ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

“Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015”

TESIS PARA OBTENER EL GRADO ACADÉMICO DE MAESTRA EN GESTIÓN PÚBLICA

AUTOR

Br. Esther Marleni Tarrillo Saldaña

ASESOR

Mg. Keller Sánchez Dávila

LÍNEA DE INVESTIGACIÓN

DIRECCIÓN

TARAPOTO – PERÚ

2016

Dr. Ramírez García Gustavo

Presidente

Dr. Bazán Vargas Kieffer Segundo

Secretario

Mg. Sánchez Dávila Keller

Vocal

DEDICATORIA

Con el cariño que brota de corazón la dedico a mis padres, gracias a ellos soy profesional, ellos han sido mi guía para salir adelante, brindándome siempre su apoyo incondicional, consejos y compresión, a mis queridos hermanos y en especial a mi hermana Kelly Tarrillo Saldaña, quien siempre me incentiva a seguir adelante

A Dios por guiarme por el buen camino, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento

A mis compañeros de la maestría con quienes hemos compartido nuevas experiencias y buenos momentos.

Esther Marleni

AGRADECIMIENTO

Agradecimiento a Dios por darme una familia con muchas cualidades a la que quiero con todo mi corazón, a mis amigos con quienes comparto momentos especiales a la Universidad Cesar Vallejo y al equipo de trabajo que conforman la Escuela de Posgrado, por su valioso apoyo y motivación en toda esta etapa de estudios de la maestría,

A la universidad Cesar Vallejo, por brindarme las facilidades y beneficios para estudiar el programa de maestría, a mi asesor Mg. Keller Sánchez Dávila por su valioso apoyo, así como a todos los docentes que formaron parte de mi proceso de formación en mis estudios de maestría.

A mis padres por la oportunidad que me brindaron y la confianza que depositaron en mí. Y a todas las personas que hicieron posible ésta decisión que ahora es un presente, mi tesis.

Esther Marleni

DECLARATORIA DE AUTENTICIDAD

Yo, Esther Marlene Tarrillo Saldaña estudiante del programa de Maestría en Gestión Pública de la Escuela de Postgrado de la Universidad César Vallejo, identificado con DNI 40439723, respectivamente, con la tesis titulada “Influencia de Gestión de Riesgos en la Seguridad de activos de Información de la Zona Registral III Sede Moyobamba, 2015”.

Declaro bajo juramento que:

1) La tesis es de mi autoría
2) He respetado las normas internacionales de citas y referencias para las fuentes consultadas.
3) La tesis no ha sido plagiada, es decir no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional.
4) Los daros presentados en los resultados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presenten en la tesis se constituirán en aportes a la realidad investigada.

De identificarse la falta de fraude (datos falsos), plagio (información sin citar a autores), auto plagio (presentar como nuevo algún trabajo de investigación propio que ya ha sido publicado), piratería (uso ilegal de información ajena) o falsificación (representar falsamente las ideas de otros), asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad César Vallejo

Tarapoto, mayo del 2016.

Br. Esther Marleni Tarrillo Saldaña
DNI 40349723

PRESENTACIÓN

Señores miembros del jurado,

Presento ante ustedes la Tesis titulada “Influencia de la Gestión de Riesgos en la seguridad de activos de Información de la Zona Registral III Sede Moyobamba, 2015”, con la finalidad de establecer la influencia de Gestionar los riesgos en relación a los activos de información de la zona Registral III Sede Moyobamba.

Dando cumplimiento del Reglamento de Grados y Títulos de la Universidad César Vallejo, con el objetivo de optar el grado de magíster en Gestión Pública.

Esperando de antemano cumplir con los requisitos de aprobación.

La autora.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

El presente trabajo de investigación tiene como finalidad conocer la influencia de la gestión de riesgos en la seguridad de activos de información de la zona Registral III Sede Moyobamba, teniendo como hipótesis planteada que Existe influencia de la Gestión De Riegos en la seguridad de activos de Información de La Zona Registral III Sede Moyobamba, para ello se obtuvo una muestra representativa de 50 trabajadores con un muestreo de tipo no Probabilístico por conveniencia: El diseño de estudio fue de tipo descriptivo correlacional y los datos fueron procesados y analizados por medios electrónicos, clasificados y sistematizados de acuerdo a las dimensiones de las variables y luego presentados mediante tablas y gráficos estadísticos, y para la prueba de correlación se usó la prueba del Chí Cuadrado.

Los resultados obtenidos muestran un Chí Cuadrado de Pearson de 15.712, mayor al Chí tabular con 4 grados de libertad (9.48), lo que indica que existe relación entre las variables de estudio. Asimismo, se encuentra en la zona probabilística de rechazo, donde acepta la hipótesis alternativa con un 95% de confianza y el estudio concluye que existe relación entre la gestión de riesgos y la seguridad de activos de información de la Zona Registral N III Sede Moyobamba.

Palabras Clave: Gestión de riesgo, seguridad de activos

ABSTRACT

This research aims to determine the influence of risk management in the security of information assets of the Registry Zone III Headquarters Moyobamba, with the hypothesis that there is influence of risk management with assets information Registry Zone N III Headquarters Moyobamba, for this purpose a representative sample of 50 workers with a sampling of non-probabilistic convenience was obtained: the study design was descriptive correlational and the data were processed and analyzed by electronic means, classified and systematized according to the dimensions of the variables and then presented by statistical tables and graphs, and correlation test chi square test was used.

The results show a Pearson Chi Square 15,712, higher than Chí tabular with 4 degrees of freedom (9.48), indicating that there is a relationship between the study variables. It also is in the probabilistic rejection zone where accepts the alternative hypothesis with 95% confidence and the study concludes that there is a relationship between risk management and security of information assets of the Registry Zone III Headquarters Moyobamba.

Keywords: Risk management, asset security

I. INTRODUCCIÓN

1.1. Realidad Problemática

Gestionar los Riesgos en los activos de información nos va a permitir minimizar las amenazas, riesgos a los que está expuesta la información y siendo este un activo de vital importancia para la institución debe protegerse para garantizar de esta manera la integridad, confidencialidad y disponibilidad de la misma en el momento que sea requerida por el usuario. En la Zona Registral III Sede Moyobamba, se maneja grandes volúmenes de información valiosa, indispensable para el buen funcionamiento de la Institución, la cual esta almacenada a través de medios físicos, magnéticos, Base de Datos, disco externo, servidores de archivos, transmitida por correo, etc. Esta información se comparte diariamente con usuarios internos y externos. En la actualidad la información está sujeto a riesgos, amenazas ya sea por fuente internas o externas que pueden atentar contra su confidencialidad, integridad y disponibilidad, ocasionando de esta manera la inviabilidad del servicio Registral, perjudicando la atención al usuario, por lo tanto no se estaría garantizando la seguridad Jurídica a través del registro y publicidad de derechos, ocasionando una pérdida de imagen para la institución, generando gastos indirectos y problemas estrictamente legales. Por eso es importante gestionar los riesgos a los que está expuesta la información estableciendo mecanismos de seguridad que permitan resguardar la información de una serie de amenazas a las que está expuesta, garantizando de esta manera que los riegos sean conocidos, asumidos, gestionados y minimizados y así evitar que el riesgo se materialice y perjudique al usuario.

1.2. Trabajos Previos

En el presente trabajo de investigación se abordó antecedentes de informes de tesis de diferentes autores tal es el caso de:

Internacional

López (2011), en su tesis titulada “Gestión De Riesgos Corporativos De TI En Guatemala” desarrollada en el 2011, con una muestra de 30 empresarios guatemaltecos, su objetivo fue, Apoyar a los ingenieros que asumen responsabilidades de dirección en la gerencia de tecnologías de información y a los encargados de la gestión de riesgos del área de informática, por medio de un marco de trabajo, aplicable en el entorno guatemalteco, el autor formuló entre otras las siguientes conclusiones la gestión de riesgos de TI en las organizaciones sirve para evitar y minimizar pérdidas, pero también es útil para generar valor por medio de la aplicación de conceptos, principios y un conjunto de acciones definidas en controles. Las empresas que poseen el nivel de sofisticación mediano o alto de TI son más dependientes de ella y crece su exposición a diversos riesgos, los cuales pueden comprometer el cumplimiento de los objetivos estratégicos. La respuesta a estos riesgos, involucra la implementación del proceso de mejora continua del grado de madurez. En el medio corporativo en Guatemala el nivel de madurez de la gestión de riesgos de TI es aceptable.

Cruz (2014), En su Tesis Titulada “Una Metodología de Análisis y Evaluación de Riesgos en Tecnologías de Información”, desarrollada en el año 2014, en la ciudad de México, su objetivo fue Apoyar a los profesionales en Tecnologías de Información cuenten con elementos que les permitan analizar y evaluar los riesgos y así fundamentar la reducción y posible eliminación de los riesgos, El autor formuló entre otras las siguientes conclusiones. En México existe una carencia y deficiencia en la difusión, capacitación y fomento de seguridad de la informática, desde la organización misma hasta los empleados. Esto tiene como consecuencia estar en desventaja frente a los riesgos más comunes, concentrándose especialmente en los virus y hackers,

dejando en segundo término la planeación de la seguridad, las políticas y procedimientos, la capacitación y educación, la disponibilidad de los sistemas; así como, las auditorías y evaluaciones de riesgos. Evaluar los riesgos en la seguridad de la información no debe ser realizada únicamente para completar una lista de tareas o solamente para satisfacer un requerimiento normativo, más bien se debe tomar como una Herramienta que permita a la empresa o institución conocer en forma ordenada el comportamiento de los riesgos a los que está expuesto la información, anticipando de esta manera posibles pérdidas de información, por ello es muy importante implementar procedimientos, controles, políticas de seguridad que permitan minimizar la ocurrencia o el impacto financiero de posibles pérdidas que pudiesen suceder. La evaluación de riesgos en tecnologías de información, es una herramienta muy valiosa para el mejor desarrollo de las labores de todos y de cada uno de los departamentos de las organizaciones y en particular del departamento del área de sistemas de información.

