UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN GESTIÓN PÚBLICA

Evaluación de riesgo de seguridad de información según ISO 27005, OGITT – Instituto Nacional de Salud

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Gestión Pública

AUTOR:

Br. Martin Elifio Montoya Ortecho (ORCID: 0000-0001-9741-4856)

ASESORA:

Dra. Eliana Soledad Castañeda Núñez (ORCID: 0000-0003-3516-1982)

LÍNEA DE INVESTIGACIÓN:

Gestión de Políticas Públicas

LIMA – PERÚ

2020

Dedicatoria

Dedico esta tesis de investigación primeramente a Dios por la bendición de permitir cumplir un objetivo en mi vida profesional y por la salud que me ha dado.

A mis padres que me animaron siempre a seguir avanzando como profesional mostrándome siempre su amor incondicional en todo momento.

A mis compañeros de clase de la maestría que juntos nos impulsábamos a seguir adelante creando un ambiente muy profesional y respeto.

Agradecimiento

Estoy muy agradecido a nuestra casa de estudio Universidad César Vallejo por su compromiso de brindarnos educación altamente profesional y por haber contribuido de manera importante en mi desarrollo profesional.

Página del Jurado

UNIVERSIDAD CÉSAR VALLEJO

DICTAMEN DE LA SUSTENTACIÓN DE TESIS

EL BACHILLER: **MONTOYA ORTECHO, MARTIN ELIFIO** para obtener el Grado Académico de ***Maestro en Gestión Pública,*** ha sustentado la tesis titulada:

EVALUACIÓN DE RIESGO DE SEGURIDAD DE INFORMACIÓN SEGÚN ISO 27005, OGITT – INSTITUTO NACIONAL DE SALUD

Fecha: Martes 21 de enero de 2020 Hora: 8: 00 a.m.

JURADOS:

PRESIDENTE (A): Dr. Freddy Antonio Ochoa Tataje **Firma:** .....

SECRETARIO (A): Mg. Sonia Romero Vela **Firma:** .....

VOCAL: Dra. Eliana Soledad Castañeda Nuñez **Firma:** .....

El Jurado evaluador emitió el dictamen de:

.....Aprobar por unanimidad.....

Habiendo encontrado las siguientes observaciones en la defensa de la tesis:

.....

.....

.....

.....

UNIVERSIDAD CÉSAR VALLEJO JEFE CAMPUS ATE POSGRADO

Recomendaciones sobre el documento de la tesis:

.....

.....

.....

.....

Nota: El tesista tiene un plazo máximo de seis meses, contabilizados desde el día siguiente a la sustentación, para presentar la tesis habiendo incorporado las recomendaciones formuladas por el jurado evaluador.

Declaratoria de Autenticidad

Yo, Martin Elifio Montoya Ortecho, identificado con DNI N° 10799595, estudiante de la Maestría de Gestión Pública de la Escuela de Posgrado de la Universidad César Vallejo, con la tesis titulada: "Evaluación de Riesgo de seguridad de información según ISO 27005, OGITT – Instituto Nacional de Salud".

Declaro bajo juramento que:

La tesis es de mi autoría

He respetado las normas internacionales de citas y referencias para las fuentes consultadas.

La tesis no ha sido autoplagiada, es decir, no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional.

Los datos presentados en los resultados son reales, no han sido falseados, ni duplicados, ni copiados y por tanto los resultados que se presentan en la tesis se constituirán en aportes a la realidad investigada.

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

Lima, 18 de enero de 2020

Martin Elifio Montoya Ortecho

DNI N° 10799595

Índice

Índice de tablas

Índice de figuras

Resumen

El proceso de realizar una evaluación de riesgos de seguridad de la información tiene como objetivo mitigar los niveles de riesgos ante una materialización de amenazas que pueden afectar a los activos de información relevantes y por ende a los procesos de una organización. No obstante, no todo control de seguridad tiene cien por ciento seguro, encontramos vulnerabilidades abiertas que pueden ser explotadas malintencionadamente cuando no se tiene claro cuales son esas debilidades. Es importante que el objetivo de este trabajo de investigación describa claramente los tres componentes importantes para gestionar los riesgos, entender bien el procedimiento de evaluación de riesgos que conlleva a una identificación de riesgos, análisis de riesgos y valoración de riesgos.

Los componentes están asociados a una metodología que me va a permitir saber cuáles son las fases. Esta metodología está basada en activos, amenazas, vulnerabilidades, riesgos bajo la norma técnica NTP-ISO/IEC 27005 versión 2018. El tipo de investigación es básica de nivel descriptivo, es decir, me va a permitir describir las fases de la realización descriptiva aplicadas en las áreas de la Oficina General de Investigación y Transferencia Tecnológica – OGITT. Los resultados mas importantes obtenidos en el trabajo de investigación fueron la identificación de los niveles de riesgos de la información de cada área de la OGITT, saber la cantidad de riesgos de nivel Muy Crítico y Crítico están expuestos y que grado de impacto económico, legal, jurídico, financiero o de imagen podría ocurrir sino aplico una metodología de gestión de riesgos de seguridad de la información. Concluyo con una determinación muy importante y es saber cuáles son los riesgos prioritarios y debe saber el representante legal de la institución para la toma de decisiones futuras aplicando estrategias de seguridad e implementación de controles necesarios.

Palabras claves: Evaluación, riesgo, seguridad, información.

Abstract

The process of conducting an information security risk assessment aims to mitigate the levels of risks in the face of a materialization of threats that may affect the relevant information assets and therefore the processes of an organization. However, not every security control has one hundred percent secure, we find open vulnerabilities that can be exploited maliciously when it is not clear what those weaknesses are. It is important that the objective of this research work clearly describes the three important components for managing risks, understanding the risk assessment procedure that involves risk identification, risk analysis and risk assessment.

The components are associated with a methodology that will allow me to know protocols are the phases. This methodology is based on the technical standard NTP-ISO / IEC 27005 version 2018. The type of research is basic of descriptive level, that is, it will allow me to describe the phases of the descriptive realization applied in the areas of the General Office of Research and Technology Transfer - OGITT. The most important results detected in the research work were the identification of the risk levels of the information of each area of the OGITT, knowing the amount of risks of level Very critical and critical are determined and the degree of economic, legal impact, Legal, financial or image could solve the problem but an information security risk management methodology. I conclude with a very important determination and that is to know what are the priority risks and should know the legal representative of the institution for future decision making applying security strategies and implementation of necessary controls.

Keywords: Evaluation, risk, security, information

I. Introducción

En el ámbito internacional las organizaciones como Industrial Automation Agedum (México), Roche Ecuador S.A. (Ecuador),m Universidad Politécnica de Madrid (España) instituciones que son parte de este estudio, producen información que están ligadas al desarrollo de sus procesos y de sus sistemas de información, y para protegerlo es un problema organizacional en el que la solución es mucho más que contratar al mejor agente especializado de seguridad. Estas organizaciones no están ajenas a los riesgos, y deben estar preparadas puesto que por falta de ello, están expuestos a robo de información confidencial, robo de contraseñas, ataques cibernéticos, amenazas que son causados por una falta organizacional de una correcta Evaluación de Riesgos de Seguridad de la Información, ERSI, en adelante. En el estado nacional, aún no se ha logrado la conciencia de una cultura de prevención en las instituciones, es decir, no se ha logrado cerrar brechas de seguridad, donde me permita gestionar riesgos mediante mecanismos estandarizados o normas que puedan ser útiles y muy necesarias para una prevención de riesgos. En los últimos años en las empresas peruanas han aumentado en 600% los ataques en seguridad de la información entre los más comunes se encuentra denegación de servicio a las redes, robo de información electrónica o ransomware, accesos a áreas no autorizadas, robo de documento confidenciales, entre otros. Esto refleja que los sistemas de seguridad de la información aún se encuentran en niveles bajos de madurez, con planes de gestión de riesgos no ejecutados o irregular, a menudo se gestiona los riesgos como un silo aislado dentro de la organización. Entre las empresas más afectadas son las entidades financieras, entidades de salud, entidades educativas, entre otras y es fundamental una gestión en seguridad de la información para mitigar los riesgos ante amenazas en un mundo interconectado, y las principales vulnerabilidades que sufre toda organización es la falta de una correcta evaluación de riesgos a la información en sus procesos como parte de sus actividades.

La Oficina General de Investigación y Transferencia Tecnológica – OGITT, cuenta con un proceso llamado Autorización de Ensayos Clínicos con áreas involucradas como la Dirección General de Investigación y Transferencia Tecnológica, Oficina Ejecutiva de Investigación, Trámite Documentario, Ensayos Clínicos, Archivo y como oficina de apoyo el área de Tecnología de Información (TI). Estas oficinas cuentan con áreas donde existe un riesgo constante de fuga de información o perdida de documentos de investigación

debido a que se encuentra expuesta a robo de documentos físicos o archivos electrónicos, ambientes no controlados sin las medidas de seguridad perimetral necesaria, puesto que son lugares vulnerables y se requiere de una buena evaluación de riesgos de seguridad de la información. Dentro de si riesgos que pueden existir sobre todo el área más vulnerable es la de "Evaluación de Ensayos Clínicos". Existen riesgos como el robo de documentos por ingreso de personas no autorizadas o por falta de controles físicos, transferencia de información no autorizada, estos riesgos son muy latente puesto que los documentos se encuentran expuestos en lugares que no tiene un armario especifico con llave o que no están protegidas con una sólida contraseña. La falta de controles físicos de entrada expone una amenaza para el área, ya que no cuenta con un registro de identificación de personas externas y que usen fotocheck de identificación. El área de investigación genera documentos que son confidenciales para la organización, y están expuestas a la divulgación por su falta de seguridad, sobre todo la ausencia de concientización sobre estos temas. Un problema que se ha identificado también es la falta de fluido eléctrico por apagones que han suscitado varias veces en el año anterior, esto ha causado que los equipos de cómputo hayan sufrido variaciones de voltaje, puesto que el área de competente en la materia no ha fortalecido los estabilizadores de voltaje. Este documento que trae lo que se ha investigado pretende evaluar la gestión de riesgos en sus dimensiones como la identificación de riesgo, análisis de riesgo y valoración del riesgo basado en la norma NTP-ISO/IEC 27005:2018 "Gestión de Riesgos de Seguridad de la Información" con el objetivo de proporcionar directrices para gestionar los riesgos.

La necesidad de contar con revisiones procedentes nacionales e internacionales vemos en el país español, realizado por Molina (2015), tuvo como objetivo desarrollar una planificación de prevención relacionado a las tecnologías que se ejecutó al centro de administración y servicios de redes informáticas de la Escuela en mención, asimismo, se usó el método Magerit, describe como una metodología que permite el análisis de administración de riesgos de los software con la finalidad de mitigar los riesgos tecnológicos y entre sus etapas metodológico tenemos: definición de los elementos de valor y relevantes de la institución, determinar las inminencias exteriorizadas, modelación de probabilidad de ocurrencia, determinar salvaguardas, estimación del impacto y el riesgo residual. El autor concluyó que la metodología Margerit fue implementada para conocer la peligrosidad a los que están expuestos los activos en el área de informática de la

institución y usó la herramienta PILAR para ejecutar evaluaciones a los activos, amenazas y protección, a fin de identificar niveles de riesgo e impacto y a su vez identificar la necesidad de efectuar procedimientos y normas cuyo resultado de su ejecución fue la reducción de los riesgos y la protección de los recursos e información. Para el caso de México, Rudas (2017), tuvo como objetivo esbozar e implantar una propuesta como un modelo de piloto para la Gestión de Riesgos en proyectos de esta compañía mexicana, con el propósito de enfrentar de forma muy activa las posibilidades de situaciones que afecten los objetos de los proyectos, usó la metodología compuesta en 5 fases: 1) Monografía de teorías sobre Administración de Proyectos y Riesgos, 2) Exploración sistemática real de la compañía, 3) Bosquejo de una proforma del Modelo de Gestión de Riesgos, 4) Experiencia y 5) Archivo de efectos y entregables. Sus resultados tuvieron impactos positivos de la implementación de un Modelo de Gestión de Riesgos reflejando beneficios tangibles de reducción de costos y aseguramiento de calidad. En tanto que en Ecuador para Burgos (2014) su objetivo fue definir las raíces y los efectos de la problemática actual de Tecnología de información de la empresa estudiada y propuso un modelo de solución de estos. Tuvo como resultado influir positivamente en la eficacia y eficiencia operativa de la compañía, que permitió conocer las vulnerabilidades que podían convertirse en amenazas. Estableció una metodología de gestión de riesgo como alternativa optima de solución y control. Como conclusión la gestión de riesgos de TI permitió conocer sus vulnerabilidades y amenazas para gestionar óptimamente y ejecutar controles adecuados.

Otro antecedente internacional fue en Argentina, para Maggiori (2014) tuvo como objetivo desarrollar un modelo que evalúe la madurez de una gestión de seguridad de documentos que completó en actividades procedimentales institucional que permitió evaluar la madurez de tal gestión para preservar esta información contenida en el oficio institucional. Tuvo un método de separación trazada, más en el aspecto del trabajo en donde el programa de proteger toda información dejó de ser integral. Como resultado fue diseñar e implementar una guía para la estimación de madurez de resguardo y aseguramiento de la información integrada en los técnicas de oficio de la empresa, así como los riesgos asociados para la utilización de los datos y los controles determinados para su tratamiento. Como conclusión se llegó tomar la tabla de evaluación de los modelos CMMI, se denominó modelo de madurez a un modelo de capacidad.

España, Guillen (2014), tuvo como objetivo identificar, evaluar y mitigar los eventos que puedan afectar a la cadena de reprocesamiento de dispositivos de ortodoncia, compuesto

por los procesos de limpieza, clasificación, etc., Aumentando la gestión de riesgo la probabilidad de éxito en el cumplimiento de los objetivos estratégicos. La metodología fue aplicado mediante un modelo de gestión de riesgos planteado mediante una herramienta sistemática de identificación, estimación, tratamiento y prevención de riesgo. Su resultado en que el uso de los procedimientos, plantilla, conceptos y herramientas de TI, fueron correctamente asimilados lo que permitió identificar los riesgos del proceso de clasificación, se asignó categoría de riesgos, la estimación de probabilidad, consecuencia y sus riesgos. Se concluyó que el proceso de gestión de riesgos administra eficazmente los riesgos de las actividades de ortodoncia, se afirmó la resultante del estudio usando una herramienta de gestión de riesgos.

Así también se consideró estudios importantes en el ámbito nacional como en el caso presentado por Pinto (2017) su objetivo estuvo determinado en la función que hay entre la administración y sus riesgos del SI en la institución policial. Se ejecutó la tesis de tipo básica, con bosquejo no experimental y de corte transversal. Se empleó la metodología estadístico de correlación. La población estuvo conformada por 117 docentes de la escuela en mención tomando toda la población como muestra. Tuvo como resultados estadísticos entre sus dimensiones información interna, información corporativa y riesgos de seguridad existiendo una relación inversa y con una magnitud de correlación moderada. Concluyó que han sido referenciadas de la gestión de riesgos y la SI, afirmó que existe analogías entre ambas.

Ayala (2017), tuvo como objetivo fijar el efecto de la implementación de la metodología del SGSI para el procedimiento que administra los riesgos. Uso la técnica del SGSI referida a la norma internacional ISO 27001) que el mejoramiento del proceso de gestión. Tuvo como resultado cuantitativamente su medición correspondiente, consiguiendo mitigar de 3.72 a 3.09, figurando un 17%. Por lo que se determinó la nivelación del riesgo más críticos identificándose la reducción de los mismos. En este trabajo de investigación concluyo que se logró la disminución de los controles inexistentes en 72% y aumento de los que si existen en 76%.

