UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud, 2019

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información

AUTOR:

Br. Oscar Yonatan Huayllani Muñoz (ORCID: 0000-0003-4060-4864)

ASESOR:

Dr. Angel Salvatierra Melgar (ORCID: 0000-0003-2817-630X)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LIMA - PERÚ

2020

Dedicatoria:

Este trabajo lo dedico a mi madre Antonia, por todo su apoyo incondicional que me brindo en mi etapa de estudios. A mi esposa Milagros, a mis Hijos Oscar y Salvador, por ser mi inspiración de superación en mi crecimiento profesional y personal. A mi Mamita Teófila que desde el cielo me cuida y me guía.

Agradecimiento:

A la Universidad César Vallejo, por la oportunidad brindada que hace posible que muchos bachilleres logremos ser Maestros. A los docentes, por las orientaciones recibidas, quienes aportaron en mis conocimientos, experiencias que fueron aprovechadas como profesional y en muchos casos constituirán metas que deseo imitar.

Página del Jurado

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

DICTAMEN DE LA SUSTENTACIÓN DE TESIS

EL / LA BACHILLER (ES): **OSCAR YONATAN HUAYLLANI MUÑOZ**

Para obtener el Grado Académico de ***Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información,*** ha sustentado la tesis titulada:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DEL RIESGO EN EL MINISTERIO DE SALUD, 2019

Fecha: 19 de enero de 2020 Hora: 2:00 p.m.

JURADOS:

PRESIDENTE: Dr. Yolvi Ocaña Fernandez **Firma:** .....

SECRETARIO: Dra. Liz Maribel Robladillo Bravo **Firma:** .....

VOCAL: Dr. Angel Salvatierra Melgar **Firma:** .....

El Jurado evaluador emitió el dictamen de:

APROBADO POR UNANIMIDAD

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

.....

.....

.....

.....

Recomendaciones sobre el documento de la tesis:

Conneciow APA

.....

.....

.....

.....

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

Declaratoria de Autenticidad

Yo, Oscar Yonatan Huayllani Muñoz, estudiante de la Escuela de Posgrado, del programa Maestría en Ingeniería de Sistemas con Mención en Tecnologías de la Información, de la Universidad César Vallejo, Sede Lima Norte; presento mi trabajo académico titulado: "Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo en el Ministerio de Salud, 2019.", en 99 folios para la obtención del grado académico de Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información, es de mi autoría.
Por tanto, declaro lo siguiente:

- He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos.
- No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.
- Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional.
- Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.
- De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinen el procedimiento disciplinario.

Lima, 06 de enero de 2019

Oscar Yonatan Huayllani Muñoz
DNI: 44030405

v

Índice

	Pág.
Dedicatoria	ii
Agradecimiento	iii
Página del jurado	iv
Declaratoria de Autenticidad	v
Índice	vi
Índice de Figuras	vii
Resumen	viii
Abstract	ix
I. Introducción	01
II. Método	10
2.1. Tipo y diseño de investigación	10
2.2. Operacionalización	10
2.2.1. Definición conceptual	10
2.2.2. Definición operacional	11
2.3. Población, muestra y muestreo	16
2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad	16
2.5. Procedimiento	22
2.6. Métodos de análisis de datos	22
2.7. Aspectos éticos	22
III. Resultados	24
IV. Discusión	30
V. Conclusiones	35
VI. Recomendaciones	36
Referencias	38
Anexos	46
Anexo 1: Matriz de consistencia	47
Anexo 2: Validación de instrumentos	51
Anexo 3: Data para procesar	72
Anexo 4: Pantalla SPSS	81
Anexo 5: Carta presentación UCV	83
Anexo 6: Consentimiento informado	84

Índice de Tablas

Pág.

Tabla 1 Matriz Operacional de la Variable SGSI 12
Tabla 2 Matriz Operacional de la Variable SGR 15
Tabla 3 Tipos de Técnicas e Instrumentos Usados en la Recolección de Datos 16
Tabla 4 Ficha Técnica del Instrumento del SGSI 17
Tabla 5 Ficha Técnica del Instrumento del SGR 17
Tabla 6 Resultados del Juicio de Expertos 18
Tabla 7 Resultados de Prueba Binomial del Instrumento que mide el SGSI y SGR 19
Tabla 8 Prueba KMO y Bartlett para el instrumento que mide el SGSI y SGR 20
Tabla 9 Varianza Total Explicada para la SGSI y la SGR 21
Tabla 10 Prueba de Confiabilidad del Instrumento que mide el SGSI y la SGR 21
Tabla 11 Distribución de Frecuencias de la Variable SGSI 24
Tabla 12 Tabla Cruzada entre la SGSI y la SGR con sus Dimensiones 25
Tabla 13 Resultados de la Prueba de Hipótesis 28

Índice de Figuras

Pág.