Nacional

Pastor (2010), en su tesis titulada “Impacto del Riesgo en el Gobierno de las Tecnologías de Información y Comunicación en la Gestión Empresarial Industrial del siglo XXI”, desarrollado en el año 2010 en la ciudad de Lima –Perú, con una muestra de 30 empresas del sector metal mecánico, su objetivo fue Identificar en qué medida la implementación de un sistema de gestión del riesgo dentro del gobierno de TIC en la gestión de los procesos contribuirá en la creación de ventajas competitivas en la gestión de los procesos de las organizaciones industriales del sector metal mecánico. El autor Formuló entre otras las siguientes conclusiones, La gran mayoría de las organizaciones consideran el riesgo como parte del proceso de planificación, donde el 32% considera en términos generales y 56% en áreas muy específicas. La mayoría de los riesgos que tienen mayor consideración en la organización, están directamente relacionadas con las capacidades de los sistemas de TI y de la organización. El 84% de las empresas

encuestadas no ha considerado necesario, crear un cargo de un jefe de riesgos. El 60% de las empresas considera que cada vez es más importante la relación entre la gestión de información y la seguridad. Se observa que el nivel general de gasto en la gestión del riesgo está aumentando en la mayoría de casos. Hay una desconexión evidente entre la TI y el negocio cuando se trata de definir los requisitos relacionados con el riesgo a nivel empresarial.

Barrantes (2012), en su tesis titulada “Diseño E Implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos” desarrollado en el año 2012 en la ciudad de lima -Perú, su objetivo fue Reducir y mitigar los riesgos de los activos de información de los procesos que se encuentran bajo la gerencia de tecnología de Car Perú S.A que ponen en peligro los recursos, servicios y continuidad de los procesos tecnológicos, el autor formulo entre otros las siguientes conclusiones. Implementando una buena metodología para gestionar los riesgos ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables gran porcentaje de riesgos que afectan a los activos de información. El factor humano es crítico para la implementación de cualquier sistema de gestión organizacional es por ello que la formación y concientización de los mismos es indispensable para lograr una implementación exitosa. La documentación de los procesos es una herramienta poderosa para el mantenimiento y mejora de cualquier sistema de gestión organizacional.

Regional

Condori (2012), en su tesis titulada “Un Modelo de Evaluación de Factores Críticos de Éxito en la implementación de la seguridad en sistemas de información para determinar su influencia en la intención del usuario” desarrollado en el año 2012, en la ciudad de Puno-Perú, con una muestra de 143 usuarios de las diferentes dependencias de la UNA-Puno, su objetivo fue determinar, mediante un modelo estructural, el grado de influencia que ejercen los factores críticos de éxito en la intención del usuario para la implementación de seguridad de sistemas

de información en la universidad nacional del Altiplano Puno durante el año 2011, el autor formulo entre otros las siguientes conclusiones, los factores más importantes por el grado de influencia en la Actitud para implementar Seguridad en Sistemas de Información son: En un primer lugar los Recursos y Presupuesto, donde el grado de influencia es -0.558, que afecta negativamente; ello en razón a que como ocurre en la mayoría de instituciones públicas, como en el caso de UNA-Puno, la falta de presupuesto es un factor determinante para implementar un plan de seguridad de información. La Cultura Organizacional donde el grado de influencia es 0.439, que revela la existencia de normas y valores que influyen positivamente en la situación estudiada., La Conciencia de la necesidad de seguridad por el personal con un grado de 0.431, que revela el grado de conciencia que tiene del personal de la UNA-Puno respecto a la necesidad de implementar seguridad en los sistemas de información, la Formación y Capacitación con grado de 0.357 que muestra que la capacitación es muy importante para garantizar la implementación del plan de seguridad de la información.

Local

García (2016), En su tesis titulada “Implementación de un Sistema de Gestión de Seguridad de la Información, Aplicado a los Riesgos Asociados a los Activos de Información En la Empresa Net – Consultores S.A.C”, desarrollado en el año 2016 en la ciudad de Tarapoto-Perú, su objetivo fue determinar la influencia de la implementación de un Sistema de Gestión de Seguridad de la Información sobre el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C. El autor formulo, entre otras las siguientes conclusiones la implementación del Sistema de Gestión de Seguridad de la Información en la Empresa NET-Consultores S.A.C, influye significativamente sobre el impacto de los riesgos asociados a los activos de información en la empresa NET–Consultores S.A.C. La aplicación de una metodología para la Gestión de riesgos, permite establecer Políticas de Seguridad en la cual contengan lineamientos para una correcta

administración de la información con el fin de garantizar la seguridad de los activos esenciales e importantes para la empresa.

1.3. Teorías Relacionadas al Tema

GESTIÓN DE RIESGOS

Según Gómez (2012) Riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Así mismo Gómez (2012) nos dice que la Gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad. Durante el proceso de gestión del riesgo en la seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los directores y al personal operativo correspondiente. Incluso antes del tratamiento de los riesgos, la información acerca de los riesgos identificados puede ser muy valiosa para la gestión de incidentes y puede ayudar a reducir el daño potencial. La toma de conciencia por parte de los directores y el personal acerca de los riesgos, la naturaleza de los controles establecidos para mitigar los riesgos y las áreas de interés para la organización facilitan el tratamiento de los incidentes y los eventos inesperados de una manera más eficaz. Se recomienda documentar los resultados detallados en cada actividad del proceso de gestión del riesgo en la seguridad de la información.

Además, la gestión de riesgos es considerada también como el proceso de ponderación de las distintas opciones en base a los resultados de la valoración de riesgos. Procesos para aumentar la probabilidad e impacto de las oportunidades y reducir la probabilidad e impacto de las amenazas. (Purdy, 2009)

Asimismo, Casares (2013) refiere que la gestión de riesgos son las actividades coordinadas para dirigir y controlar en relación con el riesgo e incluye por norma general la evaluación, el tratamiento, la aceptación y la comunicación de los riesgos. Es una parte esencial de la gestión estratégica de cualquier organización, ya que es el proceso por la cual se tratan los riesgos relacionados con las actividades, con el fin de obtener un beneficio sostenido en cada una de ellas y el conjunto de todas las actividades, es la suma de medidas adoptadas en el seno de la organización su objetivo es añadir el máximo valor sostenible a todas las actividades de la organización, introduciendo una visión común del lado positivo y del lado negativo de aquellos factores potenciales que pueden afectar a la organización. Aumenta la probabilidad de éxito y reduce tanto la probabilidad de fallo como la incertidumbre acerca de la consecución de los objetivos generales de la empresa. La gestión de los riesgos tiene que ser un proceso continuo y en constante desarrollo que se lleve a cabo en la aplicación de la estrategia de la organización debiendo tratar todos los riesgos que rodeen a las actividades pasadas, presentes y, sobre todo, futuras de la empresa. Debe estar integrada en la cultura de la organización con una política eficaz y un programa dirigido por la alta dirección. Todo el personal de la empresa, debe ser consciente de la revisión continua de los riesgos, así como tener conocimiento de las acciones que se deben llevar a cabo ante cualquier riesgo convirtiendo la estrategia en objetivos tácticos y operacionales, asignando responsabilidades en toda la organización, siendo cada gestor y cada empleado responsable de la gestión de riesgos como parte de la descripción de su trabajo. La gestión de riesgos respalda la responsabilidad, la medida y la recompensa del rendimiento de la organización, promoviendo así la eficiencia operacional a todos los niveles de la misma.

Según Bajo (2013) refiere que La gestión del riesgo es el proceso por el que las organizaciones tratan los riesgos relacionados con sus actividades, con el fin de obtener un beneficio sostenido en cada una de

ellas y en el conjunto de todas las actividades. Una Gestión de Riesgos eficaz se centra en la identificación y tratamiento de estos riesgos. Su objetivo es añadir el máximo valor sostenible a todas las actividades de la organización. Introduce una visión común del lado positivo y del lado negativo de aquellos factores que pueden afectar a la organización. La gestión del riesgo debe estar integrada en la cultura de la organización, en particular en la cultura de gestión. La implicación apropiada de las partes interesadas y, en particular, de las Personas que toman las decisiones a todos los niveles de la organización, de esta manera se asegura el éxito de la gestión. La gestión de riesgos es transparente y participativa, el factor humano, es un elemento importante en la gestión del riesgo Por ello, la gestión del riesgo debe permitir identificar las aptitudes, las percepciones y las intenciones de las personas de la organización que pueden influir en el logro de los objetivos de la organización.

Según, Ramírez (2011) difiere que en la Gestión de riesgo se debe evaluar las siguientes etapas como valoración de riesgos el cual permite identificar los activos que se quieren proteger y sus debilidades, así como las amenazas a las cuales se encuentran expuestas estas pueden ser (físicas, lógicas o estratégicas y su origen puede ser natural, técnico, humano accidental o intencional), por lo cual se deben implementar controles para la mitigación de los riesgos. En la etapa de tratamiento de riesgos se debe establecer e implementan las acciones a tomar para mitigar los riesgos encontrados y lograr riesgos residuales aceptables por la organización, dentro de las acciones a tomar encontramos principalmente: reducir, aceptar, eliminar y transferir. En este plan debe definir recursos, responsabilidades y actividades teniendo en cuenta las posibles restricciones a nivel económico, legal, temporal, técnico, operativo, político, cultural y las demás que sean determinadas. Los controles que sean recomendados deben incluir un análisis costo-beneficio (incluyendo costos de implementación y mantenimiento). El plan debe ser documentado y finalmente definidas las políticas a seguir.

