UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Análisis de riesgos a los activos de información aplicado a la gerencia de administración y finanzas de la Municipalidad Provincial de San Martín - Tarapoto

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniera de Sistemas

AUTORA:

Vilchez Morante, Denisse Katherine (orcid.org/0000-0002-7183-2213)

ASESORA:

Mg. Quito Rodríguez, Carmen Zulema (orcid.org/0000-0002-4340-5732)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información.

PIURA - PERÚ

2021

Dedicatoria

Este trabajo va dedicado en primer lugar a Dios, a quien le pido a diario para que me de mucha serenidad y mucha sabiduría en este proyecto que está pronto a culminar.

A mis pequeños hijos, quienes son el motor y motivo para mi superación del día a día, y a mis padres que son las personas por las cuales mis logros y éxitos tienen un sentido en la vida y es ser cada vez mejor.

Agradecimiento

A mi alma mater Universidad César Vallejo, A mi asesora Mg. Carmen Quito que con su amplio conocimiento ha podido guiar y encaminar la realización de esta investigación.

Índice de contenidos

Índice de tablas

Índice de gráficos

Resumen

La tesis tiene como objetivo principal la elaboración de un análisis de riesgos hacia los activos de información, el cual ayudará a que la municipalidad pueda identificar sus riesgos y vulnerabilidades que se deben considerar para evitar las amenazas que estén latentes en el medio y puedan tomar medidas de prevención oportunas que resulten ser las adecuadas.

La metodología utilizada fue de tipo cualitativa - cuantitativa, se utilizó como parte de los instrumentos una ficha con el detalle de los activos en donde el personal encargado pudo darle un valor para poder estimar el grado del riesgo, así mismo una encuesta que se entregó a los colaboradores responsables que permitió poder identificar y conocer la situación actual referente a los activos de información que se encuentran dentro de la municipalidad.

Este análisis permitirá direccionar y gestionar las evaluaciones del riesgo por sí mismos, tomando las mejores decisiones para la municipalidad haciendo una comparación del análisis del riesgo inicial con el resultado (valoración) para poder determinar si el riesgo es aceptable o no. Con estas buenas prácticas que se llevarán a cabo dentro de la investigación se puede sumar un control periódico a los activos con la finalidad de llegar a mitigar el riesgo que pueda presentarse. En resumen, lo que se pretende con el Análisis de Riesgos es reducir la probabilidad. Se debe tener en claro que la amenaza no se puede reducir, pero si podemos eliminar la vulnerabilidad y el impacto de la ocurrencia sea menor.

Palabras clave: Análisis de riesgos, activos de información, Magerit.

Abstract

This thesis has as main objective the elaboration of a risk analysis towards the information assets, which will help the municipality to identify its risks and vulnerabilities that must be considered in order to avoid threats that are latent in the environment and can take Measures that are appropriate.

The methodology used was qualitative-quantitative, used as part of the instruments a card detailing the assets in which the personnel in charge could give a value to be able to estimate the degree of risk, as well as a survey that was given to The responsible collaborators that allowed to be able to identify and to know the current situation regarding the information assets that are within the municipality.

This analysis will make it possible to address and manage risk assessments on their own, making the best decisions for the municipality by comparing the initial risk analysis with the outcome (valuation) to determine whether the risk is acceptable or not. With these good practices that will be carried out within the investigation can be added a periodic control to the assets in order to mitigate the risk that may arise. In short what is intended with Risk Analysis is to reduce the probability. It should be clear that the threat cannot be reduced but if we can eliminate the vulnerability and the Impact of the occurrence is lower.

Keywords: Risk analysis, information assets, Magerit.

I. INTRODUCCIÓN

En el tiempo actual, la gestión de riesgos está inmerso dentro de los procesos conocidos como control interno, puesto que las organizaciones en la actualidad suelen ser más dependientes de los problemas que los afecten, por tan pequeño que demuestre serlo puede llegar a complicar la continuidad en sus procedimientos, traduciendo el hecho se pueden convertir en grandes pérdidas económicas.

Año tras año, el surgimiento de las actuales redes informáticas en especial la era del internet, ha sido un factor que dio un giro de mucha importancia y se tornó a su vez relevante, en cuanto a seguridad de información, ya que esto implica verificar los recursos que los sistemas de clase seguridad de información puedan estar protegidas adecuadamente con el fin generar la minimización de daños de la organización y maximizar el ingreso de los mismos.

Sin embargo, se debe mencionar que un sistema nunca puede llegar a ser seguro, ya que continuamente existen amenazas y vulnerabilidades a las cuales está expuesta, pero en este caso existen medidas de seguridad que servirán de salvaguardas para proteger los activos de información de cualquier entidad pública o privada donde se vea en peligro su información. Por tanto, se han creado políticas y normativas con un propósito principal de la prevención de ataques y con esto controlar los riesgos que se presenten.

Se debe mencionar que la forma más adecuada de poder proteger los activos de información de cualquier entidad es mediante una adecuada gestión de riesgos de información, para de esta manera poder identificar y encaminar esfuerzos hacia aquellos activos que se encuentren con mayor exposición de ser vulnerados.

Como realidad problemática, se tuvo que en la municipalidad de San Martín-Tarapoto, siendo el área de Administración y Finanzas la evaluada, no cuenta con un sistema de gestión de riesgos hacia los activos de información, que ayude a identificar las vulnerabilidades, y amenazas a las que usualmente se encuentran expuestas gran parte de la información en cada uno de los procesos internos que se hallan dentro del área en mención, no cuenta con un sistema de estandarización de controles que permitan llegar a mitigar las diversas amenazas a las cuales están

expuestos los datos involucrando a su vez la disponibilidad, integridad y confidencialidad de la información que se considera vital para la municipalidad.

Todos los activos se ven ligados hacia un rango inmenso de amenazas y vulnerabilidades, sin embargo, la mayoría de las entidades que están sumergidas en ellos, no tienen la idea de la magnitud de problemas que conllevan. En la MPSM no se invierte en sistemas para análisis de riesgos y con esto se puede llegar a minimizar la pérdida de información en el caso que se concretase el hecho, ya que los activos de información son considerados como imprescindible para toda organización en especial en el área de Administración y Finanzas.

El problema existente en la MPSM muchas veces es la informalidad con la que realizan muchos de sus procesos ,un ejemplo claro es que no cuenta con una política de uso de claves de los colaboradores, el personal administrativo en su mayoría no cuentan con claves de acceso a las máquinas, por tanto, cualquier persona que se encuentre dentro del área puede tener acceso a las máquinas a las cuales se les asignó para realizar alguna tarea inmediata, cabe resaltar que dentro de su reglamento interno no cuentan con alguna normativa que abale el buen uso de los activos de información.

Dentro del área de Administración y Finanzas existen tres sub divisiones una de ellas es el área de Logística que han presentado ciertos inconvenientes dentro de los procesos internos de su información, debido a que ha ido incrementando paulatinamente y no se ha llegado a tener un cuidado adecuado en el manejo interno de la información y la importancia de este en acreditar que no caiga en manos de personas inescrupulosas y este a su vez se vuelva un entorno inseguro; a medida que va incrementando sus procesos de información en las diversas sub áreas también es necesario ir asegurando la información existente e ir implementando políticas en donde queden las buenas prácticas en cada uno de los procesos internos del manejo de la información, incluyendo a su vez los activos informáticos que directamente estén ligados a este proceso, tal cual se menciona en la Metodología Magerit para poder identificar los riesgos y a su vez poder tomar medidas de salvaguardas con la finalidad de poder concientizar a los usuarios

encargados de la posible existencia de riesgos y de la necesidad de que estos sean mitigados con tiempo.

Operar de esta manera trae consigo una serie de debilidades en las que se ve envuelto el municipio ya que debe proteger en gran parte su información para asegurar su buen funcionamiento de los procesos internos.

Los problemas como el no uso de políticas de control de riesgos sobre sus activos de información, no se tienen identificadas las amenazas constantes sobre sus activos, las PC no cuentan con política de usos de claves para cada usuario, muchas de las personas que se encuentran dentro del área evaluada no están capacitadas para el uso de las herramientas tecnológicas, deben ser corregidos o en su defecto minimizados, el municipio no puede seguir llevando sus actividades en muchos de sus casos de manera ineficiente, por ello realizar un análisis de riesgos sobre los activos de información se torna en una parte esencial , con la aplicación de este análisis será posible que en adelante se logren identificar las posibles amenazas que atentan a diario a sus procesos.

Como formulación del problema, se obtuvo la siguiente pregunta general:

- ¿Cómo tratar e identificar los riesgos que afecten los activos de información de la gerencia de administración y finanzas de la Municipalidad Provincial de San Martin-Tarapoto?

Y las preguntas específicas fueron:

- ¿Cuáles son los activos de información que se encuentran dentro del área de Administración y Finanzas de la Municipalidad Provincial de San Martín - Tarapoto?

- ¿Cómo se pueden valorar las vulnerabilidades y amenazas de los activos de información dentro del área de Administración y Finanzas de la Municipalidad Provincial de San Martin-Tarapoto?

- ¿Qué acciones se pueden tomar en cuenta para la evaluación de riesgos de los activos de información identificados dentro del área de Administración y Finanzas de la Municipalidad Provincial de San Martin-Tarapoto?

- ¿Qué se debe proponer para combatir los riesgos que se presenten en los activos de información dentro del área de Administración y Finanzas de la Municipalidad Provincial de San Martin-Tarapoto

La justificación es que la realización de la presente investigación ayudará al investigador a lograr tener una visión más amplia de cómo se gestiona un análisis de riesgos mediante la aplicación de la metodología Magerit bajo el estándar aplicado que es la ISO/IEC 27005:2008, quien establece directrices para gestionar riesgos, es predominante que apliquemos una metodología que nos ayude a contrarrestar los riesgos de la seguridad de la información y futuros peligros que puedan ocasionar un software malicioso o usuario no autorizado.

Tiene como finalidad optimizar y obtener mejoras en los procesos que aún son de carácter críticos con la única finalidad de obtener beneficios que conlleven a fomentar un buen servicio de calidad para el desarrollo económico y social, a fin de obtener mejoras continuas aplicada a los riesgos de seguridad de la información y poder implantar un entorno seguro para la Municipalidad provincial de San Martin-Tarapoto , esta a su vez será tomada como una decisión importante que debe así involucrar a toda los miembros de la municipalidad se tomará lineamientos y procedimientos que permite identificar fácilmente los riesgos a la cual está sometida nuestra información.

Con estos controles aplicados a los activos informáticos podemos salvaguardarlos, de esta manera, podemos desarrollar ciertos objetivos marcados por las políticas de seguridad. Con esto se logrará una reducción por cada amenaza hasta alcanzar un nivel aceptable en la Municipalidad quien aplicará esta metodología, de esta manera, si se diera el caso de algún incidente, se suma la posibilidad adecuada de que los daños serían mínimos y la continuidad del proceso puede tene una seguridad mayor.

Se formaron los objetivos, y el general fue:

- Elaborar un análisis de riesgos a los activos de información de la gerencia de administración y finanzas de la Municipalidad Provincial de San Martin-Tarapoto.

Y los objetivos específicos eran:

- Identificar los activos de información que se encuentren en el área de Administración y Finanzas de la Municipalidad Provincial de San Martín-Tarapoto.
- Evaluar las vulnerabilidades y amenazas de los activos de información que se identifiquen dentro del área de Administración y Finanzas de la Municipalidad Provincial de San Martín-Tarapoto.
- Medir el riesgo de los activos de información identificados dentro del área de Administración y Finanzas de la Municipalidad Provincial de San Martín-Tarapoto.
- Proponer controles o salvaguardas de seguridad para combatir los riesgos que se presenten en los activos de información dentro del área de Administración y Finanzas de la Municipalidad Provincial de San Martín-Tarapoto.

II. MARCO TEÓRICO

John Perafán Ruiz (2014) en su tesis “Análisis de riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca-Colombia” tuvo como objetivo realizar un análisis de riesgo que le permitió generar controles con la finalidad de llegar a disminuir la probabilidad de ocurrencia de impacto de los riesgos asociados con las vulnerabilidades y amenazas, este a su vez muestra un detalle de controles que va a permitir la mejora a sus procesos enfocados en conceptos netamente de seguridad en cuanto a su información. La metodología aplicada es la de Magerit que va a permitir evaluar los riesgos a los cuales están sometidos los activos de información.

El desarrollo del mismo se llevó a cabo en tres fases: La primera consistió en la investigación documental, lo siguiente en la investigación a campo y como tercera parte se consideró el análisis, y evaluación de los riesgos de los activos de información. Siguiendo la secuencia el análisis aplicado logra obtener desde una perspectiva macro el estado actual en cuanto a la seguridad de los activos de información dentro de la IUCMC, llegando a la conclusión final de la evaluación se logró tomar como columna vertebral de esta evaluación los controles y las políticas de seguridad que se presentó como resultados del análisis de los riesgos de seguridad de información, la aplicación del mismo se logró incrementar la confiabilidad, la integridad y la disponibilidad de la información dentro de la universidad, consiguiendo con esto optimizar sus procesos y demostrando a su vez un nivel de confianza considerable dentro de la institución.

Carlos Barrantes Porras (2012) en su tesis “Diseño e implementación de un sistema de gestión de seguridad de la información en procesos Tecnológicos.” Tuvo como objetivo reducir y mitigar los riesgos que se presentan en los procesos que ponen en peligro los recursos y continuidad de sus procesos tecnológicos, implementando controles , políticas, monitoreando vulnerabilidades, controlando al 100% la gestión de la SGSI implementada, esta aplicación estuvo acompañada por su metodología de gestión de riesgos llamada Magerit, quien aplica el análisis y gestión de riesgos a sus sistemas de Información, el propósito es brindar un método sistemático para poder analizar los riesgos existentes a su vez planificar medidas existentes para tener bajo control el sistema implementado.

El motivo por el cual se considera este antecedente fue porque se ubica dentro del estudio y análisis a lo referido con seguridad de información partiendo de la metodología implementada pues está utilizando una parte de la metodología del PDCA que tiene mucho para aportar al proyecto, se centra mucho en la estructura de la seguridad de la información comenzando por aplicar los cuatro pasos de la metodología antes mencionada.

Sus principales conclusiones de este proyecto fue llegar a implementar una política de seguridad y llegar a crear conciencia en sus colaboradores para que conozcan y se identifiquen con lo implementado de manera que deberían estar preparados para actuar de forma inmediata ante cualquier peligrosidad que se presente con el sistema de información.

Carlos Riofrio (2014) en su tésis llamado “Plan de contingencia en seguridad de tecnologías de información, basándose en la ISO 27001 para la Municipalidad Distrital de Tambogrande” Universidad César Vallejo- Piura. Muestra como objetivo desarrollar un programa efectivo de SGSI que haga recordar que los procedimientos y políticas de seguridad son una dupla de documentos que llevan interrelación entre sí. Para sumar conocimientos al proyecto aplicar, esta unión de documentación son las que permiten a una organización cumplan con los requisitos de seguridad informática existentes, de este modo los tomo como buen aporte.

La entidad en mención al igual que la Municipalidad aplicó esquemas de seguridad que permitieron una mayor confianza en cuanto a la disposición de la información implementando un sistema de contingencia en este caso fue tomado un ciclo PDCA (Ciclo de Deming). Se extrajo un detalle desplegable de resultados que se tomarán como puntos de mejora para la aplicación de la metodología, los procesos de seguridad del hardware y redes afines cuentan con procedimientos repetitivos y sucesivos, puntos que se tomarán para ser mejorados en su gestión, por tanto, deberán de aplicar su plan de contingencia (Basado en ISO 27001) como el plan para mitigar riesgos, situación de la entidad y un plan de respaldo de información, adquiriendo una sumas de herramientas tecnológicas que nos garanticen una mejora en sus procesos que conlleven a su vez a la mejora como empresa.

Karina del Rocío Gaona (2013) en su tesis llamada “Aplicación de la metodología de Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera en Industrial Bravito S.A en la ciudad de Machala”. Ecuador-Machala. Menciona como objetivo satisfacer las necesidades de la organización para una mejor gestión y la correcta toma de decisiones de la empresa, su metodología empleada de Análisis y gestión de riesgos usando la herramienta P.I.L.A.R que la uso para tomar como soporte para el análisis de riesgos de sistemas de información, esta herramienta les sirvió de mucha ayuda ya que dio aportes a la valoración de los diferentes riesgos , con este software aplicado se obtuvo de manera directa muchos mecanismos de control y seguridad que se implementarán en dicha empresa pesquera.

Con esta aplicación de la metodología se rescata la identificación oportuna de nuevos riesgos ante los diferentes cambios en sus procesos internos la cual es un punto que se torna muy relevante para la aplicación del proyecto que se puso en marcha. Se concluye al igual que en el proyecto actual demostrado que usando la metodología Magerit será considerada como una herramienta clave para el éxito de cualquier entidad en especial los municipios que nos ayuda a minimizar los riesgos para ayudar a la entidad tomando en cuenta lo vulnerable que tienden a ser los activos en cada institución o entidad estatal.

Las teorías relacionadas a la investigación son:

Según Inteco (2012), un activo de seguridad de la información es la información en poder de una organización que necesita ser protegida de riesgos y amenazas para asegurar el buen funcionamiento de su negocio. Este tipo de información comercial básica se conoce como seguridad de la información. Su protección es el objetivo de cualquier sistema de gestión de seguridad de la información.

Considerando su clasificación, en el primer tipo se encuentran los servicios, por ejemplo, la gestión de nóminas de cesantes de una entidad. En el segundo grupo se consideran los datos e información que se maneja dentro de una organización o entidad. En algunos casos son considerados el núcleo del sistema, debiendo mencionar que el resto de activos suelen darle soporte de almacenamiento. El tercer tipo está incluyendo aplicaciones de software. En el cuarto grupo están los

equipos informáticos y en el quinto grupo lo forma el personal a este activo se le considera de suma importancia. Incluye personal interno y personal que pertenece a terceros. En el sexto lugar están las redes de comunicaciones que dan soporte a la organización para completar el sétimo grupo se encuentran los soportes de información. Los soportes físicos que permiten el almacenamiento de la información durante un período dilatado de tiempo.

En el octavo grupo está el equipamiento auxiliar el cual da soporte a los sistemas de información de cualquier entidad. Por ejemplo, triturador de papeles, aires acondicionados entre otros. Y por último se encuentra el grupo de las instalaciones en donde se albergan todos los S.I. como oficinas, camionetas, edificio Junto a estos activos hay que tener en cuenta aquellos intangibles como la imagen de una organización, en resumen cada activo de información se debe tener en cuenta que estos pueden derivar de distintas fuentes y que se pueden localizar en distintos soportes, también se debe mencionar que para cada activo de información hay un ciclo de vida con respecto a la información que contengan , dado que lo que hoy en día puede tener cierto grado de criticidad para una empresa, sin embargo estos pueden dejar de tener importancia con el tiempo.

Según Álvaro Soldano (2008), el riesgo es la probabilidad de que un peligro se convierta en un desastre". Las vulnerabilidades o amenazas no son solo factores de riesgo. Pero cuando se unen, se convierten en riesgos, en posibilidad de desastre.

Entonces podemos decir que todas las organizaciones deben proteger sus activos de los riesgos a los cuales se someten para asegurar el correcto funcionamiento de sus actividades.

Por otra parte, el objetivo del análisis de riesgos es la evaluación y priorización del riesgo en base a la información de los mapas creados en la fase de identificación para clasificar los riesgos y proporcionar información para determinar el nivel de riesgo y las acciones a tomar. (ISMS,2006)

Se establecieron dos aspectos para realizar el análisis de riesgos:

Aspecto probabilístico: Que consiste en la probabilidad de que ocurra un riesgo; puede medirse por criterios de frecuencia o teniendo en cuenta las presencias internas y externas que pueden causar el riesgo incluso si nunca ocurre.

Para el análisis cualitativo, se creará una escala de medición cualitativa usando algunas categorías y una descripción de cada categoría para que cada empleado pueda usar:

- Alta: Muy probable que el hecho se presente.
- Media: Probable que el hecho se presente.
- Baja: Poco probable que el hecho se presente.

El análisis de riesgos aplicado a una organización tiende a ser de gran importancia para llevar en buena pro el desarrollo de los negocios de una organización, puesto que una vez que se identifiquen las amenazas y vulnerabilidades a las cuales está expuesta se deben tomar medidas a fin que un riesgo con alto nivel de criticidad se materialice, debiendo mencionar que todos los trabajadores de la organización deben estar involucrados en este proceso.

La evaluación de riesgos según FAO/OMS (1995) es una evaluación científica de los efectos nocivos conocidos o potencialmente dañinos de la exposición humana a los riesgos derivados de los alimentos. El proceso incluye las siguientes fases: identificación del riesgo, caracterización del riesgo, evaluación de la exposición y caracterización del riesgo.

La evaluación de riesgos implica más que simplemente calcular la probabilidad de que suceda algo malo.

