IEC 17799:2007, hará posible su respectiva implementación, influyendo positivamente en la gestión de la seguridad de la información y sirviendo de base para adecuar los procedimientos de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco a las exigencias de las normas peruanas.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

CAPÍTULO III

METODOLOGÍA

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

3.1 Tipo de Investigación.-

En el presente proyecto se empleará la **Investigación Descriptiva**, la cual consiste en describir fenómenos, situaciones, contextos y eventos; esto es, detallar cómo son y se manifiestan. Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. [29]

La Investigación descriptiva permitirá efectuar la descripción de la realidad existente sobre la Seguridad de la Información y la Gestión de Comunicaciones y Operaciones de la Unidad de Tecnologías de la Información de la Zona Registral N°X. Además, dicha metodología se complementará con la información resultante del análisis y evaluación de los controles sugeridos en las guías de implementación de la norma.

3.2 Diseño de la Investigación.-

La presente investigación se sujetará a la aplicación de la metodología del Ciclo de Deming (PDCA – Planificación, Desarrollo, Control y Acción) de la cual su uso es sugerida en el documento de la ISO/IEC 27001 para la implementación de los controles de cláusulas contenidas en dicha norma, a fin de desarrollar Sistemas de Gestión de Seguridad de la Información bajo una misma metodología.

[29] Hernandez Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. (2010). *Metodología de la Investigación* (Quinta edición ed.). México D.F., México: McGraw-Hill.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

3.3 Instrumentos.-

De acuerdo a la metodología elegida se usarán los siguientes instrumentos para la presente investigación:

- Encuestas **(Ver Anexo A.1)**
- Entrevistas
- Observaciones
- Lluvia de ideas
- Método Delphi
- Cuestionarios

3.4 Procedimientos de recolección de datos.-

- Para proceder con la recolección de datos se solicitó la autorización y el permiso correspondiente a la Jefatura Zonal de la Zona Registral N° X – Sede Cusco, mediante un documento formal, el cual nos permitió acceder e ingresar a la Unidad de Tecnologías de la Información para poder obtener los datos y la información necesaria para la presente investigación.

- Una vez obtenida dicha autorización, se realizaron encuestas y entrevistas dirigidas a todo el personal de la UTI, a quienes se les solicitó que evalúen la situación actual de su oficina y los procesos relacionados a la gestión de comunicaciones y operaciones.

- Se recolectaron documentos pertinentes a la investigación, los cuales nos proporcionaron información necesaria para continuar con la recolección de datos.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

3.5 Procedimientos de análisis de datos.-

- Una vez recolectado los datos, se procedió a evaluar la situación actual de la UTI, comparando sus procedimientos con los controles propuestos en la cláusula de Gestión de Comunicaciones y Operaciones de la NTP ISO/IEC 17799:2007.

- Para analizar y graficar cada proceso y control, se utilizaron diagramas de actividad y la herramienta BPM (Bizagi Process Modeler).

Todo ello se puede apreciar en el Capítulo IV. Desarrollo del Plan de Actividades de la Cláusula Gestión de Comunicaciones y Operaciones de la NTP-ISO/IEC 17799:2007.

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

CAPÍTULO IV

DESARROLLO DEL PLAN DE ACTIVIDADES DE LA CLÁUSULA GESTIÓN DE COMUNICACIONES Y OPERACIONES DE LA NTP-ISO/IEC 17799:2007

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

4.1 Planificación.-

4.1.1. Alcance del proyecto.-

(Ver Anexo A.2)

El documento del alcance, define el ámbito de la organización que queda sometida al proyecto en términos del negocio, delimita la cantidad de trabajo a realizar, indicando la localización, los activos, la tecnología utilizada, y la justificación de exclusión de procesos y/o servicios que no se tomarán en cuenta.

El alcance del presente proyecto está plasmado en el documento de **Versión 1.1 del Anexo A.2.**

4.1.2. Política de seguridad de la Información.-

(Ver Anexo A.3)

El documento de la política de seguridad de la información, es de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información. Incluye el marco general y los objetivos de seguridad de la información.
Una vez aprobado el documento por la dirección mediante una resolución, dicha política debe de ser difundida en toda la organización.

La política de seguridad del presente proyecto está plasmada en el documento de **Versión 1.1 del Anexo A.3.**

DERECHOS DE AUTOR RESERVADOS

4.1.3. Metodología de Gestión de Riesgos.-

(Ver Anexo A.4)

El documento de la metodología de evaluación de riesgos establece los criterios para evaluar y determinar el valor de los activos, de las amenazas, y de las vulnerabilidades que pueden presentarse en la organización.
Desarrolla además los criterios de aceptación de riesgos y determina el nivel de riesgo aceptable.

El Procedimiento de Gestión de Riesgos comprende 4 etapas: Inventario de Activos, Análisis de Riesgos, Evaluación de Riesgos y Tratamiento de Riesgos.

Imagen N°13 - *Procedimiento de Gestión de Riesgos*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

La metodología de Gestión Riesgos del presente proyecto está plasmada en el documento de **Versión 1.1 del Anexo A.4.**

DERECHOS DE AUTOR RESERVADOS

4.1.4. Inventario de Activos.-

El Inventario de Activos de la Unidad de Tecnologías de la Información se ha completado según el proceso descrito en el en el Documento de la Metodología de Gestión de Riesgos mencionado anteriormente (Anexo A.4). Cada registro del inventario se encuentra dentro del alcance del proyecto.

Imagen N°14 - *Inventario de Activos*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

Dicho inventario está plasmado en la **Tabla N° 2** , la cual podemos apreciar a continuación:

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

INVENTARIO DE ACTIVOS																		1 de 5
N°	Activo	Descripción	Categoría	Clasificación			Frecuencia de Uso					Propietario	Custodio	Valor del Activo y Nivel de Tasación				
				Pública	Uso Interno	Uso Restringido	Diario	Semanal	Quincenal	Mensual	Eventual			Confidencialidad	Integridad	Disponibilidad	Valor del Activo	Nivel de Tasación
Activos de Información																		
1	Documentación en General	Informes, Memorándums, Oficios, Resoluciones, Solicitudes, entre otros	I2		X		X					Jefe de la UTI	Central de Atenciones	3	3	2	**2.667**	**Medio**
2	Documentos de control de Acceso	Formatos de alta, de baja, de cambio de usuarios y control de acceso a internet	I2		X		X					Operador de Sistemas	Practicantes	4	3	4	**3.667**	**Alto**
3	Manuales de Usuario	Manuales de los procedimientos realizados en la UTI y de sistemas utilizados en la organización	I2		X			X				Técnico en Sistemas	Practicantes	2	3	3	**2.667**	**Medio**
4	Copias de Partidas y Títulos registrales	Copias físicas de partidas y títulos registrales obtenidos del archivo registral para ser subidas al servidor de Imágenes keyfile	I2			X					X	Operador de Sistemas	Practicantes	3	4	4	**3.667**	**Alto**
5	Documentos Digitales	Documentación general escaneada	I1		X		X					Jefe de la UTI	Central	2	2	3	**2.333**	**Medio**
6	Correos Electrónicos Zimbra	Correos electrónicos enviados y recibidos mediante el servidor de correo	I1			X	X					Todos los trabajadores de la UTI	Todos los trabajadores de la UTI	4	3	3	**3.333**	**Medio**
7	Registros de Base de Datos	Base de datos que contiene toda la información registral de los usuarios	I1			X	X					Jefe de la UTI	Especialista en Base de Datos	4	4	4	**4**	**Alto**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