El plan de tratamiento debe definir los pasos pormenorizados para gestionar los riesgos sin dejar espacio a nuevos posibles riesgos que ocurran como consecuencia de errores en la implementación de las acciones del tratamiento mismo.

Ramírez (2011) refiere que en el Monitoreo y mejora continua del proceso de gestión de riesgos el elemento primordial es el control de cambios, por lo cual el monitoreo debe realizarse sobre activos, procesos, vulnerabilidades, amenazas, controles, documentación de políticas y procedimientos con el fin de establecer acciones a seguir ante posibles y lograr que la gestión este continuamente actualizada para lograr evaluar indicadores de cumplimiento de los planes. Con el monitoreo y la mejora continua se busca asegurar la constante revisión sobre la gestión de riesgos para dar cumplimiento a los procesos de mitigación definidos.

Según ISO/IEC 27005 (2009) refiere que la evitación del riesgo es una decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación. La identificación del Riesgo es un proceso para encontrar, listar y caracterizar los elementos de riesgo. La comunicación del riesgo es Intercambiar o compartir la información acerca de los riesgos entre la persona que toma la decisión y otras partes interesadas. La reducción del riesgo acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo. Que la retención del riesgo es la aceptación de la pérdida o ganancia proveniente de un riesgo particular. Refiere que la transferencia del riesgo es Compartir con otra de las partes la pérdida o la ganancia de un riesgo.

ACTIVOS DE INFORMACIÓN

Según Poveda (2011) difiere que el Activo es todo aquello que tiene valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Poveda (2011) Los activos de información es todo aquello que se considera de alta relevancia para la organización y dicha información puede estar almacenada a través de ficheros , bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información. Para un mejor control de los activos de información se debe realizar un inventario de activos el cual es la base para la gestión de los mismos, ya que tiene que incluir toda la información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre. El inventario deberá recoger los activos que realmente tengan un peso específico y sean significativos para la organización, se debe asignar valoración de activos el cual permite estimar qué valor tienen los activos para la organización, cuál es su importancia para la misma. Para calcular este valor, se considera cual puede ser el daño que puede suponer para la organización que un activo resulte dañado en cuanto a su disponibilidad, integridad y confidencialidad. Esta valoración puede ser cuantitativa o cualitativa.

Según, ISO27001 (2013) difiere que los principios básicos de la seguridad de los activos de información son la Disponibilidad el cual permite garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario. La Confidencialidad permite garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado. La Integridad permite Salvaguardar la exactitud e integridad de la información y activos asociados

Según, Palma (2014) refiere que la gestión del riesgo en relación a los activos de información ayuda a la empresa u organismo público a evitar o mitigar los riesgos inherentes con su gestión y de esta manera posibilitar que cumpla con sus obligaciones legales, regulatorias o normativas, asegurar el funcionamiento del negocio y rentabilizar el

conocimiento corporativo. Su objetivo se centra en maximizar los efectos positivos y minimizar o anular sus efectos negativos. La gestión de riesgos de los activos de información se debe integrar en la estructura de gobierno de la organización y en sus políticas de gestión del riesgo generales, estrategias, planes, y compromisos con las partes interesadas. Las responsabilidades de la gestión de los riesgos de los activos. La gran parte de los riesgos relacionados con el negocio o actividades corporativas se producen como un resultado directo de los procesos de gestión de los activos de información: captura, control, acceso, divulgación o publicación, almacenamiento o disposición. Si en el transcurso de los procesos de negocio la entidad no ha logrado preservar la integridad, confidencialidad, y disponibilidad de sus activos de información sus actividades se verán seriamente comprometidas

SUNARP (2016) Zona Registral N° III Sede Moyobamba-SUNARP, es un organismo descentralizado autónomo del Sector Justicia y ente del Sistema Nacional de los Registros Públicos, el cual tiene entre sus principales funciones el de dictar las políticas y normas técnico - registrales de los registros públicos que integran el Sistema Nacional, además de planificar, organizar, normar, dirigir, coordinar y supervisar la inscripción y publicidad de actos y contratos en los Registros Públicos que integran el Sistema Nacional.

La Zona Registral N° III Sede Moyobamba cuenta en la actualidad con 4 Oficinas Registrales:

- ✓ Oficina Registral de Moyabamba.
- ✓ Oficina Registral de Tarapoto
- ✓ Oficina Registral de Juanjui
- ✓ Oficina Registral de Yurimaguas

Los registros existentes en SUNARP son:

- ✓ Registros de Predios
- ✓ Registros de Personas Jurídicas
- ✓ Registros de Personas Naturales

- ✓ Registro Vehicular

1.4. Formulación del Problema

1.4.1. Problema general

¿Cuál es la influencia de la gestión de riesgos en la Seguridad de activos de información de la zona Registral III Sede Moyobamba?

1.4.2. Problemas específicos.

- ¿Cuál es el nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba,
- ¿Cuáles son los factores de riesgo que afectan a los activos de información de la Zona Registral N° III Sede Moyobamba?

1.5. Justificación del Estudio

Conveniencia

Realizar la Gestión de Riegos de la información es de conveniencia para la Zona Registral III Sede Moyobamba, ya que le va a permitir hacer un estudio de las incidencias, vulnerabilidades y riesgos que puede generar la perdida de información, por tal motivo es importante gestionar los riesgos, garantizando de esta manera que el riesgo no se materialice y perjudique al usuario.

Relevancia Social

El Análisis de Gestión de riesgo en la seguridad de activos de información de la Zona Registral III Sede Moyobamba, garantizara los principios fundamentales de la seguridad de la información, lo cual será de vital importancia para la sociedad porque permitirá al ciudadano confiar en el servicio que prestamos a través del registro y publicidad de derechos y titularidades, asegurando de esta manera que la información que se maneja sea requerida por el usuario en el momento deseado y de manera íntegra y confiable.

Implicancia práctica

El presente trabajo de investigación ayudará a definir mejores procesos que garanticen un adecuado manejo de la gestión de riesgo en la

seguridad de los activos de información y con ello permitirá proteger los activos de información de una serie de amenazas a la que está expuesta.

Valor Teórico

Con la presente investigación, se pretende dar mayor realce a la gestión de riesgo en la seguridad de activos de información de la zona Registral III Sede Moyobamba, el mismo que permitirá gestionar la seguridad de la información, mediante el aporte del conocimiento adquirido en el presente estudio.

Metodológica

Los métodos, procedimientos y técnicas e instrumentos empleados en la investigación, serán de completa aplicabilidad a la realidad donde se demuestra su validez y confiabilidad el mismo que podrá ser utilizado en otras instituciones públicas o privadas.

1.6. Hipótesis

1.6.1. Hipótesis General

H_g: Existe influencia de la Gestión De Riegos en la seguridad de activos de Información de La Zona Registral III Sede Moyobamba

1.6.2. Hipótesis Específicas

H_1: El Nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba es alta

H_2: Los factores de riesgo que afectan a los activos de la información de la Zona Registral III Sede Moyobamba son altos.

1.7. Objetivos

1.7.1. Objetivo general

Conocer la influencia de la gestión de riesgos en la seguridad de activos de información de la Zona Registral III Sede Moyobamba.

1.7.2. Objetivos específicos

- Determinar el nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba

- Identificar los factores de riesgo que afectan a los activos de información de la Zona Registral III Sede Moyobamba.

II. MÉTODO

2.1. Diseño de investigación

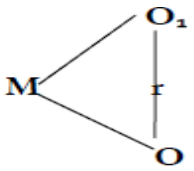
Tipo de Estudio

En el presente proyecto de investigación, el tipo de estudio es No Experimental, porque se abordará dos variables de estudio, Gestión de Riesgos y Activos de información (Hernández Sampiere 2011)

Diseño

En el presente proyecto el diseño de investigación es Correlacional: Descriptivo, porque examina la relación o asociación existente entre dos o más variables, en la misma unidad de investigación o sujeto de estudio

Esquema:



Dónde:

M= Zona Registral III- Sede Moyobamba

O1= Gestión de riesgos

O2 = Activos de información

r = Influencia de la gestión de riesgos en la seguridad de activos de información

2.2. Variables, Operacionalización.

Variables

V1: Gestión de Riesgos

V2: Activos de información

Operacionalización

Variable	Definición conceptual	Definición operacional	Dimensiones	indicadores	Escala valorativa
Gestión de Riesgos	Casares (2013) refiere que la Gestión de riesgos Son las actividades coordinadas para dirigir y controlar una empresa en relación con el riesgo e incluye, por norma general, la evaluación, el tratamiento, la aceptación y la comunicación de los riesgos.	La Gestión de Riesgos, está comprometida con el nivel de gestión de la alta dirección, con la disposición de Recursos y presupuestas, infraestructura Tecnología y RR: HH	Cultura	Nª personal Capacitado Nª personal Sensibilizado	Nominal
			Gestión Gerencial	Grado de Planeamiento Nivel de Identificación Nivel de Valoración Grado de respuesta	
			Recursos y presupuesto	Nivel de disponibilidad Nivel de atención	
			Infraestructura Tecnológica	Nª Tecnología Adecuada Grado de infraestructura	
			RR: HH	Nivel de conocimiento Nivel de competencia Nivel de habilidad	
Activos de información	Poveda (2011) Los activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información.	ISO27001 (2013) los principios básicos de la seguridad de activos de información son la integridad, Disponibilidad y Confidencialidad, y para una mejor gestión de activos de información se deben implementar procesos de gestión	Seguridad	Nivel de confidencialidad Nivel de disponibilidad Nivel de integridad Nivel de Incidencias	
			Procesos	Nª de políticas Nº de Controles Nª de Procedimientos	

2.3. Población y muestra

Población

La población objeto de estudio, está constituido por 150 trabajadores de la Zona Registral III Sede Moyobamba.