Aquí la evaluación de riesgos es considerada el periodo en donde los instrumentos se aplicarán más intensamente, en este periodo se podrá reconocer aquellas amenazas que tiendan a materializarse, provocando consigo resultados negativos y por ende deben ser tratados con prioridad. Lo fundamental durante la evaluación de Riesgos es la aplicación de los criterios a realizar propios de cada entidad a ello se suma una correcta valoración hacia cada riesgo de algún activo, y como es el paso a seguir se consideran los controles para su tratamiento correspondiente.

Según la Inteco (2012) manifiesta que las Una amenaza es un evento que puede causar un daño material o inmaterial. Se dividen de la siguiente manera.

- Amenaza natural: Se origina en la dinámica de la tierra y se encuentra en siempre en transformación.

- Amenaza socio-cultural: Se da mediante fenómenos de naturaleza, pero de acuerdo al actuar de las personas al intervenir en la ocurrencia o intensidad.
- Amenaza antrópica: Se da con el accionar humano encima de los componentes de la naturaleza (aire, agua, tierra). Es muy grave, ya que afecta a la calidad de vida y a la integridad tipo física.

La vulnerabilidad, según Inteco (2012) dice que es una debilidad en un activo o grupo de activos que puede ser explotada por una amenaza.

Para tener una idea clara del significado de vulnerabilidad es una característica particular que tiene un activo y va a significar un riesgo para la seguridad de la información de una organización, por ejemplo: si tenemos las pc sin contraseñas y que la red interna de una empresa no se encuentre protegida ante cualquier ente extraño este puede ser “aprovechado” por los famosos malware.

El concepto de salvaguardas, según Inteco (2012) menciona que las salvaguardas son las prácticas, procedimientos o mecanismos que reducen el riesgo. Estas pueden actuar disminuyendo el impacto o la probabilidad.

En este caso cabe mencionar que las salvaguardas se crean para eliminar las amenazas o llegar a reducirlas a un nivel aceptable

El riesgo residual, según INTECO (2012) es aquel riesgo que queda tras la aplicación de salvaguardas. Es aquel riesgo que subsiste, después de haber implementado controles. Por muy bien que protejamos nuestros activos es imposible eliminar los riesgos al 100%, por lo que siempre quedará un riesgo residual en el sistema que la organización deberá asumir y vigilar.

Es importante tener en cuenta que el nivel de riesgo al que está expuesta una empresa nunca puede eliminarse por completo. Por lo tanto, se debe lograr un

equilibrio entre el nivel de recursos y mecanismos que se deben asignar para minimizar o reducir estos riesgos y el nivel de confianza (nivel de riesgo tolerable) que se puede considerar suficiente. El riesgo residual se puede considerar como la diferencia entre una empresa y la seguridad absoluta.

La confidencialidad es una “propiedad que impide la propagación de la información a usuarios o sistemas no autorizados. A groso modo, aseguran el acceso a la información única y exclusivamente a aquellas personas que cuenten con la debida autorización”. (ISO/IEC 27002,2012).

La integridad es un componente del sistema, la información o los sistemas de información que no han sido modificados o destruidos de forma autorizada (NICCS,2015).

El objetivo principal es mantener los datos libres de modificaciones no autorizadas por usuarios no autorizados. A grandes rasgos, la integridad es el conservar con precisión la información tal cual fue creada, sin ser alterada por usuarios o procesos no autorizados. (ISO/IEC 27002,2015).

La disponibilidad es: “La propiedad que pueda ser asequible y utilizable cuando se lo demande”. (NICCS ,2015).

En resumen, consideramos que es una de las características o situación en que la información debe de encontrarse a disposición de las personas o sistemas que pueden acceder a ella. Por tanto, la disponibilidad la consideramos como un acceso hacia la información y a los sistemas por entes autorizados en el momento que se consideren oportunos. (ISO,2015).

La metodología Magerit, según ISO 27001(2012) es una metodología de análisis de riesgos de carácter público elaborada por el consejo superior de Administración Electrónica. Esto está directamente relacionado con el uso generalizado de las tecnologías de la información y trae claros beneficios para los usuarios, pero también presenta ciertos riesgos que deben mitigarse con medidas de seguridad que generen confianza.

Es de interés para cualquier persona que utilice información digital y sistemas informáticos para procesarla. Si esa información o los servicios que brinda son valiosos, Magerit les dirá cuánto valor está en juego y los ayudará a protegerlos. Para gestionarlos, es importante comprender los riesgos de los elementos de trabajo.

Magerit tiene la finalidad de saber cuánto valor está en juego y esta metodología ayudará a adoptar medidas para salvaguardarlo, a su vez, va a proponer una contigüidad sistemática que no dejará lugar a espontaneidad.

La ISO / IEC 27005: 2008 es la normativa que proporciona directrices para gestionar los riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en ISO/IEC 27001 y está diseñado para ayudar a implementar con éxito la seguridad de la información basada en un enfoque de gestión de riesgos.

Esta normativa tiene como aporte el no tener dudas sobre los elementos para una buena gestión de riesgos, por lo que percibido desde ese punto de vista esta ISO ha nacido claramente para apoyar la tarea del análisis de riesgo.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

El diseño de esta indagación se encontró dentro del parámetro de una investigación cualitativa - descriptiva.

3.2. Variables y operacionalización

Solo hubo una única variable que se consideró y fue el análisis de riesgos a los activos de información. Acerca de la matriz de operacionalización de esta única variable se dispuso en Anexos.

3.3. Población, muestra y muestreo

Se ha considerado una población que fue representada por los colaboradores que laboran dentro del área de Administración y Finanzas y se encuentran dentro de la municipalidad de San Martin y se enfocó específicamente a los jefes de área o jefes encargados, debido a que ellos eran las responsables de cada uno de los departamentos o áreas las cuales fueron evaluadas.

Se menciona a continuación a los jefes encargados del área previamente dicho, el cual fue la población y muestra a la vez y se ha reflejado en la ulterior tabla:

Tabla 1. Población y muestra

Municipalidad Provincial de San Martín	**Personal de Adm. y Fin.**
Responsable de Sistema Administrativo	1
Asistentes administrativos	2
Especialista Administrativo I	2
TOTAL	**5**

Fuente: Información brindada por el Municipio provincial de San Martín.

3.4. Técnicas e instrumentos de recolección de datos

A fin de recolectar los datos, se ha usado la técnica observación con el instrumento cuestionario correspondiente:

- El cuestionario: Es una herramienta en forma de materiales impresos o digitales utilizados para registrar información de personas que participan en investigaciones, entrevistas u otros procedimientos como experimentos (Hechavarría Toledo, 2012). Al analizar las preguntas realizadas a los trabajadores de un área importante como Administración y Finanzas, fue posible probar y verificar si el proyecto cumplió o no con las metas y objetivos previamente definidas.
- La observación: La observación es una técnica natural para obtener información, incluyendo observar, escudriñar, registrar y analizar los aspectos que consideraremos más adelante (Serrano 2019). A través de la observación, fue posible obtener la máxima cantidad de datos que aportaron selectivamente a este proyecto, para que puedan ser registrados y luego analizados.

3.5. Procedimientos

Se solicitó una reunión con las autoridades pertinentes que participaron en la investigación. Una vez aceptada la reunión, se realizó y se explicó en qué consistía el estudio. Cuando ellos aceptaron la aplicación de ésta en la municipalidad, se hizo una pequeña entrevista para obtener más información sobre la problemática y luego se elaboró un cronograma de acuerdo a los tiempos de los trabajadores y de la investigadora, para el uso de los instrumentos de la investigación. Llegó el día de aplicar cada instrumento y se recolectó los datos. Después se analizaron los datos recolectados y, por último, se dio a conocer a través de la investigación por escrito. Los documentos que detallan la autorización y más, fueron colocadas en anexos.

3.6. Método de análisis de datos

El procesamiento de todos los datos se realizó en virtud de métodos estadísticos que salieron de las encuestas hechas y fichas de recolección y sirvió para realizar un análisis descriptivo mostrando las respuestas de cada una de las variables estadísticas.

3.7. Aspectos éticos

El proyecto fue aplicado en la Municipalidad Provincial de San Martín, en Tarapoto, entidad que se caracteriza por brindar servicios públicos de calidad y con esto promueve a los actos de desarrollar en lo económico y lo social en la población. Para este dicho estuvo guiado y aceptado por la jefa encargada Ing. Annie Chong Bartra quien dio la aprobación para llevar a cabo la propuesta que les ha de permitir atenuar cada riesgo de específica índole sobre todos, absolutamente todos los activos de la información del municipio especialmente al área el cual se llevó a cabo la propuesta que es el área de Administración y Finanzas, se da a conocer que la información que se está brindando es de carácter confidencial ya que son datos que día a día se utilizan en sus labores de rutina y que consideran de mucha importancia.

IV. RESULTADOS

La interpretación de los resultados fueron los siguientes:

En la evaluación de resultados predominan los puntos no favorables que indisponen el desempeño global de la municipalidad.

Seguidamente, se han gestionado activos en base a los críticos riesgos posteriores:

El internet, que ha sido parte de la capa llamada Servicios, la mayor amenaza fue el no previsto uso y abuso de privilegios que afecta su Integridad con un valor de 6 y afectando su confidencialidad con un valor de 6 que, si ésta se hiciera realidad, las tareas diarias no se realizarían, en particular, enviar correos corporativos, gestionar el sitio web del municipio, incluso otras.

Los antivirus, quienes se acogieron en la capa llamada Aplicaciones, se adquirieron estos resultados: considerando que una amenaza fue difundir nocivo software que ha de perjudicar a los niveles medio de riesgo como son integridad con un valor de 5 y confidencialidad con un valor de 5, debiendo mencionar que una de las principales razones fue cuando hacen uso de los dispositivos externos como USB, memorias, disco duro en muchas de las ocasiones no los hicieron un respectivo análisis mediante el antivirus, induciendo de esta manera el acto de propagar virus, gusanos, troyanos, etc.

El servidor, que contiene la Base de Datos de la Municipalidad, perteneció a una capa llamada de Equipos. Se encontraron ciertas amenazas que obtuvieron el nivel de etiqueta alto riesgo en relación de manipulación del físico, alias hardware, que ha afectado a la confidencialidad con un valor promedio de 9. Esa amenaza se ha presentado latente debido a que no hay un apropiado sitio en el que ingrese solo el recurso humano idóneo y autorizado de la municipalidad, y esta condición ha dado cabida a la posibilidad de que algún trabajador realice un uso malo de esta herramienta física, y quede insegura enteramente. Si la precedente amenaza logra materializarse, puede originar daños muy significativos en esta municipalidad, en vista de que en ella se ha almacenado gran parte de la información que se considere de gran importancia, por tanto, esta evaluada como de alta peligrosidad.

Para las Pc´s de escritorio y las Laptops, estos dos activos pertenecen a la capa de equipos y una vez que se hallaron sus amenazas se consideraron dentro del nivel rojo, alto riesgo, principalmente a causa de la utilización no prevista que ha afectado máxime a la disponibilidad e integridad, arrojando un valor de 8, esta evaluación se planteó tomando en cuenta el factor clima ya que las lloviznas constantes y la humedad que se genera después de cada evento climático hizo que muchas veces las computadoras se vean afectadas. Otra evaluación se tomó en cuenta para el abuso de privilegios de acceso con un valor de 8 en su confidencialidad. La mencionada amenaza era bastante usual puesto que una cantidad de empleados instalaban programas no relacionadas con las actividades diarias y eran de intereses propios, entre ellos los programas de uso personal o para almacenar información personal y juegos. Esto conllevó a la presencia de situaciones de retraso en relación a las actividades personales en consonancia al puesto laboral al cual ha sido asignado.

El cableado, se debe indicar que este activo se encuentra dentro de equipos auxiliares. Una vez encontradas las amenazas como la conocida contaminación medioambiental, poseyó el nivel, rojo para varios, y conocido como de riesgo alto, evaluando así en el aspecto de la disponibilidad con un valor de 6. Esta susodicha amenaza se ha originado por una mala instalación en relación al cableado con los equipos intercomunicados, exponiéndose a físicos estropicios, partículas como el polvo y al desaseo acumulado de manera diaria.

A su vez se debe mencionar que la Gerencia manifestó en su reporte que el estado del cableado no es la adecuada en su totalidad, dio a conocer que los pasadizos del área de RRHH el cableado en gran parte se encuentra algo deteriorado y algo desorganizado por el espacio que es muy reducido, por ejemplo el cableado de red de la Gerencia principal no se encuentra certificado por RETIE(Reglamento Técnico de Instalaciones Eléctricas), siguiendo con la parte evaluada con respecto al cableado lo que compromete la parte de seguridad y ambiental en los tres servidores y cableado en general quienes no cuentan con sistemas de prevención de riesgos contra incendios, no se halla una ventilación apropiada , en este caso se manifestó que el tema del aire acondicionado es muy poco probable su pronta

instalación ya que como se dio de manifiesto dentro de las restricciones es que no cuentan con parte del presupuesto.

Edificio es el activo que pertenece a la capa de Instalaciones y mantiene la implícita amenaza nombrada como ocupación adversaria, que permite afectar a la sólida confidencialidad, dándole un valor de 6 indicando que se encuentra en un lugar poco seguro, la razón es que se encuentra frente a un mercadillo que de noche tiende a ser algo inseguro. Adicional a ello se encuentra solo un personal de seguridad que permite el ingreso a personas autorizadas pero su vez tiende a ser vulnerable ante ciertos eventos inesperados (robos).

Licencia de Microsoft Windows 2008 concierne una famosa capa: a la de aplicaciones. Cuando se hallaron las implicadas amenazas se consideró como alto riesgo en su disponibilidad con un valor de 6 que se considera un riesgo alto, pues tiene una amenaza que se refiere a los errores en la actualización de software, se utilizan cuentas con licencia, lo que se pudo hallar como parte de una de sus vulnerabilidades no se tiene un revisión y controles para la instalación de algún software ilegal que permite que algún colaborador de la municipalidad pueda instalar algún software que se considere dañino sin la autorización del personal del área de soporte (Sistemas).También con el análisis realizado no existen procedimientos cuando se da de baja algún equipo o cuando se retira por inoperatividad o fallas en su S.O (sistema operativo).

Para la evaluación de la red que es la Intranet se puede considerar que si cuentan con ciertas reglas que definen parte de la protección de acceso desde su red externa como es el internet esto se da con el direccionamiento del área local, se puede obtener acceso por puertos a muchas redes que se consideren de acceso restringido, que es considerado una fuente de riesgo que se encuentra siempre presente.

Para el tema de personal el cual se considera todos los administrativos una vez hallado sus amenazas como suplantación del personal, se le dio un valor a cada indicador bajo con un valor de 1 para su disponibilidad, integridad y Confidencialidad. Eso significa que es muy poco probable que un personal ingrese a sus instalaciones suplantando su identidad.

Cabe resaltar, que la municipalidad cuenta con el personal para el mantenimiento del hardware tanto preventivo como correctivo en los diferentes equipos de la municipalidad, sin embargo, se debe mencionar que no cuenta con el personal suficiente para mantener tres de las oficinas es por ello que llegan a realizar con retardo por el tema de falta de contratación de personal por un tema de presupuesto. No cuentan con procedimientos o lineamientos definidos para realizar los mantenimientos a cada equipo a nivel técnico, es decir, cada personal del área técnica de soporte procede según los problemas que se presenten debiendo mencionar que la solución al problema puede ser exitosa en el momento, pero no se demuestra que sería una alternativa efectiva, por lo tanto, se deben de establecer controles de tipo técnico.

Debilidades o vulnerabilidades ligadas a cada activo presente de la información tienen la siguiente clasificación según su análisis de riesgos que se demuestran en el gráfico.1

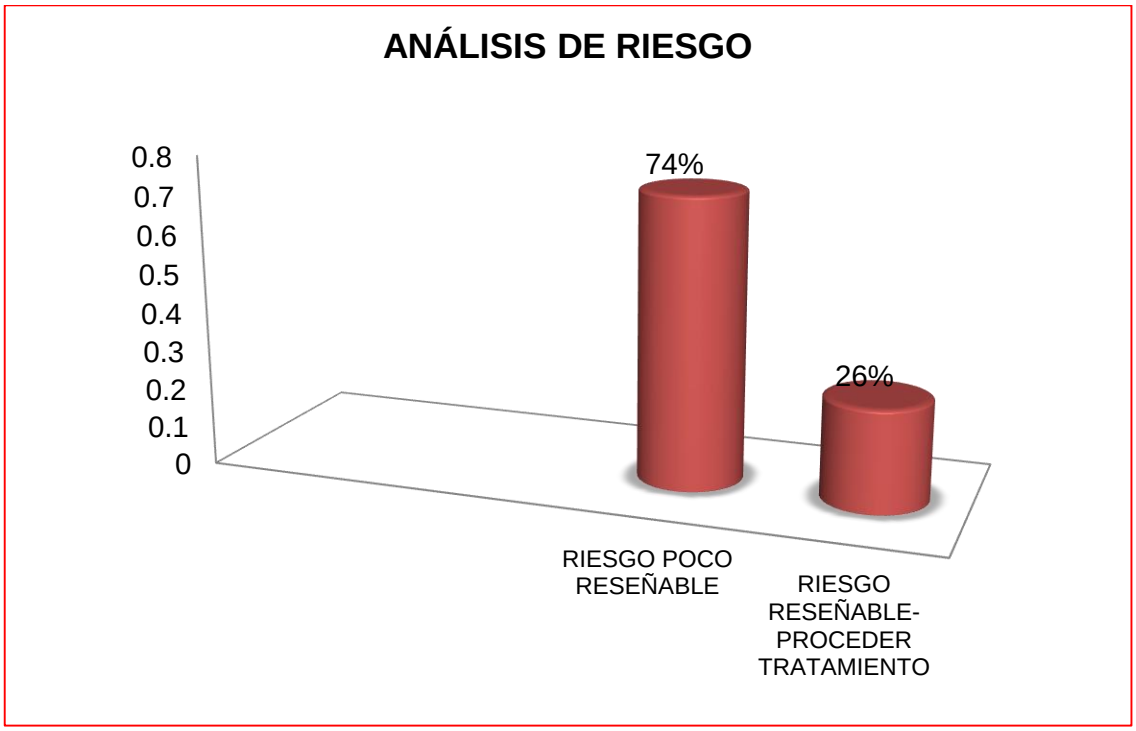


Gráfico 1. Análisis de riesgo

Fuente: Instrumento de investigación.

Como se puede observar el resultado del análisis de vulnerabilidades centrándonos en dos criterios cuando los valores arrojados demuestran que son menores igual a cuatro(<=4) entonces los riesgos son poco reseñables y cuando los riesgos son mayores a cuatro(>4) se considera riesgo reseñable por tal motivo se debe proceder a un tratamiento, esto considerando que en su mayora el resultado que arrojo en la tabla de riesgo fue un valor de 4 pero no podemos dejarlo de mencionar ya que también los consideré para como punto de mejora. Después de haber realizado este análisis quedan a la vista los riesgos y vulnerabilidades a las cuales está expuesto la gerencia evaluada, se hizo una clasificación de cada riesgo significativo determinando en su mayoría tomar una debida atención considerada de urgencia con el 26% y poder tomar una medida preventiva, la mayoría de datos se centró en la amenaza de hurto, corrupción y destrucción de la información debido a que las vulnerabilidades halladas se agrupan en que al no existir una política por ejemplo en el traspaso de información, en la poca fiabilidad con el uso de las claves, en resumen no existen controles de seguridad para determinar si existen vulnerabilidades y así poder acceder a la información sin que ésta se vea afectada.

El otro grupo de activos analizados que resulta ser un 74% no tiene la urgencia de ser evaluados sin embargo, no debemos desmerecer que si se llega a descuidar podría subir el puntaje por riesgo encontrado ya que si bien es cierto todos estos activos que se encuentran en este grupo el resultado que arrojó fue en su mayoría el número 4, resultado vertido por la probabilidad y el impacto que tienen dentro del área investigada , esto hace pensar a todo el personal en especial a las Jefaturas que deben estar alertas pues este análisis refleja que hay muchas cosas que mejorar y que esto no se convierta en una bomba de tiempo.

Muchos de los activos presentan un 65% del total de vulnerabilidades y amenazas reconocidas como por ejemplo lo de alteración y corrupción de la información que se ve reflejada en la mayoría de los activos analizados, esto significa que dentro de los controles que se van a proponer implementar estaría considera mencionar este punto que se muestra de forma muy repetitivo.

Otro de los medios que nos ayudó con el análisis fue la implementación de una Guía de Observación, se muestra por tipología de activos, en ella se detalla a cada

responsable y esto ayudó a que el análisis fuera más detallado ya que fue centrado y la información validada por cada colaborador encargado y el activo asignado que a su vez se encuentra inventariado dentro de la Gerencia analizada en mención.