Figura 1 Criterios de Evaluación del Alpha de Cronbach 22
Figura 2 Gráfica de la Distribución de Frecuencias de la Variable SGSI y Gestión del Riesgo 24
Figura 3 Gráfica Agrupada de SGSI y Gestión del Riesgo con sus Dimensiones 26

Resumen

La investigación titulada “Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo en el Ministerio de Salud, 2019.”, tuvo como objetivo medir la influencia de la aplicación de un sistema de gestión de seguridad de la información en la gestión del riesgo.

La investigación realizada tuvo un método hipotético deductivo, con un enfoque cuantitativo de tipo aplicada, de nivel correlacional y corte longitudinal. La población estuvo formada por 145 trabajadores de la Unidad de Gestión de Inversiones de Reconstrucción con Cambios del Ministerio de Salud. Los datos fueron recolectados mediante la aplicación de dos instrumentos para medir las variables. Para analizar los resultados se utilizó el estadístico de Rho de Spearman que nos permitió para validar las hipótesis a partir de los datos obtenidos mediante la aplicación de los instrumentos.

Los resultados evidenciaron que existe una relación positiva y significativa entre las variables Gestión del Riesgo y Sistemas de Gestión de la Seguridad de la Información.

Palabras clave: Seguridad, Información, Recursos, Gestión, Riesgos, Salud

Abstract

The research entitled “Information Security Management System and Risk Management in the Ministry of Health, 2019”, aimed to measure the influence of the application of an information security management system in the management of information risk.

The research carried out has a hypothetical deductive method, with a quantitative approach of applied type, correlational level and longitudinal section. The population is made up of 145 workers from the Change Management Unit for Reconstruction Investments of the Ministry of Health. Data have been collected by applying two instruments to measure the variables. To analyze the results, the Spearman Rho statistic was used, which allowed us to validate the hypotheses from the data obtained through the application of the instruments.

The results showed that there is a positive and significant relationship between the variables Risk Management and Information Security Management Systems.

Keywords: Security, Information, Resources, Management, Risks, Health

I. Introducción

Los Sistemas de Gestión de Seguridad de la Información nunca han sido considerados en épocas anteriores como un elemento importante en una organización. Sin embargo, hoy genera el interés de los directivos tanto de negocio como de TI en las instituciones públicas y privadas, como consecuencia de todo el avance tecnológico que estamos viviendo. Tener información valiosa al alcance de cualquier usuario puede ser perjudicial por estar expuesto a una posible eliminación, publicación de contenidos privados, etc. Si bien es cierto que la información de una organización debe estar alcance de todos, esto no quiere decir que toda la información va estar a libre disposición de las personas. Es por eso que cada organización estala en el Perú implemento un espacio en la web donde se almacena información de uso público (Portal de Transparencia), con el fin de disminuir posibles acciones que vayan en contra de la organización gubernamentales. Según Ponemon (2017) las principales causas de alteración de nuestra información son el ataque intencionado (47%), interrupción en los programas (25%) junto a la falla humana (28%). Según el autor se calcula que el costo total promedio vinculado a la perdida de información es de 4,67 millones de dólares, presentándose una disminución del 10% respecto al año anterior con tendencia a la baja, según se va avanzado en la definición por parte de los países de marcos normativos que permitan el uso de Sistemas de Gestión de Seguridad de la Información (en adelante lo llamaremos SGSI) en sus organizaciones.

Según publica RPP (2014), el 22 de mayo del 2014 se sufrió de una interrupción el sistema informático del área de migraciones del Aeropuerto Internacional Jorge Chávez, teniendo como consecuencia la pérdida de vuelos y un valor monetario incalculable para los usuarios y las aerolíneas, poniendo en evidencia la carencia de SGSI en nuestro país a pesar de que desde el año 2003 el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (en adelante lo llamaremos INDECOPI) había creado la NTP-ISO/IEC 27001:2003 que determina los lineamientos procedimentales para la implementación de SGSI en el Perú y cuya última versión ha sido aprobada en el año 2018 con el nombre NTP-ISO/IEC 27001:2018. Algo similar sucedió con la Gestión de Riegos, esto se puedo apreciar en la falta de acciones para minimizar los riegos como consecuencia

del Niño Costero que arraso la costa norte afectando a muchas familias y comunidades en el año 2017.

Según el informe de riesgos del Programa de las Naciones Unidas para el Desarrollo (PNUD) del año 2018, nos muestra que a nivel de salud nos situamos antepenúltimos de 13 países evaluados, pese a que en el año 2011 se forma el Sistema Nacional de Gestión de Riesgos y Desastres mediante la ley N° 29664 con el fin de ser el ente que permita el estudio de políticas de gestión del riesgo para el sector salud. Según el artículo Gestión (2013), el Perú no poseía una adecuada gestión de riesgos en el sector salud a pesar de su crecimiento económico.