INVENTARIO DE ACTIVOS																		2 de 5
N°	Activo	Descripción	Categoría	Clasificación			Frecuencia de Uso					Propietario	Custodio	Valor del Activo y Nivel de Tasación				
				Pública	Uso Interno	Uso Restringido	Diario	Semanal	Quincenal	Mensual	Eventual			Confidencialidad	Integridad	Disponibilidad	Valor del Activo	Nivel de Tasación
Activos de Información																		
8	Registro de Imágenes digitales	Imágenes de títulos y partidas generadas por los sistemas registrales	I1			X	X					Jefe de la UTI	Operador de Sistemas	4	4	4	**4**	**Alto**
9	Llamadas Telefónicas	Llamadas internas (Anexos) y externas de la UTI	I3		X		X					Todos los trabajadores de la UTI	Todos los trabajadores de la UTI	3	2	3	**2.667**	**Medio**
10	Reuniones semanales	Información obtenida, acuerdos y toma de decisiones en reuniones de todo el personal de la UTI semanalmente	I3		X			X				Jefe de la UTI	Todos los trabajadores de la UTI	3	2	2	**2.333**	**Medio**
Activos de Software																		
11	Sistema de Consulta Registral	Sistema para la consulta de títulos y partidas	SW3		X		X					Técnico de Sistemas	Todos los trabajadores de la UTI	3	4	4	**3.667**	**Alto**
12	Sistema Registro Propiedad Vehicular (RPV)	Sistema para la Inscripción y Consulta de vehículos	SW3		X		X					Técnico de Sistemas	Todos los trabajadores de la UTI	3	4	4	**3.667**	**Alto**
13	Sistema Automatizado del Registro Predial (SARP)	Sistema para la inscripción y consulta de predios rurales	SW3		X		X					Técnico de Sistemas	Todos los trabajadores de la UTI	3	4	4	**3.667**	**Alto**
14	Sistema de Trámite Documentario (SISTRAM)	Sistema para el envío de documentos internos digitales	SW3			X	X					Jefe de la UTI	Central de Atenciones	2	2	3	**2.333**	**Medio**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

INVENTARIO DE ACTIVOS																		3 de 5
N°	Activo	Descripción	Categoría	Clasificación			Frecuencia de Uso					Propietario	Custodio	Valor del Activo y Nivel de Tasación				
				Pública	Uso Interno	Uso Restringido	Diario	Semanal	Quincenal	Mensual	Eventual			Confidencialidad	Integridad	Disponibilidad	Valor del Activo	Nivel de Tasación
Activos de Software																		
15	Sistema de Control de Accesos	Sistema para generar claves de acceso a los sistemas	SW3			X		X				Técnico de Sistemas	Practicantes	4	3	3	**3.333**	**Medio**
16	Sistema de Inventario de Hardware y Software	Sistema que maneja y controla el inventario de HW y SW	SW3									Jefe de la UTI	Técnico de Sistemas	3	3	3	**3**	**Medio**
17	Sistema de Estadística y Productividad	Sistema que controla la productividad y estadística del trabajo de los registradores	SW2 / SW3			X	X					Jefe de la UTI	Técnico de Sistemas	3	4	3	**3.333**	**Medio**
18	SQL Plus	Programa que permite ejecutar comandos SQL	SW4			X	X					Especialista en Base de Datos	Todos los trabajadores de la UTI	4	4	4	**4**	**Alto**
Activos Físicos																		
19	Computador	Equipo utilizado para el trabajo diario del personal de la UTI	F1		X		X					Jefe de la UTI	Todos los trabajadores de la UTI	4	4	4	**4**	**Alto**
20	Laptop	Equipo Utilizado para el trabajo del personal de la UTI	F1		X						X	Jefe de la UTI	Todos los trabajadores de la UTI	1	1	2	**1.333**	**Bajo**
21	Servidor de Dominio Zonal	Equipo encargado de administrar el Dominio de la Zona X.	F1			X	X					Jefe de la UTI	Operador de Sistemas	4	4	4	**4**	**Alto**
22	Servidor de Keyfile	Equipo Virtual que permite administrar imágenes de títulos y partidas registrales.	F1			X	X					Jefe del UTI	Operador de Sistemas	4	4	4	**4**	**Alto**
23	Servidor de Base de Datos	Equipo físico que contiene todos los registros de Base de Datos de la Zona X.	F1			X	X					Jefe de la UTI	Especialista de Base de Datos	4	4	4	**4**	**Alto**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

INVENTARIO DE ACTIVOS																		4 de 5
N°	Activo	Descripción	Categoría	Clasificación			Frecuencia de Uso					Propietario	Custodio	Valor del Activo y Nivel de Tasación				
				Pública	Uso Interno	Uso Restringido	Diario	Semanal	Quincenal	Mensual	Eventual			Confidencialidad	Integridad	Disponibilidad	Valor del Activo	Nivel de Tasación
Activos Físicos																		
24	Servidor Authasas	Equipo Virtual que permite el acceso biométrico de los registradores a los sistemas	F1			X	X					Jefe del UTI	Operador de Sistemas	4	3	3	**3.333**	**Medio**
25	Servidores Citrix	Equipo Virtual que permite la vitalización de aplicaciones registrales.	F1			X	X					Jefe del UTI	Operador de Sistemas	2	2	2	**2**	**Bajo**
26	Servidor de Archivos	Equipo virtual que almacena y administra archivos de las oficinas de la organización	F1			X	X					Jefe del UTI	Operador de Sistemas	4	4	4	**4**	**Alto**
27	Servidor de Replicación	Equipo Virtual que sincroniza los datos con el servidor central de la organización	F1			X	X					Jefe del UTI	Especialista de Base de Datos	3	4	4	**3.667**	**Alto**
28	Discos Duros Externos	Discos utilizados para almacenar información de la UTI	F3		X						X	Técnico de Sistemas	Todos los trabajadores de la UTI	2	2	2	**2**	**Bajo**
29	Cintas de Backup DLT	Cintas magnéticas utilizadas para el backup de la información predial de la información	F3			X	X					Jefe del UTI	Operador de Sistemas	5	5	5	**5**	**Alto**
Persona (Clientes, Empleados, Personal Externo)																		
30	Jefe de la UTI	Jefe encargado de la Unidad de Tecnologías de la Información	P2		X		X					N/A	N/A	4	4	4	**4**	**Alto**
31	Operador de Sistemas	Encargado del Data Center	P2		X		X					N/A	N/A	4	4	4	**4**	**Alto**
32	Especialista en Base de Datos	Encargado de la administración de la base de datos Oracle	P2		X		X					N/A	N/A	4	4	4	**4**	**Alto**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

INVENTARIO DE ACTIVOS																		5 de 5
N°	Activo	Descripción	Categoría	Clasificación			Frecuencia de Uso					Propietario	Custodio	Valor del Activo y Nivel de Tasación				
				Pública	Uso Interno	Uso Restringido	Diario	Semanal	Quincenal	Mensual	Eventual			Confidencialidad	Integridad	Disponibilidad	Valor del Activo	Nivel de Tasación
Persona (Clientes, Empleados, Personal Externo)																		
33	Técnico de Sistemas	Encargado de la supervisión del mantenimiento de los sistemas	P2		X		X					N/A	N/A	4	4	4	**4**	**Alto**
34	Central de Atenciones	Encargado de la recepción y delegación de todos los pedidos y atenciones de los usuarios	P2	X			X					N/A	N/A	3	4	4	**3.667**	**Alto**
35	Programador de Sistemas	Encargado de continuar con el desarrollo de programas y sistemas para la institución	P2		X		X					N/A	N/A	3	2	3	**2.667**	**Medio**
36	Replicador de Base de Datos	Encargado de revisar que la replicación de la base de datos a la bodega central se realice correctamente	P2		X		X					N/A	N/A	3	3	3	**3**	**Medio**
37	Practicantes Profesionales	Apoyan en las labores diarias de la UTI, se encargan de atender los pedidos de los usuarios	P2	X			X					N/A	N/A	3	2	3	**2.333**	**Medio**
38	Servicio de Terceros	Personas contratadas temporalmente para proyectos pequeños	P4		X						X	N/A	N/A	2	2	2	**2**	**Medio**

Tabla N°2 - *Inventario de Activos de la UTI*

Fuente: *Elaboración propia*

DERECHOS DE AUTOR RESERVADOS

4.1.5. Análisis de Riesgos.-

Una vez completado el inventario de activos de la Unidad de Tecnologías de la información, se deberá realizar el correspondiente Análisis de Riesgos, en donde identificaremos las amenazas que afectan a los activos, y las vulnerabilidades existentes que las amenazas aprovechan.