Por otra parte el cuestionario que se aplicó a los jefes y encargados de la Gerencia y sub áreas consideró un 80% que aún no se ha establecido para la atención de riesgos presentes en cada activo de información mientras que un 20% considero que si hay controles o mecanismos pero en la entrevista que hice al personal de soporte y sistemas comentaron que en la municipalidad aún no se han llegado a implementar medidas de este tipo o controles, todo lo hacen vía formal o la petición de algún cambio e ingreso de información lo hacen entre gerencias, sin embargo no se mide el nivel de peligrosidad que pueda existir en el traspaso de información de una gerencia a otra,

Otras de las preguntas evaluadas por el personal fue si es que la Gerencia informa periódicamente a cerca de los riesgos y toda vulnerabilidad las cuales ven afectados cada activo de la información, a lo cual respondió 60% que no tienen conocimiento , pues la importancia que le dan es solo de cumplir con las labores diarias de envíos y registros de información sin consideran la magnitud de riesgo a la cual se ven involucrados los activos que se ven comprometidos con las actividades diarias del personal de la municipalidad, un 40% de los colaboradores manifiestan lo contrario.

V. DISCUSIÓN

N°1: Valoración de Activos (Disponibilidad, Integridad, Confidencialidad).

Como parte de la evaluación del análisis de riesgos se elaboró un cuadro siguiendo los lineamientos de la metodología de Magerit con la finalidad de darle una valoración a las amenazas halladas dentro de la municipalidad.

Con la Implementación de este cuadro se gestiona de manera eficiente y ordenada la clasificación de cada activo por amenaza agregándole un valor con una calificación de 9 al valor más alto(criticidad) y 0 al valor muy bajo.

En el Anexo: Instrumentos firmados - A, se puede visualizar el detalle de activos que se tomaron como parte de los más importantes que tienden a ser más vulnerables para el área de administración y Finanzas, se tomó un formato adaptado de la metodología de Magerit- Análisis y Riesgos.

Mediante esta adaptación de la metodología empleada se pudo saber los puntos subsecuentes: cuánto vale y de qué manera están protegidos los activos haciendo sobre ellos una evaluación de forma metódica para lograr conseguir conclusiones con fundamento. Por ejemplo, se pudo identificar que los valores considerados como Muy Altos (MA) lo tuvieron los servidores y las PC las cuales proyectaron valores con alto número de criticidad. Ver Anexos: Instrumentos.

N°2 y 3: Tipos de Activos/Vulnerabilidades presente en activos:

Por cada activo identificado se dejó registrado en un inventario de activos (Ver Anexos Tipos de Activos), indicando sus vulnerabilidades y amenazas. Ahora con este análisis se puede mencionar que existen tantas vulnerabilidades como amenazas asignado a cada activo, que pudieron ser conocidos por todos los colaboradores del área de Adm&Fin. Con la información extraída por los responsables de cada activo asignado se pudo comprobar que tenían mucha desinformación con respecto a sus riesgos y gracias a ello se pudo completar el cuadro que sirvió de mucho para la realización de esta investigación. Ahora se puede comprobar que después del análisis hecho se tiene un detalle de los activos pudiendo identificar cuál es su amenaza directa y sus vulnerabilidades asociadas. (Ver anexos).

N°4 - 5 - 6 Amenazas, Vulnerabilidades, Grado de exposición de un activo frente a la amenaza. (Probabilidad/ Impacto/ Riesgo).

En el Anexo Análisis de Riesgo/Interpretación, una vez hecha la tabla para estimar las perístasis acerca de probabilidad e impacto por cada riesgo y amenazas asignado a cada activo vigente se puede apreciar mediante el análisis hecho, el porcentaje o porcentajes resultantes de los criterios de valoración y como se muestra en la gráfica hay un resultado del 26% considerando riesgos con alto valor de exposición frente a una amenaza, seguido del 52% de un valor que permitió saber que hay riesgos de tipo medio y que no por eso se deben hacer a un lado sino también tomarle una importancia, se culmina con un porcentaje del 22% de riesgos bajos . Se considera como parte de las medidas a tomar integrar una herramienta para ejecutar copias de la información que se considere crítica y la implementación de un sistema de gestión documental. Ver Anexos.

N°7 y 8 Vulnerabilidades verificadas / Riesgos Críticos Identificados:

En el Anexo se puede apreciar mediante la gráfica las amenazas que pueden afectar al conjunto de activos vigentes dentro de la municipalidad, con la adaptación de la metodología Magerit como parte de la evaluación de riesgos se empleó un detalle que demostró con valores del 26% dentro de la bolsa de Riesgo reseñable – Con tratamiento, los riesgos considerados como críticos y un total de 74% de los activos que según resultado se consideran poco reseñable.

VI. CONCLUSIONES

Una vez concluido el estudio se lograron identificar todos activos de información, en el área evaluada consideró de mayor criticidad, identificando a sus actividades que comprometían a cada uno de ellos, a esta acción se sumaron los planes de acción que fueron tomados como acciones preventivas y correctivas contra los riesgos que fueran hallados a futuro.

Se lograron evaluar las vulnerabilidades y amenazas se pudo determinar un grado, el de la susceptibilidad a los daños de todos los componentes vulnerados, el único propósito fue disminuir brechas para que puedan reducir los riesgos que se presenten a futuro. Es necesario mencionar que esta evaluación debe ser auditada por terceros para poder medir sus niveles de vulnerabilidad al fin de mitigar los riesgos al máximo.

Se logró medir los riesgos, logrando un promedio del 26% de ocurrencia de las amenazas existentes, con esto se pudo identificar a los activos más críticos para la municipalidad y poder mantener consigo una visión más amplia de los riesgos que pueden afectar de forma peligrosa los activos que comprometan los servicios y procesos internos de la municipalidad, en especial los de un área bastante crucial, como lo es Administración y Finanzas.

Para concluir, se plantean controles y salvaguardas las cuales ayudaron a contribuir la reducción del impacto para cada amenaza, llevándolo a un nivel aceptable a los activos que se encontraron dentro de la MPSM.

VII. RECOMENDACIONES

- Una vez culminado la realización del análisis acerca de los riesgos sobre el tema de los activos de la información, se propone una investigación enfocada en la implementación relacionado a un sistema con respecto a la Seguridad de la Información, el cual debe permitir una protección al activo más valioso como es la información y los procesos que dentro de ella se manejan. Una vez culminado el proceso, si la municipalidad lo decide, tiene la opción de certificar su SGSI según la normativa ISO 27001, y se propone esta opción ya que hoy en día lo ampara la Norma Técnica Peruana, NTP ISO/IEC 27001:2014 Tecnología de la Información, Técnicas de seguridad, Sistemas de gestión de seguridad de la Información («Aprueban el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001», 2016) y esto para mejorar el desempeño total de una municipalidad y con ello establecer procedimientos que conlleven a una mejora continua en sus actividades diarias.

- Se sugiere evaluar e implementar políticas de seguridad, a su vez efectuar auditorias permanentes con cada activo de la información existente a fin de lograr restablecer todo posible control y de esta manera poder aportar con el desarrollo de mejores prácticas relacionadas con el análisis y gestión de riesgos.

- Después e inmediatamente implementada la política referida a la seguridad, es fuertemente sustancial que sea auditado y mejorado periódicamente con el único fin de incrementar la seguridad sobre los activos presentes dentro de la MPSM.

REFERENCIAS

- 27000, ISO. 1996. Guías para la Gestión de la Seguridad de TI/TECTR133351. 1996.

- García, Abdel. 2004. ABC de la Gestión de Riesgos. s.l.: Humboldt, 2004. 2004. ABC de la Gestión de Riesgos. s.l.: HUMBOLDT, 2004.

- Garcia, Riofrio. 2014. Plan de contingencia en seguridad de tecnologías de información, basándose en la ISO 27001 para la Municipalidad Distrital de Tambogrande. Piura-Perú: 2014.

- López, Francisco, Amutio, Miguel y Candau, Javier. 2006. Magerit Versión 2-Metodologia de Análisis y Gestión de Riesgos de los Sistemas de Información I, II y III. España: s.n., 2006.

- Maskrey, Andrew. 1998. Navegando entre Brumas-Aplicación de los Sistemas de Información Geográfica al Análisis de Riesgo en América Latina. Lima: La Red, 1998.

- Piers, Blaikie. 1996. Entorno político y económico de los desastres. VULNERABILIDAD. s.l.: La Red, 1996.

- Porras, C. 2012. Diseño e implementación de un sistema de gestión de seguridad de la información en procesos Tecnológicos. Lima-Perú: 2012.
- Ruiz, Hernando. 2008. Resolución 160-005326 Políticas de Seguridad de la Información. 2008.

- Suarez, Sandra. 2015. Análisis y Diseño de un Sistema de Gestión de Segurida informática en la empresa aseguradora Suarez Padilla& CIA LTDA que brinde una adecuada protección en seguridad informática en la infraestructura tecnológica de la organización. Colombia-Bogotá: 2015. (Ruiz, 2014)

- Ruiz, John Perafán. 2014. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del CAUCA. Colombia: 2014.

- Gaona, Karina del Rocio. 2013. Aplicación de la Metodología de Magerit para el Análisis y Gestión de Riesgos de la Seguridad de la Información aplicado a la empresa pesquera Industrial Bravito S.A. Machala-Ecuador: s.n. 2013.

- HECHAVARRÍA TOLEDO, S., 2012. Diferencias entre Cuestionario y Encuesta. | UVS Fajardo. [en línea]. Disponible en: http://uvsfajardo.sld.cu/diferencias-entre-cuestionario-y-encuesta.

- RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM. [en línea], 2016. 8 enero 2016. Disponible en: http://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/.

- SERRANO, V., 2019. TÉCNICAS E INSTRUMENTOS DE OBSERVACIÓN. *TÉCNICAS E INSTRUMENTOS DE OBSERVACIÓN* [en línea]. Disponible en: https://psicosociosanitario.blogspot.com/2019/01/tecnicas-e-instrumentos-de-observacion.html.

ANEXOS

Anexo: Matriz de operacionalización de variables

VARIABLE DE ESTUDIO	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escala de medición
Análisis de Riesgos a los activos de Información	Es un proceso que comprende la identificación de los activos de información, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar controles adecuados y disminuir la ocurrencia del mismo. ISO/IEC Guide 73:2002	Esta variable será medida: Cuestionarios, Guías de Observación, Tablas	Activos de Información	Valoración de Activos (Disponibilidad, Integridad, Confidencialidad). Tipos de Activos	Ordinal
			Vulnerabilidades y Amenazas	Amenazas presentes en activos	Ordinal
				Vulnerabilidades presentes en activos	
				Grado de exposición de un activo frente a la amenaza. (Probabilidad/ Impacto/ Riesgo).	
			Controles o Salvaguardas	Nro. Vulnerabilidades verificadas	Ordinal
				Nro. De Riesgos Críticos Identificados	

Anexo: Instrumento de recolección de datos

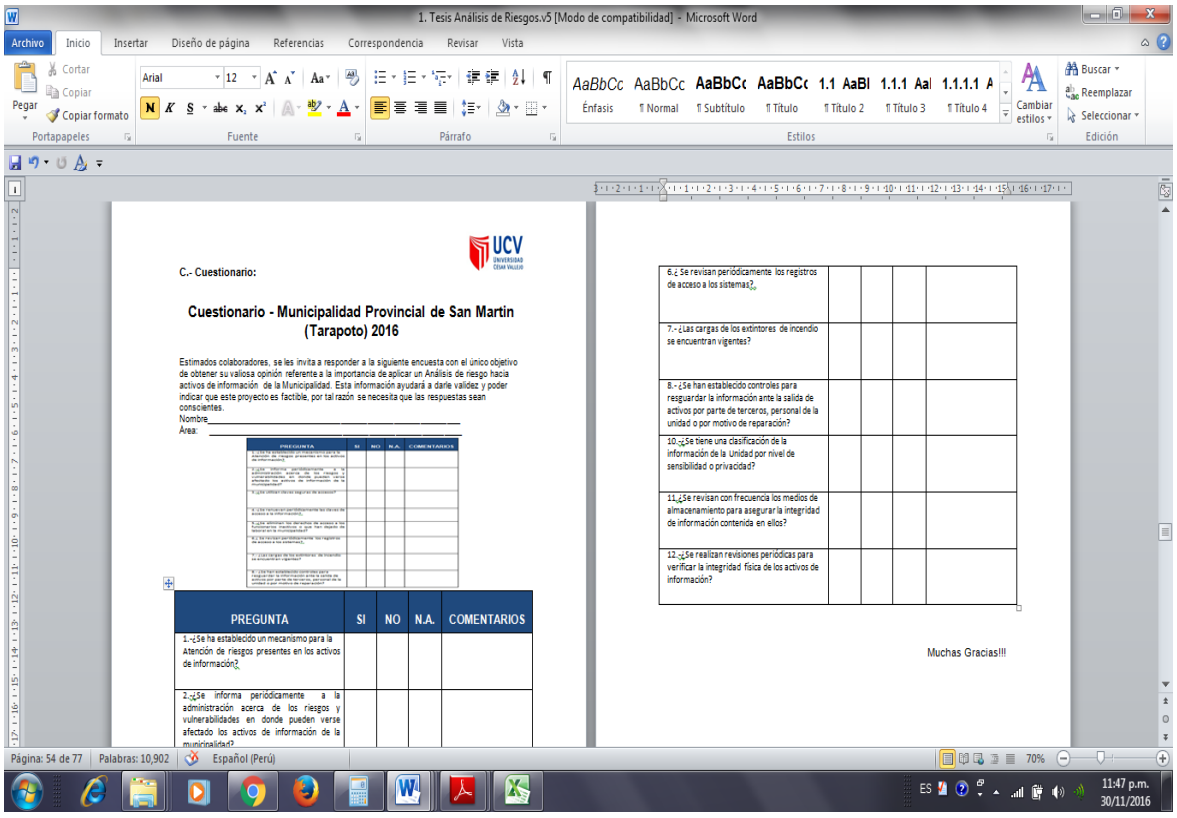
Cuestionario - Municipalidad Provincial de San Martin (Tarapoto) 2016

Estimados colaboradores, se les invita a responder a la siguiente encuesta con el único objetivo de obtener su valiosa opinión referente a la importancia de aplicar un Análisis de riesgo hacia activos de información de la Municipalidad. Esta información ayudará a darle validez y poder indicar que este proyecto es factible, por tal razón se necesita que las respuestas sean conscientes.

Nombre_____

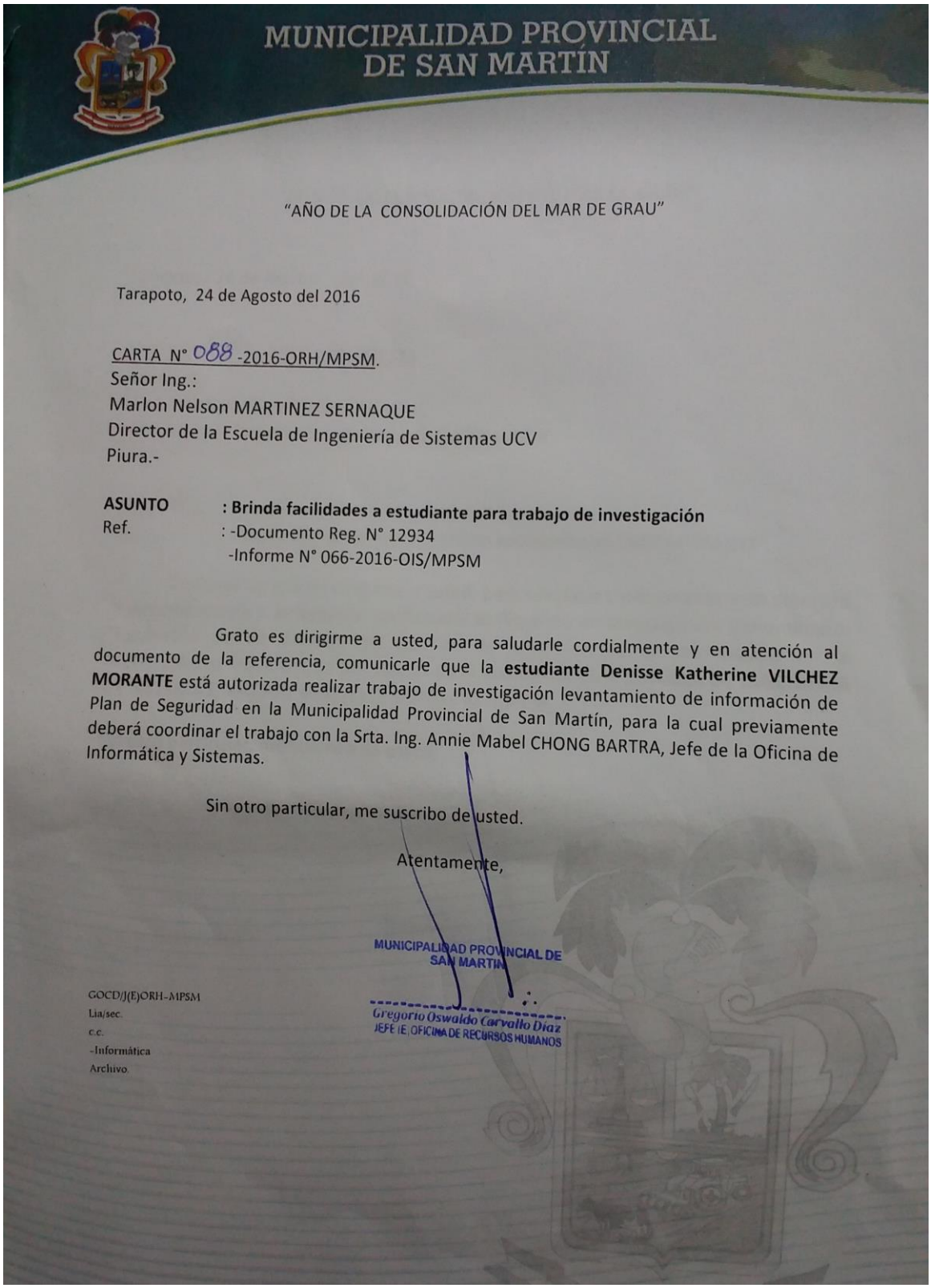
Área: _____

PREGUNTA	SI	NO	N.A.	COMENTARIOS
1.-¿Se ha establecido un mecanismo para la Atención de riesgos presentes en los activos de información?				
2.-¿Se informa periódicamente a la administración acerca de los riesgos y vulnerabilidades en donde pueden verse afectado los activos de información de la municipalidad?				
3.-¿Se utilizan claves seguras de accesos?				
4.-¿Se renuevan periódicamente las claves de acceso a la información?				
5.-¿Se eliminan los derechos de acceso a los funcionarios inactivos o que han dejado de laboral en la municipalidad?				
6.¿ Se revisan periódicamente los registros de acceso a los sistemas?				
7.- ¿Las cargas de los extintores de incendio se encuentran vigentes?				
8.- ¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal de la unidad o por motivo de reparación?				


1. Tesis Análisis de Riesgos.v5 [Modo de compatibilidad] - Microsoft Word
Archivo
Inicio
Insertar
Diseño de página
Referencias
Correspondencia
Revisar
Vista
Pegar
Cortar
Copiar
Copiar formato
Portapapeles
Arial
12
Fuente
Párrafo
Énfasis
Normal
Subtítulo
Título
Título 2
Título 3
Título 4
Cambiar estilos
Estilos
Buscar
Reemplazar
Seleccionar
Edición
C.- Cuestionario:
Cuestionario - Municipalidad Provincial de San Martin (Tarapoto) 2016
Estimados colaboradores, se les invita a responder a la siguiente encuesta con el único objetivo de obtener su valiosa opinión referente a la importancia de aplicar un Análisis de riesgo hacia activos de información de la Municipalidad. Esta información ayudará a darle validez y poder indicar que este proyecto es factible, por tal razón se necesita que las respuestas sean conscientes.
Nombre
Area:
PREGUNTA
SI
NO
N.A.
COMENTARIOS
1.-¿Se ha establecido un mecanismo para la Atención de riesgos presentes en los activos de información?
2.-¿Se informa periódicamente a la administración acerca de los riesgos y vulnerabilidades en donde pueden verse afectado los activos de información de la municipalidad?
6.¿ Se revisan periódicamente los registros de acceso a los sistemas?
7.-¿Las cargas de los extintores de incendio se encuentran vigentes?
8.-¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal de la unidad o por motivo de reparación?
10.-¿Se tiene una clasificación de la información de la Unidad por nivel de sensibilidad o privacidad?
11.¿Se revisan con frecuencia los medios de almacenamiento para asegurar la integridad de información contenida en ellos?
12.-¿Se realizan revisiones periódicas para verificar la integridad física de los activos de información?
Muchas Gracias!!!
Página: 54 de 77
Palabras: 10,902
Español (Perú)
70%
ES
11:47 p.m.
30/11/2016

Anexo: Autorización de aplicación del instrumento y consentimiento informado

Carta de Aceptación y Carta de Conformidad de la Investigación



MUNICIPALIDAD PROVINCIAL
DE SAN MARTÍN

"AÑO DE LA CONSOLIDACIÓN DEL MAR DE GRAU"

Tarapoto, 24 de Agosto del 2016

CARTA N° 088 -2016-ORH/MPSM.
Señor Ing.:
Marlon Nelson MARTINEZ SERNAQUE
Director de la Escuela de Ingeniería de Sistemas UCV
Piura.-

ASUNTO : **Brinda facilidades a estudiante para trabajo de investigación**
Ref. : -Documento Reg. N° 12934
-Informe N° 066-2016-OIS/MPSM

Grato es dirigirme a usted, para saludarle cordialmente y en atención al documento de la referencia, comunicarle que la **estudiante Denisse Katherine VILCHEZ MORANTE** está autorizada realizar trabajo de investigación levantamiento de información de Plan de Seguridad en la Municipalidad Provincial de San Martín, para la cual previamente deberá coordinar el trabajo con la Srta. Ing. Annie Mabel CHONG BARTRA, Jefe de la Oficina de Informática y Sistemas.