Asimismo, Tarrillo (2016), tuvo como objetivo principal saber cómo está influenciando la gestión de riesgos de esta zona registral. El autor expresó a continuación las conclusiones más relevantes: Podemos ver que hay acercamiento de cómo se gestiona los

riesgos en el aseguramiento de los documentos físicos y electrónicos en este lugar mencionado, se vio que hay un cálculo matemático de Pearson es 15.712, superior al Chí Cuadrado tabular con 4 grados de libertad (9.48), esto presenta analogía entre las variables de esta tesis de investigación. Tuvo como resultado que el nivel de riesgos de seguridad de la zona Registral el 52% de trabajadores que fueron encuestados se hizo ver una nivelación de riesgos muy Altos.

Para Llontop (2018), su objetivo fue hacer un demo de un modelado que ha permitido hacer un trabajo de administración y prevención de TI, que sirvió para una mejora efectiva para la servicio de riesgos en entidades con ambientes virtualizadas. La metodología se basó en la hipótesis de Westerman y estándares como ISO 17799, ISO 27001, metodología MagerIT. Tuvo como resultado la demostración del progreso de la validez en la gestión de riesgos de Tecnología de la Información (TI). Los resultados teniendo un enfoque cuantitativo se basó en la obtención de manera numerada por muestras estadísticas con una investigación elemental basándose en conocimiento anterior y posee un diseñado descriptivo comparativo. El autor concluye que este planeamiento tiene una validez que se acepta, su proceso de gobernanza de riesgo es aceptable y la cultura consiente de los riesgos tiene nivel aceptable.

Otoya (2018), en su trabajo de investigación tuvo el objeto establecer el predominio para administrar el riesgo tecnológico para la prevención de los mismos, cuyo punto importante es la identificar el predominio que se gestiona en las amenazas tecnológicas, la misma manera reconocer el impacto potencial de ejecución de riesgos de TI. Se basó la metodología Margerit acoplada a la estandarización de la I.S.O 31000. (Revisada, 2016). (Primera ed.). Tuvo como resultado la gestión de riesgos de un punto visible de análisis una visión estructurada que nos permitió en la evaluación de los riesgos. El autor concluye que se evidencia un predominio resaltante de la gestión de riesgos tecnológicos para el reforzamiento seguro de toda la información llegando a una nivelación alto obteniendo este una valoración considerable de 0.035 y una dependencia de esta variable seguridad del 44%.

Se revisó la literatura relacionada a la variable de estudio evaluación de riesgo y entre los diferentes autores se consideró a Araujo (2017), quien definió, el procedimiento por el cual la institución emplea conocimiento valuado de un evento de probabilidad en la

organización y se ha valorizado estas acciones dentro y fuera de la organización a fin de ser identificable en caso sea suprimidos, también García y Salazar (2005) la Evaluación de riesgos lo definió como un proceso dirigido a la estimación de la magnitud de aquellos riesgos que no hayan podido evitarse, obteniendo de esta manera la información necesaria para la toma de decisiones apropiadas sobre la necesidad de adoptar medidas preventivas. La definición señalada sobre Evaluación del Riesgo como lo menciona la Norma Española UNE-ISO 31000 Gestión del Riesgo – Marzo 2018, lo menciona como el proceso internacional de identificación del riesgo, análisis del riesgo y valoración del riesgo. Así como también el documento RCG nº 320, 2006, señala como el proceso que identifica y analiza los riesgos expuestos a la organización que permita obtener sus objetivos y una preparación ante una respuesta considerable. La evaluación de riesgos incluye las actividades para la administración de riesgos, que incorpora: realizar un plan, identificación, valoración, resultados y el seguimiento de los riesgos de la institución.

La evaluación de riesgo se encuentra fundamentada en la Norma NTP-ISO/IEC 27005:2018, lo que significa que expresa una determinación del valor de los activos de información, identificación de las amenazas aplicables y las vulnerabilidades existentes (o podrían existir), identificación de los objetos de prevención existente y sus efectos en el riesgo que se ha encontrado, asimismo la determinación de las consecuencias potenciales y finalmente prioriza los riesgos derivados y los ordena contra el conjunto de criterios de valoración del riesgo en el contexto establecido.

Los componentes de evaluación de riesgo de acuerdo con la norma NTP-ISO/IEC 27005 "Gestión de Riesgos de Seguridad de la Información" son: (a) Identificación de Riesgos, (b) Análisis de Riesgo y (c) Valoración de Riesgo. Las mismas que, se ha considerado en la presente tesis como las dimensiones de la evaluación de riesgo.

Es necesario definir cada una de ellas, considerando como referente la conceptualización de Araujo (2017), quien mencionó que la primera dimensión, Identificación de Riesgos, está comprendido en una mezcla de métodos concatenadas a técnicas para reforzamiento. Lo que pueden haber situaciones anteriores como por ejemplo técnicas de referencias generalizadas. Para este tipo de identificación tuvo como input la experiencia de la institución u organización en relación a las consecuencias provenientes futuros.

Según ISO 31000 (2018), Identificación de Riesgo su propósito es hallar, reconocer y referir los riesgos que ayuden o impidan a las empresas la obtención de resultados. Para el allanamiento de los riesgos es vital tener toda información oportuna, adecuada y sobre todo actual que también es importante.

Según NTP-ISO/IEC 27005 (2018), Identificación de Riesgo su propósito es establecer que podría suceder para producir una potencial perdida, y saber cómo, cuándo y por qué la sustracción podría suceder.

La Identificación de Riesgos que se da por inicio con la identificación de los activos de información que son clasificados en cinco tipos: Información, software, Físico, Personas y Servicio, el cual debe ser definido los aspectos de seguridad de la información (confidencialidad, integridad y disponibilidad - CID) para determinar el valor de cada activo de información.

Dimensión (b) Análisis de Riesgos, al respecto Ávila (2005), considera como principal fundamento la creación de valoración para una organización. Cuando es administrado todos los riesgos lo tiene enumerado en 5 pasos como así lo menciona: Primeramente identificar y escoger los riesgos. El establecer las limitaciones de aprobación de riesgos. Elección e implantación de metodología para la administración de los riesgos. Seguimiento y supervisión. Esta dimensión suministra un input a la evaluación de riesgos y a la toma de decisión en el caso que los riesgos requieran ser tratados, y sobre las estrategias y los métodos más adecuados. Esta dimensión también puede proporcionar elementos para la toma de decisiones, donde habrá que elegir y estas muestran otros niveles de riesgo.

Según ISO 31000 (2018), Análisis de Riesgos es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. También implica una consideración detallada de incertidumbre, fuentes de riesgo, consecuencia, probabilidades, eventos, escenarios, controles y su eficacia.

Según NTP-ISO/IEC 27005 (2018), Análisis del Riesgo se lleva a cabo con diversos grados de detalle en función de la criticidad de los activos, el alcance de las vulnerabilidades conocidas, y los incidentes en los que se vio involucrada la organización.

El Análisis de riesgo se trata de la identificación de amenazas, vulnerabilidades, la evaluación del impacto, las probabilidades de ocurrencia de amenazas, esto se evalúa según el nivel al que está expuesta o comprometida el CIP.

Dimensión (c) Valoración de Riesgos, según NTP-ISO/IEC 27005 (2018) lo definió como el uso del conocimiento obtenido en el análisis de riesgo para la toma de decisiones sobre acciones futuras. Al respecto Araujo (2017), comentó que la evaluación de riesgos permite a la organización tener en cuenta cómo los riesgos que son considerados potenciales perjudican el cumplimiento de las metas trazadas y por ende sus objetivos. Se pone en marcha detallando como un estudio de temas únicamente relacionado sobre riesgos se hayan querido realizar una evaluación. La meta es mostrar toda información relacionado a los riesgos para que se estime su consecuencia, período, réplica e impacto.

Según ISO 31000 (2018), Valoración del Riesgos, el motivo es apoyar a todas las decisiones. Requiere hacer una comparación de resultados del análisis del riesgo con los criterios del riesgo determinado para establecer cuando se requiere una acción más.

La Evaluación de Riesgos determina el valor de los activos de información, identifica las acciones que causan daño y las debilidades que existen, identifica los controles existentes y sus efectos en el riesgo identificado, determina las consecuencias potenciales y finalmente prioriza los riesgos derivados y los ordena contra el conjunto de criterios de valoración del riesgo en el contexto establecido, “NTP-ISO/IEC 27005:2018”.

Se planteó la formulación del problema teniendo en cuenta el problema general: ¿Cómo se da la evaluación de riesgo de seguridad de información en las diferentes áreas, según ISO 27005, OGITT - Instituto Nacional de Salud? y los problemas Específicos: (1) ¿De qué manera se da la identificación de riesgo de seguridad de información en las diferentes áreas, según ISO 27005, OGITT - Instituto Nacional de Salud? (2) ¿De qué manera se da el análisis de riesgo de seguridad de la información en las diferentes áreas, según ISO 27005, OGITT - Instituto Nacional de Salud? (3) ¿Como se da el análisis de riesgo de seguridad de la información en las diferentes áreas, según norma NTP-ISO/IEC 27005:2018 en OGITT del Instituto Nacional de Salud 2019? (3) ¿Cómo se da la valorización del riesgo de seguridad de la información en las diferentes áreas, según ISO 27005, OGITT - Instituto Nacional de Salud?

El presente trabajo se justifica desde una perspectiva teórica, práctica, normativa y metodológica, los cuales se sustentan: (a) justificación teórica: surge como requerimiento de realizar una evaluación de los riesgos mediante una metodología establecida para generar las evaluaciones y evidencias del estado situacional de las probabilidades de impacto. Los niveles de estos riesgos van a determinar el criterio de los de los elementos de valor de la institución que están expuestas ante amenazas, vulnerabilidades, probabilidad de ocurrencia y el impacto que pueda causar la explotación de un riesgo al materializarse. Este estudio debe generar que los usuarios conozcan y sepan desarrollar las buenas prácticas del SGSI bajo el proceso de gestión de riesgos. (b) Desde el punto de vista práctico, este estudio tiene la justificación práctica de implementar herramientas, es decir, documentos de sistema de gestión que permite recoger la información de todos los componentes (identificación, análisis y valoración de riesgos) registrándolo en formularios, matrices, determinación de los niveles y valorización de los riesgos para un tratamiento de riesgos adecuado. (c) Justificación metodológica: porque tiene un procedimiento estructurado bajo una estandarización internacional. Su metodología permite tener resultados objetivos en la etapa de la identificación de riesgos, análisis de riesgos y valoración de riesgos, lo cual genera información importante para llevar acabo los niveles de riesgos y su tratamiento. (d) Justificación normativa: está basado en la norma técnica NTP-ISO/IEC 27005:2018 y tiene como nombre Tecnología de la Información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información. Esta norma proporciona directrices para la gestión de riesgos de seguridad de la información.

El presente documento de tesis de investigación tiene como planteamiento el objetivo general y los objetivos específicos; se considera como objetivo general; Describir la evaluación de riesgo de seguridad de información según ISO 27005, OGITT - Instituto Nacional de Salud, Seguidamente se considera los objetivos específicos como: (a) Describir la identificación de riesgo de seguridad de información según ISO 27005, OGITT - Instituto Nacional de Salud. (b) Describir el análisis de riesgo de seguridad de la información según ISO 27005, OGITT - Instituto Nacional de Salud. (c) Describir la valorización del riesgo de seguridad de la información según ISO 27005, OGITT - Instituto Nacional de Salud. OGITT es la Oficina General Tecnológica comprendida en 6

áreas llamadas Trámite Documentario, Dirección Ejecutiva de Investigación, Evaluación de Ensayos Clínicos, Dirección General, Archivo y TI (Tecnología de Información).

II. Método

2.1. Tipo y diseño de investigación

Paradigma.

Al respecto Martínez (2013), describe el paradigma positivista que indaga los acontecimientos u orígenes de los fenómenos generales independiente de las situaciones subjetivas de los individuos; estableciendo que solo un conocimiento aprobado es el científico que acata a tales principios de metodologías únicas. Se caracteriza su naturaleza cuantitativa para asegurar la precisión. Para el positivismo la realidad es absoluta se rige por leyes y mecanismos naturales. De ahí se determina los diferentes factores de un estudio Field (2009).

Enfoque.

Este trabajo o tesis se realizó enfocado de manera cuantitativa porque mide la variable de estudio de evaluación de riesgo. Es observable y medible. Para Hernández, Fernández y Batista (2014) el enfoque cuantitativo "es secuencial y probatorio. Cada fase precede a la siguiente y no se puede eludir los pasos". La secuencia que prescribe es la determinación del valor de los activos de información, identificación de amenazas, vulnerabilidades, probabilidad e impacto que conlleva seguidamente la identificación de riesgos y la determinación de sus niveles.

Tipo de investigación.

La investigación se realizó de forma básica con nivel descriptivo según la clasificación de Hernández, Fernández y Baptista (2014). La presente tesis de investigación se orientó al tipo de investigación básica, ya que se basa en el conocimiento previo que se plasma en el marco teórico para aplicarlo al caso de estudio.

Diseño.

Según Sánchez y Reyes (2015) definió que es diseño no experimental, es de corte transversal y es descriptivo simple. Es decir, en la presente tesis de investigación busca recoger la información actual con respecto a una situación previamente determinada, dado el objetivo de estudio se describió la ERSI. El diseño de la investigación se basa en la

caracterización de la variable descrita en sus tres dimensiones (identificación de riesgos, análisis de riesgos y valorización del riesgo) desarrollada bajo una base de datos de probabilidad e impacto y una matriz de niveles de riesgos que la componen.

De esta manera, el diseño del esquema es el siguiente:

M _____ O

Leyenda:

M: muestra 40, trabajadores de la Oficina de (OGITT).

O1: Variable 1, Evaluación de Riesgos de Seguridad de la Información.

2.2. Operacionalización de la variable

Definición Conceptual de las variables.

***Variable 1; Evaluación de* Riesgos de Seguridad de la Información**

Comité Técnico de Normalización de Codificaciones e intercambio electrónico de datos.
La evaluación del riesgo de seguridad de la información establece su valor para los activos de información, identifica las amenazas aplicables y las vulnerabilidades que existen (o podrían existir), señala los controles existentes y sus efectos en el riesgo identificado, determina los impactos potenciales y los riesgos.

La Evaluación de riesgos va permitir mitigar los peligros que están expuestas la información confidencial, secreta o de investigación; este último, la OGITT del Instituto Nacional de Salud (INS) es una organización que asesora a la Alta Dirección, encargada de desarrollar investigación y tecnología en salud y de su transferencia al sector salud como es el Ministerio de Salud como ente rector principal; es por ello que una de las principales preocupaciones de la institución son la información con riesgos críticos y altos, que requiere definir directrices de prevención con la finalidad de mitigarlos y mantener a salvo los productos de documentos de investigación. Las áreas principales de OGITT, son la Oficina Ejecutiva de Investigación (OEI), es la encargada del desarrollo de la investigación y de la tecnología en salud a nivel institucional y tiene la función proponer lineamientos de política en salud, promover la investigación de los problemas prioritarios de salud y el desarrollo de las tecnologías, ésta oficina tiene una área crítica llamada “Área de Ensayos Clínicos”, en ésta área se procesan los documentos de ensayos clínicos por parte de los patrocinadores (son profesionales peruanos o extranjeros que realizan los ensayos clínicos

en el Perú) es un área donde se produce mucha información interna y confidencial, física y electrónica, que se transmite por conductos electrónicos como correos, carpetas de red, equipos de cómputo en red, traslado de documentos de una área a otra.

Definición Operacional de Evaluación de Riesgos.

En base a 104 activos de información divididos en tres dimensiones, cada una cuenta con indicadores por cada dimensión. Los niveles y escalas utilizados son:

2.3. Población

Sánchez y Reyes (2018), definió la población, como un conjunto de elementos que pueden ser individuos, objetos o hechos, que presentan características o criterios comunes, lo cual permite identificarlos en un área de interés para ser objeto de estudio e hipótesis de una investigación. Cuando estos elementos son personas se le llama población y cuando no lo son es conveniente nombrarlo como universo de estudio (p. 201).