Muestra

Se ha tomado como muestra para el desarrollo del presente proyecto a un total de 50 trabajadores de la Oficina Registral Tarapoto.

Criterios de Selección

Inclusión

Personal Nombrado, CAS y practicante del área de Tecnología de Información de la Oficina Registral de Tarapoto.

Personal Nombrado, CAS y practicante del área de la Unidad Registral de la Oficina Registral de Tarapoto

Personal Nombrado, CAS y practicante no capacitado en protección de activos de información

Personal de convenio del GORESAM

Exclusión

Personal que no desea participar en las capacitaciones

Personal que se encuentre con Licencia

Personal que se encuentre de vacaciones

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Técnica

La Técnica utilizada para la recolección de datos en el presente proyecto de investigación es la Encuesta, a través de formulación de preguntas.

Validación Y Confiabilidad Del Instrumento

El presente instrumento ya fue utilizado por: Condori (2012) en el estudio “Un Modelo de Evaluación de Factores Críticos de Éxito en la implementación de la seguridad en sistemas de información para

determinar su influencia en la intención del usuario", desarrollado por Henry Iván Condori Alejo en la ciudad de Lima en el año 2012.

2.5. Métodos de análisis de datos

La información será procesada mediante cuadros y gráficos estadísticos utilizando el programa SPSS versión 21, el cual permitirá comprender de manera sencilla los resultados obtenidos. Los resultados de la investigación se resolverán bajo un enfoque descriptivo correlacional, en donde se utilizará la prueba de independencia Chí – cuadrado de Pearson como instrumento fiable, para establecer la relación de cada una de las variables.

III. RESULTADOS

El análisis de los datos se realizó mediante la utilización de tablas y gráficos estadísticos, a fin de observar de manera rápida las características de la muestra de estudio, al igual que se utilizó la prueba de independencia Chí – cuadrado de Pearson, la misma que permitirán la comprobación de la hipótesis planteada. De acuerdo a nuestros objetivos planteados se realizará dicho análisis

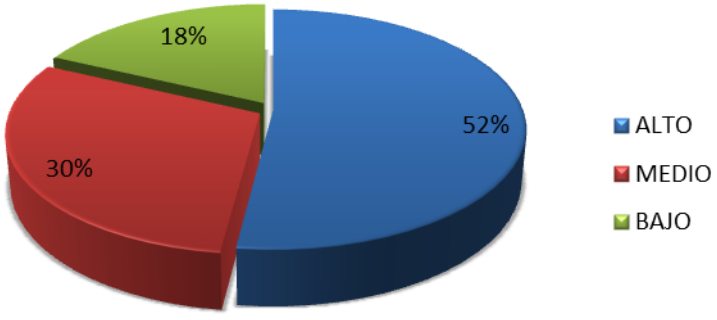
3.1. De acuerdo al objetivo planteando sobre El nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, se obtuvo que el 52% del personal encuestado indicaron que el nivel del riesgo de los activos de información es de “Alto” riesgo. Tal como se detalla en la tabla y grafico 01.

Tabla 1: Nivel de riesgo de los activos de información

ESCALA	PUNTAJES	N°	PORCENTAJE
ALTO	35 a 71	26	52%
MEDIO	72 a 113	15	30%
BAJO	114 a 155	9	18%
TOTAL		50	100%

Fuente: Encuesta realizada por el autor: ZONA REGISTRAL III – Sede Moyobamba.

Gráfico 1: Nivel de riesgo de los activos de información



FUENTE: Tabla 06.

Interpretación: De la tabla y gráfico 01, observamos las respuestas de los colaboradores encuestados de la variable Nivel de riesgo de los activos de información de la zona Registral N° III Sede Moyobamba, de los cuales 26 trabajadores que representan el 52% indicaron que el Nivel de riesgo de los activos de información es “Alto”, mientras que 15 encuestados que representan el 30% indicaron que es de riesgo “Medio”, sólo 9 trabajadores que representan el 18% indicaron que es de “Bajo” riesgo.

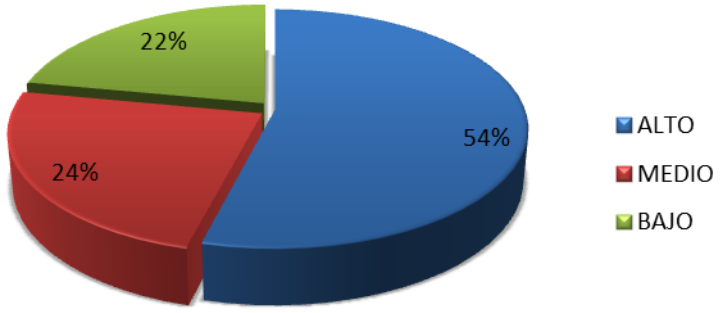
Asimismo, para lograr el resultado sobre el objetivo Nivel de riesgo de los activos de información se evaluaron las siguientes dimensiones:

Tabla 2: Nivel de riesgo de los activos de información - Cultura

ESCALA	PUNTAJES	N°	PORCENTAJE
ALTO	7 a 16	27	54%
MEDIO	17 a 26	12	24%
BAJO	27 a 35	11	22%
TOTAL		50	100%

FUENTE: Encuesta realizada por el autor: ZONA REGISTRAL III – Sede Moyobamba.

Gráfico 2: Nivel de riesgo de los activos de información - Cultura (%)



FUENTE: Tabla 01.

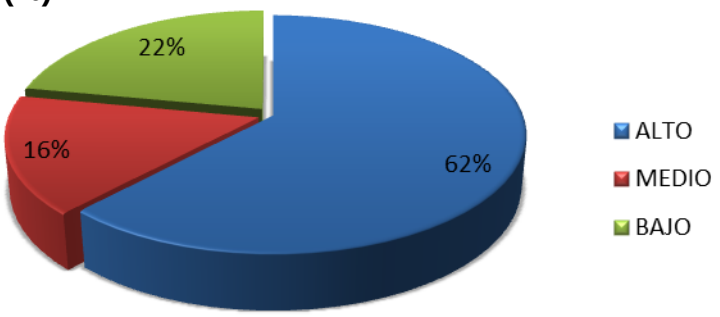
Interpretación: De la tabla y gráfico 02, observamos las respuestas de los colaboradores encuestados a la dimensión Cultura de la variable Nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, 27 trabajadores que representan el 54% indicaron que el Nivel de riesgo de los activos de información en su dimensión cultura es “Alto”, mientras que 12 encuestados que representan el 24% indicaron que es de riesgo “Medio”, sólo 11 trabajadores que representan el 22% indicaron que es de “Bajo” riesgo.

Tabla 3: Nivel de riesgo de los activos de información - Gestión Gerencial

ESCALA	PUNTAJES	N°	PORCENTAJE
ALTO	8 a 18	31	62%
MEDIO	19 a 29	8	16%
BAJO	30 a 40	11	22%
TOTAL		50	100%

FUENTE: Encuesta realizada por el autor: ZONA REGISTRAL III – Moyobamba.

Gráfico 3: Nivel de riesgo de los activos de información - Gestión Gerencial (%)



FUENTE: Tabla 02.

Interpretación: De la tabla y gráfico 03, observamos las respuestas de los colaboradores encuestados a la dimensión Gestión Gerencial de la variable Nivel de riesgo de los activos de información de la zona Registral

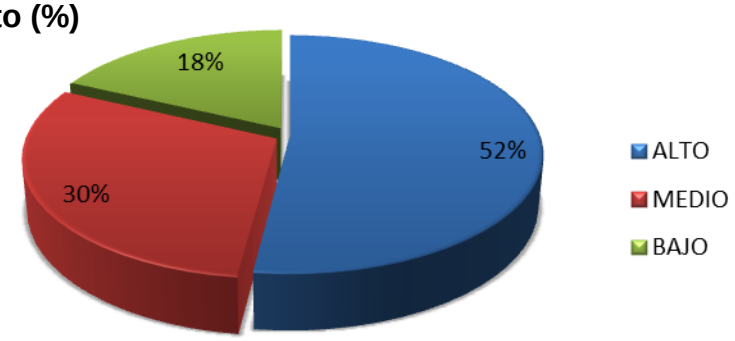
III Sede Moyobamba, 31 trabajadores que representan el 62% indicaron que el Nivel de riesgo de los activos de información en su dimensión Gestión Gerencial es “Alto”, mientras que 8 encuestados que representan el 16% indicaron que es de riesgo “Medio”, sólo 11 trabajadores que representan el 22% indicaron que es de “Bajo” riesgo.

Tabla 4: Nivel de riesgo de los activos de información - Recursos y Presupuesto

ESCALA	PUNTAJES	N°	PORCENTAJE
ALTO	4 a 9	26	52%
MEDIO	10 a 15	15	30%
BAJO	16 a 20	9	18%
TOTAL		50	100%

FUENTE: Encuesta realizada por el autor: ZONA REGISTRAL III – Moyobamba.

Gráfico 4: Nivel de riesgo de los activos de información - Recursos y Presupuesto (%)



FUENTE: Tabla 03.