Sin otro particular, me suscribo de usted.

Atentamente,

MUNICIPALIDAD PROVINCIAL DE SAN MARTIN
Gregorio Oswaldo Carvallo Diaz
JEFE (E) OFICINA DE RECURSOS HUMANOS

GOCD/J(E)ORH-MPSM
Lia/sec.
c.c.
-Informática
Archivo.

MUNICIPALIDAD PROVINCIAL DE SAN MARTÍN

"AÑO DE LA CONSOLIDACIÓN DEL MAR DE GRAU"

Tarapoto, 24 de Agosto del 2016

CARTA N°089 -2016-ORH/MPSM.
Señor Ing.:
Marlon Nelson MARTINEZ SERNAQUE
Director de la Escuela de Ingeniería de Sistemas UCV
Piura.-

ASUNTO : Confirmación de Proyecto de Investigación
Ref. : Carta de Presentación Denisse Kartherine VILCHEZ MORANTE

Tengo el agrado de dirigirme a usted, para saludarle cordialmente y en atención al documento de la referencia, confirmarle el Proyecto de Investigación denominado: "Aplicación de un Sistema de Gestión de seguridad de la información en la Municipalidad Provincial de San Martín de la estudiante de la **ESCUELA DE INGENIERIA DE SISTEMAS, VILCHEZ MORANTE Denisse Katherine.**

Sin otro particular, me suscrito de usted.

Atentamente,

MUNICIPALIDAD PROVINCIAL DE SAN MARTIN
Gregorio Oswaldo Carvallo Diaz
JEFE (E) OFICINA DE RECURSOS HUMANOS

GOCD/J(E)ORH-MPSM
Lia/sec.
c.c.
Archivo.

constancia de ejecucion de proyecto.pdf - Adobe Reader

Archivo Edición Ver Ventana Ayuda

1 / 1 60% Herramientas Comentario

MUNICIPALIDAD PROVINCIAL
DE SAN MARTIN

CONSTANCIA

La que suscribe, Jefa de la oficina de Informática y Sistemas de la Municipalidad Provincial de San Martín, Ing. Annie Mabel Chong Bartra.

CERTIFICA QUE:

DENISSE KATHERINE VILCHEZ MORANTE

Identificada con DNI Nº 42520247, ha elaborado el "Análisis de Riesgos a los activos de información aplicado a la Gerencia de Administración y Finanzas de la Municipalidad Provincial de San Martín – Tarapoto", desde el 01/09/2016 hasta el 15/11/2016, demostrando en todo momento puntualidad, responsabilidad, eficiencia y deseo de superación.

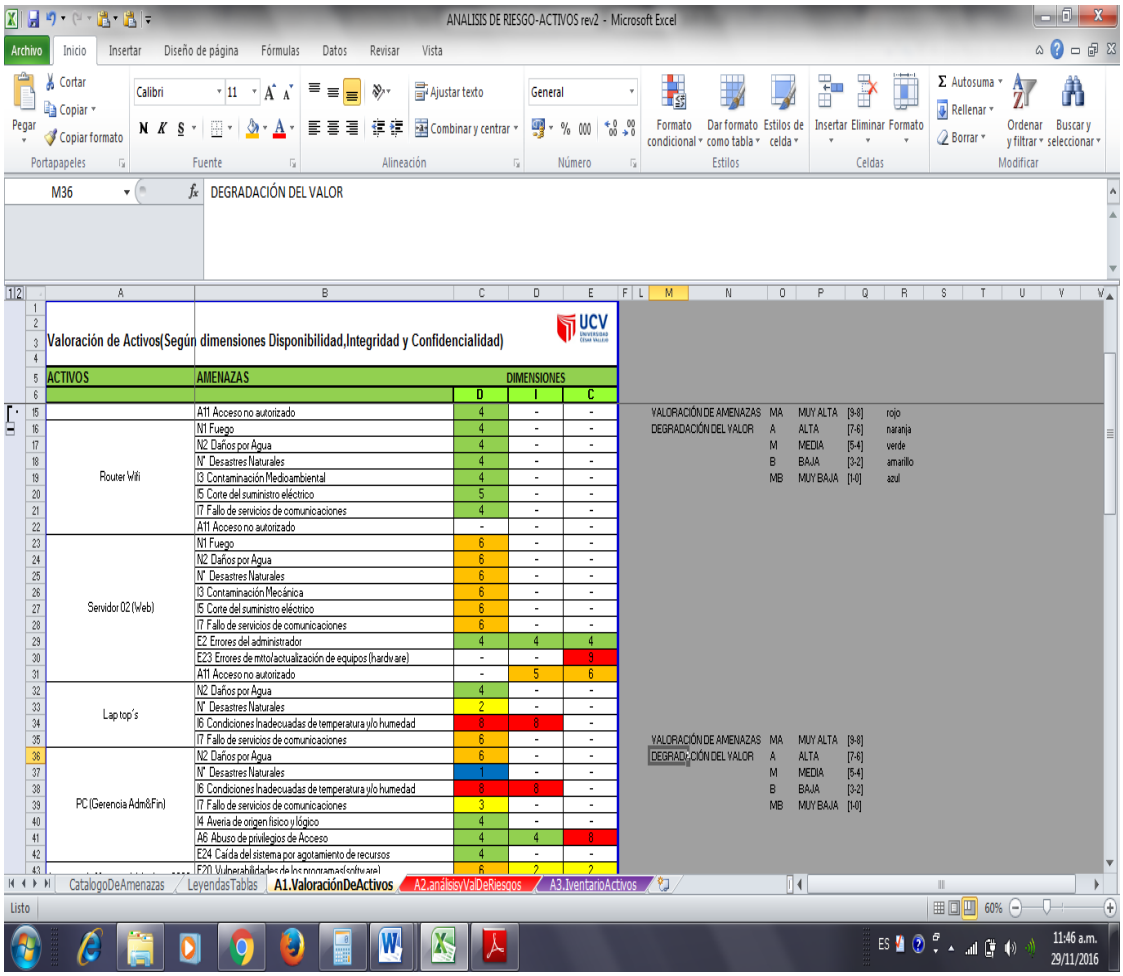
Se expide la presente constancia a solicitud de la interesada, para los fines que estime pertinente.

Tarapoto 29 de Noviembre de 2016.

MUNICIPALIDAD PROVINCIAL DE SAN MARTIN
Ing. Annie Mabel Chong Bartra
JEFA OFICINA INFORMATICA Y SISTEMAS

ES 12:18 p.m. 29/11/2016

Anexo: Cuadro de Valoración de Activos (C, I, D)



ANALISIS DE RIESGO-ACTIVOS rev2 - Microsoft Excel

M36: DEGRADACIÓN DEL VALOR

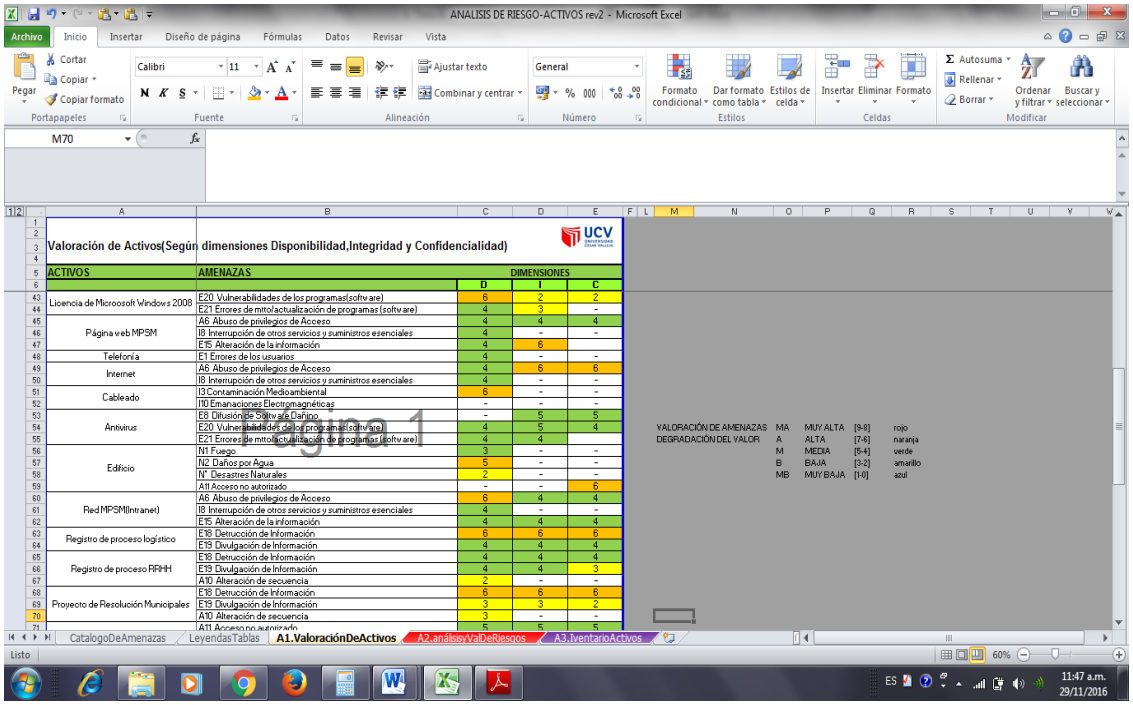
Valoración de Activos(Según dimensiones Disponibilidad,Integridad y Confidencialidad)

ACTIVOS	AMENAZAS	D	I	C
	A11 Acceso no autorizado	4	-	-
	N1 Fuego	4	-	-
	N2 Daños por Agua	4	-	-
	N* Desastres Naturales	4	-	-
Router Wifi	I3 Contaminación Medioambiental	4	-	-
	I5 Corte del suministro eléctrico	5	-	-
	I7 Fallo de servicios de comunicaciones	4	-	-
	A11 Acceso no autorizado	-	-	-
	N1 Fuego	6	-	-
	N2 Daños por Agua	6	-	-
	N* Desastres Naturales	6	-	-
	I3 Contaminación Mecánica	6	-	-
Servidor 02 (Web)	I5 Corte del suministro eléctrico	6	-	-
	I7 Fallo de servicios de comunicaciones	6	-	-
	E2 Errores del administrador	4	4	4
	E23 Errores de mtto/actualización de equipos (hardware)	-	-	9
	A11 Acceso no autorizado	-	5	6
	N2 Daños por Agua	4	-	-
	N* Desastres Naturales	2	-	-
Lap top's	I6 Condiciones inadecuadas de temperatura y/o humedad	8	8	-
	I7 Fallo de servicios de comunicaciones	6	-	-
	N2 Daños por Agua	6	-	-
	N* Desastres Naturales	1	-	-
	I6 Condiciones inadecuadas de temperatura y/o humedad	8	8	-
PC (Gerencia Adm&Fin)	I7 Fallo de servicios de comunicaciones	3	-	-
	I4 Avería de origen físico y lógico	4	-	-
	A6 Abuso de privilegios de Acceso	4	4	8
	E24 Caída del sistema por agotamiento de recursos	4	-	-
	E20 Vulnerabilidades de los programas(software)	6	2	2

VALORACIÓN DE AMENAZAS				
DEGRADACIÓN DEL VALOR	MA	MUY ALTA	[9-8]	rojo
	A	ALTA	[7-6]	naranja
	M	MEDIA	[5-4]	verde
	B	BAJA	[3-2]	amarillo
	MB	MUY BAJA	[1-0]	azul

Hojas: CatalogoDeAmenazas | LeyendasTablas | A1.ValoraciónDeActivos | A2.análisisyValDeRiesgos | A3.IventarioActivos

Listo | 60% | 11:46 a.m. 29/11/2016



ANALISIS DE RIESGO-ACTIVOS rev2 - Microsoft Excel

M70

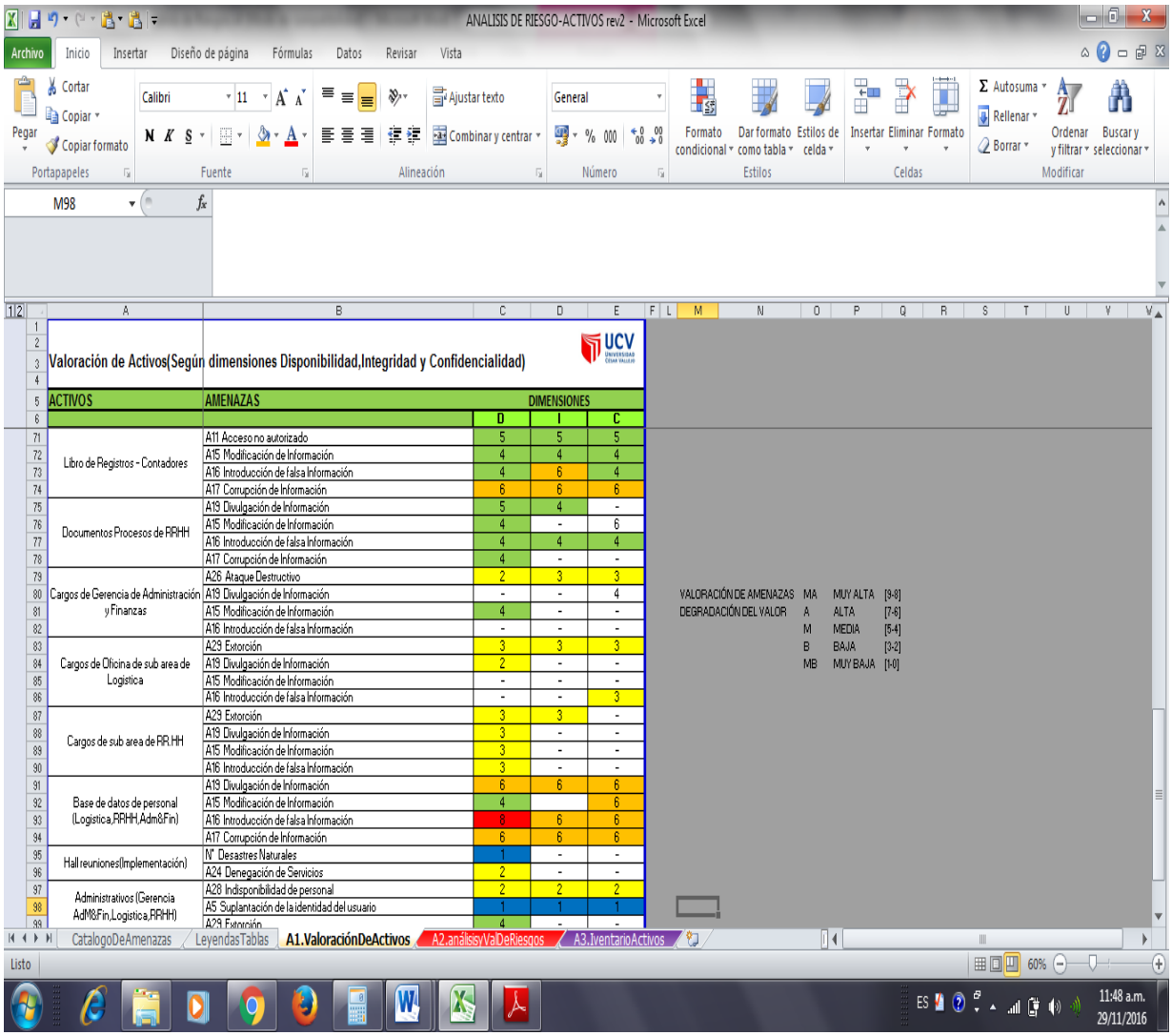
Valoración de Activos(Según dimensiones Disponibilidad,Integridad y Confidencialidad)

ACTIVOS	AMENAZAS	D	I	C
Licencia de Microosoft Windows 2008	E20 Vulnerabilidades de los programas(software)	6	2	2
	E21 Errores de mtto/actualización de programas (software)	4	3	-
Página web MPSM	A6 Abuso de privilegios de Acceso	4	4	4
	I8 Interrupción de otros servicios y suministros esenciales	4	-	-
	E15 Alteración de la información	4	6	
Telefonía	E1 Errores de los usuarios	4	-	-
Internet	A6 Abuso de privilegios de Acceso	4	6	6
	I8 Interrupción de otros servicios y suministros esenciales	4	-	-
Cableado	I3 Contaminación Medioambiental	6	-	-
	I10 Emanaciones Electromagnéticas	-	-	-
	E8 Difusión de Software Dañino	-	5	5
Antivirus	E20 Vulnerabilidades de los programas(software)	4	5	4
	E21 Errores de mtto/actualización de programas (software)	4	4	
	N1 Fuego	3	-	-
Edificio	N2 Daños por Agua	5	-	-
	N* Desastres Naturales	2	-	-
	A11 Acceso no autorizado	-	-	6
	A6 Abuso de privilegios de Acceso	6	4	4
Red MPSM(Intranet)	I8 Interrupción de otros servicios y suministros esenciales	4	-	-
	E15 Alteración de la información	4	4	4
Registro de proceso logístico	E18 Detrucción de Información	6	6	6
	E19 Divulgación de Información	4	4	4
Registro de proceso RRHH	E18 Detrucción de Información	4	4	4
	E19 Divulgación de Información	4	4	3
	A10 Alteración de secuencia	2	-	-
	E18 Detrucción de Información	6	6	6
Proyecto de Resolución Municipales	E19 Divulgación de Información	3	3	2
	A10 Alteración de secuencia	3	-	-
	A11 Acceso no autorizado	5	5	5

VALORACIÓN DE AMENAZAS				
DEGRADACIÓN DEL VALOR	MA	MUY ALTA	[9-8]	rojo
	A	ALTA	[7-6]	naranja
	M	MEDIA	[5-4]	verde
	B	BAJA	[3-2]	amarillo
	MB	MUY BAJA	[1-0]	azul

Hojas: CatalogoDeAmenazas | LeyendasTablas | A1.ValoraciónDeActivos | A2.análisisyValDeRiesgos | A3.IventarioActivos

Listo | 60% | 11:47 a.m. 29/11/2016


ANALISIS DE RIESGO-ACTIVOS rev2 - Microsoft Excel
Archivo
Inicio
Insertar
Diseño de página
Fórmulas
Datos
Revisar
Vista
M98
Valoración de Activos(Según dimensiones Disponibilidad,Integridad y Confidencialidad)
ACTIVOS
AMENAZAS
DIMENSIONES
D
I
C
Libro de Registros - Contadores
A11 Acceso no autorizado 5 5 5
A15 Modificación de Información 4 4 4
A16 Introducción de falsa Información 4 6 4
A17 Corrupción de Información 6 6 6
Documentos Procesos de RRHH
A19 Divulgación de Información 5 4 -
A15 Modificación de Información 4 - 6
A16 Introducción de falsa Información 4 4 4
A17 Corrupción de Información 4 - -
Cargos de Gerencia de Administración y Finanzas
A26 Ataque Destructivo 2 3 3
A19 Divulgación de Información - - 4
A15 Modificación de Información 4 - -
A16 Introducción de falsa Información - - -
Cargos de Oficina de sub area de Logistica
A29 Extorción 3 3 3
A19 Divulgación de Información 2 - -
A15 Modificación de Información - - -
A16 Introducción de falsa Información - - 3
Cargos de sub area de RR.HH
A29 Extorción 3 3 -
A19 Divulgación de Información 3 - -
A15 Modificación de Información 3 - -
A16 Introducción de falsa Información 3 - -
Base de datos de personal (Logistica,RRHH,Adm&Fin)
A19 Divulgación de Información 6 6 6
A15 Modificación de Información 4 6
A16 Introducción de falsa Información 6 6 6
A17 Corrupción de Información 6 6 6
Hall reuniones(Implementación)
N° Desastres Naturales 1 - -
A24 Denegación de Servicios 2 - -
Administrativos (Gerencia AdM&Fin,Logistica,RRHH)
A28 Indisponibilidad de personal 2 2 2
A5 Suplantación de la identidad del usuario 1 1 1
A29 Extorción 4 - -
VALORACIÓN DE AMENAZAS
DEGRADACIÓN DEL VALOR
MA MUY ALTA [9-8]
A ALTA [7-6]
M MEDIA [5-4]
B BAJA [3-2]
MB MUY BAJA [1-0]
CatalogoDeAmenazas
LeyendasTablas
A1.ValoraciónDeActivos
A2.análisisyValDeRiesgos
A3.InventarioActivos
Listo
60%
ES
11:48 a.m.
29/11/2016

Anexo: B. Análisis y Valoración de Riesgos

e la tabla:
Nombre del activo sobre el que se evalúa el riesgo.
a: Descripción de la amenaza a la que está expuesta el activo.
lidad. Probabilidad de materialización de la amenaza.
. Impacto derivado de la materialización de la amenaza.
Valor de riesgo resultante.