La presente investigación cuenta con una población censal de 40 trabajadores en seis áreas como Trámite Documentario, Dirección Ejecutiva de Investigación, Evaluación de Ensayos Clínicos, Dirección General, Archivo y TI (Tecnología de Información) entre funcionarios y empleados de la OGITT del Instituto Nacional de Salud (INS).

2.4. Técnicas e instrumentos de recolección de datos y validez

Tabla 1

Distribución del personal de OGITT del INS

Dirección de General	Cantidad
Director General	01
Director Ejecutivo	02
Personal técnico y administrativo	37
Total:	40

Está definida como “medios que el investigador viene a levantar todo dato que se pida de un contexto real o fenómeno en relación con los objetivos. (Sánchez y Reyes, p.149). La técnica en esta investigación será mediante la técnica de observación estructurada porque se trabaja con fichas de observación donde se recoge la identificación de riesgos con tablas para los activos de información, tablas de amenazas y vulnerabilidades; para el análisis de riesgos será mediante tablas de evaluación de impacto, evaluación de probabilidad e

identificación de los riesgos; y para la valorización de los riesgos mediante una matriz que mide el nivel de los riesgos para determinar los riesgos priorizados.

Instrumento.

Para hacer validar el instrumento, en línea frecuente, hace referencia a la altura en que un instrumento verdaderamente calcula esta variable que quiere medir (Hernández, Fernández y Baptista, 2014). Las fichas de observación son llamadas "Lista de Activos de Información", Edición N° 02 aprobada con Resolución Directoral N° 005-2019-DG-OGIS/INS y "Evaluación de Riesgos de Activos de Información" Edición N° 02 aprobada con Resolución Directoral N° 005-2019-DG-OGIS/INS.

La primera ficha de observación es una herramienta que me permite recoger los nombres de los activos de información consignando sus características y valorizaciones según sus niveles de los aspectos de seguridad como son el CID y su clasificación (confidencial, interno o público). La segunda ficha de observación es una instrumento que me admite hacer un estudio de amenazas, vulnerabilidades, la probabilidad (en escala de 5 valores "Muy alta=5", "Alta=4", "Moderada=3", "Baja=2" y "Muy baja=1"), impacto (es escala de 5 valores "Catastrófico=5", "Significativo=4", "Moderado=3", "Menor=2" y "No significativo=1") y niveles de riesgo definido como Extremo, Alto, Mediano y Bajo.

Las fichas de observación se describen en "Lista de activos de información" distribuido en mi primera dimensión "Identificación de Riesgos", me permitió recoger datos de los activos de información y sus características. En su valorización me permitió evaluar en función a los niveles de los aspectos de seguridad de la información como son CID, es decir según su combinación se determinó su criticidad como "No significativo", "Menor", "Moderado", "Crítico", "Muy crítico". La ficha de observación "Evaluación de Riesgos de Activos de Información" distribuido en mi segunda dimensión "Análisis de Riesgos", me permitió recoger información de los activos de información como sus amenazas, vulnerabilidades, las escalas del impacto y probabilidad, y la determinación del nivel del riesgo.

Validación del instrumento

Validez de contenido.

Según Hernández et al (2014) la validez es una graduación en que los instrumentos permitan realizar una medición a una variable en la que se busca hacer medir. Cuando se quiera hacer valido un instrumento, definitivamente se efectuó el sometimiento a considerar para juicio de expertos. Para Hernández et al (2014), este juicio de expertos es el grado en que la variable tiene una medición a través de un instrumento según y en acuerdos de expertos del tema. En este caso se consideró "aplicable" para la muestra de

Tabla 2

Validación del instrumento por juicio de expertos

N°	Grado académico	Nombres y apellidos del experto	Dictamen
1	DOCTORA	ELIANASOLEDAD CASTAÑEDA NUÑEZ	Aplicable
2	DOCTORA	ROSA VILLALBA	Aplicable

estudio elegida.

2.5. Procedimiento

El procedimiento de mi tesis de investigación se basa para Evaluación de Riesgos de Seguridad de la información. Empieza con identificación de los activos de información del proceso que ha definido la OGITT, en este caso el proceso de "Autorización de Ensayo Clínicos" comprendidos en las área de Trámite Documentario, Oficina Ejecutiva de Investigación, Evaluación de Ensayos Clínicos, Archivo, Dirección General y Tecnología. Los activos de información están categorizados en información, software, hardware, personas y servicios (ver anexos) de los anexos lo que da facilidad de añadirle una codificación, características, que tipo de activo es, su ubicación (físico o digital), el propietario, su frecuencia de uso y está clasificada como pública, uso interno y confidencial. En este punto vemos también su aspecto de seguridad relacionado al CID según sea su valor. Esta información una vez obtenida, se realiza la identificación de amenazas y vulnerabilidades a la que encontramos exposición el activo de información valorado como crítico o muy crítico, esto se tomó como referencia el registro de amenazas (ver anexos) de los anexo. y registro de vulnerabilidades (ver anexos). Toda esta

información se registra en la ficha de observación llamada “Lista de Activos de Información”.

Una vez recogido esta información, se procede a analizar los riesgos, comprendido en la evaluación del impacto de la amenaza, lo cual, se ha establecido una escala de cinco niveles, (ver anexos). Asimismo, se realizó la evaluación de posibilidad de que ocurra peligros de acuerdo al que está expuesta o comprendida la CID de los activos de información. Para lo cual se ha establecido en la escala de cinco niveles, (ver anexos).

Se determina el nivel del riesgo (ver anexos), a los cuales están expuesto los activos de información, multiplicando el valor de la probabilidad con el valor del impacto:

Impacto x Probabilidad = Nivel del Riesgo

Según el resultado obtenido, se identifica en la Matriz de Probabilidad e Impacto, llamado también Matriz de Riesgos o Mapa de Calor (ver anexos) nivel de riesgo. Toda esta información se registra en la ficha de observación llamada “Evaluación de Riesgos de Activos de Información.

Luego de recoger la información con las fichas de observación se usaron las tablas correspondientes (ver anexo). Luego se provino a la tabulación de los resultados dejando listo para el procesamiento estadístico. Cabe señalar que estas fichas de observación cuentan con sus resoluciones directorales como se mencionó en el punto anterior Instrumentos.

2.6. Método de análisis de datos

Consistió en valorizar todos los activos que mide la relación con los tres pilares de seguridad usando los criterios Alto, Medio y Bajo para cada uno de ellos. Según la combinación se dio la valorización denominados “No Significativo”, “Menor, Moderado”, “Crítico” y “Muy Crítico”. Para definir las valorizaciones se usó formulas y administración de reglas en la herramienta Excel dándole los formatos a las celdas según sea los colores que corresponde a cada nivel.

Luego se procedió a clasificar el activo de acuerdo con lo siguiente: “Información Pública”, “Información de Uso Interno” e “Información Confidencial”

Se determinó de la siguiente manera:

Si determino que la Confidencialidad es Baja, la Clasificación de la información es Pública, si la Confidencialidad es Media, la Clasificación de la información es Interna, si la Confidencialidad es Alta, la Clasificación de la información es Confidencial. Esta información se registró en la ficha de observación llamada "Lista de estos importantes Activos". Estos activos de información que fueron identificados con los valores "Crítico" y "Muy Crítico" solo estos serán analizados en la fase de análisis de riesgos.

En este paso que analiza los riesgos consistió registrar las amenazas y las vulnerabilidades según los códigos hayan sido asignado en las tablas 21 y 22. Luego con los usuarios de cada área se procedió a evaluar la probabilidad, el impacto y los niveles de riesgo.

En la valorización de la probabilidad se dio la siguiente escala:

Muy Alta = 5; Alta = 4; Moderada = 3, Baja = 2; Muy Baja = 1.

En la valorización del impacto se dio la siguiente escala:

Catastrófico=5; Significativo=4; Moderado=3, Menor=2; No significativo=1.

Los resultados de este proceso de evaluación de riesgos de SI se dieron en función a la cantidad y niveles de riesgos de las áreas de Trámite Documentario, Oficina Ejecutiva de Investigación, Evaluación de Ensayos Clínicos, Archivo, Dirección General y Tecnología de Información de la Oficina General (OGITT) del INS.

2.7. Aspectos éticos

La información mostrada en esta investigación fue recogida por el área especializada en el tema de la Oficina General de Información y Sistemas del INS. Se ejecutó adecuadamente sin ningún tipo de falsificaciones, pues esta información está fundamentada en el instrumento aplicado. La tesis que se investiga cuenta con la autorización (Director General y Directores Ejecutivos de esta área general en mención OGITT.

III. Resultados

3.1 Resultados descriptivos

Dimensión 1 - Identificación de Riesgos

Tabla 3

Frecuencias y porcentajes para la dimensión Identificación de Riesgos

IDENTIFICACIÓN DE RIESGOS	Trámite Documentario		Dirección Ejecutiva de Investigación		Evaluación de Ensayos Clínicos		Dirección General OGITT		Archivo		Tecnología de Información (TI)	
Niveles	Frec.	%	Frec.	%	Frec.	%	Frec.	%	Frec.	%	Frec.	%
No significativo	0	0	0	0	0	0	1	8	0	0	0	0
Menor	24	75	1	8	0	0	0	0	1	6	0	0
Moderado	4	12.5	6	50	6	33	9	69	12	71	2	17
Crítico	4	13	2	17	9	50	2	15	3	18	10	83
Muy crítico	0	0.00	3	25	3	17	1	8	1	6	0	0.00
Total de activos identificados	32	100.00	12	100.00	18	100.00	13	100.00	17	100.00	12	100.00

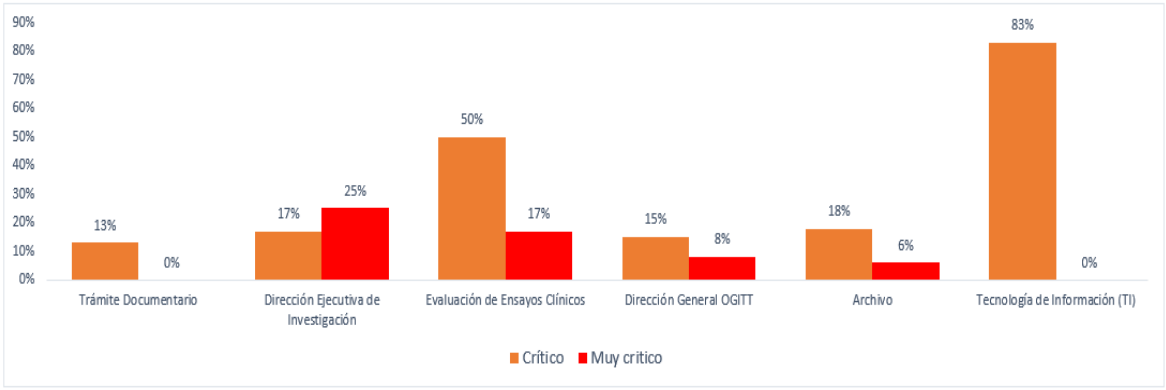


Figura 1. Porcentaje de la dimensión Identificación de Riesgos

En cuanto a la dimensión 1 “Identificación de Riesgos” de la variable “Evaluación de Riesgos” tuvo el resultado el nivel o niveles que valorizan estos activos de las áreas de la Oficina de OGITT. El área de mayor porcentaje con activos críticos es Tecnología de Información (TI) con 83% y con mayor porcentaje de activos muy críticos es Dirección Ejecutiva de Investigación con 25%.

Dimensión 1: Identificación de Riesgos

Tabla 4
Valoración de activos

Total activos de información	104
Activos con valor Crítico	30
Activos con valor Muy Crítico	8

Podemos decir que: $\frac{\text{Activos con valor Crítico}}{\text{Total activos de información}} \times 100$

$\frac{30}{104} \times 100 =$ **29%**

$\frac{\text{Activos con valor Muy Crítico}}{\text{Total activos de información}} \times 100$

$\frac{8}{104} \times 100 =$ **8%**

El 37% del total de los activos de información tiene una valoración entre críticos y muy críticos.

Dimensión 2 - Análisis de Riesgos

Tabla 5

Frecuencias y porcentajes para la dimensión Análisis de Riesgo.

ANÁLISIS DE RIESGOS	Trámite Documentario		Dirección Ejecutiva de Investigación		Evaluación de Ensayos Clínicos		Dirección General OGITT		Archivo		Tecnología de Información (TI)	
Niveles	Frec.	%	Frec.	%	Frec.	%	Frec.	%	Frec.	%	Frec.	%
Extremo	0	0	0	0	2	4	0	0	0	0	0	0
Alto	4	25	6	46	15	27	0	0	11	29	13	33
Mediano	12	75	7	54	36	65	8	100	25	66	26	67
Bajo	0	0	0	0.00	2	4	0	0	2	5	0	0
Total de activos identificados	16	100	13	100	55	100	8	100	38	100	39	100

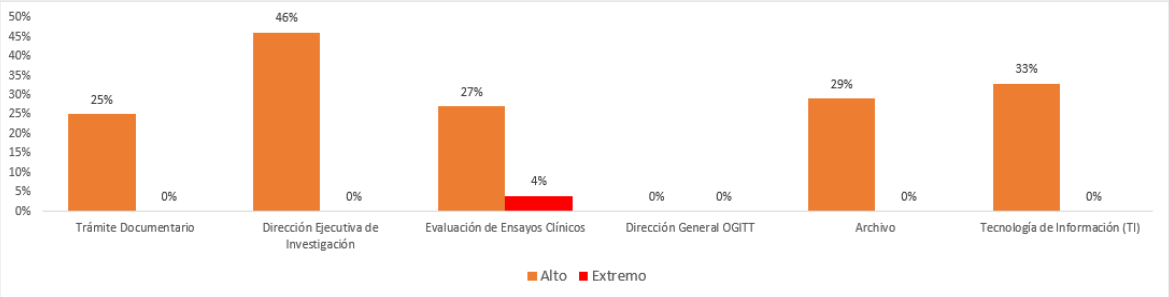


Figura 2. Porcentaje de la dimensión Análisis de Riesgo

En cuanto a la dimensión 2 “Análisis de Riesgos” de la variable “comités” considerando que los activos de información de la dimensión 1 que resultaron con nivel de valorización crítico y muy crítico, fueron sometidos al análisis de riesgos. Se tuvo como resultado que el área de mayor porcentaje con riesgos alto es Dirección Ejecutiva de Investigación con 46% y con mayor porcentaje de riesgo extremo es Evaluación de Ensayos Clínicos con 4%

Dimensión 2: Análisis de Riesgos.

Tabla 6

Niveles de riesgo

Total de riesgos de activos de información	169
Riesgos con nivel alto	49
Riesgos con nivel extremo	2

Podemos decir que:

$$\frac{\text{Riesgos con nivel Alto}}{\text{Total de riesgos de act. Inf.}} \times 100$$

$$\frac{49}{169} \times 100 = \mathbf{29\%}$$

$$\frac{\text{Riesgos con nivel Extremo}}{\text{Total de riesgos de act. Inf.}} \times 100$$

$$\frac{2}{169} \times 100 = \mathbf{1.2\%}$$

El 30% del total de los riesgos analizados, tienen niveles entre altos y extremos.

Dimensión 3 - Valorización del Riesgo

Tabla 7

Frecuencias y porcentajes para la dimensión Valoración del Riesgo

VALORIZACIÓN DE RIESGOS	Trámite Documentario		Dirección Ejecutiva de Investigación		Evaluación de Ensayos Clínicos		Dirección General OGITT		Archivo		Tecnología de Información (TI)	
Niveles	Frec.	%	Frec.	%	Frec.	%	Frec.	%	Frec.	%	Frec.	%
Extremo	0	0	0	0	2	4	0	0	0	0	0	0
Alto	4	25	6	46	15	27	0	0	11	29	13	33

En cuanto a la dimensión 3 “Valoración de Riesgos” de la variable “Evaluación de Riesgos” las áreas que tuvieron la mayor cantidad de riesgos con nivel extremo y alto son considerados prioritarios para una tratamiento de riesgos.