Interpretación: De la tabla y gráfico 04, observamos las respuestas de los colaboradores encuestados a la dimensión Recursos y Presupuesto de la variable Nivel de riesgo de los activos de información de la zona Registral N° III Sede Moyobamba, 26 trabajadores que representan el 52% indicaron que el Nivel de riesgo de los activos de

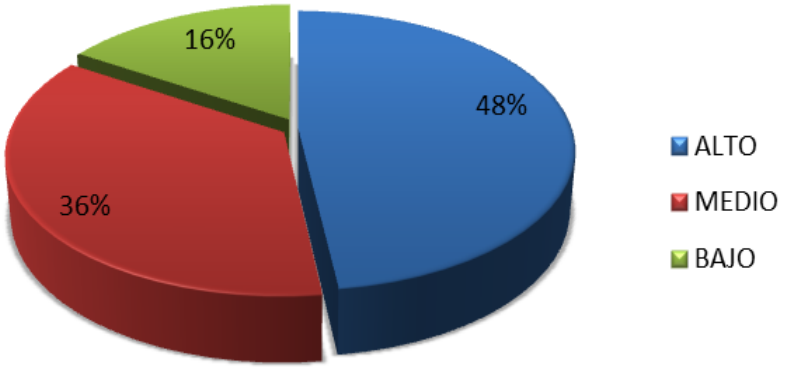
información en su dimensión Recursos y Presupuesto es “Alto”, mientras que 15 encuestados que representan el 30% indicaron que es de riesgo “Medio”, sólo 9 trabajadores que representan el 18% indicaron que es de “Bajo” riesgo.

Tabla 5: Nivel de riesgo de los activos de información - Infraestructura tecnológica

ESCALA	PUNTAJES	N°	PORCENTAJE
ALTO	6 a 14	24	48%
MEDIO	14 a 22	18	36%
BAJO	23 a 30	8	16%
TOTAL		50	100%

FUENTE: Encuesta realizada por el autor: ZONA REGISTRAL III – Moyobamba.

Gráfico 5: Nivel de riesgo de los activos de información - Infraestructura tecnología



FUENTE: Tabla 04.

Interpretación: De la tabla y gráfico 05, observamos las respuestas de los colaboradores encuestados a la dimensión Infraestructura tecnología de la variable Nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, 24 trabajadores que representan el 48% indicaron que el Nivel de riesgo de los activos de información en su dimensión Infraestructura tecnología es “Alto”, mientras que 18

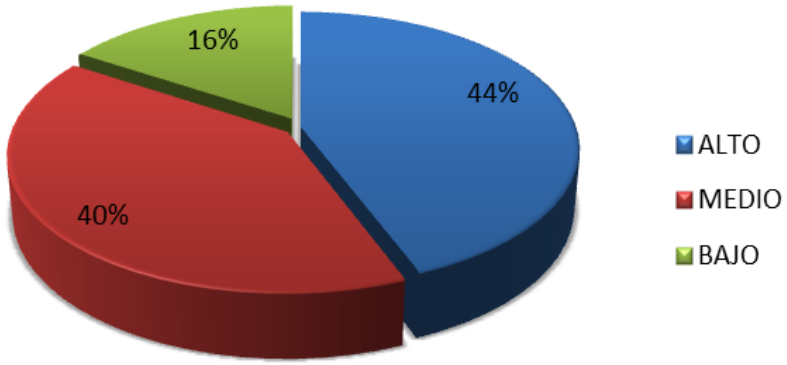
encuestados que representan el 36% indicaron que es de riesgo “Medio”, sólo 8 trabajadores que representan el 16% indicaron que es de “Bajo” riesgo.

Tabla 6: Nivel de riesgo de los activos de información - Recursos Humanos

ESCALA	PUNTAJES	N°	PORCENTAJE
ALTO	5 a 15	22	44%
MEDIO	15 a 20	20	40%
BAJO	20 a 25	8	16%
TOTAL		50	100%

FUENTE: Encuesta realizada por el autor: ZONA REGISTRAL III – Moyobamba.

Gráfico 6: Nivel de riesgo de los activos de información - Recursos Humanos (%)



FUENTE: Tabla 05.

Interpretación: De la tabla y gráfico 06, observamos las respuestas de los colaboradores encuestados a la dimensión Recursos Humanos de la variable Nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, 22 trabajadores que representan el 44% indicaron que el Nivel de riesgo de los activos de información en su dimensión Recursos Humanos es “Alto”, mientras que 20 encuestados que representan el 40% indicaron que es de riesgo “Medio”, sólo 8 trabajadores que representan el 16% indicaron que es de “Bajo” riesgo.

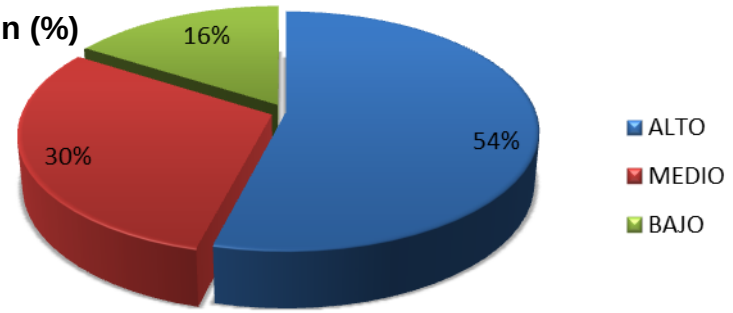
3.2. De acuerdo al objetivo planteando sobre Factores de riesgo que afectan a los activos de información de la zona Registral III Sede Moyobamba, se obtuvo que el 54% del personal encuestado indicaron que el nivel de riesgo de los factores que afectan a los activos de información es de "Alto" riesgo. Tal como se detalla en la tabla y grafico 07.

Tabla 7: Niveles de factores de riesgo que afectan a los activos de información

ESCALA	PUNTAJES	N°	PORCENTAJE
ALTO	18 a 42	27	54%
MEDIO	42 a 66	15	30%
BAJO	66 a 90	8	16%
TOTAL		50	100%

FUENTE: Encuesta realizada por el autor: ZONA REGISTRAL III – Moyobamba.

Gráfico 7: Niveles de factores de riesgo que afectan a los activos de información (%)



FUENTE: Tabla 09.

Interpretación: De la tabla y gráfico 07, observamos las respuestas de los colaboradores encuestados de la variable Niveles de riesgo que afectan a los activos de información de la zona Registral III Sede Moyobamba, 27 trabajadores que representan el 54% indicaron que el Nivel de riesgo que afectan a los activos de información es "Alto", mientras que 15 encuestados que representan el 30% indicaron que es de riesgo "Medio", sólo 8 trabajadores que representan el 16% indicaron que es de "Bajo" riesgo.

Asimismo, para lograr el resultado sobre el objetivo Factores de riesgo que afectan a los activos de información de la Zona Registral N° III Sede

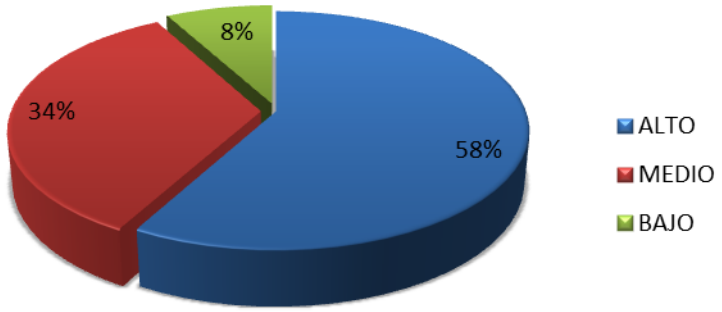
Moyobamba se evaluaron las siguientes dimensiones: Procesos y Seguridad tal como se detallan en las siguientes tablas y gráficos respectivamente.

Tabla 8: Activos de información - Procesos

ESCALA	PUNTAJES	N°	PORCENTAJE
ALTO	11 a 25	29	58%
MEDIO	26 a 40	17	34%
BAJO	41 a 55	4	8%
TOTAL		50	100%

Fuente: Encuesta realizada por el autor: ZONA REGISTRAL III – Moyobamba.

Gráfico 8: Activos de información - Procesos



FUENTE: Tabla 07.

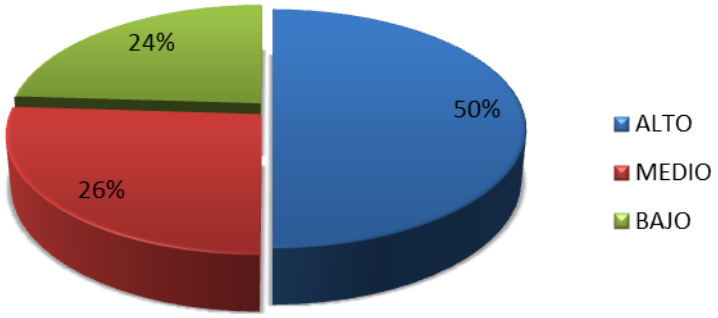
Interpretación: De la tabla y gráfico 08, observamos las respuestas de los colaboradores encuestados a la dimensión Procesos de la variable Niveles de riesgo que afectan a los activos de información de la zona Registral III Sede Moyobamba, 29 trabajadores que representan el 58% indicaron que el Nivel de riesgo que afectan a los activos de información en su dimensión Procesos es “Alto”, mientras que 17 encuestados que representan el 34% indicaron que es de riesgo “Medio”, sólo 4 trabajadores que representan el 8% indicaron que es de “Bajo” riesgo.

Tabla 9: Activos de información - Seguridad

ESCALA	PUNTAJES	N°	PORCENTAJE
ALTO	7 a 16	25	50%
MEDIO	17 a 26	13	26%
BAJO	27 a 35	12	24%
TOTAL		50	100%

FUENTE: Encuesta realizada por el autor: ZONA REGISTRAL III – Moyobamba.

Gráfico 9: Activos de información - Seguridad de datos (%)



FUENTE: Tabla 08.