ANÁLISIS DE RIESGOS(MATRIZ)						
TIPOS DE ACTIVO	VULNERABILIDAD	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO	INTERPRETACIÓN
Servidor 01(Contabilidad)	Vulnerabilidades de servicios	Fuga de información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Vulnerabilidad de aplicaciones	Degradación de los soportes de almacenamiento de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Router Wifi (Clientes)	Fallo con protocolo WPS	Caída del sistema por sobrecarga	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
Router Wifi (Clientes)	Claves por defecto de routers afectados	Denegación de servicio	MEDIO	BAJO	BAJO	RIESGO POCO RESEÑABLE
Servidor 02 (Web)	Suplatanción de IP	Denegación de servicio	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Vulnerabilidades de servicios	Corte del suministro eléctrico	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Lap top´s	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Sensibilidad de golpes o caídas	Pérdida de equipos	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
PC (Gerencia Adm&Fin)	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	No cierran sesión al momento de retirarse de oficinas	Alteración de la información / Introducción de falsa información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Instalacion de equipos de computo de manera incorrecta	Pérdida de equipos	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Sensibilidad de golpes o caídas	Pérdida de equipos	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de backups de información.	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Mantenimiento insuficiente /Instalacion Fallida	Incumplimiento del SI	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
Licencia de Microosoft Windows 2008	Falta de mecanismos de autenticacion de usuarios	Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Contraseñas poco fiables	Corrupción de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Mala distribución de contraseñas	Introducción de falsa información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Página web MPSM	Falta de terminacion de la sesion cuando se abandona la estación de trabaj	Abuso de los derechos	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Interfaz de usuario complicada	Errores de mantenimiento / actualización de programas (software)	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Servicios innecesarios para el usuario	Difusión de software dañino	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
Internet	Trafico de información desprotegido	Interceptación de información (escucha)	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Cableado desprotegido	Robo/Daños por calor extremo	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de pruebas de envio o recepcion de mensajes	Negación de Activos	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Interrupciones frecuentes de sistemas de comunicación o algún servicio independiente	Corrupción de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Gestión inadecuada de la red	Corrupción de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de privilegios en los permisos	Abuso de privilegios de acceso	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO

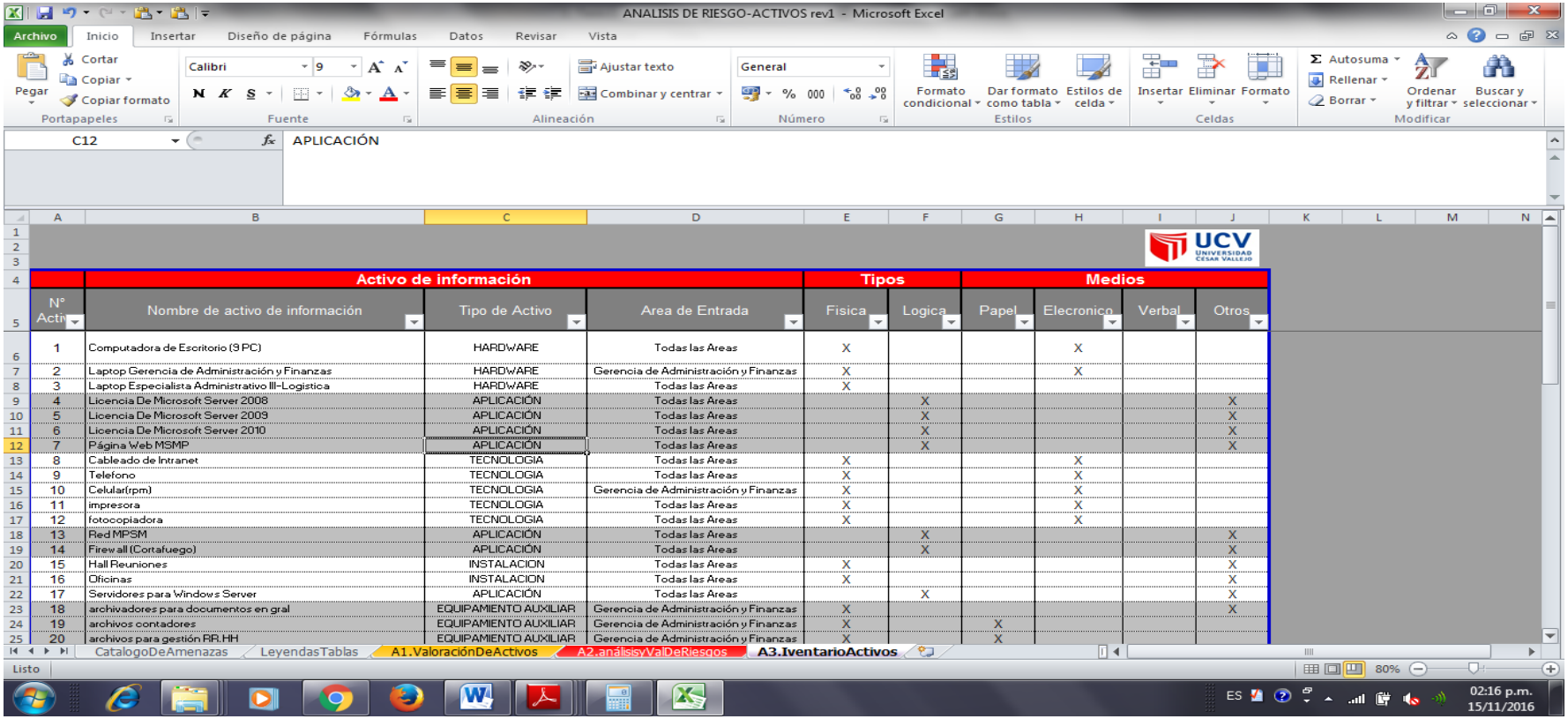
TIPOS DE ACTIVO	VULNERABILIDAD	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO	INTERPRETACIÓN
Red MPSM(Intranet)	Gestión inadecuada de la red	Corrupción de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de privilegios en los permisos	Abuso de privilegios de acceso	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Poca fiabilidad en contraseñas	Corrupción de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Falta de procedimientos para el traspaso de información	Alteración de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Conexiones de red desprotegidas	Desastres Industriales/Corte de suministro eléctrico	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Registro de proceso logístico	Falta de backups de información.	Destrucción de información / Alteración de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Traspaso de información-debil	Alteración de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Introducción de falsa información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
Registro de proceso RRHH	Falta de backups de información.	Destrucción de información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Traspaso de información-debil	Alteración de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Pocos controles de acceso	Introducción de falsa información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Proyecto de Resolución Municipales	Falta de backups de información.	Destrucción de información / Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Poca fiabilidad en transferencia	Corrupción de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Libro de Registros - Contadores	Falta de backups de información.	Destrucción de información / Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Falta de cuidado en transferencia	Introducción de falsa información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	MEDIO	BAJO	BAJO	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Documentos Procesos de RRHH	Falta de backups de información.	Destrucción de información / Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Poca fiabilidad en transferencia de dotos	Introducción de falsa información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Cargos de Dirección Gerencia de Administración y Finanzas	Falta de backups de información.	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Poca fiabilidad en transferencia	Introducción de falsa información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	BAJO	BAJO	RIESGO POCO RESEÑABLE
Cargos de Dirección de Oficina de sub area de Logistica	Falta de backups de información.	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de cuidado en transferencia de datos	Introducción de falsa información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE

TIPOS DE ACTIVO	VULNERABILIDAD	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO	INTERPRETACIÓN
Cargos de Dirección Gerencia de Administración y Finanzas	Falta de backups de información.	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Poca fiabilidad en transferencia	Introducción de falsa información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	BAJO	BAJO	RIESGO POCO RESEÑABLE
Cargos de Dirección de Oficina de sub area de Logistica	Falta de backups de información.	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de cuidado en transferencia de datos	Introducción de falsa información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Cargos de Dirección sub area de RR.HH	Falta de backups de información.	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Poca fiabilidad en transferencia	Introducción de falsa información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	BAJO	BAJO	RIESGO POCO RESEÑABLE
Base de datos de personal (Logistica,RRHH,Adm&Fin)	Abuso de privilegios	Corrupción de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Provilegios excesivos	Corrupción de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Vulnerabilidades de la plataforma	Errores de configuración	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Autenticacion débil	Introducción de falsa información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
Hall reuniones(Implementación)	Descuido del control de acceso físico	Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Area vulnerable para inundaciones y lluvias	Daños por agua	MEDIO	BAJO	BAJO	RIESGO POCO RESEÑABLE
	Falta de proteccion Fisica de las puertas y ventanas del hall	Robo	ALTO	MEDIO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Administrativos (Gerencia AdM&Fin,Logistica,RRHH)	Procedimiento con algunas falencias para contratación de personal	Incumplimiento de disponibilidad inmediata de personal	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Entrenamiento insuficiente en seguridad	Indisponibilidad del personal	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	falta de conciencia acerca de la seguridad	Indisponibilidad del personal	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	falta de mecanismos de monitoreo	Indisponibilidad del personal	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE

Revisado Por_____

Municipalidad Provincial de San Martin-Tarapoto

Anexo: C. Inventario de Activos

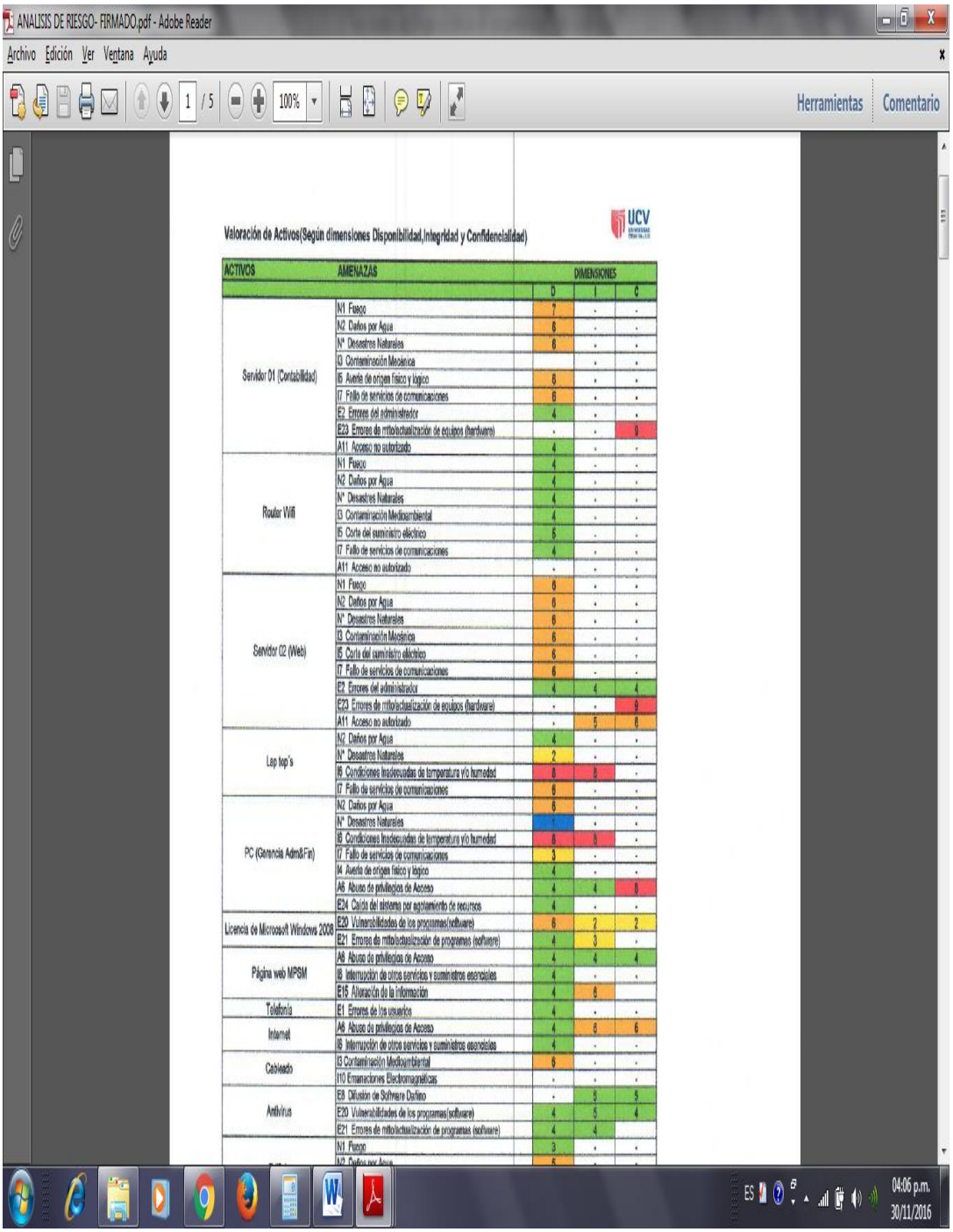


ANALISIS DE RIESGO-ACTIVOS rev1 - Microsoft Excel

	Activo de información			Tipos		Medios			
N° Acti	Nombre de activo de información	Tipo de Activo	Area de Entrada	Fisica	Logica	Papel	Electronico	Verbal	Otros
1	Computadora de Escritorio (9 PC)	HARDWARE	Todas las Areas	X			X		
2	Laptop Gerencia de Administración y Finanzas	HARDWARE	Gerencia de Administración y Finanzas	X			X		
3	Laptop Especialista Administrativo III-Logistica	HARDWARE	Todas las Areas	X					
4	Licencia De Microsoft Server 2008	APLICACIÓN	Todas las Areas		X				X
5	Licencia De Microsoft Server 2009	APLICACIÓN	Todas las Areas		X				X
6	Licencia De Microsoft Server 2010	APLICACIÓN	Todas las Areas		X				X
7	Página Web MSMP	APLICACIÓN	Todas las Areas		X				X
8	Cableado de Intranet	TECNOLOGIA	Todas las Areas	X			X		
9	Telefono	TECNOLOGIA	Todas las Areas	X			X		
10	Celular(rpm)	TECNOLOGIA	Gerencia de Administración y Finanzas	X			X		
11	impresora	TECNOLOGIA	Todas las Areas	X			X		
12	fotocopiadora	TECNOLOGIA	Todas las Areas	X			X		
13	Red MPSM	APLICACIÓN	Todas las Areas		X				X
14	Firewall (Cortafuego)	APLICACIÓN	Todas las Areas		X				X
15	Hall Reuniones	INSTALACION	Todas las Areas	X					X
16	Oficinas	INSTALACION	Todas las Areas	X					X
17	Servidores para Windows Server	APLICACIÓN	Todas las Areas		X				X
18	archivadores para documentos en gral	EQUIPAMIENTO AUXILIAR	Gerencia de Administración y Finanzas	X					X
19	archivos contadores	EQUIPAMIENTO AUXILIAR	Gerencia de Administración y Finanzas	X		X			
20	archivos para gestión RR.HH	EQUIPAMIENTO AUXILIAR	Gerencia de Administración y Finanzas	X		X			

Anexo: INSTRUMENTOS FIRMADOS

A. Cuadro de Valoración de Activos (C, I, D) (VISADO)



ANALISIS DE RIESGO- FIRMADO.pdf - Adobe Reader

Archivo Edición Ver Ventana Ayuda

Herramientas Comentario

Valoración de Activos(Según dimensiones Disponibilidad,Integridad y Confidencialidad)

ACTIVOS	AMENAZAS	DIMENSIONES		
		D	I	C
Servidor 01 (Contabilidad)	N1 Fuego	7	-	-
	N2 Daños por Agua	6	-	-
	N* Desastres Naturales	6	-	-
	I3 Contaminación Mecánica		-	-
	I5 Avería de origen físico y lógico	6	-	-
	I7 Fallo de servicios de comunicaciones	6	-	-
	E2 Errores del administrador	4	-	-
	E23 Errores de mtto/actualización de equipos (hardware)	-	-	8
	A11 Acceso no autorizado	4	-	-
Router Wifi	N1 Fuego	4	-	-
	N2 Daños por Agua	4	-	-
	N* Desastres Naturales	4	-	-
	I3 Contaminación Medioambiental	4	-	-
	I5 Corte del suministro eléctrico	5	-	-
	I7 Fallo de servicios de comunicaciones	4	-	-
	A11 Acceso no autorizado	-	-	-
Servidor 02 (Web)	N1 Fuego	6	-	-
	N2 Daños por Agua	6	-	-
	N* Desastres Naturales	6	-	-
	I3 Contaminación Mecánica	6	-	-
	I5 Corte del suministro eléctrico	6	-	-
	I7 Fallo de servicios de comunicaciones	6	-	-
	E2 Errores del administrador	4	4	4
	E23 Errores de mtto/actualización de equipos (hardware)	-	-	8
	A11 Acceso no autorizado	-	5	8
Lap top's	N2 Daños por Agua	4	-	-
	N* Desastres Naturales	2	-	-
	I6 Condiciones inadecuadas de temperatura y/o humedad	8	8	-
	I7 Fallo de servicios de comunicaciones	6	-	-
PC (Gerencia Adm&Fin)	N2 Daños por Agua	6	-	-
	N* Desastres Naturales	7	-	-
	I6 Condiciones inadecuadas de temperatura y/o humedad	8	8	-
	I7 Fallo de servicios de comunicaciones	3	-	-
	I4 Avería de origen físico y lógico	4	-	-
	A6 Abuso de privilegios de Acceso	4	4	8
	E24 Caída del sistema por agotamiento de recursos	4	-	-
Licencia de Microsoft Windows 2008	E20 Vulnerabilidades de los programas(software)	6	2	2
	E21 Errores de mtto/actualización de programas (software)	4	3	-
Página web MPSM	A6 Abuso de privilegios de Acceso	4	4	4
	I8 Interrupción de otros servicios y suministros esenciales	4	-	-
	E15 Alteración de la información	4	6	
Telefonía	E1 Errores de los usuarios	4	-	-
Internet	A6 Abuso de privilegios de Acceso	4	6	6
	I8 Interrupción de otros servicios y suministros esenciales	4	-	-
Cableado	I3 Contaminación Medioambiental	6	-	-
	I10 Emanaciones Electromagnéticas	-	-	-
Antivirus	E8 Difusión de Software Dañino	-	5	5
	E20 Vulnerabilidades de los programas(software)	4	5	4
	E21 Errores de mtto/actualización de programas (software)	4	4	
	N1 Fuego	3	-	-
	N2 Daños por Agua	5		