Tabla 8

Niveles de riesgo de los activos de información

Total de riesgos de activos de información	169
Riesgos con nivel alto	49
Riesgos con nivel extremo	2

Se dice que: $\frac{\text{Riesgos con nivel Alto}}{\text{Total de riesgos de act. Inf.}} \times 100$

$\frac{49}{169} \times 100 =$ **28.99%**

$\frac{\text{Riesgos con nivel Extremo}}{\text{Total de riesgos de act. Inf.}} \times 100$

$\frac{2}{169} \times 100 =$ **1.18%**

El 30.17% del total de los riesgos analizados, tienen niveles entre altos y extremos.

Variable. Evaluación de riesgo

Resultado general respecto a la variable Evaluación de Riesgos de Seguridad de la Información según ISO 27005 para la Oficina General de Investigación y Transferencia Tecnológica - OGITT del Instituto Nacional de Salud:

Tabla 9

Resultados finales de las dimensiones

Identificación de Riesgos			Análisis de Riesgos			Valoración de Riesgos		
Total de activos	104	100%	Total de riesgos	169	100%	Priorizados		
Crítico (C)	30	28%	Altos (A)	49	29%	Altos (A)	49	29%
Muy Crítico (MC)	8	7%	Extremos (E)	2	1%	Extremos (E)	2	1%
Total (C) y (MC)	38	37%	Total (A) y (E)	51	30%	Total (A) y (E)	51	30%

La tendencia de evaluación de riesgos es que el nivel de riesgo extremo se encuentra en el área de Evaluación de Ensayos Clínico y el nivel de riesgo alto se encuentra en el

área de la Dirección Ejecutiva de Investigación. Las áreas que tienen la menor cantidad de riesgos alto es la Dirección General de OGITT del INS.

Estas áreas con riesgo extremo y alto son las que están más expuestas por su vulnerabilidad y requiere de un tratamiento especializado, es decir, una planificación estratégica que implemente sus controles para asegurar toda información. Los riesgos con niveles medianos y bajos vistos en el análisis de riesgo, la institución decide aceptar y solo los de nivel alto y extremo serán tratados.

IV. Discusión

Habiendo aplicado mi variable Evaluación de Riesgos a través de las tres dimensiones correspondientes, el objetivo es describir cómo se lleva a cabo esta metodología que me va permitir determinar a valorarle estos activos, para identificar los peligros más latentes, sus debilidades, sus consecuencias en el riesgo que fueron encontrados, sus consecuencias, la priorización y los criterios de valorización.

La dimensión 1 denominada "Identificación de riesgo", consistió en la valorización de los activos de información para las áreas de la Oficina General de Investigación y Transferencia Tecnológica (OGITT). Previo a ello se realizó la identificación de los activos de información según como se ha clasificado como "Documentos", "Software", "Hardware", "Personas" y "Servicios" (ver anexos). De los 104 activos de información identificados de las 6 áreas, se generó las combinaciones de los niveles altos, medio o bajo en los aspectos de seguridad Confidencialidad, Integridad y Disponibilidad (ver anexos); ocho de los activos son valorizados de nivel Muy Crítico y 30 de nivel Crítico. Es decir que el 36% de mi población total de activos de información son considerados entre críticos y muy críticos; a estos 30 recurren a una identificación de amenazas, vulnerabilidades, controles implementados y su eficacia.

La Dimensión Identificación de Riesgo para Molina (2015) lo llama Modelo de Valor, que esta conforma a identificar activos estimados como principales, relación entre los activos, la valorización, su árbol de dependencia y su importancia que incurre en cada una de ellas. Usó la herramienta Pilar para la clasificación de sus activos como Activos esenciales, servicios internos, equipamiento, servicio subcontratado, instalaciones y personal. El autor determina la valoración de amenaza por activo, es decir, cada activo tiene diferentes tipos de amenaza y la valoración de activo por amenaza, es decir en cada amenaza está comprometido varios activos. Se empleó la herramienta Pilar para la identificación de activos definido como "Dependencia entre activos" y esto lo clasificó como "Activos esenciales", "Servicios Internos", "Equipamiento", "Servicios Subcontratados", "Instalaciones", y "Personal". La herramienta que usé en mi trabajo de investigación para la identificación de activos y su clasificación fue la ficha de observación llamada "Lista de Activos de Información" que me permite recoger los nombres de los activos y sus características.

En cuanto a la Dimensión Análisis de Riesgo, el autor lo denomina Estado de Riesgo, donde realiza la evaluación de consecuencias y riesgos de las amenazas que produce afectación a los activos; generación de riesgo acumulado, mide la criticidad de los riesgos. Es similar el trabajo del autor con mi tesis, pero, hay una diferencia, en esta etapa se ejecuta una evaluación de la probabilidad de ocurrencia ante amenazas por una escala del 1 al 5, donde 5 la probabilidad es muy alta y 1 es muy baja; la evaluación del impacto se trabaja mediante una escala del 1 al 5, donde 5 tiene nivel Catastrófico y 1 nivel No Significativo y el producto de ellos me determina el nivel de riesgo.

La Dimensión Valoración de Riesgos, el autor lo llama Riesgo Acumulado que mide los niveles críticos los cuales se encuentran expuesto. En mi caso, la valoración de riesgo se basa en la prioridad de los riesgos por sus niveles, es decir, los riesgos con nivel Extremo y los de nivel Alto tienen mayor relevancia para planificarlos a medidas de control con la finalidad de mitigar su riesgo.

Para Rudas (2017), en el caso de este autor buscó una manera práctica o experimental para plantear una guía de prevención (gestión) de los riesgos que pueda enfrontar eventos que ponen en peligro sus objetivos. Su método consistió en analizar patrones de Administración de Riesgos como son norma ISO 21500:2012, Estandarización PMI PMBOK (Project Management Institute), guía PRAM – APM (Association for Project Management) y Estándar PRINCE2 (Projects IN Controlled Environments). El diseño de su metodología consistió en el desarrollo de una investigación comprendido en cuatro fases como el estudio sobre teorías de gestión de riesgos, revisión sistemática de la empresa, diseño de propuesta del prevención de gestión de riesgos y experimentación y en base a ello presentó un diseño metodológico que describe la metodología aplicada y las fuentes de información. Hay una diferenciación con mi tesis de investigación, es que usé la norma técnica NTP-ISO/IEC 27005 versión 2018, que consiste en llevar acabo la gestión de riesgos de manera esquematizada y por fases. Pero en el fondo se virtualiza manteniendo un sentido similar que lleva a un objetivo.

En la Dimensión Análisis de Riesgo si hago una comparación con el modelo del autor en relación con la gestión de riesgos, está propuesto por cuatro procesos: Identificación, Análisis y Evaluación, Plan de respuesta y Seguimiento y Control. En este modelo no se emplea la identificación de activos de información, sino la generación de una lista de riesgos con base a eventos que podrían impactar el logro de sus proyectos, teniendo en

cuenta categoría de riesgos, lecciones aprendidas de otros proyectos, matriz de riesgos, banco de proyectos y documentación de proyectos. Asimismo emplea el Análisis y Evaluación de riesgo que consiste asignar valores a la probabilidad de cada riesgo en una escala de 1 a 5, 1 probabilidad muy baja de que ocurra, 2 probabilidad baja donde no es probable que ocurra, 3 probabilidad moderada que puede ocurrir, 4 probabilidad alta donde es altamente probable de que ocurra y 5 probabilidad muy alta que es casi seguro de que ocurra el evento. Así mismo se determina el impacto de cada riesgo en el éxito del proyecto (definido por el tiempo, costo y calidad) de en una escala de 1 a 5. Es muy similar a las escalas que se usó para la Dimensión Análisis de Riesgo del presente trabajo.

Esta Dimensión 2 denominada "Análisis de Riesgo", para el actual tesis de investigación se evaluó los niveles de impacto de la amenaza mediante una escala de 1 al 5 desde No significativo a Catastrófico, (ver anexos). Para la evaluación de las probabilidades de que ocurran amenazas mediante una escala de 1 al 5 desde Muy baja a Muy Alta, (ver anexos) y en la combinación de ellos se determinó los niveles de riesgo descrito como Extremo, Alto, Mediano y Bajo (ver anexos). Es decir, el producto de la probabilidad y la consecuencia (impacto) se evalúa el nivel del peligro (riegos), (ver anexos). El resultado de estas evaluaciones me determina la cantidad de los riesgos de cada área, la suma de ellos dio como resultado 169 riesgos identificados en total entre los niveles Extremo, Alto, Mediano, Bajo. El criterio de esta investigación de tesis es que los riesgos de nivel Extremo y Alto son los riesgos que serán tratados y los de nivel Mediano y Bajo la OGITT ha decidido aceptarlo.

V. Conclusiones

Primera. En relación con el objetivo específico 1 se concluye que:

Dentro de OGITT se ha logrado identificar 104 activos de información comprendidas entre las áreas de Trámite Documentario, Dirección Ejecutiva de Investigación, Dirección General, Evaluación de Ensayos Clínicos, Archivo y Tecnología de Información. En su valorización son 8 activos con valor Muy Crítico y 30 con valor Crítico. El área que obtuvo mayor cantidad con valor Muy Crítico es Evaluación de Ensayos Clínicos con 3 activos; y la mayor cantidad con valor Crítico es el área de Tecnología de Información con 83 activos. El área que obtuvo menos cantidad de activos con valor Menor es el área de Trámite Documentario con 24 activos.

Segunda. En relación con el segundo objetivo específico se da como conclusión que:

Se determinó el análisis de riesgos a los 38 activos de información con valoración Muy Crítico y Crítico valorados en la primera fase. De los 38 activos se identificó 169 riesgos de nivel Extremo, Alto, Mediano y Bajo. Se determinó 2 riesgos con nivel Extremo, 49 riesgos de nivel Alto, 114 riesgos de nivel Mediano y 4 riesgos de nivel Bajo. El área que obtuvo los riesgos Muy Alto es Evaluación de Ensayos Clínicos y el área que obtuvo riesgos Altos es la misma área en mención. El área que obtuvo riesgo Bajo es Archivo.

Tercera. En relación con el tercer objetivo se está concluyendo que:

Se determinó la valoración de riesgos en el sentido en que los riesgos de nivel Extremo y Alto son los riesgos prioritarios y definidos para su tratamiento.

Cuarta. Para el objetivo general se describió según como lo menciona en el titulo del presente trabajo que permite gestionarlos con la finalidad de tenerlo mapeado y reducir los peligros que están expuestas la información confidencial, secreta o de investigación que produce la Oficina General de Investigación y Transferencia Tecnológica (OGITT) y en cada una de sus áreas.

VI. Recomendaciones

Primera. En relación con la identificación de riesgos, recomiendo que la oficina de OGITT y a todas sus áreas comprendidas asegurar sus activos de información que han sido considerados con valoración Crítico y Muy Crítico con una capacitación de seguridad de la información haciendo relevancia la clasificación de los activos de información confidencial y secreta.

Segunda. En relación con el análisis de riesgo se recomienda implementar controles de seguridad de la información a los riesgos que tienen como resultado niveles Extremos y Altos, basándose del anexo A de la ISO 27001:2013 formulando el Plan de Tratamiento de Riesgos (PTR), asimismo, capacitar al personal sobre la gestión de estos controles con el apoyo de los especialistas en seguridad de la Información.

Tercera. En relación con la valoración de riesgos trabajado en este trabajo de investigación se recomienda priorizar estos activos con niveles Extremos y Altos asegurar su implementación con el apoyo de la alta dirección del INS, asimismo, una herramienta de administración y monitoreo riesgos que permita visualizar su tratamiento a cada uno de ellos, es decir, verificación de la aplicabilidad de los controles seleccionados por la organización.

Cuarta. Se recomienda también ampliar el alcance de aplicabilidad en los procesos de Evaluación de Riesgos donde se realice los tres componentes fundamentales descrito en su dimensionamiento. Tener en cuenta los procesos más críticos puesto que se maneja información sensible o confidencial.

Quinta. Hacer conocer a la jefatura del INS sobre el estado situacional los riesgos críticos organizativos con el fin de que se tomen mejores decisiones presupuestales a fin de cubrir todo proyecto relacionado a la gestión de riesgos en seguridad de la información.

Sexta. Elaborar el plan que evalúe riesgos que establezcan los periodos de evaluación en los tres procesos importantes que componen un macroproceso en la organización.

Referencias

Aguirre, D. (2014). *Diseño de un Sistema de Gestión de Seguridad de la Información para Servicios Postales del Perú S.A. (tesis de pregrado). Pontificia Universidad Católica del Perú.* http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/5677

Aguirre, J. y C. Aristizabal. (2013). *Diseño del Sistema de Gestión de Seguridad de la Información para el grupo empresarial La Ofrenda. (tesis de pregrado). Universidad Tecnológica de Pereira, Facultad de Ingenierías, Programa de Ingeniería de Sistemas y Computación Pereira.* https://core.ac.uk/download/pdf/71397730.pdf

Alexander, G., Alberto. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información; Óptica ISO/ IEC 27001:2005. Bogotá: Alfaomega Colombiana S.A.* https://www.worldcat.org/title/diseno-de-un-sistema-de-gestion-de-seguridad-de-informacion-optica-iso-270012005/oclc/630664498

Aliaga, L. (2013). *Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo. Tesis para optar por el título de Ingeniero Informático, Pontificia Universidad Católica del Perú.* http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/4721

Ampuero, Chang, Carlos. (2011). *Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros. Pontificia Universidad Católica del Perú.* http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/933

Araujo, T. (2017). *Evaluación de Riesgo, Supervisión y Monitoreo en el Logro de Objetivos, en el Fondo de Aseguramiento Saludpol – Perú.* http://repositorio.ucv.edu.pe/bitstream/handle/UCV/4360/Araujo_BTA.pdf?sequence=1&isAllowed=y

Baca, V. (2016). *Diseño de un Sistema de Gestión de la Seguridad de la Información para la Unidad de Gestión Educativa Local - Chiclayo" - Rev. Ingeniería: Ciencia, Tecnología e Innovación VOL. 3/N° 1 – ISSN 2313-1926/Julio 2016.* http://revistas.uss.edu.pe/index.php/ING/article/view/357

Berg, Ernst (2008): *"Policy Options for Risk Management with Recomentations for Design and Implementation". En prensa.* https://ageconsearch.umn.edu/record/48104/

Barrantes, C. y H. Herrera. (2012). *Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos. Tesis para optar el título de Ingeniero en Computación y Sistemas, Universidad de San Martín de Porres.*

Bernaldo, N. (2018). *Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC. San Borja. Lima 2016.* http://repositorio.ucv.edu.pe/handle/UCV/12657

Buenaño, J. y M. Granda. (2009). *Planeación y diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 270001-27002. Universidad Politécnica Salesiana Sede Guayaquil.*

Burgos, J. (2014). *Elaboración del Plan de Gestión de Riesgos de las Tecnologías de la Información para Roche Ecuador S.A. en la ciudad de Quito, provincia de Pichincha, para el año 2014.* http://dspace.udla.edu.ec/handle/33000/1836

Cruz, R. (2018). M*odelo de gestión de riesgos de TI para el cumplimiento de las exigencias de la SBS en sector microfinanciera de Chiclayo.* http://repositorio.unprg.edu.pe/handle/UNPRG/6116

Espinoza, H. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.. Pontificia Universidad Católica del Perú.*

Fitzgerald, T. (2007). *Information Secutrity Governance. En H. Tipton, & M. Krause, Information Security Management Handbook. USA: Auerbach Publication.* http://ftp.icm.edu.pl/packages/Hacked%20Team/FileServer/FileServer/OLD%20Fileserver/books/SICUREZZA/Information%20security/aggiornamento.pdf

García, J. (2015). *Métodos de Administración y Evaluación de Riesgos; Universidad de Chile; Facultad de Economía y Negocios; Escuela de Sistemas de Información y Auditoria; Santiago de Chile. Recuperado de: (http://repositorio.uchile.cl/tesis/uchile/2005/garcia_j2/sources/garcia_j2.pdf)*