Interpretación: De la tabla y gráfico 09, observamos las respuestas de los colaboradores encuestados a la dimensión Seguridad de datos de la variable Niveles de riesgo que afectan a los activos de información de la zona Registral III Sede Moyobamba, 12 trabajadores que representan el 24% indicaron que el Nivel de riesgo que afectan a los activos de información en su dimensión Seguridad de datos es “Alto”, mientras que 13 encuestados que representan el 26% indicaron que es de riesgo “Medio”, sólo 25 trabajadores que representan el 50% indicaron que es de “Bajo” riesgo.

3.3. Relación entre la influencia de gestión de riesgos y la seguridad de los activos de información de la Zona Registral N III Sede Moyobamba.

Para el análisis de relación entre las variables se usó la prueba de independencia Chí – cuadrado al 95% de confianza.

Hipótesis Estadística:

Ho: No existe relación entre la gestión de riesgos y la seguridad de los activos de información de la Zona Registral N III Sede Moyobamba.

H1: Existe relación entre la gestión de riesgos y la seguridad de los activos de información de la Zona Registral N III Sede Moyobamba

Tabla 10: Contingencia entre las variables

		Activos de informacion			
		Alto	Medio	Bajo	total
Riesgos	Alto	15	4	7	26
	Medio	5	10	0	15
	Bajo	7	1	1	9
	Total	27	15	8	50

FUENTE: BASE DE DATOS ELABORADO POR EL AUTOR

Interpretación: La tabla 10, muestra el cruce de respuestas entra las variables de estudio, para la variable gestión de riesgos se muestra su escala valorativa de Alto, Medio y Bajo; y para la variable Nivel de Factores de riesgo que afectan a los activos de información se muestran la escala valorativa de Alto, Medio y Bajo, estos valores nos servirán para la construcción de nuestra prueba Chi cuadrado y analizar los resultados de su correlación.

Tabla 11: Resultados Chí cuadrado

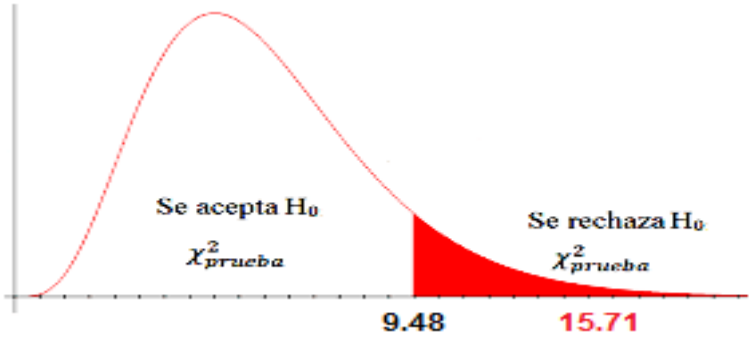
Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	15,712	4	.003
Razón de verosimilitudes	17.465	4	.002
Asociación lineal por lineal	1.201	1	.273
N de casos válidos	50		

FUENTE: BASE DE DATOS ELABORADO POR EL AUTOR – SPSS VER. 21

Interpretación: Aplicado la prueba de independencia Chi Cuadrado a base de la tabla de contingencia anterior, podemos observar que el resultado Chí Cuadrado de Pearson es 15.712, mayor al Chí tabular con 4 grados de libertad (9.48), lo que indica que existe relación entre las variables de estudio.

Gráfico 10: Zona de aceptación probabilística - chí cuadrado



Fuente: BASE DE DATOS ELABORADO POR EL AUTOR – SPSS VER. 21

Interpretación: Como el Chí Cuadrado de Pearson (15.71), es mayor al Chí tabular con 4 grados de libertad (9.48) y se encuentra en la zona probabilística de rechazo, aceptamos la hipótesis alternativa con un 95% de confianza y concluimos que: Existe relación entre la influencia de gestión de riesgos y la seguridad de los activos de información de la Zona Registral N III Sede Moyobamba.

IV. DISCUSIÓN

Al determinar el nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, se evaluó las dimensiones de Cultura, Gestión gerencial, Recursos y Presupuestos, Infraestructura Tecnológica y Recursos Humanos.

En La dimensión cultura de la variable Nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, se obtuvo un 54% que indicaron que el Nivel de riesgo de los activos de información es “Alto”. De igual manera en la dimensión Gestión Gerencial de la variable Nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, se obtuvo un 62% que indicaron que el Nivel de riesgo de los activos de información es “Alto”.

Al contrastar con los hallazgos de Cruz (2014), en su tesis titulada “Una Metodología de análisis y evaluación de riesgos en Tecnologías de Información” refiere que la evaluación de riesgos en la seguridad de la información no debe ser realizada exclusivamente para completar una lista de tareas o solamente para satisfacer un requerimiento normativo más bien se debe tomar como una Herramienta que permita a organización conocer en forma ordenada el comportamiento de los riesgos a los que está expuesto la información. Por ello es muy importante que la gestión gerencial se vea comprometida en implementar procedimientos, controles, políticas de seguridad y sensibilizar al personal, esto va a permitir minimizar la ocurrencia o el impacto financiero de posibles pérdidas que pudiesen suceder.

En la dimensión Infraestructura Tecnología de la variable Nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, se obtuvo un 48% que indicaron que el Nivel de riesgo de los activos de información es “Alto”. El mismo que se encuentra similitud con los hallazgos de López (2011) en su tesis titulada “Gestión de Riesgos Corporativos De TI En Guatemala” quien concluye que la gestión de riesgos de TI en las organizaciones sirve para evitar y minimizar pérdidas, pero también es útil para generar valor por medio de la aplicación de conceptos, principios y un conjunto de acciones definidas en controles. Por tanto, refiere que las empresas que poseen el nivel

de sofisticación mediano o alto de Tecnologías de Información son más dependientes de ella y crece su exposición a diversos riesgos, los cuales pueden comprometer el cumplimiento de los objetivos estratégicos.

Asimismo en la dimensión Recursos Humanos de la variable Nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, obtuvo un 44% que indicaron que el Nivel de riesgo de los activos de información en su dimensión Recursos Humanos es “Alto”, Al contrastar con los hallazgo de Cruz (2014), en su tesis “Una metodología de análisis y evaluación de riesgos en tecnologías de información”, menciona que en México existe una carencia y deficiencia en la difusión, capacitación y fomento de la seguridad informática, desde la organización misma hasta los empleados. Esto tiene como consecuencia estar en desventaja frente a los riesgos más comunes, dejando en segundo término la planeación de la seguridad, las políticas y procedimientos, la capacitación y educación, la disponibilidad de los sistemas; así como, las auditorías y evaluaciones de riesgos. En tanto, la dimensión de recursos es aun débil que debe ser tomada en consideración por la dirección de la institución con el fin de prevenir eventos no deseados y poder cumplir las metas institucionales.

La variable Nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba, obtuvo un 52% indicaron que el Nivel de riesgo de los activos de información es “Alto”, un 30% indicaron que es de riesgo “Medio”, y el 18% indicaron que es de “Bajo” riesgo. Al relacionar con los hallazgos Barrantes (2012), en su tesis titulada “Diseño e implementación de un sistema de Gestión de seguridad de información en procesos tecnológicos”, refiere que implementando una buena metodología para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables gran porcentaje de riesgos que afectan a los activos de información, el factor humano es crítico para la implementación de cualquier sistema de gestión organizacional es por ello que la formación y concientización de los mismos es indispensable para lograr una implementación exitosa, la documentación de los procesos es una

herramienta poderosa para el mantenimiento y mejora de cualquier sistema de gestión organizacional.

Al abordar la variable Nivel de Factores de riesgo que afectan a los activos de información de la zona Registral III Sede Moyobamba, obtuvo un 54% indicaron que el Nivel de los factores de riesgo que afectan a los activos de información es “Alto”, mientras un 30% indicaron que es de riesgo “Medio” y un 16% indicaron que es de “Bajo” riesgo. En tanto, Condori (2012) en su tesis titulada. “Un Modelo de Evaluación de Factores Críticos de Éxito en la implementación de la seguridad en sistemas de información para determinar su influencia en la intención del usuario”, menciona que dentro de todo el modelo, los factores más importantes por el grado de influencia en la Actitud para implementar Seguridad en Sistemas de Información son: En un primer lugar los Recursos y Presupuesto, donde el grado de influencia es -0.558, que afecta negativamente; ello en razón a que como ocurre en la mayoría de instituciones públicas, como en el caso de UNA-Puno, la falta de presupuesto es un factor determinante para implementar un plan de seguridad de información. La Cultura Organizacional donde el grado de influencia es 0.439, que revela la existencia de normas y valores que influyen positivamente en la situación estudiada., La Conciencia de la necesidad de seguridad por el personal con un grado de 0.431, que revela el grado de conciencia que tiene del personal de la UNA-Puno respecto a la necesidad de implementar seguridad en los sistemas de información.

Finalmente, el estudio muestra un Chí Cuadrado de Pearson de 15.712, mayor al Chí tabular con 4 grados de libertad (9.48), lo que indica que existe relación entre las variables de estudio. Por lo tanto, el estudio muestra relación entre la gestión de riesgos y la seguridad de los activos de información de la Zona Registral III Sede Moyobamba.

V. CONCLUSIONES

Luego de presentar los resultados aplicando las técnicas estadísticas descritas en los capítulos anteriores en la Influencia de Gestión de Riesgos en la Seguridad de Activos de Información de la Zona Registral III sede Moyobamba, se concluye que:

5.1. Existe influencia de la gestión de riesgos en la seguridad de los activos de información de la Zona Registral III Sede Moyobamba, donde existe un Chí Cuadrado de Pearson es 15.712, mayor al Chí Cuadrado tabular con 4 grados de libertad (9.48), lo que indica que existe relación entre las variables de estudio. Asimismo, se encuentra en la zona probabilística de rechazo por lo que se acepta la hipótesis alternativa con un 95% de confianza.