ES 04:06 p.m. 30/11/2016

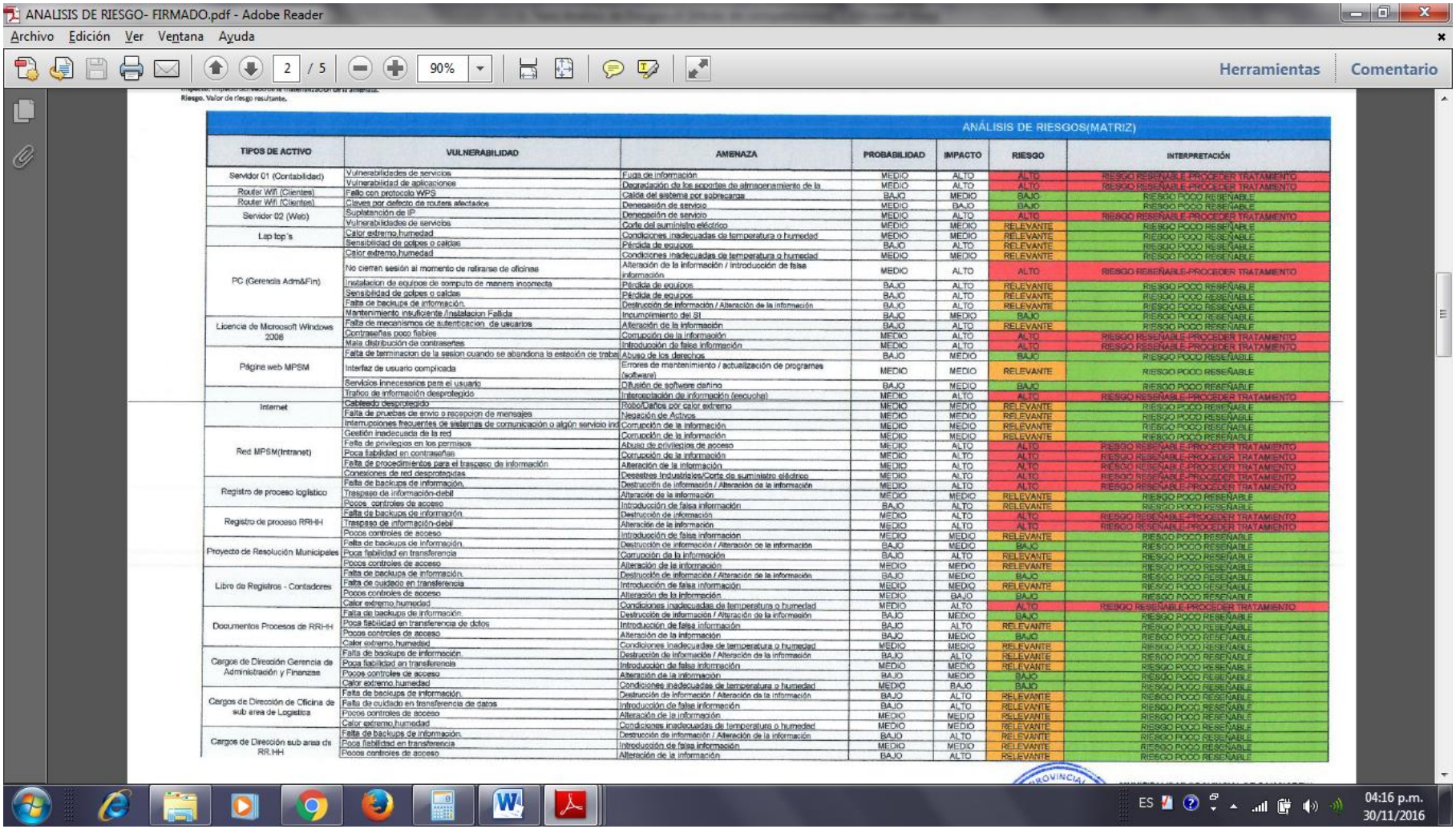
	I10 Emanaciones Electromagnéticas		-	-	-
Antivirus	E8 Difusión de Software Dañino		-	5	5
	E20 Vulnerabilidades de los programas(software)		4	5	4
	E21 Errores de mito/actualización de programas (software)		4	4	
Edificio	N1 Fuego		3	-	-
	N2 Daños por Agua		5	-	-
	N* Desastres Naturales		2	-	-
	A11 Acceso no autorizado		-	-	6
Red MPSM(Intranet)	A6 Abuso de privilegios de Acceso		6	4	4
	I8 Interrupción de otros servicios y suministros esenciales		4	-	-
	E15 Alteración de la información		4	4	4
Registro de proceso logistico	E18 Destrucción de Información		6	6	6
	E19 Divulgación de Información		4	4	4
Registro de proceso RRHH	E18 Destrucción de Información		4	4	4
	E19 Divulgación de Información		4	4	3
Proyecto de Resolución Municipales	A10 Alteración de secuencia		2	-	-
	E18 Destrucción de Información		6	6	6
	E19 Divulgación de Información		3	3	2
	A10 Alteración de secuencia		3	-	-
Libro de Registros - Contadores	A11 Acceso no autorizado		5	5	5
	A15 Modificación de Información		4	4	4
	A16 Introducción de falsa Información		4	6	4
	A17 Corrupción de Información		6	6	6
Documentos Procesos de RRHH	A19 Divulgación de Información		5	4	-
	A15 Modificación de Información		4	-	6
	A16 Introducción de falsa Información		4	4	4
	A17 Corrupción de Información		4	-	-
Cargos de Gerencia de Administración y Finanzas	A26 Ataque Destructivo		2	3	3
	A19 Divulgación de Información		-	-	4
	A15 Modificación de Información		4	-	-
	A16 Introducción de falsa Información		-	-	-
Cargos de Oficina de sub area de Logistica	A29 Extorción		3	3	3
	A19 Divulgación de Información		2	-	-
	A15 Modificación de Información		-	-	-
	A16 Introducción de falsa Información		-	-	3
Cargos de sub area de RR.HH	A29 Extorción		3	3	-
	A19 Divulgación de Información		3	-	-
	A15 Modificación de Información		3	-	-
	A16 Introducción de falsa Información		3	-	-
Base de datos de personal (Logistica,RRHH,Adm&Fin)	A19 Divulgación de Información		6	6	6
	A15 Modificación de Información		4		6
	A16 Introducción de falsa Información		8	6	6
	A17 Corrupción de Información		6	6	6
Hall reuniones(Implementación)	N* Desastres Naturales		1	-	-
	A24 Denegación de Servicios		2	-	-
Administrativos (Gerencia AdM&Fin,Logistica,RRHH)	A28 Indisponibilidad de personal		2	2	2
	A5 Suplantación de la identidad del usuario		1	1	1
	A29 Extorción		4	-	-

Revisado Por:

MUNICIPALIDAD PROVINCIAL DE SAN MARTIN

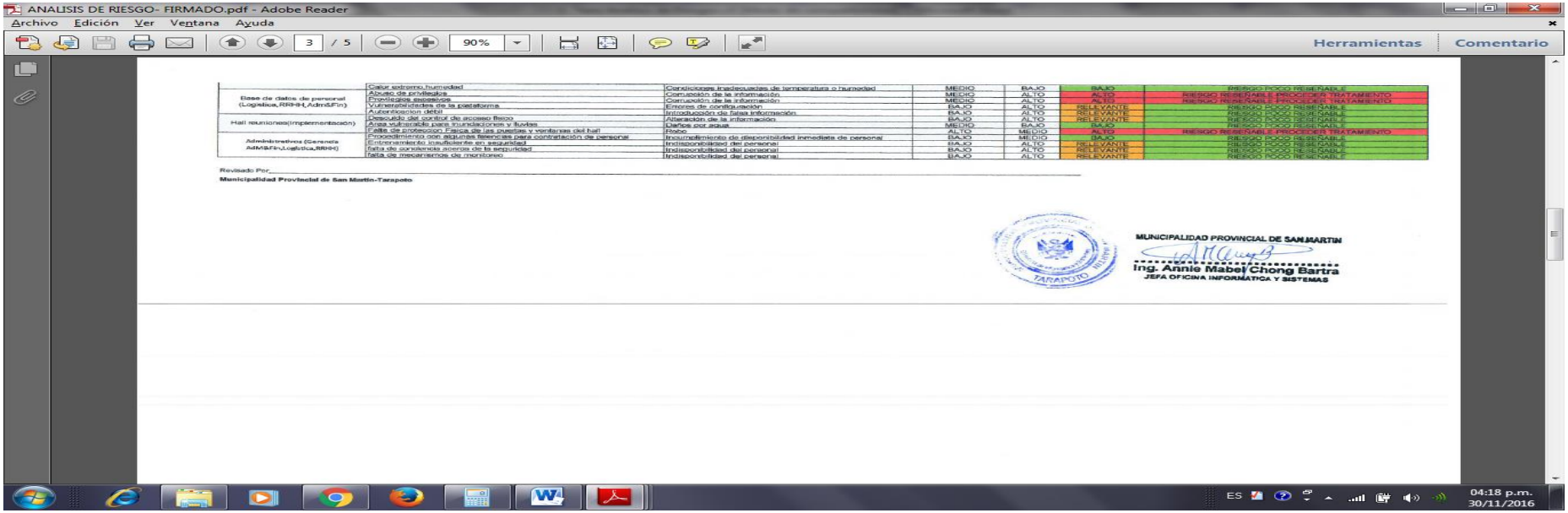
Ing. Annie Mabel Chong Bartra
JEFA OFICINA INFORMATICA Y SISTEMAS

Anexo: B. Análisis y Valoración de Riesgos (VISADO)

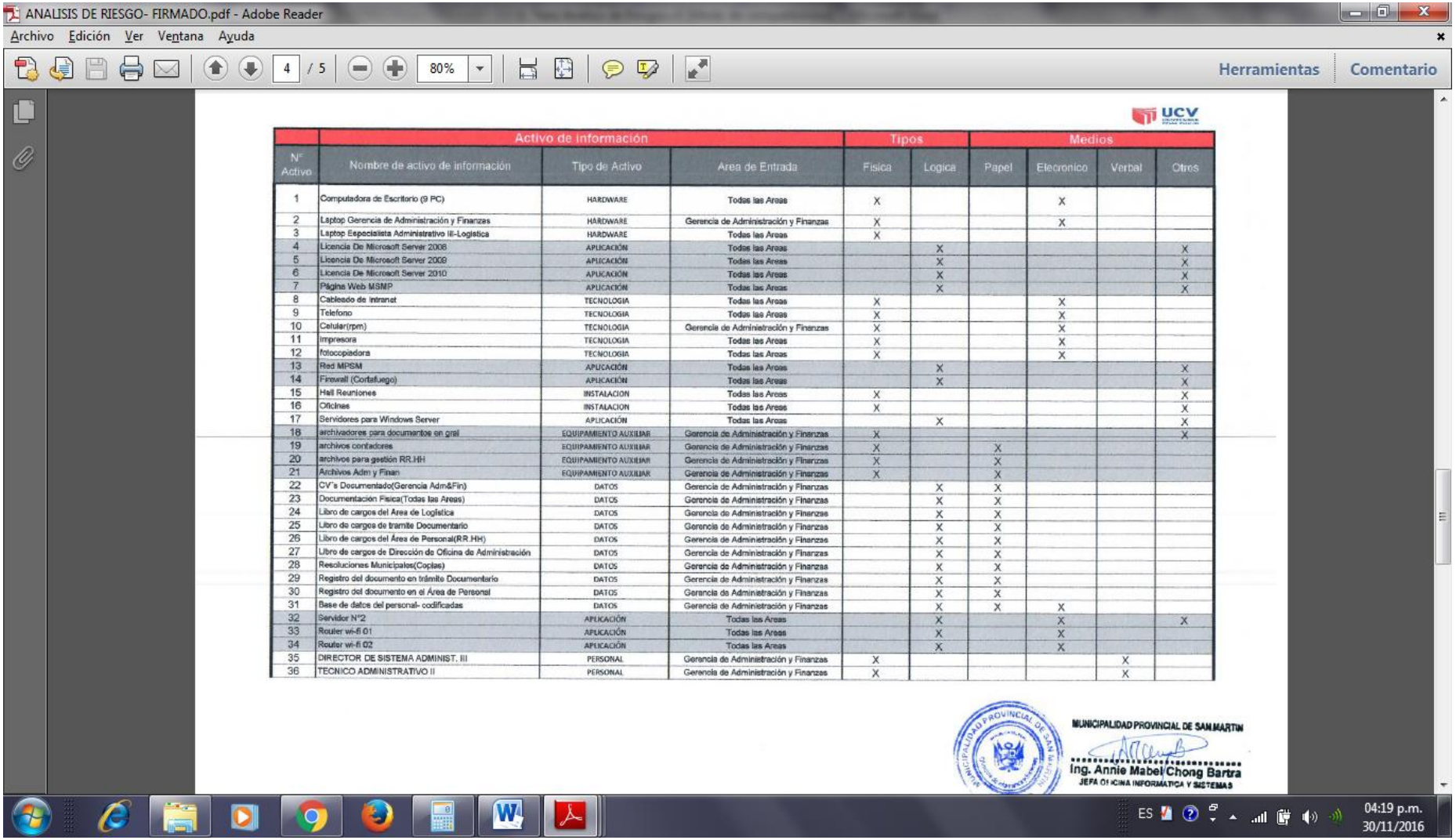


ANÁLISIS DE RIESGOS(MATRIZ)

TIPOS DE ACTIVO	VULNERABILIDAD	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO	INTERPRETACIÓN
Servidor 01 (Contabilidad)	Vulnerabilidades de servicios	Fuga de información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Vulnerabilidad de aplicaciones	Degradación de los soportes de almacenamiento de la	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Router Wifi (Clientes)	Fallo con protocolo WPS	Caída del sistema por sobrecarga	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
Router Wifi (Clientes)	Claves por defecto de routers afectados	Denegación de servicio	MEDIO	BAJO	BAJO	RIESGO POCO RESEÑABLE
Servidor 02 (Web)	Suplantación de IP	Denegación de servicio	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Lap top's	Vulnerabilidades de servicios	Corte del suministro eléctrico	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Sensibilidad de golpes o caidas	Pérdida de equipos	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
PC (Gerencia Adm&Fin)	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	No cierran sesión al momento de retirarse de oficinas	Alteración de la información / introducción de falsa información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Instalacion de equipos de computo de manera incorrecta	Pérdida de equipos	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Sensibilidad de golpes o caidas	Pérdida de equipos	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de backups de información	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Mantenimiento insuficiente /Instalacion Fallida	Incumplimiento del SI	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
Licencia de Microsoft Windows 2008	Falta de mecanismos de autenticacion de usuarios	Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Contraseñas poco fiables	Corrupción de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Mala distribución de contraseñas	Introducción de falsa información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Página web MPSM	Falta de terminacion de la sesion cuando se abandona la estación de trabaj	Abuso de los derechos	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Interfaz de usuario complicada	Errores de mantenimiento / actualización de programas (software)	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Servicios innecesarios para el usuario	Difusión de software dañino	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Trafico de información desprotegido	Interceptación de información (escucha)	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Internet	Cableado desprotegido	Robo/Daños por calor extremo	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de pruebas de envio o recepcion de mensajes	Negación de Actvos	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Interrupciones frecuentes de sistemas de comunicación o algún servicio ind	Corrupción de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Red MPSM(Intranet)	Gestión inadecuada de la red	Corrupción de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de privilegios en los permisos	Abuso de privilegios de acceso	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Poca fiabilidad en contraseñas	Corrupción de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Falta de procedimientos para el traspaso de información	Alteración de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Conexiones de red desprotegidas	Desastres Industriales/Corte de suministro eléctrico	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Registro de proceso logistico	Falta de backups de información	Destrucción de información / Alteración de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Traspaso de información-debil	Alteración de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Introducción de falsa información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
Registro de proceso RRHH	Falta de backups de información	Destrucción de información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Traspaso de información-debil	Alteración de la información	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
	Pocos controles de acceso	Introducción de falsa información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Proyecto de Resolución Municipales	Falta de backups de información	Destrucción de información / Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Poca fiabilidad en transferencia	Corrupción de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Libro de Registros - Contadores	Falta de backups de información	Destrucción de información / Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Falta de cuidado en transferencia	Introducción de falsa información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	MEDIO	BAJO	BAJO	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	ALTO	ALTO	RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
Documentos Procesos de RRHH	Falta de backups de información	Destrucción de información / Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Poca fiabilidad en transferencia de datos	Introducción de falsa información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Cargos de Dirección Gerencia de Administración y Finanzas	Falta de backups de información	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Poca fiabilidad en transferencia	Introducción de falsa información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	BAJO	MEDIO	BAJO	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	BAJO	BAJO	RIESGO POCO RESEÑABLE
Cargos de Dirección de Oficina de sub area de Logistica	Falta de backups de información	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Falta de cuidado en transferencia de datos	Introducción de falsa información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Calor extremo,humedad	Condiciones inadecuadas de temperatura o humedad	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
Cargos de Dirección sub area de RR.HH	Falta de backups de información	Destrucción de información / Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE
	Poca fiabilidad en transferencia	Introducción de falsa información	MEDIO	MEDIO	RELEVANTE	RIESGO POCO RESEÑABLE
	Pocos controles de acceso	Alteración de la información	BAJO	ALTO	RELEVANTE	RIESGO POCO RESEÑABLE


ANALISIS DE RIESGO- FIRMADO.pdf - Adobe Reader
Archivo Edición Ver Ventana Ayuda
3 / 5
90%
Herramientas
Comentario
Calor extremo,humedad
Base de datos de personal (Logística,RRHH,Adm&Fin)
Abuso de privilegios
Amenazas externas
Vulnerabilidades de la plataforma
Autenticacion débil
Hall reuniones(implementación)
Descuido del control de acceso físico
Area vulnerable para inundaciones y lluvias
Falta de protección Física de las puertas y ventanas del hall
Administrativos (Gerencia Adm&Fin,Logística,RRHH)
Procedimiento con algunas falencias para contratación de personal
Entrenamiento insuficiente en seguridad
falta de constancia acerca de la seguridad
falta de mecanismos de monitoreo
Condiciones inadecuadas de temperatura o humedad
Corrupción de la información
Corrupción de la información
Errores de configuración
Introducción de falsa información
Alteración de la información
Daños por agua
Robo
Incumplimiento de disponibilidad inmediata de personal
Indisponibilidad del personal
Indisponibilidad del personal
Indisponibilidad del personal
MEDIO BAJO BAJO
MEDIO ALTO ALTO RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
MEDIO ALTO ALTO RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
BAJO ALTO RELEVANTE RIESGO POCO RESEÑABLE
BAJO ALTO RELEVANTE RIESGO POCO RESEÑABLE
BAJO ALTO RELEVANTE RIESGO POCO RESEÑABLE
MEDIO BAJO BAJO RIESGO POCO RESEÑABLE
ALTO MEDIO ALTO RIESGO RESEÑABLE-PROCEDER TRATAMIENTO
BAJO MEDIO BAJO RIESGO POCO RESEÑABLE
BAJO ALTO RELEVANTE RIESGO POCO RESEÑABLE
BAJO ALTO RELEVANTE RIESGO POCO RESEÑABLE
BAJO ALTO RELEVANTE RIESGO POCO RESEÑABLE
Revisado Por:
Municipalidad Provincial de San Martin-Tarapoto
TARAPOTO
MUNICIPALIDAD PROVINCIAL DE SAN MARTIN
Ing. Annie Mabel Chong Bartra
JEFA OFICINA INFORMÁTICA Y SISTEMAS
ES
04:18 p.m.
30/11/2016

C: Inventario de Activos



ANALISIS DE RIESGO- FIRMADO.pdf - Adobe Reader

Archivo Edición Ver Ventana Ayuda

4 / 5 80% Herramientas Comentario

	Activo de información			Tipos		Medios			
N° Activo	Nombre de activo de información	Tipo de Activo	Area de Entrada	Fisica	Logica	Papel	Electronico	Verbal	Otros
1	Computadora de Escritorio (9 PC)	HARDWARE	Todas las Areas	X			X		
2	Laptop Gerencia de Administración y Finanzas	HARDWARE	Gerencia de Administración y Finanzas	X			X		
3	Laptop Especialista Administrativo III-Logistica	HARDWARE	Todas las Areas	X					
4	Licencia De Microsoft Server 2008	APLICACIÓN	Todas las Areas		X				X
5	Licencia De Microsoft Server 2009	APLICACIÓN	Todas las Areas		X				X
6	Licencia De Microsoft Server 2010	APLICACIÓN	Todas las Areas		X				X
7	Página Web MSMP	APLICACIÓN	Todas las Areas		X				X
8	Cableado de Intranet	TECNOLOGIA	Todas las Areas	X			X		
9	Telefono	TECNOLOGIA	Todas las Areas	X			X		
10	Celular(rpm)	TECNOLOGIA	Gerencia de Administración y Finanzas	X			X		
11	Impresora	TECNOLOGIA	Todas las Areas	X			X		
12	fotocopiadora	TECNOLOGIA	Todas las Areas	X			X		
13	Red MPSM	APLICACIÓN	Todas las Areas		X				X
14	Firewall (Cortafuego)	APLICACIÓN	Todas las Areas		X				X
15	Hall Reuniones	INSTALACION	Todas las Areas	X					X
16	Oficinas	INSTALACION	Todas las Areas	X					X
17	Servidores para Windows Server	APLICACIÓN	Todas las Areas		X				X
18	archivadores para documentos en gral	EQUIPAMIENTO AUXILIAR	Gerencia de Administración y Finanzas	X					X
19	archivos contadores	EQUIPAMIENTO AUXILIAR	Gerencia de Administración y Finanzas	X		X			
20	archivos para gestión RR.HH	EQUIPAMIENTO AUXILIAR	Gerencia de Administración y Finanzas	X		X			
21	Archivos Adm y Finan	EQUIPAMIENTO AUXILIAR	Gerencia de Administración y Finanzas	X		X			
22	CV's Documentado(Gerencia Adm&Fin)	DATOS	Gerencia de Administración y Finanzas		X	X			
23	Documentación Fisica(Todas las Areas)	DATOS	Gerencia de Administración y Finanzas		X	X			
24	Libro de cargos del Area de Logistica	DATOS	Gerencia de Administración y Finanzas		X	X			
25	Libro de cargos de tramite Documentario	DATOS	Gerencia de Administración y Finanzas		X	X			
26	Libro de cargos del Área de Personal(RR.HH)	DATOS	Gerencia de Administración y Finanzas		X	X			
27	Libro de cargos de Dirección de Oficina de Administración	DATOS	Gerencia de Administración y Finanzas		X	X			
28	Resoluciones Municipales(Copias)	DATOS	Gerencia de Administración y Finanzas		X	X			
29	Registro del documento en trámite Documentario	DATOS	Gerencia de Administración y Finanzas		X	X			
30	Registro del documento en el Área de Personal	DATOS	Gerencia de Administración y Finanzas		X	X			
31	Base de datos del personal- codificadas	DATOS	Gerencia de Administración y Finanzas		X	X	X		
32	Servidor N°2	APLICACIÓN	Todas las Areas		X		X		X
33	Router wi-fi 01	APLICACIÓN	Todas las Areas		X		X		
34	Router wi-fi 02	APLICACIÓN	Todas las Areas		X		X		
35	DIRECTOR DE SISTEMA ADMINIST. III	PERSONAL	Gerencia de Administración y Finanzas	X				X	
36	TECNICO ADMINISTRATIVO II	PERSONAL	Gerencia de Administración y Finanzas	X				X	