Gonzales, I. (2017*). Diseño e implementación de controles de seguridad para las comunicaciones de red de red de un centro de datos de una entidad del Estado basado en la NTP-ISO/IEC 27001:2014.*

Guillen, M. (2014). *Planeamiento de Modelo de Gestión de Riesgo para empresas de reprocesamiento de dispositivos de ortodoncia, apoyado en TI.*

Huerta, R. (2017). *Gestión y riesgos de seguridad de la información en la Escuela de Suboficiales de la Policía Nacional del Perú, Puente Piedra 2016*

Jara, O. (2018). *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018.*

Kasperso,. *R. Renn. O. Slovic. P.. Brown. H.. Emel. J.. Goble. R.. Kasperson. J.. Ratick. S. (1988). The Social Amplification of Risk A Conceptual Framework. Risk Analysis. 8(2). 177-187. Recuperado de*: https://pdfs.semanticscholar.org/4b33/419863b96c270d5875af9bd5af3ce5dbb1e2.pdf

Kosutic, D. (2016) *ISO 27001 Risk Management in Plain English – ISO Pocket Book Series.* https://es.scribd.com/book/367531882/ISO-27001-Risk-Management-in-Plain-English-A-Step-by-Step-Handbook-for-Information-Security-Practitioners-in-Small-Businesses

Lara H., Reyes J. y W. Navarrete. (2006). *Diseño de Sistema de Gestión de Seguridad de Información para Ecuacolor. Diplomado en Auditoría Informática, Escuela Superior Politécnica del Litoral.*

Leiva, R. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015"*

Llontop, G. (2018). *Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks, 2017.* http://repositorio.ucv.edu.pe/handle/UCV/17596

Maggiore, M. (2014). *Implementación de la estrategia de cero papel para la optimización del proceso de la gestión documental en la Defensoría del Pueblo.* http://repositorio.ucv.edu.pe/handle/UCV/4728

Mejía, L. (2015). *Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio.*

Mercado, H. (2010). *Auditoría de Estados Contables Basada en la Evaluación de Riesgos (RISK BASED). Universidad Nacional de la Pampa. Facultad de Ciencias Económicas y Jurídicas. Argentina. Recuperado de: (http://www.eco.unlpam.edu.ar/sitio/objetos/materias/contador-publico/4ano/control-interno-y-auditoria/aportesteoricos/Riesgo%20de%20Auditoria.pdf)*

Molina, M. (2015). *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela*
Superior Politécnica del Litoral.

Moro, M. (2015). *Diseño de un Sistema de Gestión para proteger el acceso a la información*

Mujica, M. (2007). *Diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" Sede Rectoral. (tesis de Maestría). Universidad Centro Occidental "Lisandro Alvarado", 2007.*

Otoya, M. (2018). *Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017.*

Pallas, G. (2009). *Metodología de implantación de un SGSI en un grupo empresarial jerárquico. (tesis de Maestría). Instituto de Computación.*

Pinto, J (2017). *Gestión y riesgos de seguridad de la información en la Escuela de Suboficiales de la Policía Nacional del Perú, Puente Piedra 2016*

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

Rudas L. (2017). *Modelo De Gestión De Riesgos Para Proyectos De Desarrollo Tecnológico*

Ríos J. (2014). *Diseño de un Sistema de Gestión de Seguridad de la Información para una Central Privada de Información de Riesgos. (tesis de pregrado). Pontificia Universidad Católica del Perú.*

Rodríguez, Y. (2016). *Diseño y formulación de un sistema de gestión de riesgos basado en los lineamientos establecidos por la norma NTC-ISO 31000 versión 2011 para la empresa SIMA LTDA*

Rowe, W. (1975). *An anatomy of risk. Whashington - USA. Enviromental Protection Agency. Recuperadode:https://books.google.com.pe/books?hl=es&lr=&id=O9JRAQAAMAAJ&oi=fnd49&pg=PR2&dq=rowe+risk+anatomy&ots=zPnyuXAkhX&sig=fSpMK_M1hxIT3EGT45V9hFuuYtU#v=onepage&q=rowe%20risk%20anatomy&f=false*

Sánchez, A. (2013). *Diseño de un Sistema de Gestión de la Seguridad de la Información para Comercio Electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito. (tesis de pregrado). Pontificia Universidad Católica del Ecuador.*

Sandoval, A. (2017). *Relación entre Gestión del Riesgo Crediticio y Morosidad en clientes del segmento empresa del BBVA Continental, Moyobamba, 2016*

Sichez, V. (2019). *Identificación de peligros, evaluación de riesgos y las medidas de control en el área administrativa de la empresa Costa del Pacífico Perú S.A.C., 2018*

Stoneburner, A. Goghen. A. y Feringa. A. (2002). *Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology Special Publication 800-30. Recuperado de: https://www.archives.gov/files/era/recompete/sp800-30.pdf*

Tamayo, Y. (2017). *Gestión de riesgo y recursos humanos Dirección de Investigación Tutelar Ministerio de la Mujer y Poblaciones Vulnerables.*

Tapia, K. (2017). *Gestión de riesgo y productividad organizacional en el almacén central de la SUNAT- Lima, 2017.* http://repositorio.ucv.edu.pe/handle/UCV/7223

Tarrillo, E. (2016). *Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015.*

Tersek, R. (2008). *Information Security Management System for an information system (Case study: Integrated Administrative System SAI in the UNEXPO Data Network - Puerto Ordaz). (Master's Thesis). Central Western University "Lisandro Alvarado".*

Vásquez, J (2017). *La gestión documental y la administración de archivos en el Programa Nacional de Infraestructura educativa – 2016.*

Villena, M. (2006). *Sistema de Gestión de Seguridad de Información para una Institución Financiera. Pontificia Universidad Católica del Perú. http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/362*

Westerman, G. (2006). *IT Risk Management: From IT Necessity to Strategic Business Value. M. S. Center for information systems research. Ed. MIT Sloan Managment. 12. Recuperado de: https://dspace.mit.edu/bitstream/handle/1721.1/39809/4658-07.pdf*

Anexos

Anexo 1

Tabla 10

Matriz de consistencia

MATRIZ DE CONSISTENCIA					
TÍTULO: EVALUACIÓN DE RIESGO DE SEGURIDAD DE INFORMACIÓN SEGÚN ISO 27005, OGITT – INSTITUTO NACIONAL DE SALUD					
Problemas	**objetivos**	**Variables e indicadores**			
		Variable 1: Evaluación de riesgos			
		Dimensiones	Indicadores	Escala y valores	Niveles
Problema principal ¿ Cómo se da la evaluación de riesgo de seguridad de información según ISO 27005, OGITT - Instituto Nacional de Salud?	**Objetivo General:** Describir la evaluación de riesgo de seguridad de información según ISO 27005, OGITT - Instituto Nacional de Salud	D1: Identificación del riesgo	Total de activos de información		
			Activos de información criticos		
			Activos de información muy criticos		
			Valorización de activos de información		Confidencialidad: Alta, Media, Baja. Integridad: Alta, Media, Baja Disponibilidad: Alta, Media, Baja
			Identificación de amenazas		
			Identificación de vulnerabilidades		
Problema específico 1: ¿Existe la identificación de riesgo de seguridad de información según ISO 27005, OGITT - Instituto Nacional de Salud?	**Objetivo específico 1:** Determinar la identificación de riesgo de seguridad de información según ISO 27005, Oficina General de Investigación y Transferencia Tecnológica (OGITT) - Instituto Nacional de Salud	D2: Análisis del riesgo	Evaluación de Impacto de la amenaza	Catastrófico= 5 Significativo= 4 Moderado= 3 Menor= 2 No significativo= 1	
Problema específico 2: ¿Existe el análisis de riesgo de seguridad de la información según ISO 27005, OGITT - Instituto Nacional de Salud?	Objetivo específico 2: Determinar el análisis de riesgo de seguridad de la información según ISO 27005, Oficina General de Investigación y Transferencia Tecnológica (OGITT) - Instituto Nacional de Salud		Evaluación de Probabilidad de ocurrencia de amenaza	Muy Alta=5 Alta=4 Moderada=3 Baja=2 Muy Baja=1	
Problema específico 3: ¿Existe la valorización del riesgo de seguridad de la información según ISO 27005, OGITT - Instituto Nacional de Salud?	Objetivo específico 3: Determinar la valoración del riesgo de seguridad de la información según ISO 27005, Oficina General de Investigación y Transferencia Tecnológica (OGITT) - Instituto Nacional de Salud		Total de riesgos de activos de información		
		D3: Valoración del riesgo	Determinación del nivel de riesgo	Nivel de Riesgo Riesgo extremo 25 - 15 Riesgo alto 16 - 10 Riesgo mediano 9 - 4 Riesgo bajo 3 - 1	

Tabla 11

Matriz de operacionalización

Operacionalización de la variable Evaluación de Riesgos

Dimensiones	Indicadores	ESCALA	NIVELES
Identificación De Riesgos	Total de activos de información Activos de información crítico Activos de información muy críticos		
	Valorización de activos de información		Confidencialidad: Alta Media Baja Integridad: Alta Media Baja Disponibilidad: Alta Media Baja
Análisis del Riesgo	Evaluación de Impacto de la amenaza	Catastrófico= 5 Significativo= 4 Moderado= 3 Menor= 2 No significativo= 1	
	Evaluación de Probabilidad de ocurrencia de amenaza	Muy Alta=5 Alta=4 Moderada=3 Baja=2 Muy Baja=1	
	Total de riesgo de activos de información		
Valorización del Riesgo	Determinación del nivel de riesgo		Nivel de Riesgo Riesgo extremo 25 - 15 Riesgo alto 16 - 10 Riesgo mediano 9 - 4 Riesgo bajo 3 - 1

Anexo 2

Instrumento

Tabla 12

Ficha de observación Lista de Activos de Información

	FORMULARIO	FOR-INS-033
	LISTA DE ACTIVOS DE INFORMACIÓN	Edición N° 02
		Pág. de

Sistema de Gestión de Seguridad de la Información (SGSI) ISO 27001

Proceso/Sub proceso :		**Fecha:**
Responsable :		

N°	**CÓDIGO ACTIVO**	**NOMBRE DEL ACTIVO**	**DETALLE DEL ACTIVO**	**TIPO DEL ACTIVO**	**UBICACIÓN FÍSICA**	**UBICACIÓN LÓGICA**	**PROPIETARIO**	**FRECUENCIA DE USO**	**ASPECTO DE SEGURIDAD**			**VALOR DEL ACTIVO**	**CLASIFICACIÓN DE ACTIVO**	**ESTATUS**	
									CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**			**SITUACION**	**FECHA BAJA**

Formulario aprobado por: RD Nº 005-2019-DG-OGIS/INS **Fecha: 23/10/2019**

Información elaborada por:	Información revisada por:	Información aprobada por:
Nombre: Fecha:	Nombre: Fecha:	Nombre: Fecha:

Tabla 13

Ficha de observación Evaluación de Riesgos de Activos de Información

	FORMULARIO	FOR-INS-034
	EVALUACIÓN DE RIESGOS DE ACTIVOS DE INFORMACIÓN	Edición N° 02
		Pág. de

Sistema de Gestión de Seguridad de la Información (SGSI) ISO 27001		
Proceso/Sub proceso:		Fecha:
Responsable:		

N°	CÓDIGO ACTIVO	NOMBRE ACTIVO	CÓDIGO AMENAZA	CÓDIGO VULNERABILIDAD	RIESGO AFECTA A:			Control Implementado	Eficacia del control	Probabilidad	Impacto	Nivel Riesgo	NIVEL DE RIESGO	CODIGO DEL RIESGO	NOMBRE DEL RIESGO	FUENTE DE RIESGO	OPCIÓN DE TRATAMIENTO
					C	I	D										

Formulario aprobado por: RD Nº 005-2019-DG-OGIS/INS Fecha: 23/10/2019

Información elaborada por:	Información revisada por:	Información aprobada por:
Nombre: Fecha:	Nombre: Fecha:	Nombre: Fecha:

Validez de los instrumentos

Resolución que aprueba los instrumentos para el uso en este trabajo d investigación:

SECTOR SALUD

INSTITUTO NACIONAL DE SALUD

N° 005-2019-D6-OGIS/INS

RESOLUCION DIRECTORAL

Lima, 23 de octubre de 2019

Visto el Expediente Nº 00018610-19, presentado por la Oficina Ejecutiva de Estadística e Informática /OGIS, que contiene los proyectos de Formularios para el Desarrollo de la implantación del Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Salud;

CONSIDERANDO:

Que, el Decreto Supremo que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública Decreto Supremo N° 123-2018-pcm y, según la Política Nacional de Modernización de la Gestión Pública al 2021;

Que, la Política de Calidad del Instituto Nacional de Salud, aprobada por Resolución Jefatural N° 104-2019-J-OPE/INS, declara que existe un compromiso de mejorar continuamente los procesos incrementando la eficacia y eficiencia de los mismos dentro del Sistema Integrado de Gestión; garantizando la confidencialidad, integridad y disponibilidad de los activos de información mediante la gestión de riesgos;

Que, en el marco de implementación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos, 2ª. Edición, aprobado con Resolución Ministerial N° 004-2016-PCM, se ha revisado los formularios FOR-INS-033 "Lista de Activos de Información del Instituto Nacional de Salud" edición N° 01; FOR-INS-034 "Evaluación de Riesgos de Activos de Información del Instituto Nacional de Salud", edición N° 01; FOR-INS-041 "Plan de Tratamiento de Riesgos de Seguridad de la Información del Instituto Nacional de Salud", edición N° 01 y FOR-INS-036 "Compromiso de Confidencialidad en el Uso y Divulgación de Información del INS" edición N° 01, habiéndose generado modificaciones en el mismo, por lo cual se solicita su aprobación;

Que, en este contexto, la Oficina Ejecutiva de Estadística e Informática ha propuesto la aprobación de los Formularios para el desarrollo de la implantación del Sistema de Gestión de Seguridad de la Información del Instituto Nacional de Salud, en mérito al D.S 001-2003-S.A. Art. 32 Lit C- ROF/INS;

Estando a lo propuesto y con la visación de la Oficina Ejecutiva de Estadística e Informática; y

De conformidad con lo establecido en el Anexo 2 de la Directiva N° 001-INS/OGAT V.04 Directiva para la planificación, elaboración, revisión, aprobación, difusión y actualización de los documentos del Sistema de Gestión del Instituto Nacional de Salud, aprobada por Resolución Jefatural N° 175-2013-J-OPE/INS;

Figura 3. Resolución Directoral que aprueba los instrumentos

SE RESUELVE:

Artículo 1°.- APROBAR los formularios FOR-INS-033 "Lista de Activos de Información", edición N° 02; FOR-INS-034 "Evaluación de Riesgos de Activos de Información", edición N° 02; FOR-INS-036 "Compromiso de Confidencialidad en el Uso y Divulgación de Información del INS", edición N° 02; FOR-INS-041 "Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información", Edición N° 02; FOR-INS-107 "Evaluación de Oportunidades de Seguridad de la Información", edición N° 01 y FOR-INS-108 "Lista de Proyectos", Edición N° 01, que en anexo adjunto forma parte de la presente Resolución Directoral.

Artículo 2°.- DEROGAR, los formularios FOR-INS-033 "Lista de Activos de Información del Instituto Nacional de Salud" edición N° 01, aprobado con Resolución Directoral N° 002-2013-DG-OGIS-OPE/INS de fecha 05 de diciembre del 2013; FOR-INS-034 "Evaluación de Riesgos de Activos de Información del Instituto Nacional de Salud", edición N° 01, aprobado con Resolución Directoral N° 003-2013-DG-OGIS-OPE/INS de fecha 05 de diciembre del 2013; FOR-INS-041 "Plan de Tratamiento de Riesgos de Seguridad de la Información del Instituto Nacional de Salud", edición N° 01 aprobado con Resolución Directoral N° 005-2015-DG-OGIS-OPE/INS de fecha 02 de julio del 2015; FOR-INS-036 "Compromiso de Confidencialidad en el Uso y divulgación de Información del Instituto Nacional de Salud, edición N° 01 aprobado con Resolución Directoral N° 002-2014-DG-OGIS/INS de fecha 04 de febrero del 2014.