Imagen N°15 - *Análisis de Riesgos*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

El Análisis de Riesgos de la Unidad de Tecnologías de la Información se ha completado según el proceso descrito en el en el Documento de la Metodología de Gestión de Riesgos mencionado anteriormente (Anexo A.4).

Dicho análisis está plasmado en la **Tabla N° 3** , la cual podemos apreciar a continuación:

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN													1 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos de Información													
1	Documentación en General	Divulgación no autorizada	4	Armarios con llave	2	-	1	-	1	Personal descontento o solicitud de favores	4.667	**4.334**	**Alto**
		Robo de información	3	Armarios con llave	2	-	1	-	1	Personal con malas intenciones	4.667	**3.834**	**Alto**
		Deterioro por el ambiente y medio de almacenaje	2	Servicio de Limpieza	2	-	1	Servicio de Limpieza	1	Los documentos de años pasados se almacena en cajas y no tienen un control de limpieza	4.667	**3.334**	**Alto**
		Incendio originado dentro de la organización	1	Extinguidores	3	-	1	Bomberos se encuentran cerca	2	Cortos circuitos por bajas de energía	4	**2.5**	**Medio**
2	Documentos de control de Acceso	Divulgación no autorizada	4	Armarios con llave	2	-	1	-	1	Personal con malas intenciones	4.667	**4.334**	**Alto**
		Mal uso de la información por personas no autorizadas	3	Control de entrega de documentos	3	-	1	-	1	Personal con malas intenciones	4.333	**3.667**	**Alto**
3	Manuales de Usuario	Falla en el correcto uso de los manuales	3	Revisión constante de los manuales	2	Personal de la UTI	2	Revisión y actualización de manuales	2	Manuales desactualizados y/o no completos	4	**3.5**	**Alto**
		Procedimientos de trabajo no se realizan correctamente	4	Enseñar el uso de los manuales a inicio de trabajo de cada personal	2	Personal de la UTI	2	Hacer de conocimiento la existencia de los manuales a todo el personal	2	La mayoría de los trabajadores que ingresan a trabajar a la UTI desconocen la existencia de dichos manuales	4	**4**	**Alto**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN													2 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos de Información													
4	Copias de partidas y Títulos registrales	Robo de información	3	Archivo seguro para dichas partidas y títulos	2	Personal de la UTI	2	-	1	Las copias de los títulos y partidas no están clasificadas ni están guardadas en un lugar seguro	4.333	**3.667**	**Alto**
		Divulgación no autorizada, venta de la información	3	Archivo seguro para dichas partidas y títulos	2	-	1	Llamadas de atención al personal sobre la no divulgación	2	Las copias de los títulos y partidas no se encuentran en un lugar seguro	4.333	**3.667**	**Alto**
5	Documentos Digitales	Sustracción de información	3	Accesos a carpetas restringidas	2	-	1	-	1	El acceso a las carpetas que contienen dichos documentos no es restringido	4.667	**3.834**	**Alto**
		Modificación no autorizada de la información	3	Accesos a carpetas restringidas	2	Personal de la UTI	2	-	1	El acceso a las carpetas que contienen dichos documentos no es restringido	4.333	**3.667**	**Alto**
6	Correos Electrónicos Zimbra	Virus y Pishing	3	Prevenir a los usuarios sobre correos con remitentes desconocidos	2	Personal de la UTI	2	Reportes de existencia de virus y pishing a la sede central	2	Usuarios desconocen cuáles son los correos en donde pueden ser atacados por pishing y/o virus	4	**3.5**	**Alto**
		Divulgación no autorizada	2	Acceso a correos electrónicos restringidos	2	-	1	-	1	Usuarios comparten su clave del correo electrónico o ésta no cuenta con la seguridad necesaria	4.667	**3.334**	**Alto**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN													3 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos de Información													
7	Registros de Base de Datos	Sustracción de información	3	Acceso restringido a la base de datos	3	-	1	Revisión tablas de auditoría	2	No existen alertas cuando sustraen información sin autorización	4	**3.5**	**Alto**
		Divulgación no autorizada	3	Permisos restringidos	3	-	1	Revisión tablas de auditoría	2	No existen alertas cuando divulgan información sin autorización	4	**3.5**	**Alto**
		Modificación no autorizada de la información	3	Permisos restringidos	3	-	1	Revisión tablas de auditoría	2	Los permisos de manejo de las tablas no están totalmente definidas	4	**3.5**	**Alto**
8	Registro de Imágenes digitales	Sustracción de información	3	Acceso restringido	3	-	1	-	1	Existen cuentas generales para el acceso al registro de imágenes en las sedes de la Zona X	4.333	**3.665**	**Alto**
		Divulgación no autorizada	3	Acceso restringido	3	-	1	-	1	No existen restricciones de acceso para el registro de imágenes de todas las sedes de la Zona X	4.333	**3.665**	**Alto**
		Modificación no autorizada de la información	3	Permisos restringidos	3	-	1	-	1	Existen cuentas generales para el acceso al registro de imágenes en las sedes de la Zona X	4.333	**3.665**	**Alto**
9	Llamadas Telefónicas	Caída del servicio de telefonía fija	2	-	1	Personal de la UTI	2	Informe del problema a la empresa del servicio	3	Problemas externos que presenta la empresa de telefonía	4	**3**	**Medio**
10	Reuniones semanales	Divulgación no autorizada	5	-	1	Personal de la UTI	2	Llamadas de atención	2	Falta de ética	4.333	**4.665**	**Alto**
		Parte de la información ya mencionada se pierde	5	Apuntes y notas sobre lo hablado	2	-	1	-	1	No hay control de reuniones ni un acta de la información mencionada	4.667	**4.834**	**Alto**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN												4 de 13	
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos de Software													
11	Sistema de Consulta Registral	Sistema desactualizado	3	Correos electrónicos indicando nuevas actualizaciones	3	Mensaje de advertencia	2	Actualización del Sistema	2	Las actualizaciones del sistema no están documentadas y no siempre se realizan a tiempo	3.667|	**3.334**	**Alto**
		Acceso no autorizado	3	Entrega de claves de acceso en sobres sellados	3	Mensajes de advertencia	2	-	1	Algunos trabajadores comparten sus usuarios y claves	4	**3.5**	**Alto**
		Impresiones no autorizadas	3	Permisos controlados bajo perfiles para impresiones	3	Mensajes de advertencia	2	Corrección de perfiles y retiro de privilegios de impresión	2	No todos los usuarios cuentan con restricciones de impresión	3.667	**3.334**	**Alto**
12	Sistema Registro Propiedad Vehicular (RPV)	Sistema desactualizado	3	Correos electrónicos indicando nuevas actualizaciones	3	Mensaje de advertencia	2	Actualización del Sistema	2	Las actualizaciones del sistema no están documentadas y no siempre se realizan a tiempo	3.667	**3.334**	**Alto**
		Acceso no autorizado	2	Entrega de claves de acceso en sobres sellados	3	Mensajes de advertencia	2	-	1	Algunos trabajadores comparten sus usuarios y claves	4	**3**	**Medo**
		Impresiones no autorizadas	2	Permisos controlados bajo perfiles para impresiones	3	Mensajes de advertencia	2	Corrección de perfiles y retiro de privilegios de impresión	2	No todos los usuarios cuentan con restricciones de impresión	3.667	**2.834**	**Medio**
13	Sistema Automatizado del Registro Predial (SARP)	Sistema desactualizado	2	Correos electrónico. indicando nuevas actualizaciones	3	Mensaje de advertencia	2	Actualización del Sistema	2	Las actualizaciones del sistema no están documentadas y no siempre se realizan a tiempo	3.667	**2.834**	**Medio**