MUNICIPALIDAD PROVINCIAL DE SAN MARTIN

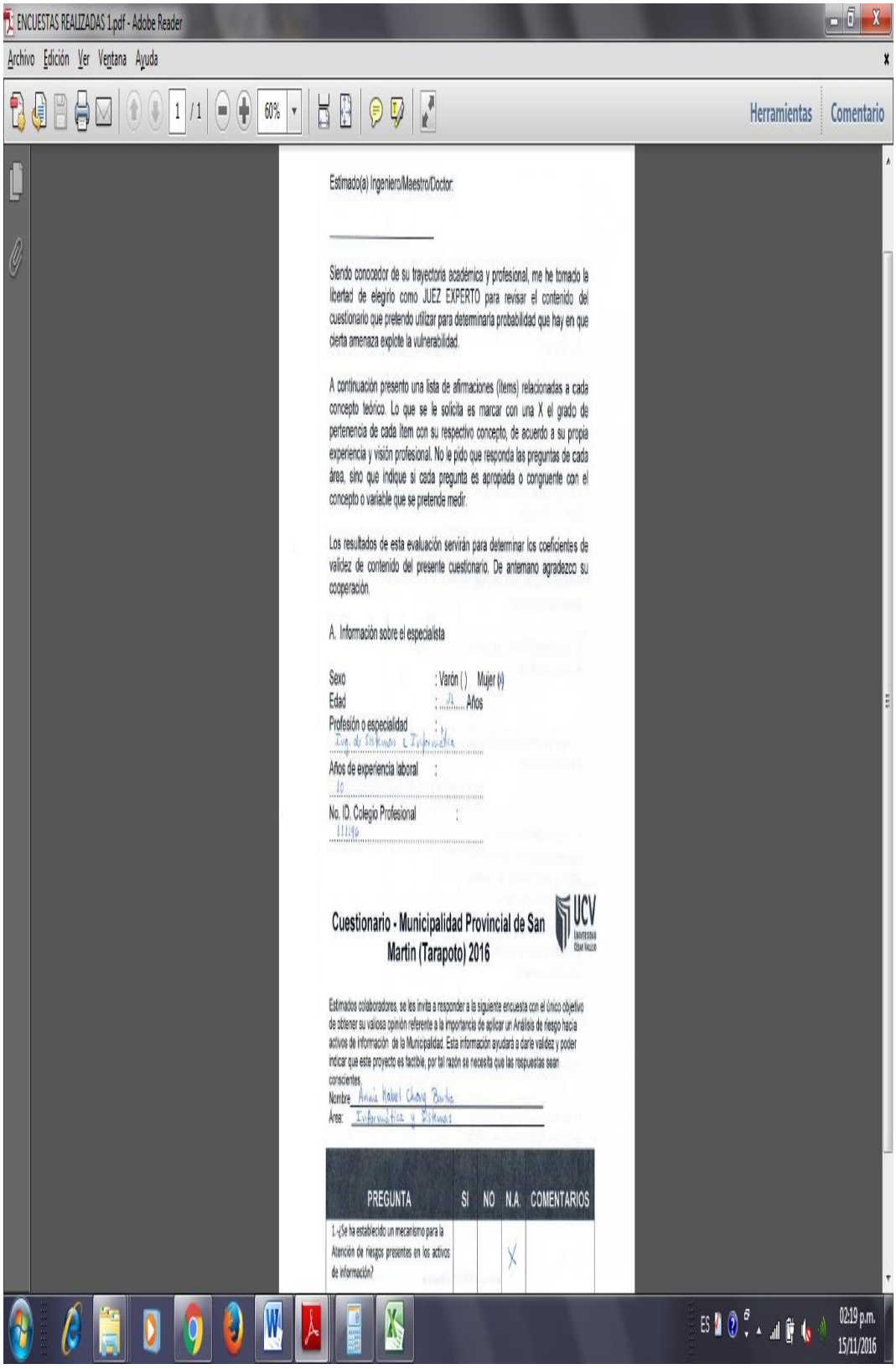
Ing. Annie Mabel Chong Bartra

JEFA OFICINA INFORMATICA Y SISTEMAS

ES 04:19 p.m. 30/11/2016


ANALISIS DE RIESGO- FIRMADO.pdf - Adobe Reader
Archivo Edición Ver Ventana Ayuda
5 / 5
80%
Herramientas
Comentario
37 TÉCNICO ADMINISTRATIVO I PERSONAL Gerencia de Administración y Finanzas X X
38 ESPECIALISTA ADMINISTRATIVO III PERSONAL Logística y Almacenes X X
39 ASISTENTE ADMINISTRATIVO II PERSONAL Logística y Almacenes X X
40 ASISTENTE ADMINISTRATIVO II PERSONAL Logística y Almacenes X X
41 TECNICO ADMINISTRATIVO III PERSONAL Logística y Almacenes X X
42 ASISTENTE ADMINISTRATIVO I PERSONAL Logística y Almacenes X X
43 TECNICO ADMINISTRATIVO II PERSONAL Logística y Almacenes X X
44 AUXILIAR DE SIST.ADMINISTRATIVO II PERSONAL Logística y Almacenes X X
45 SECRETARIA I PERSONAL Logística y Almacenes X X
46 ESPECIALISTA ADMINISTRATIVO III PERSONAL RR.HH X X
47 TECNICO ADMINISTRATIVO III PERSONAL RR.HH X X
48 TECNICO ADMINISTRATIVO II PERSONAL RR.HH X X
49 TECNICO ADMINISTRATIVO II PERSONAL RR.HH X X
50 TECNICO ADMINISTRATIVO II PERSONAL RR.HH X X
51 TRABAJADOR DE SERVICIOS III PERSONAL RR.HH X X
52 TRABAJADOR DE SERVICIOS II PERSONAL RR.HH X X
Revisado Por
Municipalidad Provincial de San Martin-Tarapoto
MUNICIPALIDAD PROVINCIAL DE SAN MARTIN
Ing. Annie Mabel Chong Bartra
JEFA OFICINA INFORMATICA Y SISTEMAS
ES
04:20 p.m.
30/11/2016

D. Encuesta: Realizada



ENCUESTAS REALIZADAS 1.pdf - Adobe Reader

Archivo Edición Ver Ventana Ayuda

Herramientas Comentario

Estimado(a) Ingeniero/Maestro/Doctor:

Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como JUEZ EXPERTO para revisar el contenido del cuestionario que pretendo utilizar para determinarla probabilidad que hay en que cierta amenaza explote la vulnerabilidad.

A continuación presento una lista de afirmaciones (ítems) relacionadas a cada concepto teórico. Lo que se le solicita es marcar con una X el grado de pertenencia de cada ítem con su respectivo concepto, de acuerdo a su propia experiencia y visión profesional. No le pido que responda las preguntas de cada área, sino que indique si cada pregunta es apropiada o congruente con el concepto o variable que se pretende medir.

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido del presente cuestionario. De antemano agradezco su cooperación.

A. Información sobre el especialista

Sexo : Varón ( ) Mujer (x)
Edad : 31 Años
Profesión o especialidad : Ing. de Sistemas e Informática
Años de experiencia laboral : 10
No. ID. Colegio Profesional : 111186

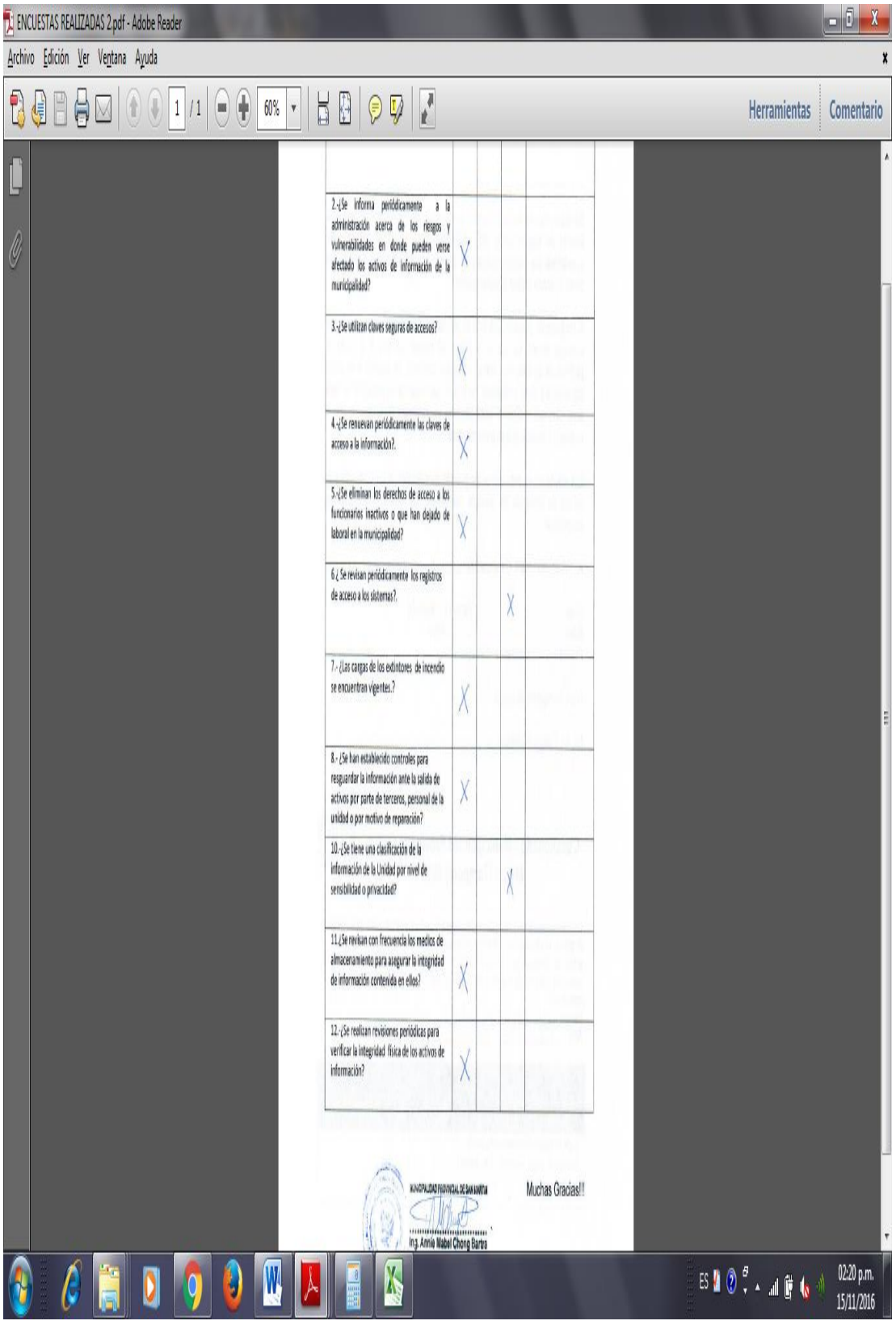
Cuestionario - Municipalidad Provincial de San Martín (Tarapoto) 2016

Estimados colaboradores, se les invita a responder a la siguiente encuesta con el único objetivo de obtener su valiosa opinión referente a la importancia de aplicar un Análisis de riesgo hacia activos de información de la Municipalidad. Esta información ayudará a darle validez y poder indicar que este proyecto es factible, por tal razón se necesita que las respuestas sean conscientes.

Nombre: Arnie Nabel Chavez Barba
Área: Informática y Sistemas

PREGUNTA	SI	NO	N.A.	COMENTARIOS
1.-¿Se ha establecido un mecanismo para la Atención de riesgos presentes en los activos de información?			X	

02:19 p.m. 15/11/2016



ENCUESTAS REALIZADAS 2.pdf - Adobe Reader

Archivo Edición Ver Ventana Ayuda

1 / 1 60% Herramientas Comentario

2.-¿Se informa periódicamente a la administración acerca de los riesgos y vulnerabilidades en donde pueden verse afectado los activos de información de la municipalidad?	X			
3.-¿Se utilizan claves seguras de accesos?	X			
4.-¿Se renuevan periódicamente las claves de acceso a la información?.	X			
5.-¿Se eliminan los derechos de acceso a los funcionarios inactivos o que han dejado de laboral en la municipalidad?	X			
6.¿ Se revisan periódicamente los registros de acceso a los sistemas?.			X	
7.- ¿Las cargas de los extintores de incendio se encuentran vigentes.?	X			
8.- ¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal de la unidad o por motivo de reparación?	X			
10.-¿Se tiene una clasificación de la información de la Unidad por nivel de sensibilidad o privacidad?			X	
11.¿Se revisan con frecuencia los medios de almacenamiento para asegurar la integridad de información contenida en ellos?	X			
12.-¿Se realizan revisiones periódicas para verificar la integridad física de los activos de información?	X			

MUNICIPALIDAD PROVINCIAL DE SAN MARTIN

Ing. Annie Mabel Chong Barba

Muchas Gracias!!!

ES 02:20 p.m. 15/11/2016

Estimado(a) Ingeniero/Maestro/Doctor:

_____

Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como JUEZ EXPERTO para revisar el contenido del cuestionario que pretendo utilizar para determinarla probabilidad que hay en que cierta amenaza explote la vulnerabilidad.

A continuación presento una lista de afirmaciones (ítems) relacionadas a cada concepto teórico. Lo que se le solicita es marcar con una X el grado de pertenencia de cada ítem con su respectivo concepto, de acuerdo a su propia experiencia y visión profesional. No le pido que responda las preguntas de cada área, sino que indique si cada pregunta es apropiada o congruente con el concepto o variable que se pretende medir.

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido del presente cuestionario. De antemano agradezco su cooperación.

A. Información sobre el especialista

Sexo : Varón (X) Mujer ( )
Edad : 32 Años
Profesión o especialidad : T. Computación
Años de experiencia laboral : 7
No. ID. Colegio Profesional :

Cuestionario - Municipalidad Provincial de San Martin (Tarapoto) 2016

Estimados colaboradores, se les invita a responder a la siguiente encuesta con el único objetivo de obtener su valiosa opinión referente a la importancia de aplicar un Análisis de riesgo hacia activos de información de la Municipalidad. Esta información ayudará a darle validez y poder indicar que este proyecto es factible, por tal razón se necesita que las respuestas sean conscientes.

Nombre Cristian Cerro Chota
Area Informática

PREGUNTA	SI	NO	N.A.	COMENTARIOS
1.-¿Se ha establecido un mecanismo para la Atención de riesgos presentes en los activos de información?	X			

2.-¿Se informa periódicamente a la administración acerca de los riesgos y vulnerabilidades en donde pueden verse afectado los activos de información de la municipalidad?	X			
3.-¿Se utilizan claves seguras de accesos?	X			
4.-¿Se renuevan periódicamente las claves de acceso a la información?.		X		
5.-¿Se eliminan los derechos de acceso a los funcionarios inactivos o que han dejado de laboral en la municipalidad?	X			
6.¿ Se revisan periódicamente los registros de acceso a los sistemas?.	X			
7.- ¿Las cargas de los extintores de incendio se encuentran vigentes.?	X			
8.- ¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal de la unidad o por motivo de reparación?	X			
10.-¿Se tiene una clasificación de la información de la Unidad por nivel de sensibilidad o privacidad?		X		
11.¿Se revisan con frecuencia los medios de almacenamiento para asegurar la integridad de información contenida en ellos?	X			
12.-¿Se realizan revisiones periódicas para verificar la integridad física de los activos de información?	X			

Muchas Gracias!!!

ENCUESTAS REALIZADAS 3.pdf - Adobe Reader

Archivo Edición Ver Ventana Ayuda

3 / 8 57% Herramientas Comentario

Estimado(a) Ingeniero/Maestro/Doctor:

____

Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como JUEZ EXPERTO para revisar el contenido del cuestionario que pretendo utilizar para determinarla probabilidad que hay en que cierta amenaza explote la vulnerabilidad.

A continuación presento una lista de afirmaciones (ítems) relacionadas a cada concepto teórico. Lo que se le solicita es marcar con una X el grado de pertenencia de cada ítem con su respectivo concepto, de acuerdo a su propia experiencia y visión profesional. No le pido que responda las preguntas de cada área, sino que indique si cada pregunta es apropiada o congruente con el concepto o variable que se pretende medir.

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido del presente cuestionario. De antemano agradezco su cooperación.

A. Información sobre el especialista

Sexo : Varón ( ) Mujer (√)
Edad : ..29... Años
Profesión o especialidad :
T. Contabilidad..........................
Años de experiencia laboral :
....
No. ID. Colegio Profesional :
....

Cuestionario - Municipalidad Provincial de San Martin (Tarapoto) 2016

UCV Universidad César Vallejo

Estimados colaboradores, se les invita a responder a la siguiente encuesta con el único objetivo de obtener su valiosa opinión referente a la importancia de aplicar un Análisis de riesgo hacia activos de información de la Municipalidad. Esta información ayudará a darle validez y poder indicar que este proyecto es factible, por tal razón se necesita que las respuestas sean conscientes.

Nombre: Janet Marina Ramirez Valera
Área: Recursos Humanos

PREGUNTA	SI	NO	N.A.	COMENTARIOS
1.-¿Se ha establecido un mecanismo para la Atención de riesgos presentes en los activos de información?		X		

ES 02:31 p.m. 22/11/2016

2.-¿Se informa periódicamente a la administración acerca de los riesgos y vulnerabilidades en donde pueden verse afectado los activos de información de la municipalidad?		NO		
3.-¿Se utilizan claves seguras de accesos?	X			
4.-¿Se renuevan periódicamente las claves de acceso a la información?	NO			
5.-¿Se eliminan los derechos de acceso a los funcionarios inactivos o que han dejado de laboral en la municipalidad?	X			
6.¿ Se revisan periódicamente los registros de acceso a los sistemas?.		X		
7.- ¿Las cargas de los extintores de incendio se encuentran vigentes.?	X			
8.- ¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal de la unidad o por motivo de reparación?	X			
10.-¿Se tiene una clasificación de la información de la Unidad por nivel de sensibilidad o privacidad?		X		
11.¿Se revisan con frecuencia los medios de almacenamiento para asegurar la integridad de información contenida en ellos?		X		
12.-¿Se realizan revisiones periódicas para verificar la integridad física de los activos de información?	SI			

Muchas Gracias!!!

Estimado(a) Ingeniero/Maestro/Doctor:

Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como JUEZ EXPERTO para revisar el contenido del cuestionario que pretendo utilizar para determinarla probabilidad que hay en que cierta amenaza explote la vulnerabilidad.

A continuación presento una lista de afirmaciones (ítems) relacionadas a cada concepto teórico. Lo que se le solicita es marcar con una X el grado de pertenencia de cada ítem con su respectivo concepto, de acuerdo a su propia experiencia y visión profesional. No le pido que responda las preguntas de cada área, sino que indique si cada pregunta es apropiada o congruente con el concepto o variable que se pretende medir.

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido del presente cuestionario. De antemano agradezco su cooperación.

A. Información sobre el especialista

Sexo : Varón (X) Mujer ( )
Edad : 48 Años
Profesión o especialidad : Bachiller en Contabilidad
Años de experiencia laboral : 19
No. ID. Colegio Profesional :

Cuestionario - Municipalidad Provincial de San Martín (Tarapoto) 2016

Estimados colaboradores, se les invita a responder a la siguiente encuesta con el único objetivo de obtener su valiosa opinión referente a la importancia de aplicar un Análisis de riesgo hacia activos de información de la Municipalidad. Esta información ayudará a darle validez y poder indicar que este proyecto es factible, por tal razón se necesita que las respuestas sean conscientes.

Nombre: Juan Coronado Quintero
Área: Administración y Finanzas

PREGUNTA	SI	NO	N.A.	COMENTARIOS
1.-¿Se ha establecido un mecanismo para la Atención de riesgos presentes en los activos de información?		X		

2.-¿Se informa periódicamente a la administración acerca de los riesgos y vulnerabilidades en donde pueden verse afectado los activos de información de la municipalidad?	X			
3.-¿Se utilizan claves seguras de accesos?	X			
4.-¿Se renuevan periódicamente las claves de acceso a la información?	X			
5.-¿Se eliminan los derechos de acceso a los funcionarios inactivos o que han dejado de laboral en la municipalidad?	X			
6.¿ Se revisan periódicamente los registros de acceso a los sistemas?	X			
7.- ¿Las cargas de los extintores de incendio se encuentran vigentes?	X			
8.- ¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal de la unidad o por motivo de reparación?		X		
10.-¿Se tiene una clasificación de la información de la Unidad por nivel de sensibilidad o privacidad?		X		
11.¿Se revisan con frecuencia los medios de almacenamiento para asegurar la integridad de información contenida en ellos?	X			
12.-¿Se realizan revisiones periódicas para verificar la integridad física de los activos de información?	X			

Muchas Gracias!!!

Estimado(a) Ingeniero/Maestro/Doctor:

_____

Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como JUEZ EXPERTO para revisar el contenido del cuestionario que pretendo utilizar para determinarla probabilidad que hay en que cierta amenaza explote la vulnerabilidad.

A continuación presento una lista de afirmaciones (ítems) relacionadas a cada concepto teórico. Lo que se le solicita es marcar con una X el grado de pertenencia de cada ítem con su respectivo concepto, de acuerdo a su propia experiencia y visión profesional. No le pido que responda las preguntas de cada área, sino que indique si cada pregunta es apropiada o congruente con el concepto o variable que se pretende medir.

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido del presente cuestionario. De antemano agradezco su cooperación.