5.2. El nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba es de nivel de riesgo “Alto”, con un 52%, este resultado se obtuvo en base a las dimensiones evaluadas en la variable Gestión de riesgo con los siguientes porcentajes: La dimensión cultura muestra un 54% de nivel de Gestión de riesgo de los activos de información, posicionando en un nivel “Alto”; la dimensión Gestión Gerencial tiene un nivel “Alto” con un 62% de nivel de riesgo; de la misma manera, la dimensión Recursos y Presupuesto tiene un nivel “Alto” con un 52% de nivel de riesgo; asimismo, la dimensión Infraestructura tecnología tiene un nivel “Alto” con un 48% de nivel de riesgo; y la dimensión Recursos Humanos tiene un nivel “Alto” con un 44% de nivel de riesgo.

5.3. Los Factores de riesgo que afectan a los activos de información de la zona Registral N° III Sede Moyobamba, representa un 54% con un nivel “Alto” de riesgo que afectan a los activos de información. Este resultado se obtuvo en base a las dimensiones evaluadas en la Activos de información con los siguientes porcentajes: donde el factor procesos representa un 58% con un nivel de riesgo “Alto”, el mismo que afectan a

los activos de información. En tanto, el factor seguridad muestra un 50% posicionando en un nivel “Alto”.

VI. RECOMENDACIONES

6.1. A los altos directivos de la Zona Registral III Sede Moyobamba deben insertar estrategias y acciones que generen una adecuada gestión de riesgo con el propósito de garantizar la seguridad de los activos de información en la Zona Registral, todo ello contemplado en una gestión de documentos que acredite la secuencialidad de las acciones para concretar unos verdaderos procesos de gestión de cambio.

6.2. Al equipo decisor de la Zona Registral III Sede Moyobamba incorporar recurso humano idóneo, los mismo que tengan competencias en manejo de gestión de riesgo con ello fortalecer la gestión y salvaguardar los procesos de riesgo que se instalen en la Zona Registral N III Sede Moyobamba.

6.3. A los directivos deben implementar políticas, controles institucionales que garantice la seguridad de los activos de información en la Zona Registral III Sede Moyobamba. Asimismo, todas las políticas que serán implementadas deben estar contempladas en un documento de gestión para asegurar el medio adecuado de la implementación y su difusión con todo el personal.

VII. REFERENCIAS BIBLIOGRÁFICAS

Bajo, J. (2013). *Guia para la Gestion de riesgos Empresariales ISO 31000.* Madrid: Ampell Consultores Asociados.

Barrantes, C. (2012). *Diseño E Implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos.* Lima.

Casares, I. (2013). *Proceso de Gestion de Riesgos en la Empresas.* España: Molinuevo, Gráficos, S.L.

Caseres, Y. (2013). *Proceso de Gestion de Riesgos y seguros en las Empresas.* España: Molinuevo, Gráficos, S.L.

Condori, H. (2012). *Un Modelo de Evaluación de Factores Críticos de Éxito en la implementación de la seguridad en sistemas de información para determinar su influencia en la intención del usuario.* Tesis, Puno.

Cruz Mendoza, J., Jalpilla Jimenez, R., & Ramirez San miguel, E. (2014). *Una Metodología de análisis y evaluación de riesgos en Tecnologías de Información.* Tesis, Mexico.

Gómez, M. A., & MAGERIT. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* España: Subdirección General de Información, Documentación y Publicaciones. Obtenido de http://administracionelectronica.gob.es/pae_Home/dms

Information Technology -Security Techniques - Management of Information and Communications Technology Security. (2013).

ISO27001. (09 de 10 de 2007). *El portal de ISO 27001*. Obtenido de http://www.iso27000.es/

Lopez, N. (2011). *Gestion de Riesgos Corporativos de Tecnologias de Informacion en Guatemala.* Tesis, Guatemala, Guatemala.

NTP-27005:2009. (2009). *Tecnologia de la Informacion-Tecnicas de Seguridad -Gestion de riesgos de seguridad de la informacion.* Primera edición .

Palma, M. (2014). *Los 12 grandes retos en la gestión de los activos de información y evidencias en la era digital.* AENOR.

Paredes, G. (2016). *Implementación de un Sistema de Gestión de Seguridad de la Información, Aplicado a los Riesgos Asociados a los Activos de Información En la Empresa Net – Consultores S.A.C.* Tesis, Tarapoto.

Pastor, C. A. (2010). *Impacto del Riesgo en el Gobierno de las Tecnologías de Información y Comunicación en la Gestión Empresarial Industrial del siglo XXI.* Lima.

Perafan, J. (2014). *Analisis de Riesgo de la Seguridad de la Informacion para la institucion Universitaria Colegia Mayor del Cauca.*

Poveda, J. (2011). Los Activos de la Seguridad de la informacion.

Purdy, G. (2009). *ISO 31000:2009- setting a new standard for risk management .*

Ramirez, A. (2011). Gestion de Riesgo Tecnologicos Basados en ISO 3100 e iso 27005 y su aporte a la continuidad de Negocio. 56-66.

Romeral, L. (2008). *Gestion de Riesgos Tecnologicias.* Madrid: Aosciacion Española para la Gobernaza, la Gesstion y la medicion de las Tecnologias de la Informacion .

SGSI. (06 de 04 de 2015). *ISO 27001: Amenazas y vulnerabilidades*. Obtenido de http://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

SUNARP. (2016). *SUNARP*. Obtenido de SUNARP: www.sunarp.gob.pe

ANEXOS

Anexo 01: MATRIZ DE CONSISTENCIA

"Análisis de la Gestión de Riesgo en la protección activos de Información de la Zona Registral N° III Sede Moyobamba"

<table>
<tr><th colspan="4">REALIDAD PROBLEMÁTICA</th></tr>
<tr><td colspan="4">En la Zona Registral III Sede Moyobamba, se maneja grandes volúmenes de información de vital importancia, las cual esta almacenada a través de Base de Datos, discos externos, servidores de archivos, transmitida por correo, medios magnéticos, física, etc. la cual se comparte diariamente con usuarios internos y externos, en la actualidad la información están sujeto a riesgos y amenazas ya sea por fuente internas o externas que pueden atentar contra su confidencialidad, integridad y disponibilidad de la misma, ocasionando de esta manera la inviabilidad del servicio Registral, perjudicando la atención al usuario, ya que no se estaría garantizando la seguridad Jurídica a través del registro y publicidad de derechos, ocasionando una pérdida de imagen para la institución, generando gastos indirectos y problemas estrictamente legales. Por eso es importante gestionar los riesgos a los que está expuesta la información estableciendo mecanismos de seguridad que permitan proteger la información de un amplio rango de amenazas, garantizando de esta manera que los riegos sean conocidos, asumidos, gestionados y minimizados y así evitar que el riesgo se materialice y perjudique al usuario.</td></tr>
<tr><th>FORMULACIÓN DEL PROBLEMA</th><th>OBJETIVOS DE LA INVESTIGACIÓN</th><th>HIPÓTESIS DE INVESTIGACIÓN</th><th>FUNDAMENTO TEÓRICO</th></tr>
<tr>
<td>PROBLEMA GENERAL
¿Cuál es la influencia de la gestión de riesgos en relación a los activos de información de la zona Registral N III Sede Moyobamba?

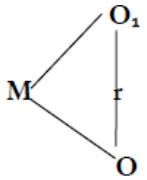
PROBLEMAS ESPECÍFICOS.
▪ ¿Cuál es el nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba,
▪ ¿Cuáles son los factores de riesgo que afectan a los activos de información de la Zona Registral III Sede Moyobamba?</td>
<td>OBJETIVO GENERAL
¿Conocer la influencia de la gestión de riesgos en la seguridad de los activos de información de la Zona Registral III Sede Moyobamba

OBJETIVOS ESPECÍFICOS
▪ Determinar el nivel de riesgo de los activos de información de la zona Registral III Sede Moyobamba.
▪ Identificar los factores de riesgo que afectan a los activos de información de la Zona Registral III Sede Moyobamba.</td>
<td>HIPÓTESIS GENERAL H_1
H_G Existe influencia de la Gestión De Riegos en la seguridad de los activos de Información de La Zona Registral N III Sede Moyobamba

HIPÓTESIS ESPECÍFICAS
H_1: El Nivel de riesgo de los activos de información de la zona Registral N° III Sede Moyobamba es alta

H_2: Los factores de riesgo que afectan a los activos de la información de la Zona Registral N° III Sede Moyobamba es alta</td>
<td>Gómez (2012) nos dice que la Gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.
Casares (2013) refiere que la Gestión de riesgos Son las actividades coordinadas para dirigir y controlar una organización en relación con el riesgo e incluye, por norma general, la evaluación, el tratamiento, la aceptación y la comunicación de los riesgos
Bajo (2013) refiere que La gestión del riesgo es el proceso por el que las organizaciones tratan los riesgos relacionados con sus actividades, con el fin de obtener un beneficio sostenido en cada una de ellas y en el</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>conjunto de todas las actividades</td></tr>
<tr><td>DISEÑO DE INVESTIGACIÓN</td><td>POBLACIÓN Y MUESTRA</td><td>VARIABLES DE ESTUDIO</td><td>INSTRUMENTOS DE RECOLECCIÓN DE DATOS</td></tr>
<tr>
<td>Es de tipo Correlacional descriptivo porque los datos se recolectaron en un solo espacio y tiempo, con el propósito de describir y analizar las variables en el momento dado.

Esquema
 

Dónde:
M= Zona Registral III- Sede Moyobamba
O1= Representa los datos de Gestión de riesgos
O2 = Representa los datos de activos de información
r = Influencia de la gestión de riesgos en la seguridad de activos de información</td>
<td>POBLACIÓN.
La población objeto de estudio está conformada por los 150 trabajadores, de la Zona Registral N° III Sede Moyobamba

MUESTRA.