		Acceso no autorizado	2	Entrega de claves de acceso en sobres sellados	3	Mensajes de advertencia	2	-	1	Algunos trabajadores comparten sus usuarios y claves	4	**3**	**Medio**
		Impresiones no autorizadas	3	Permisos controlados bajo perfiles para impresiones	3	Mensajes de advertencia	2	Corrección de perfiles y retiro de privilegios de impresión	2	No todos los usuarios cuentan con restricciones de impresión	3.667	**3.334**	**Alto**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN													5 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos de Software													
14	Sistema de Trámite Documentario (SISTRAM)	Sistema desactualizado	2	Correos electrónicos indicando nuevas actualizaciones	1	-	1	Actualización del Sistema	2	Las actualizaciones del sistema no están documentadas y no siempre se realizan a tiempo	4.667	**3.334**	**Alto**
		Acceso no autorizado	4	Entrega de claves de acceso en sobres sellados	3	Mensajes de advertencia	2	-	1	Algunos trabajadores comparten sus usuarios y claves	4	**4**	**Alto**
15	Sistema de Control de Accesos	Acceso no autorizado	3	El número de personas con acceso es limitado	1	-	1	-	1	Existe solo un usuario y clave genérico para todo aquel que usa el sistema	5	**4**	**Alto**
16	Sistema de Inventario de Hardware y Software	Acceso no autorizado	2	Entrega de claves de acceso en sobres sellados	3	Mensajes de advertencia	2	-	1	Algunos trabajadores comparten sus usuarios y claves	4	**3**	**Medio**
		Mal uso del sistema por desactualización de datos	4	Ingreso de datos y revisiones constantes	2	-	1	Corrección/ Actualización de datos del sist.	2	El inventario de Hardware y Software no suele estar actualizado	4.333	**4.167**	**Alto**
17	Sistema de Estadística y Productividad	Acceso no autorizado	2	Entrega de claves de acceso en sobres sellados	3	Mensajes de advertencia	2	-	1	Algunos trabajadores comparten sus usuarios y claves	4	**3**	**Medio**
		Información proporcionada incorrecta	3	Revisión de la información del sistema	1	Usuarios del Sistema	2	Corrección y actualización de datos del sistema	2	El sistema presenta algunos errores emitiendo información precisa	4.333	**3.667**	**Alto**
18	SQL Plus	Acceso no autorizado	3	Entrega de claves de acceso en sobres sellados	3	Mensajes de advertencia	2	Bloqueos de cuenta	2	Algunos trabajadores comparten sus usuarios y claves	2.333	**2.667**	**Medio**
		Modificación no autorizada de la información	4	Permisos de usuarios controlados	3	Mensajes de advertencia	2	Cambios en los permisos de los usuarios	2	No todas las restricciones de cuentas son monitoreadas	2.333	**3.167**	**Medio**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN												6 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos Físicos													
19	Computadora	Daño físico de equipos	4	Mantenimiento periódico de equipos	2	Personal de UTI	2	Garantías de equipos	2	Descuido del personal	4	**4**	**Alto**
		Virus	4	Antivirus instalados en los equipo	3	Personal de la UTI	2	Aplicación de políticas de seguridad	3	No todos los puertos USB ni las lectoras están deshabilitadas	3.333	**3.667**	**Alto**
		Accesos no autorizados	3	Políticas de acceso	3	-	1	Limitación de accesos	2	Mala administración de privilegios de acceso	4	**3.5**	**Alto**
		Información usada indebidamente una vez dado el bien de baja	2	Control de bienes para baja	3	Técnico de Sistemas	3	-	1	Falta de destrucción de la información	3.667	**2.834**	**Medio**
		Incongruencia de fecha y hora	3	Revisión periódica del tiempo en las computadoras	2	Técnico de Sistemas	3	Sincronización de tiempo con todos los servidores	2	No contar con un estándar de tiempo ni con los servidores sincronizados	3.667	**3.334**	**Alto**
20	Laptop	Daño físico de equipo	3	Mantenimiento periódico de equipos	1	Personal de la UTI	2	Garantía de equipos	2	Descuido del personal	4.333	**3.667**	**Alto**
		Robo de equipo	2	Control de seguridad externo	2	Control de seguridad externo	2	-	1	No controlan el movimiento del equipo por la institución	4.333	**3.167**	**Medio**
		Información usada indebidamente una vez dado el bien de baja	2	Control de bienes para baja	3	Personal de Almacén	3	-	1	Falta de destrucción de la información	3.667	**2.834**	**Medio**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN												7 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos Físicos													
21	Servidor de Dominio Zonal	Daño físico de equipos	2	Mantenimiento periódico de equipos	3	Operador de Sistemas	3	Garantía de equipos	1	Descuido del personal	3.667	**2.834**	**Medio**
		Virus	2	Antivirus instalados en los equipo	3	Operador de Sistemas	2	Aplicación de políticas de seguridad	3	Circulación de virus en la red por el descuido de otra computadora	3.333	**2.667**	**Medio**
		Incongruencia de fecha y hora	3	Revisión periódica del tiempo en los servidores	2	Operador de Sistemas	3	Sincronización de tiempo con todos los servidores	2	No contar con un estándar de tiempo ni con los servidores sincronizados	3.667	**3.334**	**Alto**
22	Servidor de Keyfile	Daño físico de equipos	2	Mantenimiento periódico de equipos	3	Operador de Sistemas	3	Garantía de equipos	1	Descuido del personal	3.667	**2.834**	**Medio**
		Virus	2	Antivirus instalados en los equipo	3	Operador de Sistemas	2	Aplicación de políticas de seguridad	3	Circulación de virus en la red por el descuido de otra computadora	3.333	**2.667**	**Medio**
		Incongruencia de fecha y hora	3	Revisión periódica del tiempo en los servidores	2	Operador de Sistemas	3	Sincronización de tiempo con todos los servidores	2	No contar con un estándar de tiempo ni con los servidores sincronizados	3.667	**3.334**	**Alto**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN												8 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos Físicos													
23	Servidor de Base de Datos	Daño físico de equipos	2	Mantenimiento periódico de equipos	3	Especialista en Base de Datos	3	Garantía de equipos	1	Descuido del personal	3.667	**2.834**	**Medio**
		Virus	2	Antivirus instalados en los equipo	3	Especialista en Base de Datos	2	Aplicación de políticas de seguridad	3	Circulación de virus en la red por el descuido de otra computadora	3.333	**2.667**	**Medio**
		Incongruencia de fecha y hora	3	Revisión periódica del tiempo en los servidores	2	Especialista en Base de Datos	3	Sincronización de tiempo con todos los servidores	2	No contar con un estándar de tiempo ni con los servidores sincronizados	3.667	**3.334**	**Alto**
24	Servidor Authasas	Daño físico de equipos	2	Mantenimiento periódico de equipos	3	Operador de Sistemas	3	Garantía de equipos	1	Descuido del personal	3.667	**2.834**	**Medio**
		Virus	2	Antivirus instalados en los equipo	3	Operador de Sistemas	2	Aplicación de políticas de seguridad	3	Circulación de virus en la red por el descuido de otra computadora	3.333	**2.667**	**Medio**
25	Servidores Citrix	Daño físico de equipos	2	Mantenimiento periódico de equipos	3	Operador de Sistemas	3	Garantía de equipos	1	Descuido del personal	3.667	**2.834**	**Medio**
		Virus	2	Antivirus instalados en los equipo	3	Operador de Sistemas	2	Aplicación de políticas de seguridad	3	Circulación de virus en la red por el descuido de otra computadora	3.333	**2.667**	**Medio**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN												9 de 13	
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos Físicos													
26	Servidor de Archivos	Daño físico de equipos	2	Mantenimiento periódico de equipos	3	Operador de Sistemas	3	Garantía de equipos	1	Descuido del personal	3.667	**2.834**	**Medio**