Artículo 3°.- ENCARGAR, al Coordinador de Gestión de la Calidad de la OGIS, la publicación de la presente Resolución y anexo en el Portal de Normatividad Virtual del Instituto Nacional de Salud.

Regístrese y comuníquese

INSTITUTO NACIONAL DE SALUD

Med. Leonardo Rojas Mezarina
Director General
Oficina General de Información y Sistemas

Ficha técnica

Tabla 14

Ficha técnica del instrumento de la variable Evaluación de Riesgos

Instrumento para medir la Evaluación de Riesgos

Nombre del instrumento	:	Evaluación de Riesgo
Autor	:	Instituto Nacional de Salud
Año	:	2019
Lugar	:	Lima
Objetivo	:	Determinar los niveles de riesgos de OGITT del INS
Administración	:	Individual
Tiempo de duración	:	8 horas

Tabla 15

Baremo de la variable

Nivel del Riesgo

Dimensiones	**Escala**	**Rango**	**Categoría**
Análisis de riesgos	**Ordinal**	**25 al 15**	Riesgo Extremo
	Ordinal	**16 al 10**	Riesgo Alto
	Ordinal	**9 al 4**	Riesgo Mediano
	Ordinal	**3 al 1**	Riesgo Bajo

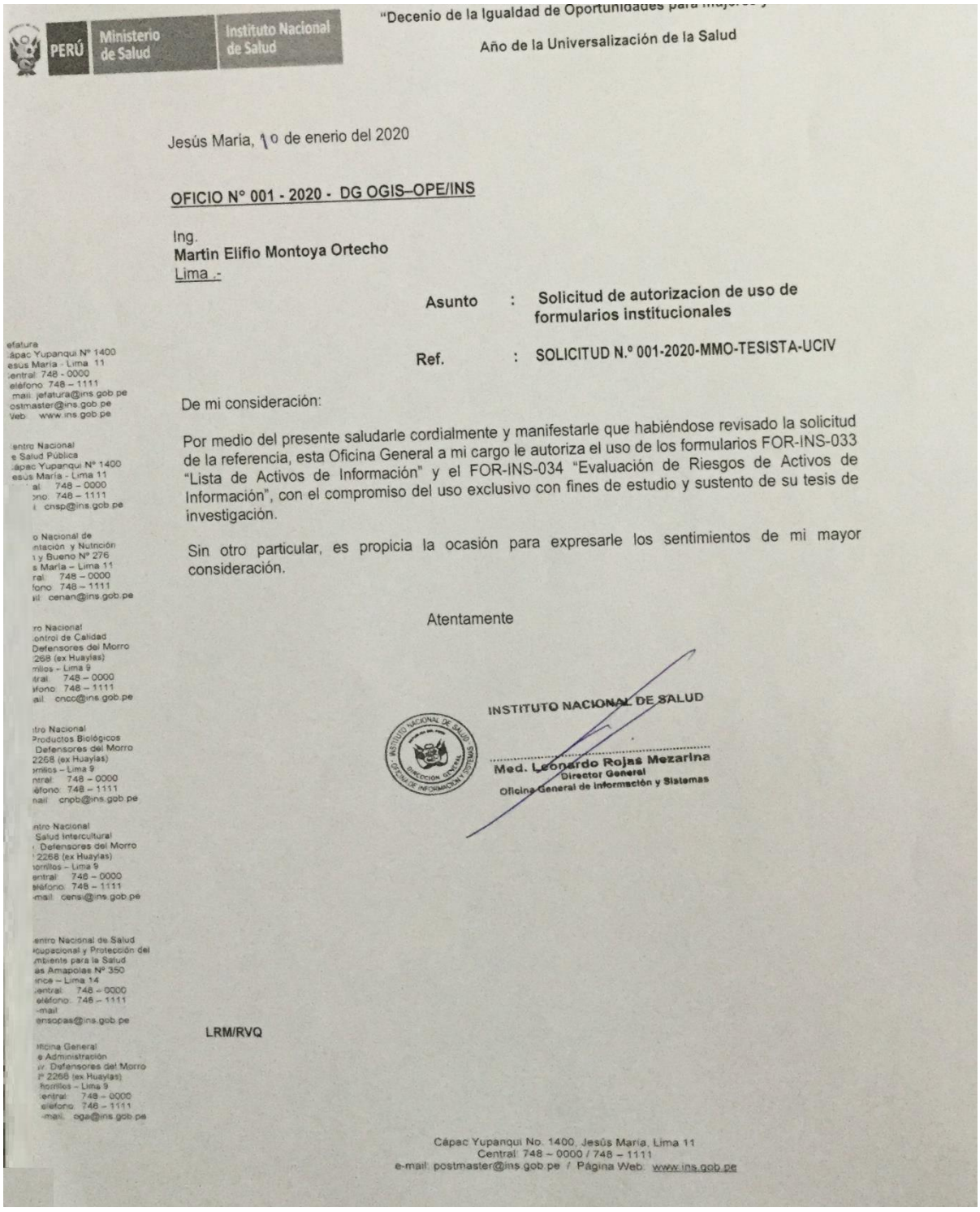
Nivel de Impacto

Dimensiones	**Nivel**	**Impacto**
Análisis de riesgos	**5**	Catastrófico
	4	Significativo
	3	Moderado
	2	Menor
	1	No significativo

Nivel de Probabilidad

Dimensiones	**Nivel**	**Impacto**
Análisis de riesgos	**5**	Muy alta
	4	Alta
	3	Moderada
	2	Baja
	1	Muy baja

Anexo 3
Carta de autorización



PERÚ Ministerio de Salud | Instituto Nacional de Salud

"Decenio de la Igualdad de Oportunidades para [illegible]

Año de la Universalización de la Salud

Jesús María, 10 de enero del 2020

OFICIO N° 001 - 2020 - DG OGIS–OPE/INS

Ing.
Martin Elifio Montoya Ortecho
Lima .-

Asunto : **Solicitud de autorizacion de uso de formularios institucionales**

Ref. : **SOLICITUD N.º 001-2020-MMO-TESISTA-UCIV**

De mi consideración:

Por medio del presente saludarle cordialmente y manifestarle que habiéndose revisado la solicitud de la referencia, esta Oficina General a mi cargo le autoriza el uso de los formularios FOR-INS-033 "Lista de Activos de Información" y el FOR-INS-034 "Evaluación de Riesgos de Activos de Información", con el compromiso del uso exclusivo con fines de estudio y sustento de su tesis de investigación.

Sin otro particular, es propicia la ocasión para expresarle los sentimientos de mi mayor consideración.

Atentamente

INSTITUTO NACIONAL DE SALUD
Med. Leonardo Rojas Mezarina
Director General
Oficina General de Información y Sistemas

LRM/RVQ

efatura
ápac Yupanqui N° 1400
esús María - Lima 11
entral: 748 - 0000
eléfono: 748 – 1111
mail: jefatura@ins.gob.pe
ostmaster@ins.gob.pe
Web: www.ins.gob.pe

entro Nacional
e Salud Pública
ápac Yupanqui N° 1400
esús María - Lima 11
al: 748 – 0000
no: 748 – 1111
cnsp@ins.gob.pe

o Nacional de
ntación y Nutrición
y Bueno N° 276
s María – Lima 11
ral: 748 – 0000
fono: 748 – 1111
il: cenan@ins.gob.pe

ro Nacional
ontrol de Calidad
Defensores del Morro
2268 (ex Huaylas)
millos – Lima 9
tral: 748 – 0000
fono: 748 – 1111
ail: cnco@ins.gob.pe

tro Nacional
Productos Biológicos
Defensores del Morro
2268 (ex Huaylas)
millos – Lima 9
ntral: 748 – 0000
léfono: 748 – 1111
nail: cnpb@ins.gob.pe

ntro Nacional
Salud Intercultural
Defensores del Morro
2268 (ex Huaylas)
millos – Lima 9
entral: 748 – 0000
léfono: 748 – 1111
mail: censi@ins.gob.pe

entro Nacional de Salud
upacional y Protección del
mbiente para la Salud
ás Amapolas N° 350
nce – Lima 14
entral: 748 – 0000
eléfono: 748 – 1111
mail:
ensopas@ins.gob.pe

ficina General
e Administración
v. Defensores del Morro
° 2268 (ex Huaylas)
millos – Lima 9
entral: 748 – 0000
elefono: 748 – 1111
mail: oga@ins.gob.pe

Cápac Yupanqui No. 1400, Jesús María, Lima 11
Central: 748 – 0000 / 748 – 1111
e-mail: postmaster@ins.gob.pe / Página Web: www.ins.gob.pe

Figura 4. Carta de autorización de uso de los instrumentos

Tabla 16
Categoría de Activos de Información

TIPO	CATEGORIA	DESCRIPCION
Información	Información-Documento electrónico	Base de datos, documentos creados y o conservados en medios electrónicos (correo electrónico, audio, video, entre otros). Ejemplo: archivos para el control del Desarrollo, SGSI.
	Información-Documento en papel	Documentos creados, impresos y o conservados en papel. Ejemplo: Documentos que recepcionamos. Documentos almacenados en las oficinas.
Software	Software comercial o herramientas, utilitarios	Es un software comercialmente conocido como de Ofimática o necesario a instalar como, por ejemplo: Office 365, Antivirus McAfee, Adobe, Winrar, Primo PDF, entre otros.
	Software desarrollado por terceros	Es un software que se ha comprado o adquirido de un tercero y que no han sido desarrollados por la organización.
	Software desarrollado internamente	Software desarrollado en la organización, fuentes de un Sistema de información, Sistema Integrado, Aplicativo Web o Módulo de Sistema.
	Software de administración de Base de Datos	Es el software que permite la administración de las bases de datos de los sistemas de información, por ejemplo, SQL Server, Oracle, DB/2, Informix, etc.
	Software – Otros	Otro tipo de software no considerado en esta matriz como por ejemplo software Telecrédito, PDT Plame, SUNAT PLE, etc.
Hardware	Hardware-Equipo de procesamiento	Equipos informáticos que sirven para el procesamiento de información como computadoras y laptops.
	Hardware-Servidor	Equipos informáticos que sirven para el procesamiento de información con una arquitectura más compleja y especializada.
	Hardware-Equipo de comunicaciones	Firewall, Router, switch, centrales digitales, máquinas de fax, Access Point
	Hardware-Medio de almacenamiento	Torre de Lectores, Discos, cintas TAPE, disquetes, CD, DVD, BR, memorias USB, disco duro externo
	Hardware-Mobiliario y equipamiento	Cajas, Estantes, cajas fuertes, archivadores, entre otros.
	Hardware-Otros equipos	Unidad Tape, Impresoras, fotocopiadoras, scanners, Lectores Ópticos, PDT, PDA, teléfono móvil
	Hardware-Equipos de Protección	Estos son equipos especializados para protección eléctrica y de ambientes, como, por ejemplo: Grupo electrógeno, Equipo UPS y Aire Acondicionado.
	Hardware-Sistemas de Seguridad	Son sistemas integrados y circuitos cerrados de cámaras de Seguridad, Alarmas contra incendios, otros sistemas de seguridad.
Personas	sponsables de tomar decisiones (Gerentes, Dire	Responsables de tomar decisiones (Gerentes, Directores y Jefes)
	Personas - Personal de la Organización	Colaboradores (Administrador de proyecto, operadores, personal de desarrollo externo).
Servicios	Servicios - Procesamiento y comunicaciones	Servicio de Procesamiento de la información, de impresión, de fotocopiado, de mensajería, correo electrónico, telefonía fija y celular, Internet, VPN.
	Servicios - Servicios generales	Calefacción, limpieza, seguridad, energía eléctrica, aire acondicionado, entre otros.
	Servicios – Otros	Servicio de intermediación laboral, entre otros.

Tabla 17

Valoración de Activos de Información

Niveles	CONFIDENCIALIDAD
(3) Alta	Su distribución debe estar restringida a un pequeño grupo de personas, pues revelarla sin permiso puede tener un impacto negativo de grandes alcances para el INS, empleados y/o terceros. Su acceso debe ser expresamente autorizado por el Propietario de la Información y restringido a un grupo reducido de usuarios que la necesite para el desarrollo de sus tareas habituales. Revelarla sin autorización puede repercutir negativamente, originando un impacto mayor en las operaciones.
(2) Media	La clasificación interna es la más común que se maneja en el INS. Su distribución está generalmente restringida a un grupo más grande de personas. Revelarla sin autorización puede repercutir negativamente, originando un impacto moderado en las operaciones. La información de uso interno se convertirá en pública solo con la autorización del propietario de la información, quién deberá autorizar cualquier difusión de la misma.
(1) Baja	La información pública no es confidencial y está enfocada al uso general tanto dentro como fuera del INS. Podrá ser revelada por el propietario de la misma que tenga dentro de sus funciones la autorización para revelarla al público.
Niveles	**INTEGRIDAD**
(3) Alta	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdidas de imagen severas al INS, impacta a terceros.
(2) Media	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdida de imagen moderado al INS.
(1) Baja	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para el INS o externos.
Niveles	**DISPONIBILIDAD**
(3) Alta	La no disponibilidad de la información puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdidas de imagen severas al INS, impacta a terceros.
(2) Media	La no disponibilidad de la información puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdida de imagen moderado al INS, puede afectar a terceros.
(1) Baja	La no disponibilidad de la información puede afectar la operación normal del INS o terceros, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

Tabla 18

Registro de amenazas

REGISTRO DE AMENAZAS		
Sistema de Gestión de Seguridad de la Información (SGSI) / NTP-ISO/IEC 27001		
CÓDIGO	**AMENAZAS**	**TIPO**
AM01	Incendio	Daño Físico
AM02	Daño por agua	
AM03	Contaminación	
AM04	Accidente mayor	
AM05	Destrucción del equipo o los medio	
AM06	Polvo, corrosión, congelación	
AM07	Fenómeno Climático	Eventos Naturales
AM08	Fenómeno sísmico	
AM09	Fenómeno volcánico	
AM10	Fenómeno meteorológico	
AM11	Inundación	
AM12	Fallas del sistema de aire acondicionado o del suministro de agua	Pérdida de servicios esenciales
AM13	Perdida del suministro de electricidad	
AM14	Falla del equipo de telecomunicaciones	
AM15	Radiación electromagnética	Perturbación debido a radiación
AM16	Radiación térmica	
AM17	Pulsos electromagnéticos	
AM18	Intercepción de señales de interferencia comprometedoras	Compromiso
AM19	Espionaje remoto	
AM20	Interceptación de comunicaciones	
AM21	Robo de medios o documentos	
AM22	Robo de equipos	

Tabla 19

Registro de vulnerabilidades

REGISTRO DE VULNERABILIDADES		
Sistema de Gestión de Seguridad de la Información (SGSI) / NTP-ISO/IEC 27001		
CÓDIGO	**VULNERABILIDAD**	**CATEGORIA**
VU01	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	Hardware
VU02	Falta de esquemas de reemplazo periódicos	
VU03	Susceptibilidad a la humedad, al polvo y a la suciedad	
VU04	Sensibilidad a la radiación electromagnética	
VU05	Falta de control eficiente del cambio de configuración	
VU06	Susceptibilidad a variación de voltaje	
VU07	Susceptibilidad a variaciones de temperatura	
VU08	Almacenamiento no protegido	
VU09	Falta de cuidado al descartarlo	
VU10	Copia no controlada	
VU11	Pruebas al software inexistentes o insuficientes	Software
VU12	Errores conocidos en el software	
VU13	No hacer "logout" cuando se sale de la estación de trabajo	
VU14	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	
VU15	Falta de evidencia de auditoria	
VU16	Asignación equivocada de derechos de acceso	
VU17	Software ampliamente distribuido	
VU18	Aplicar programas de aplicación a datos incorrectos en términos del tiempo	
VU19	Interfaz de usuario complicada	
VU20	Falta de documentación	
VU21	Seteo incorrecto de parámetros	
VU22	Fechas incorrectas	

Tabla 20

Criticidad de Activos de Información

No Significativo	Es cuando en el aspecto de Confidencialidad, Integridad y Disponibilidad, los valores son todos Bajos
Menor	Es cuando en el aspecto de Confidencialidad, Integridad y Disponibilidad, al menos tiene un valor Medio
Moderado	Es cuando en el aspecto de Confidencialidad, Integridad y Disponibilidad, tiene dos valores Medios
Crítico	Es cuando en el aspecto de Confidencialidad, Integridad y Disponibilidad al menos tiene un valor Alto
Muy Crítico	Es cuando en el aspecto de Confidencialidad, Integridad y Disponibilidad tiene dos o tres valores Altos

Tabla 21

Tabla de Impacto

VALOR	IMPACTO	DESCRIPCIÓN
5	Catastrófico	Impacta en forma severa en la institución al punto de comprometer la confidencialidad o integridad de información crítica de la institución o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a toda la institución y su efecto se siente en todo el personal involucrado.
4	Significativo	Impacta en forma grave a un área o servicio específico de la institución, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves de la institución por un tiempo considerable. Su efecto está limitado dentro de la institución.
3	Moderado	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	Menor	El impacto es leve y se puede prescindir del mismo en un tiempo limitado.
1	No Significativo	No representa un impacto importante para la institución.