Se ha tomado como muestra para el desarrollo del presente proyecto a un total de 50 trabajadores de la Oficina Registral de Tarapoto</td>
<td>
<table>
<tr><th>Variable</th><th>Dimensiones</th><th>Indicador</th><th>Escala</th></tr>
<tr><td>Gestión de Riesgos</td><td>• cultura
• Gestión
• Recursos y presupuesto
• Infraestructura tecnológica
• RR:HH</td><td>Capacitación
Sensibilizado
Planeamiento
Identificación
Valoración
Respuesta
Tecnología
Infraestructura
Conocimiento
Competencia
habilidad</td><td>Nominal</td></tr>
</table>
<table>
<tr><th>Variable</th><th>Dimensiones</th><th>Indicador</th><th>Escala</th></tr>
<tr><td>Activos de información</td><td>•Seguridad
•Procesos</td><td>Confidencialidad
Disponibilidad
Integridad
Incidencias
Copias
Políticas
Controles
procedimientos</td><td>Nominal</td></tr>
</table>
</td>
<td>Se procederá mediante el llenado de nuestra base de datos a partir de la encuesta correspondiente a la gestión de Riesgos en la seguridad de activos de información de la zona Registral III Sede Moyobamba.

El análisis de los datos se realizarán mediante la utilización de tablas y gráficos estadísticos, a fin de observar de manera rápida las características de la muestra de estudio, al igual que se utilizará la prueba de chi cuadro de Pearson, la misma que permitirán la comprobación de la hipótesis planteada.</td>
</tr>
</table>

Anexo 02: Instrumentos de recolección de datos

ENCUESTA

Para medir la gestión de riesgos asociados a los activos de información (HARDWARE, Software, Base de datos, Archivos) dirigido al personal de la Zona Registral Nª III Sede Moyobamba

DATOS GENERALES:

Área: ……

Cargo: ……

Se ha diseñado el presente cuestionario con el objeto de tener un buen procedo de medición sobre la Gestión de Riesgos asociados a los activos de información, por lo que necesitamos de su colaboración. Marcar con una equis (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

Leyenda: 5. Siempre 4. Casi Siempre 3. A veces 2. Casi nunca 1. Nunca

	DIMENSIONES	ESCALA				
		1	2	3	4	5
	Cultura					
1	¿Ha recibido capacitación útil por parte del área de UTI de cómo proteger su información?					
2	¿La institución ha implementado un plan de capacitación sobre gestión de riesgo en seguridad de la información?					
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?					
4	¿La institución recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?					
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información?					
6	Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza.					
7	¿El personal está concientizado en prevención y control de los riesgos según sus roles y responsabilidades en la institución?					
	Gestión Gerencial					
8	¿La institución ha implementado un plan de tratamiento de riesgos para la seguridad de la información?					
9	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?					
10	¿Están identificados los riesgos significativos a los que están expuesta la información?					
11	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?					
12	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?					
13	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados					
14	¿se han establecido las acciones necesarias para afrontar los riesgos evaluados					

15	¿Se han definido lineamientos para efectuar seguimiento periódico a los controles desarrollados con respecto a la gestión de riesgos de información?					
	Recursos y Presupuesto					
17	Existe disponibilidad de los recursos materiales (CPU, Muebles, antivirus etc.) que se usa para que los Sistemas funcionen adecuadamente.					
18	Los recursos que Usted Solicita para los sistemas son Oportunamente atendidos.					
19	Si se implementa un proyecto de sistemas, siente que se le asignara los recursos y presupuestos Necesarios oportunamente.					
20	Percibe que se asigna el suficiente personal técnico y De apoyo para el soporte de los sistemas.					
	Infraestructura tecnología					
21	¿La institución cuenta con tecnología adecuada para el desarrollo de las actividades?					
22	¿La institución invierte en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para una mayor seguridad de la información?					
23	Las computadoras asignadas para el desarrollo de sus actividades trabajan eficientemente y sin fallas					
24	Cuenta con el servicio de internet adecuado, de acuerdo a las labores que realiza					
25	Las computadoras están interconectadas a una red De corriente estabilizada					
26	Las computadoras están interconectadas por una red Para compartir de información.					
	RRHH					
27	El personal conoce y utiliza métodos de seguridad de información para proteger la información					
28	En cuanto a los problemas que se presentan con el Sistema no requiere asistencia técnica.					
29	Es natural navegar por internet y sabe cómo protegerse de virus y otros ataques					
30	Es natural utilizar correo electrónico, y sabe cómo Protegerse de virus y otros ataques.					
31	Se considera usted un experto en el manejo de computadoras y sistemas.					

ENCUESTA

Para medir los activos de la información dirigido a personal de la Zona Registral NIII Sede Moyobamba

DATOS GENERALES:

Cargo:

……

Se ha diseñado el presente cuestionario para el personal del área de tecnologías de información de la Zona Registral N° III Sede Moyobamba, Con la finalidad de llevar buen proceso de medición sobre las Tecnologías de Información, por lo que necesitamos de su colaboración. Marcar con una equis (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

Leyenda: 5. Siempre 4. Casi Siempre 3. A veces 2. Casi nunca 1. Nunca

	DIMENSIONES	ESCALA				
		1	2	3	4	5
	Procesos					
32	Se ha establecido políticas para el uso adecuados de los activos de información (Base de Datos, Hardware, software, archivos físicos, etc.)					
33	Se han establecido controles para el uso adecuado de los activos de información (Base de Datos, Hardware, software, archivos físicos, etc)					
34	cumple con las políticas establecidos en el uso adecuado de los activos de información (Base de Datos, Hardware, software, archivos físicos, etc)					
35	¿Se han establecido procedimientos para el resguardo de la información?					
36	¿Cumple con los procedimientos establecidos para el resguardo de la información ¿					
37	¿Se han establecido políticas para el acceso al servicio de internet?					
38	Se ha implementado políticas para el uso adecuado de contraseñas de seguridad					
39	El personal conoce las políticas para el uso adecuado de contraseñas de seguridad					
40	¿Se tiene un registro codificado de las incidencias que se presentan en el manejo de los activos de información?					
41	¿Usted comunica oportunamente sobre las incidencias que se presentan en el manejo de los activos de información?					
42	¿Existe un procedimiento para el tratamiento especial a los incidentes de alto nivel de impacto?					
	Seguridad del personal					
43	Siente que necesita seguridad y protección confiable en su computador para evitar pérdida, daños y Modificación de la información con que trabaja.					
44	Siente que podría ocurrir que un virus informático ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se Debe proteger la información.					
45	Siente que podría ocurrir que un fallo eléctrico ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se Debe proteger la información.					
46	Siente que podría ocurrir que un robo ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger La información.					
47	Es importante no compartir su computador, Contraseñas del sistema con otras personas.					
48	Es importante cambiar las contraseñas de acceso al Sistema frecuentemente.					
49	Realiza frecuentemente copias de su información					

Anexo 03: Ficha de Validación de Instrumento

FICHA DE VALIDACIÓN DE INSTRUMENTO

I. **DATOS INFORMATIVOS:**

Apellidos y Nombre del Experto	Institución donde labora	Grado académico	Autores del Instrumento
SÁNCHEZ DÁVILA, Keller	UNSM-T/UCV	MAGISTER	Br. TARRILLO SALDAÑA, Esther Marleni
TITULO: "INFLUENCIA DE LA GESTION DE RIESGOS EN LA SEGURIDAD DE ACTIVOS DE INFORMACION DE LA ZONA REGISTRAL NIII SEDE MOYOBAMBA,2015"			

INSTRUCCIONES: Lee cada uno de los indicadores correspondientes a los criterios que estructura la validación de los instrumentos de tesis, valóralos con Honestidad y Humildad según la evaluación. Así mismo su observación.

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

II. **ASPECTOS DE VALIDACIÓN : LISTA DE COTEJO**

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Está formulado con lenguaje apropiado.				X	
OBJETIVIDAD	Está expresado en conductas observables				X	
ACTUALIDAD	Adecuado al avance de la ciencia y tecnología.					X
ORGANIZACIÓN	Existe una organización Lógica.					X
SUFICIENCIA	Comprende los aspectos en cantidad y calidad.					X
INTENCIONALIDAD	Adecuado para valorar aspectos de las estrategias.				X	
CONSISTENCIA	Basado en los aspectos teóricos científicos.				X	
COHERENCIA	Entre los índices, indicadores y las dimensiones.					X
METODOLOGIA	Las estrategias responden al propósito del diagnóstico.				X	
PERTINENCIA	El instrumento responde al momento oportuno o más adecuado.					X
Subtotal					20	25
Total		45				

III. **OPINION DE APLICACIÓN:** Este instrumento está listo para aplicarse dado que muestra coherencia y tiene pertinencia entre la misma.

IV. **PROMEDIO DE EVALUACIÓN: 4.5**

Tarapoto, 22 de Mayo del 2016

Mg. Keller Sánchez Dávila
DOCENTE POS GRADO

Anexo 04: Carta de autorización

sunarp
Superintendencia Nacional de los Registros Públicos

Tarapoto 13 de Junio del 2016

CARTA DE AUTORIZACION

Por medio del presente el Jefe de la oficina Registral de Tarapoto- de la Zona Registral N III- Sede Moyobamba, autoriza a la servidora, ESTHER MARLENI TARRILLO SALDAÑA, identificada con DNI 40349723, a realizar la aplicación de encuestas con el personal de la oficina Registral de Tarapoto, los datos obtenidos serán exclusivamente utilizados para la elaboración de la tesis de maestría en Gestión Pública.

Atentamente

José W. Romero Asenjo
Registrador Público
Zona Registral N° III
Sede Moyobamba