		Virus	2	Antivirus instalados en los equipo	3	Operador de Sistemas	2	Aplicación de políticas de seguridad	3	Circulación de virus en la red por el descuido de otra computadora	3.333	**2.667**	**Medio**
27	Servidor de Replicación	Daño físico de equipos	2	Mantenimiento periódico de equipos	3	Operador de Sistemas	3	Garantía de equipos	1	Descuido del personal	3.667	**2.834**	**Medio**
		Virus	2	Antivirus instalados en los equipo	3	Operador de Sistemas	2	Aplicación de políticas de seguridad	3	Circulación de virus en la red por el descuido de otra computadora	3.333	**2.667**	**Medio**
		Incongruencia de fecha y hora	3	Revisión periódica del tiempo en los servidores	2	Especialista en Base de Datos	3	Sincronización de tiempo con todos los servidores	2	No contar con un estándar de tiempo ni con los servidores sincronizados	3.667	**3.334**	**Alto**
28	Discos Duros Externos	Robo de disco duro	3	Discos almacenados en gavetas	1	Personal de UTI	2	-	1	Los discos duros no están guardados en ligares seguros	4.667	**3.834**	**Alto**
		Daño físico del disco duro	2	Uso correcto por parte del personal de UTI	2	Personal de UTI	2	Arreglo del disco / recuperación de información	2	Descuido del personal	4	**3**	**Medio**
		Información usada indebidamente una vez dado el bien de baja	2	Control de bienes para baja	3	Personal de Almacén	3	-	1	Falta de destrucción de la información	3.667	**2.834**	**Medio**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN												10 de 13
N°	Activo	Amenaza		Mecanismo de protección existente					Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos Físicos													
29	Cintas de Backup DLT	Robo de cintas	2	Cintas almacenadas en caja fuerte	3	Personal de UTI	2	-	1	La combinación de la caja fuerte la conocen varias personas	4	**3**	**Medio**
		Daño físico de cintas	2	Uso correcto por parte del personal de UTI	3	Operador de sistemas	3	-	1	Descuido del personal	3.667	**2.834**	**Medio**
Amenazas al Personal (Clientes, Empleados, Personal Externo)													
30	Jefe de la UTI	Renuncia del personal	1	Aumento de sueldo para el personal de planta	4	Personal de la UTI	2	Contratación de un personal para dicho puesto	4	Falta de motivaciones o incentivos laborales	2.667	**1.834**	**Medio**
		Personal descontento	2	Motivaciones laborales	2	Personal de la UTI	2	Trata con el personal para resolver inquietudes	2	Falta de motivaciones o incentivos laborales	4	**3**	**Medio**
31	Operador de Sistemas	Renuncia del personal	1	Aumento de sueldo para el personal de planta	4	Personal de la UTI	2	Contratación de un personal para dicho puesto	4	Falta de motivaciones o incentivos laborales	2.667	**1.834**	**Medio**
		Personal descontento	2	Motivaciones laborales	2	Personal de la UTI	2	Trata con el personal para resolver inquietudes	2	Falta de motivaciones o incentivos laborales	4	**3**	**Medio**
32	Especialista en Base de Datos	Renuncia del personal	2	Aumento de sueldo para el personal de planta	4	Personal de la UTI	2	Contratación de un personal para dicho puesto	4	Falta de motivaciones o incentivos laborales	2.667	**2.334**	**Medio**
		Personal descontento	2	Motivaciones laborales	2	Personal de la UTI	2	Trata con el personal para resolver inquietudes	2	Falta de motivaciones o incentivos laborales	4	**3**	**Medio**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN												11 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas al Personal (Clientes, Empleados, Personal Externo)													
33	Técnico de Sistemas 1	Renuncia del personal	2	Aumento de sueldo para el personal de planta	4	Personal de la UTI	2	Contratación de un personal para dicho puesto	4	Falta de motivaciones o incentivos laborales	2.667	**2.334**	**Medio**
		Personal descontento	2	Motivaciones laborales	2	Personal de la UTI	2	Trata con el personal para resolver inquietudes	2	Falta de motivaciones o incentivos laborales	4	**3**	**Medio**
		Sobrecarga de tareas	4	Funciones correctamente definidas	3	Personal de la UTI	2	Delegación de funciones a otras personas	2	Personal realiza además las funciones del puesto de un técnico de sistemas 2 el cual actualmente nadie lo ocupa	3.667	**3.834**	**Alto**
34	Central de Atenciones	Renuncia del personal	3	Motivaciones laborales, seguro de salud	2	Personal de la UTI	2	Contratación de un personal para dicho puesto	4	Cuenta con un sueldo promedio que no justifica el trabajo realizado	3.333	**3.167**	**Medio**
		Personal descontento	2	Brindar motivación para un mejor desempeño laboral	2	Personal de la UTI	2	Trata con el personal para resolver inquietudes	2	Falta de motivaciones o incentivos laborales. No existe línea de carrera	4	**3**	**Medio**
		Sobrecarga de tareas	4	Funciones correctamente definidas	3	Personal de la UTI	2	Delegación de funciones a otras personas	2	El número de personas trabajando en la UTI no cubre con la cantidad de pedidos a atender	3.667	**3.834**	**Alto**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN												12 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas al Personal (Clientes, Empleados, Personal Externo)													
35	Programador de Sistemas	Renuncia del personal	2	Motivaciones laborales, seguro de salud	2	Personal de la UTI	2	Contratación de un personal para dicho puesto	4	Cuenta con un sueldo mínimo que no justifica el trabajo realizado	3.333	**2.667**	**Medio**
		Personal descontento	2	Brindar motivación para un mejor desempeño laboral	2	Personal de la UTI	2	Trata con el personal para resolver inquietudes	2	Falta de motivaciones o incentivos laborales. No existe línea de carrera	4	**3**	**Medio**
		Delegación de funciones no correspondientes a su puesto	3	Funciones correctamente definidas	3	Personal de la UTI	2	Delegación de funciones a otras personas	2	El número de personas trabajando en la UTI no cubre con la cantidad de pedidos a atender	3.667	**3.334**	**Alto**
36	Replicador de Base de Datos	Renuncia del personal	2	Motivaciones laborales, seguro de salud	2	Personal de la UTI	2	Contratación de un personal para dicho puesto	4	Cuenta con un sueldo promedio que no justifica el trabajo realizado	3.333	**2.667**	**Medio**
		Personal descontento	2	Brindar motivación para un mejor desempeño laboral	2	Personal de la UTI	2	Trata con el personal para resolver inquietudes	2	Falta de motivaciones o incentivos laborales. No existe línea de carrera	4	**3**	**Medio**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN												13 de 13
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas al Personal (Clientes, Empleados, Personal Externo)													
37	Practicantes Profesionales	Renuncia del personal	3	Brindar primera experiencia laboral	3	Personal de la UTI	2	Convocatoria para más practicantes	4	Cuenta con un sueldo mínimo que no justifica el trabajo realizado	3	**3**	**Medio**
		Personal descontento	3	Motivaciones laborales, seguro de salud	2	Personal de la UTI	2	Tratar con el personal para resolver inquietudes	2	Falta de motivaciones o incentivos laborales. No existe línea de carrera	4	**3.5**	**Alto**
		Sobrecarga de tareas	4	Funciones correctamente definidas	3	Personal de la UTI	2	Delegación de funciones a otras personas	2	El número de personas trabajando en la UTI no cubre con la cantidad de pedidos a atender	3.667	**3.834**	**Alto**
38	Servicio de Terceros	Incumplimiento de trabajo en el tiempo indicado	2	Planificación correcta de las metas propuestas	2	Personal de la UTI	2	-	1	No todos los servicios de terceros se planifican ni monitorean	4.333	**3.167**	**Medio**