Tabla 22

Tabla de Probabilidad

NIVEL	PROBABILIDAD	DESCRIPCIÓN
5	Muy Alta	Ocurriría en la mayoría de las circunstancias: por lo menos una vez a la semana.
4	Alta	Probablemente ocurriría en la mayoría de las circunstancias: cuando menos una vez al mes.
3	Moderada	Puede ocurrir en algún momento: cuando menos una vez al año.
2	Baja	Puede ocurrir en algún momento: cuando menos una vez cada 5 años.
1	Muy Baja	Puede ocurrir en circunstancias excepcionales: una vez cada 20 años.

Tabla 23

Tabla de Nivel de Riesgos

TABLA DE NIVEL DE RIESGO	
Nivel de Riesgo	**Descripción de las Consecuencias**
EXTREMO	Puede afectar seriamente a la Institución, en términos de incumplimiento de sus objetivos estratégicos, paralización de las operaciones más allá del tiempo tolerable. Pérdidas económicas y daño considerable a la imagen de la Institución.
ALTO	Puede afectar a los niveles de operación y servicio de la Institución, incumplimiento de metas, divulgación no autorizada de la información fuera de la Institución.
MEDIANO	Afecta al cumplimiento de un objetivo secundario o de soporte. Puede afectar la operación de ciertas áreas específicas de la Institución. La divulgación no autorizada no representa un perjuicio importante para la Institución.
BAJO	No representa un riesgo importante para la Institución, puede afectar a un activo secundario o de soporte.

Tabla 24

Matriz de Riesgos o Mapa de Calor

MATRIZ DE PROBABILIDAD E IMPACTO					
IMPACTO	**RIESGOS**				
5. CATASTRÓFICO	**5** RIESGO MEDIANO	10 RIESGO ALTO	15 RIESGO EXTREMO	20 RIESGO EXTREMO	25 RIESGO EXTREMO
4. SIGNIFICATIVO	**4** RIESGO MEDIANO	8 RIESGO MEDIANO	12 RIESGO ALTO	16 RIESGO ALTO	20 RIESGO EXTREMO
3. MODERADO	**3** RIESGO BAJO	6 RIESGO MEDIANO	9 RIESGO MEDIANO	12 RIESGO ALTO	15 RIESGO EXTREMO
2. MENOR	2 RIESGO BAJO	4 RIESGO MEDIANO	6 RIESGO MEDIANO	8 RIESGO MEDIANO	10 RIESGO ALTO
1. NO SIGNIFICATIVO	1 RIESGO BAJO	2 RIESGO BAJO	3 RIESGO BAJO	4 RIESGO MEDIANO	5 RIESGO MEDIANO
PROBABILIDAD	**1. MUY BAJA**	**2. BAJA**	**3. MODERADA**	**4.ALTA**	**5. MUY ALTA**

Tabla 25

Lista de riesgos

Sistema de Gestión de Seguridad de la Información (SGSI) / NTP-ISO/IEC 27001		
CÓDIGO	**RIESGOS**	
RI001	Daños a los equipos del Data Center Sede Chorrillos ocasionados por incendios	Riesgos por Desastres Naturales / Humanos / Ambientales
RI002	Daños a los equipos del Data Center Sede Chorrillos ocasionados por terremoto	
RI003	Daños a los equipos del Data Center Sede Chorrillos ocasionados por inundaciones	
RI004	Pèrdida de equipos ocasionados por robo	
RI005	Falla en el software	Riesgos de los Activos de Software
RI006	Daños en Sistemas de Información	
RI007	Falla en el software - Motor de Base de Datos	
RI008	Falla en el software - Servidor con Aurix Portal System	
RI009	Manipulación de Datos Inadvertida - Sistemas de Información INS	
RI010	Acceso no autorizado a los sistemas de inforamción	
RI011	Infección de software malicios en red interna	
RI012	Fallas en Sistemas de Información	
RI013	Falla en equipo dedicado - Servidores de Base de Datos, Correo, Web	Riesgos de los Activos Físicos
RI014	Falla en los Equipos principales de Red - Servidores (Controlador de Dominio, Servidor de Virtualización)	
RI015	Falla en equipo dedicado - Servidores de aplicaciones (NETLAB, SIGANET, otros)	
RI016	Falla en equipos especializados de seguridad en la Red - Firewall	
RI017	Falla en equipos especializados de seguridad en la Red - Servidor de Administración de Antivirus	
RI018	Falla en equipos especializados de seguridad en la Red - Servidor para control de acceso de navegación en intern	
RI019	Falla en equipo dedicado - Unidad de tape backup internas / externas	
RI020	Deterioro de medios de almacenaje	
RI021	Falla en equipos de comunicación	
RI022	Falla en Equipos de comunicación - Equipos Wireless	
RI023	Falla en equipo dedicado	
RI024	Falla en suminsitro de aire acondicionado	
RI025	Falla en suminsitro de energia elèctrica de contingencia	
RI026	Falla en la infraestrctura de la red LAN - Estaciones de trabajo, servidores, equipos de comunicación	
RI027	Acceso no autorizado a red interna	
RI028	Falla en servicio de internet	Riesgos de los Servicios
RI029	Fluctuaciones o cortes del suminstro electrico	
RI030	Falla en servicio de telefonia IP	
RI031	Ausencia de personal por enfermedde/servicios/comisiones	

Anexo 04: Artículo Científico

Evaluación de riesgo de seguridad de información según ISO 27005, OGITT – Instituto Nacional de Salud

Br. Martin Elifio Montoya Ortecho

mmontoyao@ins.gob.pe

Resumen

El proceso de realizar una evaluación de riesgos de seguridad de la información tiene como objetivo mitigar los niveles de riesgos ante una materialización de amenazas que pueden afectar a los activos de información relevantes y por ende a los procesos de una organización. No obstante, no todo control de seguridad tiene cien por ciento seguro, encontramos vulnerabilidades abiertas que pueden ser explotadas malintencionadamente cuando no se tiene claro cuáles son esas debilidades. Los componentes están asociados a una metodología que me va a permitir saber cuáles son las fases. Esta metodología está basada en activos, amenazas, vulnerabilidades, riesgos bajo la norma técnica NTP-ISO/IEC 27005 versión 2018. El tipo de investigación es básica de nivel descriptivo, es decir, me va a permitir describir las fases de la realización descriptiva aplicadas en las áreas de la Oficina General de Investigación y Transferencia Tecnológica – OGITT. Los resultados más importantes obtenidos en el trabajo de investigación fueron la identificación de los niveles de riesgos de la información de cada área de la OGITT, saber la cantidad de riesgos de nivel Muy Crítico y Crítico están expuestos y que grado de impacto económico, legal, jurídico, financiero o de imagen podría ocurrir sino aplico una metodología de gestión de riesgos de seguridad de la información.

Concluyo con una determinación muy importante y es saber cuáles son los riesgos prioritarios y debe saber el representante legal de la institución para la toma de decisiones futuras aplicando estrategias de seguridad e implementación de controles necesarios.

Palabras claves: Evaluación, riesgo, seguridad, información.

Abstract

The process of conducting an information security risk assessment aims to mitigate the levels of risks in the face of a materialization of threats that may affect the relevant information assets and therefore the processes of an organization. However, not every security control has one hundred percent secure, we find open vulnerabilities that can be exploited maliciously when it is not clear what those weaknesses are. It is important that the objective of this research work clearly describes the three important components for managing risks, understanding the risk assessment procedure that involves risk identification, risk analysis and risk assessment.

The components are associated with a methodology that will allow me to know protocols are the phases. This methodology is based on the technical standard NTP-ISO / IEC 27005 version 2018. The type of research is basic of descriptive level, that is, it will allow me to describe the phases of the descriptive realization applied in the areas of the General Office of Research and Technology Transfer - OGITT. The most important results detected in the research work were the identification of the risk levels of the information of each area of the OGITT, knowing the amount of risks of level Very critical and critical are determined and the degree of economic, legal impact, Legal, financial or image could solve the problem but an information security risk management methodology. I conclude with a very important determination and that is to know what are the priority risks and should know the legal representative of the institution for future decision making applying security strategies and implementation of necessary controls.
Keywords: Evaluation, risk, security, information.

Introducción

En el ámbito internacional las organizaciones como Industrial Automation Agedum (México), Roche Ecuador S.A. (Ecuador), Universidad Politécnica de Madrid (España) instituciones que son parte de este estudio, producen información que están ligadas al desarrollo de sus procesos y de sus sistemas de información, y para protegerlo es un problema organizacional en el que la solución es mucho más que contratar al mejor agente especializado de seguridad. Estas organizaciones no están ajenas a los riesgos, y deben estar preparadas puesto que por falta de ello, están expuestos a robo de información confidencial, robo de contraseñas, ataques cibernéticos, amenazas que son causados por una falta organizacional de una correcta evaluación de riesgos de seguridad de la información. En el estado nacional, aún no se ha logrado la conciencia de una cultura de prevención en las instituciones, es decir, no se ha logrado cerrar brechas de seguridad, donde me permita gestionar riesgos mediante mecanismos estandarizados o normas que puedan ser útiles y muy necesarias para una prevención de riesgos. En los últimos años en las empresas peruanas han aumentado en 600% los ataques en seguridad de la información entre los más comunes se encuentra denegación de servicio a las redes, robo de información electrónica o ransomware, accesos a áreas no autorizadas, robo de documento confidenciales, entre otros. Esto refleja que los sistemas de seguridad de la información aún se encuentran en niveles bajos de madurez, con planes de gestión de riesgos no

ejecutados o irregular, a menudo se gestiona los riesgos como un silo aislado dentro de la organización. Entre las empresas más afectadas son las entidades financieras, entidades de salud, entidades educativas, entre otras y es fundamental una gestión en seguridad de la información para mitigar los riesgos ante amenazas en un mundo interconectado, y las principales vulnerabilidades que sufre toda organización es la falta de una correcta evaluación de riesgos a la información en sus procesos como parte de sus actividades.

La Oficina General de Investigación y Transferencia Tecnológica – OGITT, cuenta con un proceso llamado Autorización de Ensayos Clínicos con áreas involucradas como la Oficina General de Investigación y Transferencia Tecnológica, Oficina Ejecutiva de Investigaciòn, Trámite Documentario, Ensayos Clínicos, Archivo y como oficina de apoyo el área de Tecnología de Información (TI). Estas oficinas cuentan con áreas donde existe un riesgo constante de fuga de información o perdida de documentos de investigación debido a que se encuentra expuesta a robo de documentos físicos o archivos electrónicos, ambientes no controlados sin las medidas de seguridad perimetral necesaria, puesto que son lugares vulnerables y se requiere de una buena evaluación de riesgos de seguridad de la información. Dentro de los riesgos que pueden existir sobre todo el área más vulnerable es la de "Evaluación de Ensayos Clínicos". Existen riesgos como el robo de documentos por ingreso de personas no autorizadas o por falta de controles físicos, transferencia de información no autorizada, estos riesgos son muy latente puesto que los documentos se encuentran expuestos en lugares que no tiene un armario especifico con llave o que no están protegidas con una sólida contraseña. La falta de controles físicos de entrada expone una amenaza para el área, ya que no cuenta con un registro de identificación de personas externas y que usen fotocheck de identificación. El área de investigación genera documentos que son confidenciales para la organización, y están expuestas a la divulgación por su falta de seguridad, sobre todo la ausencia de concientización sobre estos temas. Un problema que se ha identificado también es la falta de fluido eléctrico por apagones que han suscitado varias veces en el año anterior, esto ha causado que los equipos de cómputo hayan sufrido variaciones de voltaje, puesto que el área de competente en la materia no ha fortalecido los estabilizadores de voltaje. El presente trabajo de investigación pretende evaluar la gestión de riesgos en sus dimensiones como la identificación de riesgo, análisis de riesgo y valoración del riesgo basado en la norma NTP-ISO/IEC 27005:2018 "Gestión de Riesgos de Seguridad de la Información" con el objetivo de proporcionar directrices para gestionar los riesgos.

Materiales y métodos

Tipo de investigación.

La investigación fue básica de nivel descriptivo según la clasificación de Hernández, Fernández y Baptista (2014). La presente tesis de investigación se orientó al tipo de investigación básica, ya que se basa en el conocimiento previo que se plasma en el marco teórico para aplicarlo al caso de estudio.

Diseño.

Según Sánchez y Reyes (2015) definió que es diseño no experimental, es de corte transversal y es descriptivo simple. Es decir, en la presente tesis de investigación busca recoger la información actual con respecto a una situación previamente determinada, dado el objetivo de estudio se describió la evaluación de riesgo de seguridad de la información. El diseño de la investigación se basa en la caracterización de la variable descrita en sus tres dimensiones (identificación de riesgos, análisis de riesgos y valorización del riesgo) desarrollada bajo una base de datos de probabilidad e impacto y una matriz de niveles de riesgos que la componen.

Leyenda:

M: muestra 40, trabajadores de la Oficina General de Investigación y Transferencia Tecnológica (OGITT).

O1: Variable 1, Evaluación de Riesgos de Seguridad de la Información.