A. Información sobre el especialista

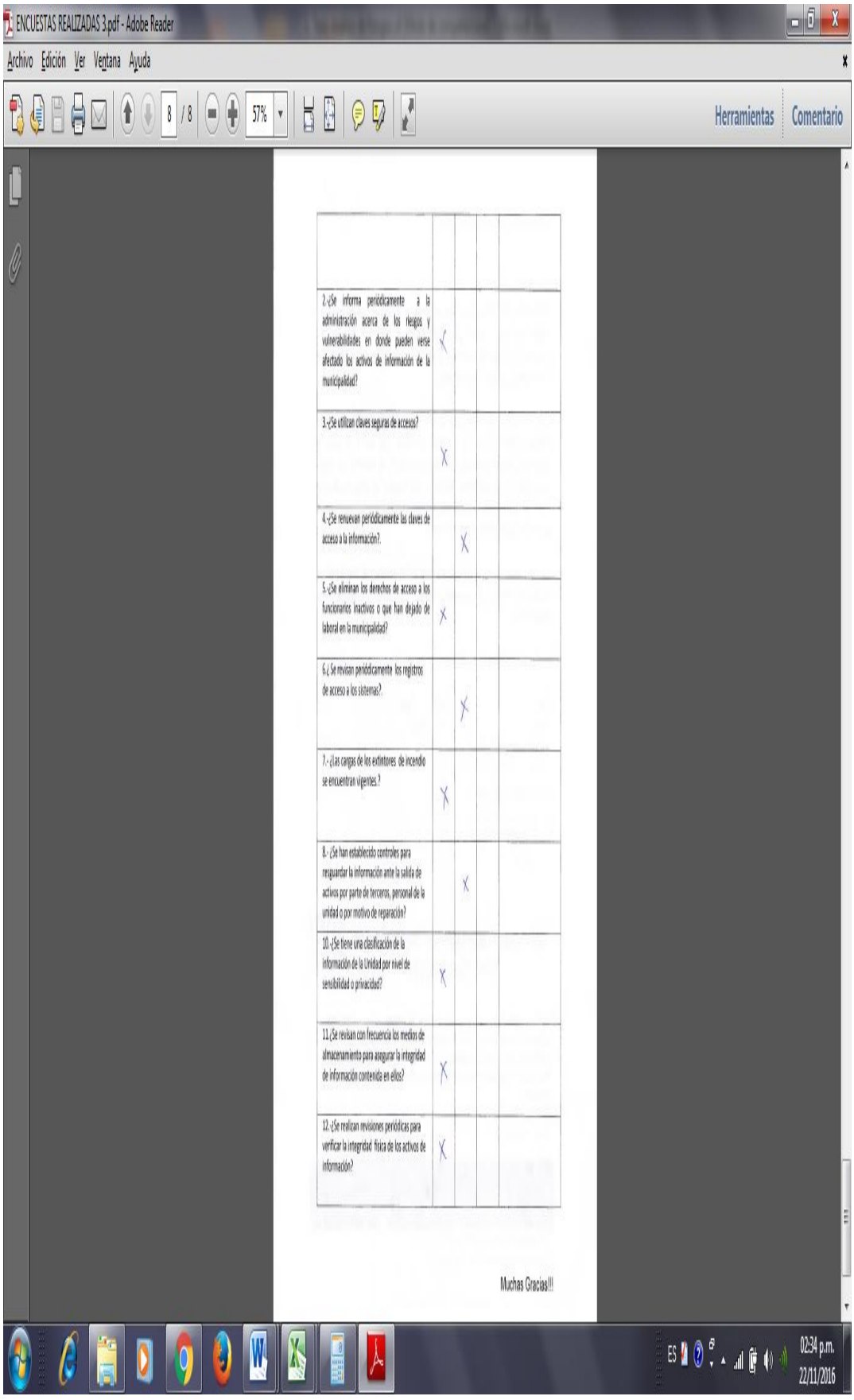
Sexo : Varón (x) Mujer ( )
Edad : 36 Años
Profesión o especialidad :
Ing. de Sistemas (Bachiller)
Años de experiencia laboral :
10
No. ID. Colegio Profesional :
.....

Cuestionario - Municipalidad Provincial de San Martin (Tarapoto) 2016

Estimados colaboradores, se les invita a responder a la siguiente encuesta con el único objetivo de obtener su valiosa opinión referente a la importancia de aplicar un Análisis de riesgo hacia activos de información de la Municipalidad. Esta información ayudará a darle validez y poder indicar que esta proyecto es factible, por tal razón se necesita que las respuestas sean consecuentes.

Nombre: Elmer Ruiz Gonzales
Area: Catastro y Alcabala

PREGUNTA	SI	NO	N.A.	COMENTARIOS
1.-¿Se ha establecido un mecanismo para la Atención de riesgos presentes en los activos de información?	X			


ENCUESTAS REALIZADAS 3.pdf - Adobe Reader
Archivo Edición Ver Ventana Ayuda
8 / 8
57%
Herramientas
Comentario
2.-¿Se informa periódicamente a la administración acerca de los riesgos y vulnerabilidades en donde pueden verse afectado los activos de información de la municipalidad?
3.-¿Se utilizan claves seguras de accesos?
4.-¿Se renuevan periódicamente las claves de acceso a la información?.
5.-¿Se eliminan los derechos de acceso a los funcionarios inactivos o que han dejado de laboral en la municipalidad?
6.-¿ Se revisan periódicamente los registros de acceso a los sistemas?
7.- ¿Las cargas de los extintores de incendio se encuentran vigentes.?
8.- ¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal de la unidad o por motivo de reparación?
10.-¿Se tiene una clasificación de la información de la Unidad por nivel de sensibilidad o privacidad?
11.¿Se revisan con frecuencia los medios de almacenamiento para asegurar la integridad de información contenida en ellos?
12.-¿Se realizan revisiones periódicas para verificar la integridad física de los activos de información?
Muchas Gracias!!!
ES
02:34 p.m.
22/11/2016

Anexo: Evidencias Fotográficas

Gerencia de Administración y Finanzas

Figura 1. No tienen autorización para software sin Licencias, como se aprecia en la fotografía, el personal administrativo sin haber obtenido una aprobación instalo una versión de Windows sin licencia. Esta imagen fue tomada como ejemplo a lo que no se puede realizar.

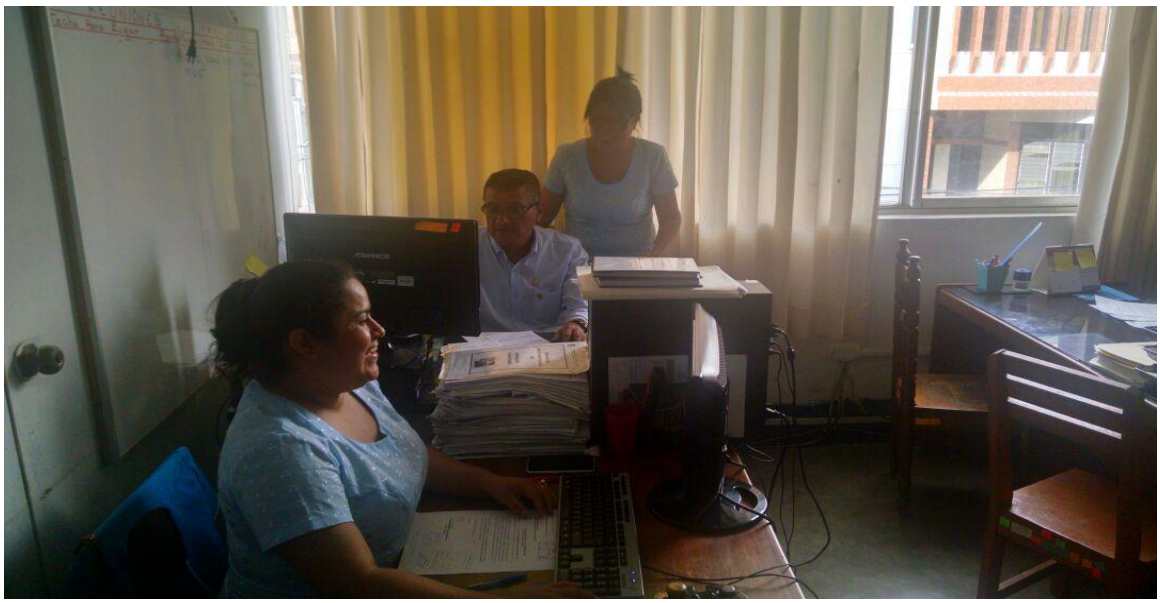


Figura 2. Computadoras y Laptops expuestas a factor clima, el techo es de drywall.

Figura 3. Cableado, conexiones y equipamiento de oficina desordenado, poco espacio entre áreas.

Figura 4. Las actividades diarias se llevan a cabo en espacios reducidos.

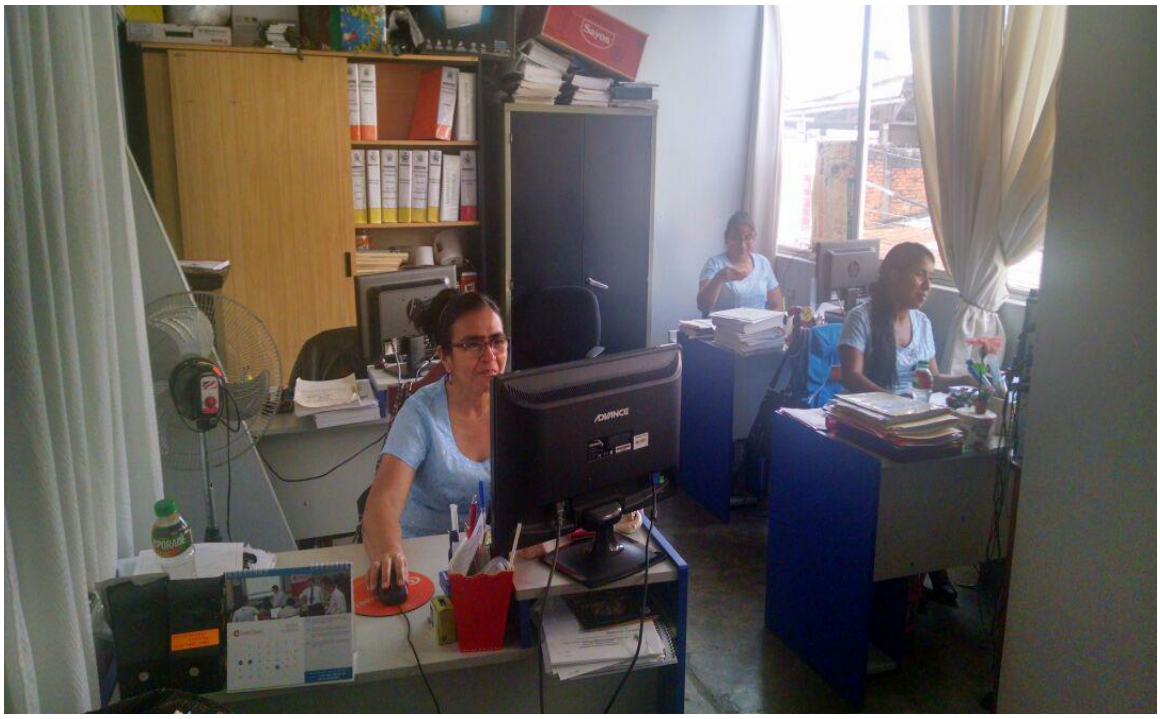


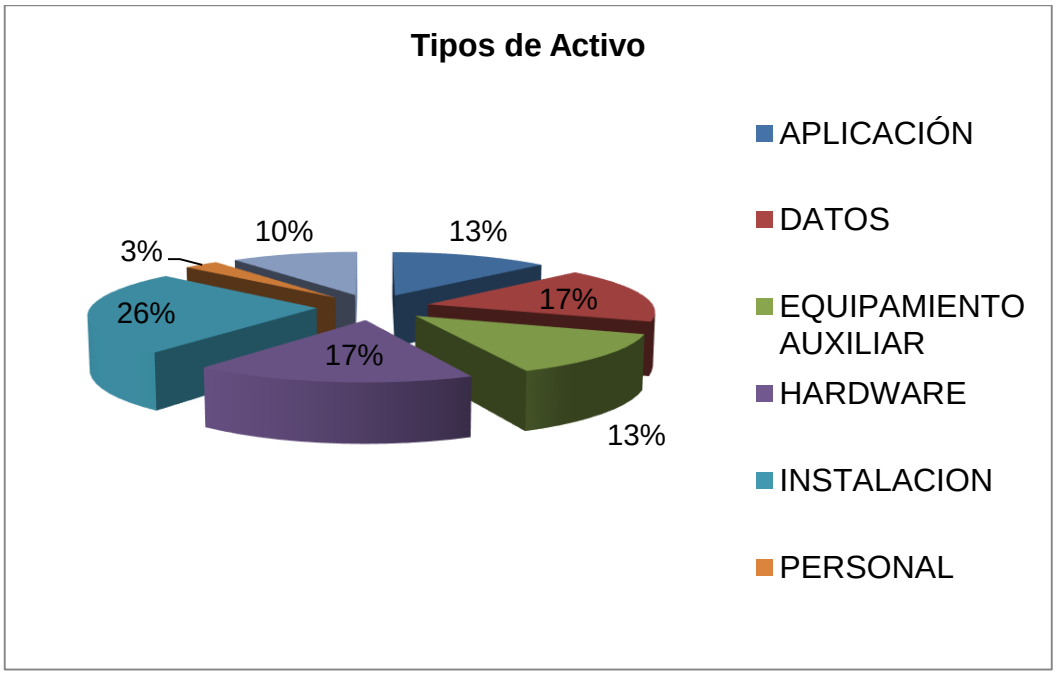
Figura 5. Sub Área de Logística, la actividad diaria controlar el sistema de Adquisiciones y Contrataciones del estado(SEACE).Registros de procesos logísticos tiende a ser destruido por ingreso de personal no autorizado.

Figura 6. Se encontraban realizando las actividades trimestrales del CONSUCODE.

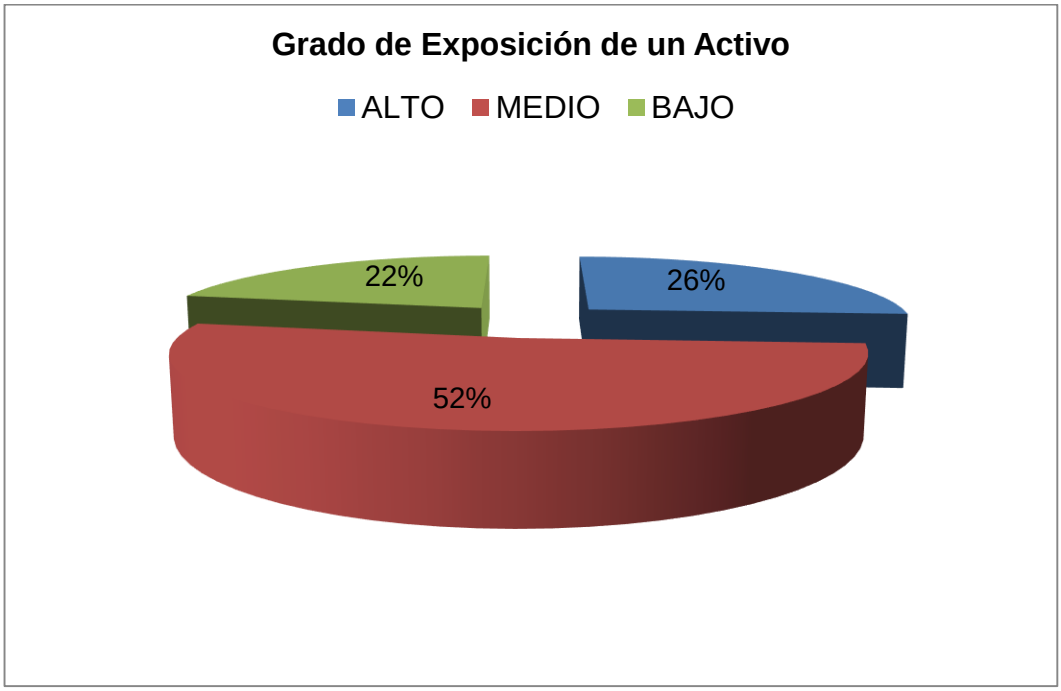
Figura 7. Los asistentes de Logística se encontraban controlando la entrega de suministros, instalaciones con poca ventilación (No hay presupuesto).

Figura 8. Abuso de privilegios de acceso con la red MPSM.

Anexo: Gráficos Estadísticos



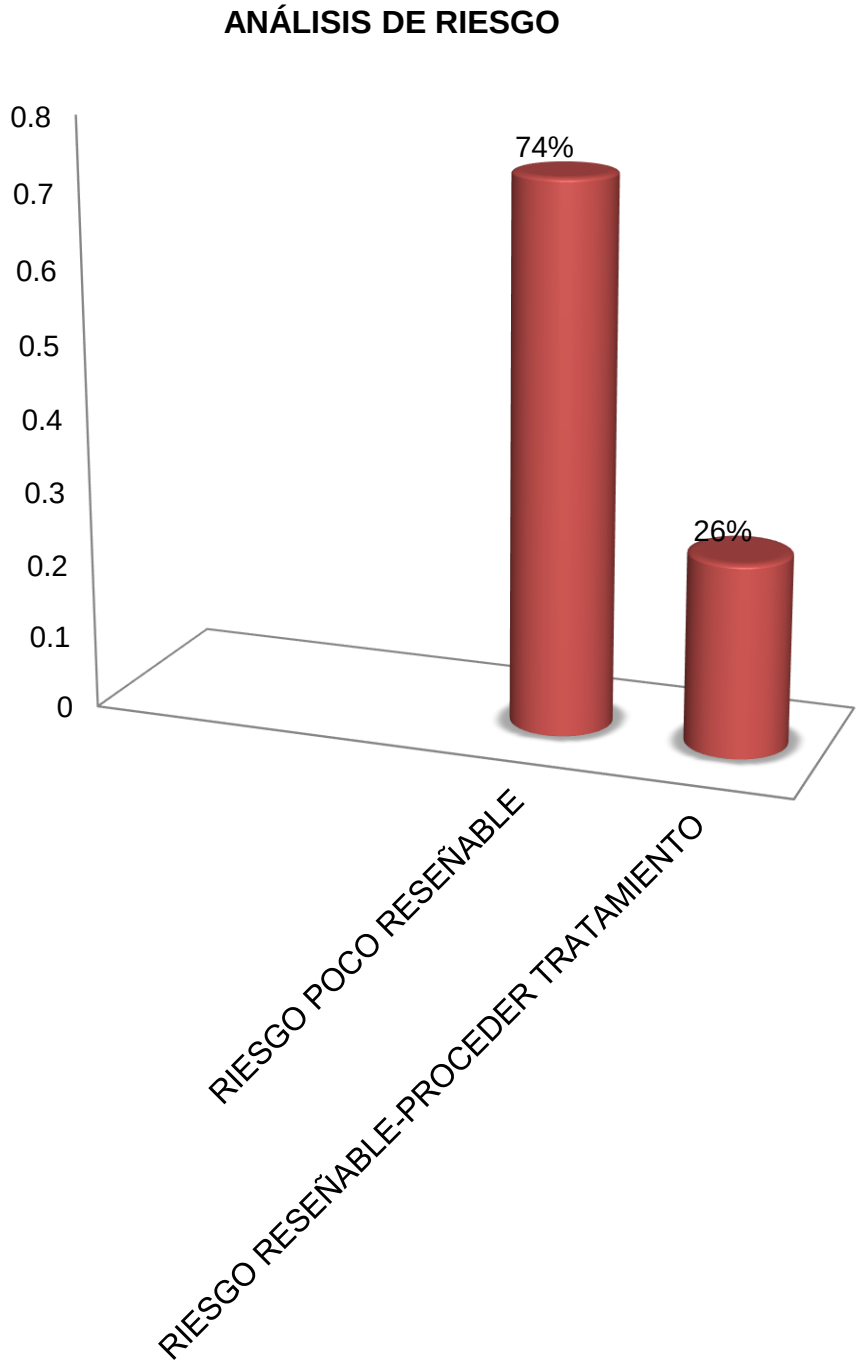
Fuente: Elaboración Propia



.

Fuente: Elaboración Propia

Análisis de Riesgo: Interpretación



Fuente: Elaboración Propia

UNIVERSIDAD CÉSAR VALLEJO

Declaratoria de Autenticidad del Asesor

Yo, **Quito Rodríguez Carmen Zulema**, docente de la Facultad de **Ingeniería y Arquitectura** y Escuela Profesional de **Ingeniería de Sistemas** de la Universidad César Vallejo – Piura, asesora de la Tesis titulada:

"Análisis de riesgos de los activos de información,aplicado a la gerencia de Administración y Finanzas de la Municipalidad Provincial de San Martin-Tarapoto"

del autor Vilchez Morante, Denisse Katherine, constato que la investigación tiene un índice de similitud de 19.00% verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Piura, 18 de noviembre del 2021

Apellidos y Nombres del Asesor: **Quito Rodríguez, Carmen Zulema**	
DNI: 42520247	Firma 
ORCID: 0000-0002-4340-5732	