Tabla N°3 - *Análisis de riesgos de la UTI*

Fuente: *Elaboración propia*

DERECHOS DE AUTOR RESERVADOS

4.1.6. Evaluación de Riesgos.-

El siguiente paso, una vez analizado los riesgos de la Unidad de Tecnologías de la Información, será realizar su correspondiente evaluación, en donde identificaremos cuan crítico es el nivel de riesgo de acuerdo al impacto legal, económico/imagen u operacional que tiene la amenaza.

Imagen N°16 - *Evaluación de Riesgos*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

La Evaluación de Riesgos de la Unidad de Tecnologías de la Información se ha completado según el proceso descrito en el en el Documento de la Metodología de Gestión de Riesgos mencionado anteriormente (Anexo A.4).

Dicha evaluación está plasmada en la **Tabla N°4** , la cual podemos apreciar a continuación:

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

EVALUACIÓN DE RIESGOS										1 de 7
N°	Activo	Amenaza	Criterios de Evaluación						Riesgo Efectivo	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico / Imagen Institucional	Impacto Operacional	Nivel de Impacto				
Amenazas a los Activos de Información										
1	Documentación en General	Divulgación no autorizada	3	1	1	1.667	4.334	2.667	**2.889**	**Moderado**
		Robo de información	4	2	2	2.667	3.834		**3.056**	**Moderado**
		Deterioro por el ambiente y medio de almacenaje	2	1	1	1.333	3.334		**2.445**	**Moderado**
		Incendio originado dentro de la organización	3	1	3	2.333	2.5		**2.5**	**Moderado**
2	Documentos de control de Acceso	Divulgación no autorizada	3	1	3	2.333	4.334	3.667	**3.445**	**Crítico**
		Mal uso de la información por personas no autorizadas	2	1	2	1.667	3.667		**3**	**Moderado**
3	Manuales de Usuario	Falla en el correcto uso de los manuales	3	1	2	2	3.5	2.667	**2.722**	**Moderado**
		Procedimientos de trabajo no se realizan correctamente	3	2	4	3	4		**3.222**	**Moderado**
4	Copias de partidas y Títulos registrales	Robo de información	4	3	3	3.333	3.667	3.667	**3.556**	**Crítico**
		Divulgación no autorizada, venta de la información	4	3	2	3	3.667		**3.445**	**Crítico**
5	Documentos Digitales	Sustracción de información	2	1	2	1.667	3.834	2.333	**2.611**	**Moderado**
		Modificación no autorizada de la información	2	2	2	2	3.667		**2.667**	**Moderado**
6	Correos Electrónicos Zimbra	Virus y Pishing	2	1	2	1.667	3.5	3.333	**2.833**	**Moderado**
		Divulgación no autorizada	2	2	1	1.667	3.334		**2.778**	**Moderado**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

EVALUACIÓN DE RIESGOS 2 de 7

N°	Activo	Amenaza	Criterios de Evaluación						Riesgo Efectivo	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico / Imagen Institucional	Impacto Operacional	Nivel de Impacto				
Amenazas a los Activos de Información										
7	Registros de Base de Datos	Sustracción de información	4	3	4	3.667	3.5	4	**3.722**	**Crítico**
		Divulgación no autorizada	4	2	3	3	3.5		**3.5**	**Crítico**
		Modificación no autorizada de la información	4	3	4	3.667	3.5		**3.722**	**Crítico**
8	Registro de Imágenes digitales	Sustracción de información	4	3	4	3.667	3.665	4	**3.777**	**Crítico**
		Divulgación no autorizada	4	2	3	3	3.665		**3.555**	**Crítico**
		Modificación no autorizada de la información	4	3	4	3.667	3.665		**3.777**	**Crítico**
9	Llamadas Telefónicas	Caída del servicio de telefonía fija	2	1	3	2	3	2.667	**2.556**	**Moderado**
10	Reuniones semanales	Divulgación no autorizada	2	1	1	1.333	4.665	2.333	**2.777**	**Moderado**
		Información no es comprendida en un 100% por los participantes	2	1	2	1.667	4.834		**2.945**	**Moderado**
Amenazas a los Activos de Software										
11	Sistema de Consulta Registral	Sistema desactualizado	2	1	3	2	3.334	3.667	**3**	**Moderado**
		Acceso no autorizado	3	1	2	2	3.5		**3.056**	**Moderado**
		Impresiones no autorizadas	3	1	2	2	3.334		**3**	**Moderado**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

EVALUACIÓN DE RIESGOS										3 de 7
N°	Activo	Amenaza	Criterios de Evaluación						Riesgo Efectivo	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico / Imagen Institucional	Impacto Operacional	Nivel de Impacto				
Amenazas a los Activos de Software										
12	Sistema Registro Propiedad Vehicular (RPV)	Sistema desactualizado	2	1	3	2	3.334	3.667	3	Moderado
		Acceso no autorizado	3	1	2	2	3		2.889	Moderado
		Impresiones no autorizadas	3	1	2	2	2.834		2.834	Moderado
13	Sistema Automatizado del Registro Predial (SARP)	Sistema desactualizado	2	1	3	2	2.834	3.667	2.834	Moderado
		Acceso no autorizado	3	1	2	2	3		2.889	Moderado
		Impresiones no autorizadas	3	1	2	2	3.334		3	Moderado
14	Sistema de Trámite Documentario (SISTRAM)	Sistema desactualizado	2	1	2	1.667	3.334	2.333	2.445	Moderado
		Acceso no autorizado	3	1	1	1.667	4		2.667	Moderado
15	Sistema de Control de Accesos	Acceso no autorizado	2	1	2	1.667	4	3.333	3	Moderado
16	Sistema de Inventario de Hardware y Software	Acceso no autorizado	2	1	2	1.667	3	3	2.556	Moderado
		Mal uso del sistema por desactualización de datos	2	1	1	1.333	4.167		2.833	Moderado
17	Sistema de Estadística y Productividad	Acceso no autorizado	2	1	2	1.667	3	3.333	2.667	Moderado
		Información proporcionada incorrecta	2	2	3	2.333	3.667		3.111	Moderado
18	SQL Plus	Acceso no autorizado	3	1	2	2	2.667	4	2.889	Moderado
		Modificación no autorizada de la información	4	3	3	3.333	3.167		3.5	Crítico