De esta manera, el diseño del esquema es el siguiente:

Instrumentos

Tabla 1

Ficha de observación Lista de Activos de Información

	FORMULARIO	FOR-INS-033
	LISTA DE ACTIVOS DE INFORMACIÓN	Edición N° 02
		Pág. de

Sistema de Gestión de Seguridad de la Información (SGSI) ISO 27001

Proceso/Sub proceso :		Fecha:
Responsable :		

N°	CÓDIGO ACTIVO	NOMBRE DEL ACTIVO	DETALLE DEL ACTIVO	TIPO DEL ACTIVO	UBICACIÓN FÍSICA	UBICACIÓN LÓGICA	PROPIETARIO	FRECUENCIA DE USO	ASPECTO DE SEGURIDAD			VALOR DEL ACTIVO	CLASIFICACIÓN DE ACTIVO	ESTATUS	
									CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD			SITUACION	FECHA BAJA

Formulario aprobado por: RD Nº 005-2019-DG-OGIS/INS Fecha: 23/10/2019

Información elaborada por:	Información revisada por:	Información aprobada por:
Nombre: Fecha:	Nombre: Fecha:	Nombre: Fecha:

Tabla 2

	FORMULARIO	FOR-INS-034
	EVALUACIÓN DE RIESGOS DE ACTIVOS DE INFORMACIÓN	Edición N° 02
		Pág. de

Sistema de Gestión de Seguridad de la Información (SGSI) ISO 27001

Proceso/Sub proceso:		Fecha:
Responsable:		

Nº	CÓDIGO ACTIVO	NOMBRE ACTIVO	CÓDIGO AMENAZA	CÓDIGO VULNERABILIDAD	RIESGO AFECTA A:			Control Implementado	Eficacia del control	Probabilidad	Impacto	Nivel Riesgo	NIVEL DE RIESGO	CODIGO DEL RIESGO	NOMBRE DEL RIESGO	FUENTE DE RIESGO	OPCIÓN DE TRATAMIENTO
					C	I	D										

Formulario aprobado por: RD Nº 005-2019-DG-OGIS/INS Fecha: 23/10/2019

Información elaborada por:	Información revisada por:	Información aprobada por:
Nombre: Fecha:	Nombre: Fecha:	Nombre: Fecha:

Ficha de observación Evaluación de Riesgos de Activos de Información

III. Resultados

3.1 Resultados descriptivos

Dimensión 1 - Identificación de Riesgos

Figura 1. Porcentajes de la dimensión Identificación de Riesgos

Dimensión 2 - Análisis de Riesgos

Tabla 5

Figura 2. Porcentaje de la dimensión Análisis de Riesgo

Dimensión 3 – Valoración de Riesgos

Figura 2. Porcentaje de la dimensión Análisis de Riesgo

Discusión

Habiendo aplicado mi variable Evaluación de Riesgos a través de las tres dimensiones correspondientes, el objetivo es describir cómo se lleva a cabo esta metodología que me va permitir determinar el valor de los activos de información, identificar las amenazas latentes, sus vulnerabilidades, sus efectos en el riesgo identificado, las consecuencias, la priorización y los criterios de valorización.

La Dimensión Identificación de Riesgo para Molina (2015) lo llama Modelo de Valor, que está conformado por la identificación de los activos considerados prioritarios, relación entre los activos, la valorización, su árbol de dependencia y su importancia que incurre en cada una de ellas. Usó la herramienta Pilar para la clasificación de sus activos como Activos esenciales, servicios internos, equipamiento, servicio subcontratado, instalaciones y personal. El autor determina la valoración de amenaza por activo, es decir, cada activo tiene diferentes tipos de amenaza y la valoración de activo por amenaza, es decir en cada amenaza está comprometido varios activos. Se empleó la herramienta Pilar para la identificación de activos definido como "Dependencia entre activos" y esto lo clasificó como "Activos esenciales", "Servicios Internos", "Equipamiento", "Servicios Subcontratados", "Instalaciones", y "Personal". La herramienta que usé en mi trabajo de investigación para la identificación de activos y su clasificación fue la ficha de observación llamada "Lista de Activos de Información" que me permite recoger los nombres de los activos y sus características.

En cuanto a la Dimensión Análisis de Riesgo, el autor lo denomina Estado de Riesgo, donde realiza la evaluación de impacto y riesgo de cada amenaza que afecta a los activos; generación de riesgo acumulado, mide la criticidad de los riesgos. Es similar el trabajo del autor con mi tesis, pero, hay una diferencia, en esta etapa se realiza una evaluación de la probabilidad de ocurrencia ante amenazas mediante una escala del 1 al 5, donde 5 la probabilidad es muy alta y 1 es muy baja; la evaluación del impacto se trabaja mediante una escala del 1 al 5, donde 5 tiene nivel Catastrófico y 1 nivel No Significativo y el producto de ellos me determina el nivel de riesgo.

La Dimensión Valoración de Riesgos, el autor lo llama Riesgo Acumulado que mide los niveles de criticidad de los riesgos los cuales se encuentran expuesto. En mi caso, la valoración de riesgo se basa en la prioridad de los riesgos por sus niveles, es decir, los

riesgos con nivel Extremo y los de nivel Alto tienen mayor relevancia para planificarlos a medidas de control con la finalidad de mitigar su riesgo.

Conclusiones.

Primera. En relación con el objetivo específico 1 se concluye que:

> Dentro de la Oficina General de Investigación y Transferencia Tecnológica (OGITT) se ha logrado identificar 104 activos de información comprendidas entre las áreas de Trámite Documentario, Dirección Ejecutiva de Investigación, Dirección General, Evaluación de Ensayos Clínicos, Archivo y Tecnología de Información. En su valorización son 8 activos con valor Muy Crítico y 30 con valor Crítico. El área que obtuvo mayor cantidad con valor Muy Crítico es Evaluación de Ensayos Clínicos con 3 activos; y la mayor cantidad con valor Crítico es el área de Tecnología de Información con 83 activos. El área que obtuvo menos cantidad de activos con valor Menor es el área de Trámite Documentario con 24 activos.

Segunda. En relación con el objetivo específico 2 se concluye que:

> Se determinó el análisis de riesgos a los 38 activos de información con valoración Muy Crítico y Crítico valorados en la primera fase. De los 38 activos se identificó 169 riesgos de nivel Extremo, Alto, Mediano y Bajo. Se determinó 2 riesgos con nivel Extremo, 49 riesgos de nivel Alto, 114 riesgos de nivel Mediano y 4 riesgos de nivel Bajo. El área que obtuvo los riesgos Muy Alto es Evaluación de Ensayos Clínicos y el área que obtuvo riesgos Altos es la misma área en mención. El área que obtuvo riesgo Bajo es Archivo.

Tercera. En relación con el objetivo específico 3 se concluye que:

> Se determinó la valoración de riesgos en el sentido en que los riesgos de nivel Extremo y Alto son los riesgos prioritarios y definidos para su tratamiento.

Referencias

Aguirre, D. (2014). *Diseño de un Sistema de Gestión de Seguridad de la Información para Servicios Postales del Perú S.A. (tesis de pregrado). Pontificia Universidad Católica del Perú.* http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/5677

Aguirre, J. y C. Aristizabal. (2013). *Diseño del Sistema de Gestión de Seguridad de la Información para el grupo empresarial La Ofrenda. (tesis de pregrado). Universidad Tecnológica de*

Pereira, Facultad de Ingenierías, Programa de Ingeniería de Sistemas y Computación Pereira. https://core.ac.uk/download/pdf/71397730.pdf

Alexander, G., Alberto. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información; Óptica ISO/ IEC 27001:2005. Bogotá: Alfaomega Colombiana S.A.* https://www.worldcat.org/title/diseno-de-un-sistema-de-gestion-de-seguridad-de-informacion-optica-iso-270012005/oclc/630664498

.

Aliaga, L. (2013). *Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo. Tesis para optar por el título de Ingeniero Informático, Pontificia Universidad Católica del Perú.* http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/4721

Ampuero, Chang, Carlos. (2011). *Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros. Pontificia Universidad Católica del Perú.* http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/933

Araujo, T. (2017). *Evaluación de Riesgo, Supervisión y Monitoreo en el Logro de Objetivos, en el Fondo de Aseguramiento Saludpol – Perú.* http://repositorio.ucv.edu.pe/bitstream/handle/UCV/4360/Araujo_BTA.pdf?sequence=1&isAllowed=y

Baca, V. (2016). *Diseño de un Sistema de Gestión de la Seguridad de la Información para la Unidad de Gestión Educativa Local - Chiclayo" - Rev. Ingeniería: Ciencia, Tecnología e Innovación VOL. 3/N° 1 – ISSN 2313-1926/Julio 2016.* http://revistas.uss.edu.pe/index.php/ING/article/view/357

Berg, Ernst (2008): *"Policy Options for Risk Management with Recomentations for Design and Implementation". En prensa.* https://ageconsearch.umn.edu/record/48104/

Anexo 5: Declaración Jurada de autoría y autorización

Para la publicación del artículo científico

Yo, Martin Elifio Montoya Ortecho, estudiante del Programa Maestría en Gestión Pública de la Escuela de Posgrado de la Universidad César Vallejo, identificado con DNI 1079995, con el artículo titulado: "Evaluación de riesgo de seguridad de información según ISO 27005, OGITT – Instituto Nacional de Salud", declaro bajo juramento que:

1) El artículo pertenece a mi autoría.
2) El artículo no ha sido plagiado ni total no parcialmente.
3) El artículo no ha sido auto plagiado; es decir, no ha sido publicada ni presentada anteriormente para alguna revista.
4) De identificarse la falta de fraude (datos falsos), plagio (información sin citar a autores), auto plagio (presentar como nuevo algún trabajo de investigación propio que ya ha sido publicado), piratería (uso ilegal de información ajena) o falsificación (representar falsamente las ideas de otros), asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad César Vallejo.
5) Si, el artículo fuese aprobado para su publicación en la revista u otro documento de difusión, cedo mis derechos patrimoniales y autorizo a la Escuela de Posgrado de la Universidad César Vallejo, la publicación del documento en las condiciones, procedimientos y medios que disponga la Universidad.

Ate, 11 enero 2020

Martin Elifio Montoya Ortecho

Anexo 06: Acta de aprobación de originalidad de Tesis

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Acta de Aprobación de originalidad de Tesis

Yo, **Eliana Soledad Castañeda Núñez**, docente de la Escuela de Posgrado de la Universidad César Vallejo filial Ate, revisora de la tesis titulada **Evaluación de Riesgo de seguridad de información según ISO 27005, OGITT – Instituto Nacional de Salud** del (de la) estudiante **Martin Elifio Montoya Ortecho**, constato que la investigación tiene un índice de similitud de 18% verificable en el reporte de originalidad del programa Turnitin.

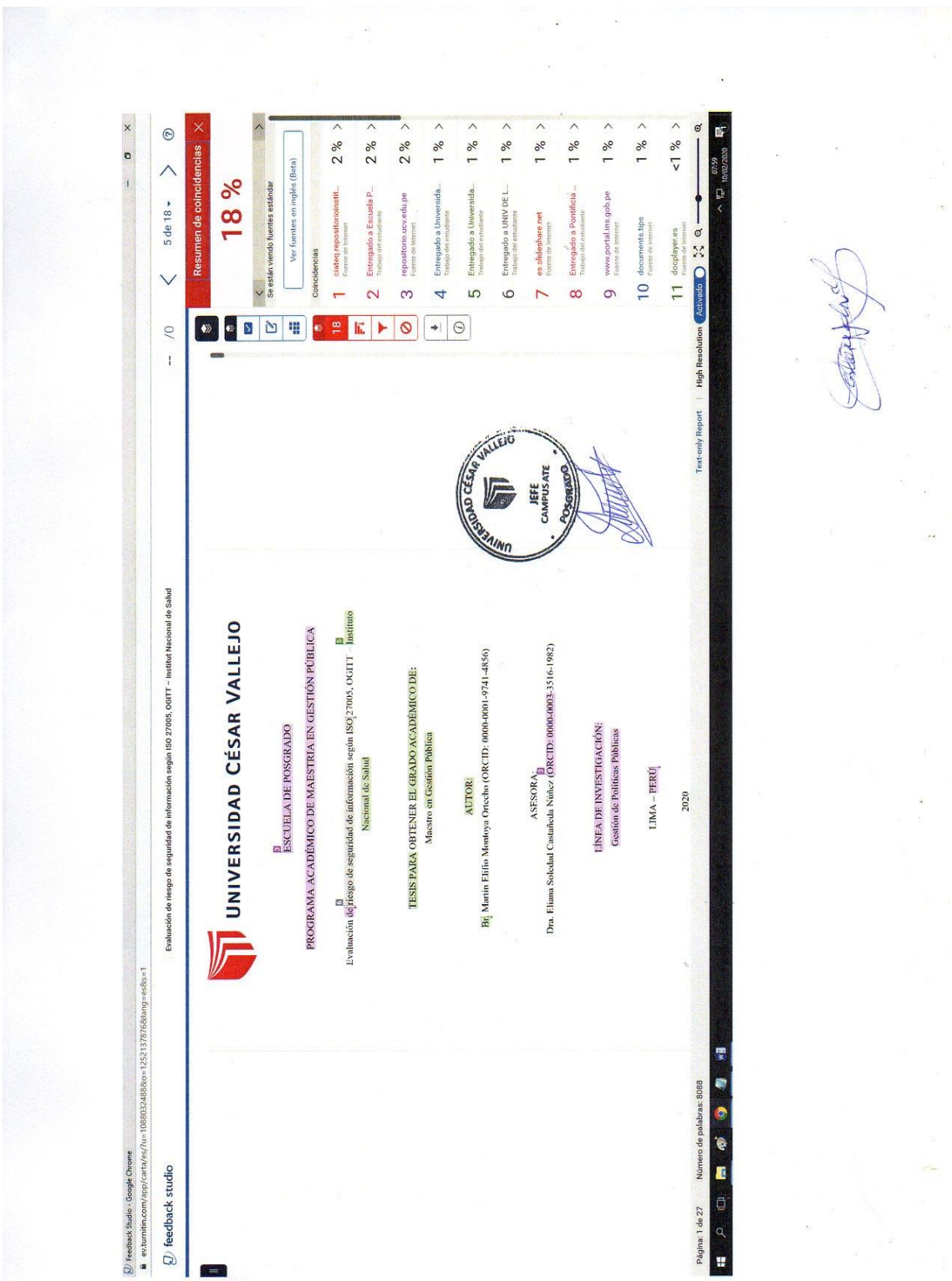
El/la suscrito(a) analizo dicho reporte y concluyo que cada una de las coincidencias detectadas no constituye plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

Lima,11 de Enero de 2020

UNIVERSIDAD CÉSAR VALLEJO
JEFE
CAMPUS ATE
POSGRADO

Eliana Soledad Castañeda Nuñez
DNI: 08104562

Anexo 07: Pantallazo de Turnitin



Anexo 08: Formulario de autorización para la publicación electrónica de las tesis

UNIVERSIDAD CÉSAR VALLEJO

Centro de Recursos para el Aprendizaje y la Investigación (CRAI)
"César Acuña Peralta"

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN ELECTRÓNICA DE LAS TESIS

1. **DATOS PERSONALES**
Apellidos y Nombres: (solo los datos del que autoriza)
MONTOYA ORTECHO, MARTIN ELIFIO
D.N.I. : 10799595
Domicilio : AV. EL SANTUARIO 2410 HUANCAYO
Teléfono : Fijo : ..... Móvil : 954155046
E-mail : martinmontoyaing@gmail.com

2. **IDENTIFICACIÓN DE LA TESIS**
Modalidad:
☐ Tesis de Pregrado
Facultad : .....
Escuela : .....
Carrera : .....
Título : .....

☒ Tesis de Posgrado
☒ Maestría ☐ Doctorado
Grado : MAESTRO
Mención: MAESTRIA EN GESTIÓN PÚBLICA

3. **DATOS DE LA TESIS**
Autor (es) Apellidos y Nombres:
MONTOYA ORTECHO, MARTIN ELIFIO
Título de la tesis:
EVALUACIÓN DE RIESGO DE SEGURIDAD DE INFORMACIÓN SEGÚN ISO 27005, OGTI-INSTITUTO NACIONAL DE SALUD
Año de publicación : 2020

4. **AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN VERSIÓN ELECTRÓNICA:**
A través del presente documento, autorizo a la Biblioteca UCV-Lima Norte, a publicar en texto completo mi tesis.

Firma : .....
Fecha : 11/01/2020

Anexo 09: Autorización de la versión final del trabajo de investigación

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

ESCUELA DE POSGRADO

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

MONTOYA ORTECHO, MARTIN ELIFIO

TESIS TÍTULADA :

Evaluación de riesgo de seguridad de información según ISO 27005, OGTI – Instituto Nacional de Salud

PARA OBTENER EL TÍTULO O GRADO DE:

MAESTRO (A) Maestro en Gestión Pública

SUSTENTADO EN FECHA: 21 ENERO 2020

NOTA O MENCIÓN: Aprobado por unanimidad

UNIVERSIDAD CÉSAR VALLEJO
JEFE
CAMPUS ATE
POSGRADO