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

EVALUACIÓN DE RIESGOS										4 de 7
N°	Activo	Amenaza	Criterios de Evaluación						Riesgo Efectivo	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico / Imagen Institucional	Impacto Operacional	Nivel de Impacto				
Amenazas a los Activos de Físicos										
19	Computadora	Daño físico de equipos	2	2	3	2.333	4	4	**3.444**	**Crítico**
		Virus	2	1	2	1.667	3.667		**3.111**	**Moderado**
		Accesos no autorizados	3	1	2	2	3.5		**3.167**	**Moderado**
		Información usada indebidamente una vez dado el bien de baja	4	2	2	2.667	2.834		**3.167**	**Moderado**
		Incongruencia de fecha y hora	3	3	3	3	3.334		**3.444**	**Crítico**
20	Laptop	Daño físico de equipo	2	2	2	2	3.667	1.333	**2.333**	**Moderado**
		Robo de equipo	3	2	2	2.333	3.1674		**2.278**	**Moderado**
		Información usada indebidamente una vez dado el bien de baja	4	2	2	2.667	2.834		**3.167**	**Moderado**
21	Servidor de Dominio Zonal	Daño físico de equipos	3	3	4	3.333	2.834	4	**3.389**	**Crítico**
		Virus	2	2	3	2.333	2.667		**3**	**Moderado**
		Incongruencia de fecha y hora	3	3	3	3	3.334		**3.444**	**Crítico**
22	Servidor de Keyfile	Daño físico de equipos	3	3	4	3.333	2.834	4	**3.389**	**Crítico**
		Virus	2	2	3	2.333	2.667		**3**	**Moderado**
		Incongruencia de fecha y hora	3	3	3	3	3.334		**3.444**	**Crítico**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

EVALUACIÓN DE RIESGOS										5 de 7
N°	Activo	Amenaza	Criterios de Evaluación						Riesgo Efectivo	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico / Imagen Institucional	Impacto Operacional	Nivel de Impacto				
Amenazas a los Activos de Físicos										
23	Servidor de Base de Datos	Daño físico de equipos	3	3	4	3.333	2.834	4	**3.389**	**Crítico**
		Virus	2	2	3	2.333	2.667		**3**	**Moderado**
		Incongruencia de fecha y hora	3	3	3	3	3.334		**3.444**	**Crítico**
24	Servidor Authasas	Daño físico de equipos	2	3	4	3	2.834	3.333	**3.056**	**Moderado**
		Virus	2	2	3	2.333	2.667		**2.778**	**Moderado**
25	Servidores Citrix	Daño físico de equipos	2	2	3	2.333	2.834	**2**	**2.389**	**Moderado**
		Virus	2	2	2	2	2.667		**2.222**	**Moderado**
26	Servidor de Archivos	Daño físico de equipos	3	3	3	3	2.834	4	**3.278**	**Moderado**
		Virus	2	1	2	1.667	2.667		**2.778**	**Moderado**
27	Servidor de Replicación	Daño físico de equipos	2	2	3	2.333	2.834	3.667	**2.945**	**Moderado**
		Virus	2	2	2	2	2.667		**2.778**	**Moderado**
		Incongruencia de fecha y hora	3	3	3	3	3.334		**3.444**	**Crítico**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

EVALUACIÓN DE RIESGOS										6 de 7
N°	Activo	Amenaza	Criterios de Evaluación						Riesgo Efectivo	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico / Imagen Institucional	Impacto Operacional	Nivel de Impacto				
Amenazas a los Activos de Físicos										
28	Discos Duros Externos	Robo de disco duro	3	1	2	2	3.834	2	**2.611**	**Moderado**
		Daño físico del disco duro	2	1	1	1.333	3		**2.111**	**Moderado**
		Información usada indebidamente una vez dado el bien de baja	4	2	2	2.667	2.834		**3.167**	**Moderado**
29	Cintas de Backup DLT	Robo de cintas	4	3	5	4	3	5	**4**	**Crítico**
		Daño físico de cintas	3	3	4	3.333	2.834		**3.722**	**Crítico**
Amenazas al Personal (Clientes, Empleados, Personal Externo)										
30	Jefe de la UTI	Renuncia del personal	3	2	4	3	1.834	4	**2.945**	**Moderado**
		Personal descontento	2	1	3	2	3		**3**	**Moderado**
31	Operador de Sistemas	Renuncia del personal	3	2	4	3	1.834	4	**2.945**	**Moderado**
		Personal descontento	2	1	3	2	3		**3**	**Moderado**
32	Especialista en Base de Datos	Renuncia del personal	3	2	4	3	2.334	4	**3.111**	**Moderado**
		Personal descontento	2	1	3	2	3		**3**	**Moderado**
33	Técnico de Sistemas	Renuncia del personal	3	2	4	3	2.334	4	**3.111**	**Moderado**
		Personal descontento	2	1	3	2	3		**3**	**Moderado**
		Sobrecarga de tareas	2	1	3	2	3.834		**3.278**	**Moderado**

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

EVALUACIÓN DE RIESGOS										7 de 7
N°	Activo	Amenaza	Criterios de Evaluación						Riesgo Efectivo	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico / Imagen Institucional	Impacto Operacional	Nivel de Impacto				
Amenazas al Personal (Clientes, Empleados, Personal Externo)										
34	Central de Atenciones	Renuncia del personal	2	1	3	2	3.167	3.667	**2.945**	**Moderado**
		Personal descontento	2	1	2	1.667	3		**2.778**	**Moderado**
		Sobrecarga de tareas	2	1	3	2	3.834		**3.167**	**Moderado**
35	Programador de Sistemas	Renuncia del personal	2	1	2	1.667	2.667	2.667	**2.334**	**Moderado**
		Personal descontento	2	1	2	1.667	3		**2.445**	**Moderado**
		Delegación de funciones no correspondientes a su puesto	2	1	2	1.667	3.334		**2.556**	**Moderado**
36	Replicador de Base de Datos	Renuncia del personal	2	1	2	1.667	2.667	3	**2.445**	**Moderado**
		Personal descontento	2	1	2	1.667	3		**2.556**	**Moderado**
37	Practicantes Profesionales	Renuncia del personal	1	1	3	1.667	3	2.333	**2.333**	**Moderado**
		Personal descontento	1	1	2	1.333	3.5		**2.389**	**Moderado**
		Sobrecarga de tareas	2	1	2	1.667	3.834		**2.611**	**Moderado**
38	Servicio de Terceros	Incumplimiento de trabajo en el tiempo indicado	2	1	2	1.667	3.167	2	**2.278**	**Moderado**

Tabla N°4 - *Evaluación de Riesgos de la UTI*

Fuente: *Elaboración Propia*

DERECHOS DE AUTOR RESERVADOS

4.1.7. Selección de Controles y Declaración de la Aplicabilidad (SOA).-

(Ver Anexo A.5)

Los 10 Objetivos de control y 32 controles que sugiere la cláusula de Gestión de Comunicaciones y Operaciones de la NTP ISO/IEC 17799:2007, fueron evaluados para ser incluidos o no en la implementación.

Dicha evaluación está plasmada en el documento de **Versión 1.1 del Anexo A.5** Declaración de la Aplicabilidad.

La declaración de la aplicabilidad es el documento que describe los objetivos de control y los controles que son relevantes y aplicables al proyecto de la organización

De acuerdo a la evaluación, 24 de los 32 controles han sido seleccionados para su implementación, los cuales se listan a continuación:

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.1 Procedimientos y responsabilidades de operación
- 10.1.1 Documentación de procedimientos operativos
- 10.1.2 Gestión de cambios
- 10.1.3 Segregación de tareas
- 10.1.4 Separación de los recursos para desarrollo y para producción

10.3 Planificación y Aceptación del sistema
- 10.3.1 Planificación de la Capacidad
- 10.3.2 Aceptación del sistema

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

10.4 Protección contra software malicioso

10.4.1 Medidas y controles contra software malicioso

10.4.2 Medidas y controles contra código móvil

10.5 Gestión de respaldo y recuperación

10.5.1 Recuperación de la información

10.6 Gestión de seguridad en redes

10.6.1 Controles de red

10.6.2 Seguridad en los servicios de redes

10.7 Utilización de los medios de información

10.7.1 Gestión de medios removibles

10.7.2 Eliminación de medios

10.7.3 Procedimientos de manipulación de la información

10.7.4 Seguridad de la documentación de sistemas

10.8 Intercambio de información

10.8.1 Políticas y procedimientos para el intercambio de información y software

10.8.3 Medios físicos en tránsito

10.8.5 Sistemas de información de negocios

10.10 Monitoreo

10.10.1 Registro de la auditoría

10.10.2 Monitoreando el uso del sistema

10.10.3 Protección de la información de registro

10.10.4 Registro de administradores y operadores

10.10.5 Registro de la avería

10.10.6 Sincronización del reloj

Tabla N°5 - *Controles de la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO/IEC 17799:2007 seleccionados para ser implementados*

DERECHOS DE AUTOR RESERVADOS

4.2 Desarrollo.-

4.2.1. Tratamiento de riesgos.-

Una vez culminado la etapa de Planificación del Ciclo de Deming, empieza la etapa del Desarrollo, en el que primordialmente se realizará el tratamiento de los riesgos evaluados con anterioridad y se pondrán en marcha e implementación los controles seleccionados en el documento de aplicabilidad.

Imagen N°17 - *Tratamiento de Riesgos*

Fuente: *"Introducción a la Gestión de la Seguridad de la Información" - Material de estudio de la empresa capacitadora BSgrupo.*

El Tratamiento de Riesgos de la Unidad de Tecnologías de la Información se ha completado según el proceso descrito en el en el Documento de la Metodología de Gestión de Riesgos mencionado anteriormente (Anexo A.4).

Dicha evaluación está plasmada en la **Tabla N°6** , la cual podemos apreciar a continuación:

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

TRATAMIENTO DE RIESGOS												1 de 7
N°	Activo	Amenaza	Riesgo Efectivo					Control Propuesto	Cumplimiento del Control (Según NTP-ISO/IEC 17799:2007	Costo Aprox	Tiempo Aprox	Opción para el Tratamiento
			Nivel de Impacto	Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Tolerancia					
Amenazas a los Activos de Información												
1	Documentos de control de Acceso	Divulgación no autorizada	2.333	4.334	3.667	3.445	Crítico	Establecer una lista de usuarios autorizados para el acceso a la documentación y almacenar la información en un lugar seguro	**10.7.3** Procedimientos de manipulación de la información **10.7.4** Seguridad de la documentación de sistemas	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses)	**R** Reducir
2	Copias de partidas y Títulos registrales	Robo de información	3.333	3.667	3.667	3.556	Crítico	Establecer el procedimiento correcto para el uso de las copias realizadas.	**10.1.1** Procedimientos y responsabilidades de operación	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses)	**R** Reducir
		Divulgación no autorizada, venta de la información	3	3.667		3.445	Crítico	Realizar seguimiento y registro del uso de cada copia realizada para determinar quienes tuvieron acceso a ella	**10.7.3** Procedimientos de manipulación de la información	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses)	**R** Reducir

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

TRATAMIENTO DE RIESGOS												2 de 7
N°	Activo	Amenaza	Riesgo Efectivo					Control Propuesto	Cumplimiento del Control (Según NTP-ISO/IEC 17799:2007	Costo Aprox	Tiempo Aprox	Opción para el Tratamiento
			Nivel de Impacto	Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Tolerancia					
Amenazas a los Activos de Información												
3	Registros de Base de Datos	Sustracción de información	3.667	3.5	4	3.722	Crítico	Auditar frecuentemente la información consultada en la base de datos por cada usuario	**10.10.1** Registro de la auditoría **10.10.2** Monitoreando el uso del sistema	**1** Menor a S/. 15,000	**M** Mediano plazo (De 3 a 12 meses)	**R** Reducir
		Divulgación no autorizada	3	3.5		3.5	Crítico	Auditar frecuentemente la información consultada en la base de datos por cada usuario	**10.10.1** Registro de la auditoría **10.10.2** Monitoreando el uso del sistema	**1** Menor a S/. 15,000	**M** Mediano plazo (De 3 a 12 meses)	**R** Reducir
		Modificación no autorizada de la información	3.667	3.5		3.722	Crítico	Establecer y revisar con frecuencia los permisos de los usuarios que cuentan con acceso a la base de datos	**10.1.3** Segregación de tareas **10.10.4** Registro de administradores y operadores	**2** De S/. 15,000 a S/. 30,000	**M** Mediano plazo (De 3 a 12 meses) 9:44 8:	**R** Reducir

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

N°	Activo	Amenaza	Riesgo Efectivo					Control Propuesto	Cumplimiento del Control (Según NTP-ISO/IEC 17799:2007	Costo Aprox	Tiempo Aprox	Opción para el Tratamiento
			Nivel de Impacto	Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Tolerancia					
Amenazas a los Activos de Información												
4	Registro de Imágenes digitales	Sustracción de información	3.667	3.665	4	3.777	Crítico	Monitorear con frecuencia la información consultada por los usuarios	**10.10.1** Registro de la auditoría **10.10.2** Monitoreando el uso del sistema	**1** Menor a S/. 15,000	**M** Mediano plazo (De 3 a 12 meses)	**R** Reducir
		Divulgación no autorizada	3	3.665		3.555	Crítico	Monitorear con frecuencia la información consultada por los usuarios	**10.10.1** Registro de la auditoría **10.10.2** Monitoreando el uso del sistema	**1** Menor a S/. 15,000	**M** Mediano plazo (De 3 a 12 meses)	**R** Reducir
		Modificación no autorizada de la información	3.667	3.665		3.777	Crítico	Revisar frecuentemente y establecer correctos permisos para cada cuenta de keyfile	**10.1.3** Segregación de tareas	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses)	**R** Reducir

DERECHOS DE AUTOR RESERVADOS

UNIVERSIDAD ANDINA DEL CUSCO
Repositorio Digital de Tesis

TRATAMIENTO DE RIESGOS												4 de 7
N°	Activo	Amenaza	Riesgo Efectivo					Control Propuesto	Cumplimiento del Control (Según NTP-ISO/IEC 17799:2007	Costo Aprox	Tiempo Aprox	Opción para el Tratamiento
			Nivel de Impacto	Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Tolerancia					
Amenazas a los Activos de Software												
5	SQL Plus	Modificación no autorizada de la información	3.333	3.167	4	3.5	Crítico	Establecer y revisar con frecuencia los permisos de los usuarios que cuentan con acceso a la base de datos	**10.1.3** Segregación de tareas **10.10.3** Protección de la información de registro **10.10.4** Registro de administradores y operadores	**1** Menor a S/. 15,000	**M** Mediano plazo (De 3 a 12 meses)	**R** Reducir
Amenazas a los Activos Físicos												
6	Computadora	Daño físico de equipos	2.333	4	4	3.444	Crítico	Dar buen uso a la computadora y protegerla cuando se realicen cambios y movimientos	**10.1.1** Documentación de procesos operativos **10.8.3** Medios físicos en tránsito	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses	**R** Reducir
		Incongruencia de fecha y hora	3	3.334	4	3.444	Crítico	Revisar que los relojes de las computadoras estén sincronizados con los de los servidores	**10.10.6** Sincronización del reloj	**1** Menor a S/. 15,000	**C** Corto plazo (Menos de 3 meses	**R** Reducir

DERECHOS DE AUTOR RESERVADOS