Es frente a esta realidad que a finales del año 2018 se crea la Dirección General de Gestión del Riesgo de Desastres (en adelante lo llamaremos DIGERD) que desde entonces es el órgano encargado del desarrollo de la Política Nacional de la Gestión del Riesgo de Desastres, según menciona la página web del Ministerio de Salud (en adelante lo llamaremos MINSA), pero ante la falta de un marco normativo el INDECOPI crea la NTP-ISO 31000:2018, estableciendo los lineamientos que se deben de seguir en el país por parte de las entidades público-privadas para la implementación de los Sistemas de Gestión de Riesgos (en adelante lo llamaremos SGR). Es con este marco normativo que la DIGERD implementa las políticas y lineamientos para hacer frente a los riesgos en nuestro país. Por otro lado, se tiene que el MINSA durante el año 2019 culminó la implementación de su SGSI basándose en la NTP-ISO/IEC 27001:2018, la implementación fue ordenada bajo resolución ministerial N° 580-2016/MINSA del año 2016. Es así que a la fecha podríamos decir que el MINSA posee un SGSI y un SGR recién implementados, habiéndose cumplido irrestrictamente todos los lineamientos que sus respectivas normas establecen y serán sometidos a un proceso de certificación durante el año 2020.

Sin embargo, al ser sistemas recién implementados se desconocía la forma en que ambos se relacionaban entre sí. Según manifiesta Betacourt (2018) la planificación en conjunto de implementaciones de SGSI y Gestión del Riesgo es necesaria para evitar la colisión de los alcances que dichas implementaciones poseen según sus respectivas ISOs. Esto de por si constituía un problema, pues no se contaba con algún estudio que determinara de qué manera el desempeño de uno podría estar afectando al desempeño del otro. Durante el verano del 2017, las regiones de Piura y Tumbes sufrieron el peor fenómeno del Niño de

su historia donde la ciudad de Piura (capital de la región con el mismo nombre) sufre el desborde del rio, que trajo consigo una inundación en la ciudad de tal magnitud que el Hospital Regional de Piura perdió el legajo de los documentos de las historias clínicas de sus pacientes en un 45%. Como consecuencia de esto, durante las etapas de reconstrucción que dicho nosocomio ha tenido, se incluyó la recuperación de dichos archivos, sin embargo, estos trabajos que debieron culminarse a fines del año 2019 no han podido ser completados debido a las políticas restrictivas y poco flexibles que el SGSI posee y que entran en contradicción con los lineamientos que el sistema de Gestión de Riesgo implementado exige respecto al manejo y archivado de la documentación. Es por ende que el presente estudio pretendió determinar la relación existente entre estos dos sistemas y así tener una base teórica más amplia que permita entender su comportamiento en conjunto y que pueda usarse como precedente para el mejoramiento y adecuación que pudieran tener en el futuro la NTP para la implementación de estos sistemas.

En cuanto a las teorías relacionadas a nuestras variables de estudio debemos mencionar a Ríos (2014), quien define los SGSI como un framework para gestionar la información de una organización y esta esté siempre a buen recaudo. Este framework se basa en lineamientos que definen las funciones de las personas, las fases de los procesos y los programas computacionales mediante la aplicación de procedimientos de administración de estos recursos. Según este autor la implementación de un SGSI debe realizarse mediante el cumplimiento de sus 14 dominios para alcanzar los 34 objetivos que están claramente establecidos en la ISO:27001. Por otro lado, según consigna en su página web la empresa certificadora SGS, una empresa que decide optar por la certificación del estándar ISO:27001 de un SGSI debe haber cumplido para el caso del Perú, con los 14 dominios y 34 objetivos establecidos en la Norma Técnica Peruana (en adelante la llamaremos NTP) documento que se constituye en el marco metodológico para su implementación.

Según lo establecido en el NTP-ISO/IEC 27001:2018 estos dominios son los siguientes: Dominio 1 Políticas de Seguridad: Esta dimensión está vinculada a la implementación de políticas orientadas al aseguramiento de la información. Dominio 2 Aspectos Organizativos de la Seguridad de la Información: Establece la forma en que una institución introduce en la cultura organizacional el aseguramiento de la información. Dominio 3 Seguridad Ligada a los Recursos Humanos: Es la forma en la que la institución

implementa controles para el personal que labora en ella en las diferentes etapas de la vida laboral del colaborador, es decir desde su contratación hasta su salida. Dominio 4 Gestión de Activos: Establece los lineamientos bajo los cuales se Gestionan los recursos de la organización y su interacción con los colaboradores. Domino 5 Control de Acceso: Establece los lineamientos bajo los cuales se Gestionan el uso de los activos de la institución por parte de los colaboradores. Domino 6 Cifrado de Información: Determina las técnicas a utilizar por la entidad en la encriptación de la información sensible. Domino 7 Seguridad Física y Ambiental: Aquí se determina la forma que los activos de entidad se ubicaran físicamente y bajo qué condiciones. Domino 8 Seguridad Operativa: Establece los mecanismos que la entidad implementa para protegerse de posibles pérdidas de información. Domino 9 Seguridad en las Telecomunicaciones: Establece los mecanismos en que será compartida la información entre los colaboradores externos e internos de la organización. Domino 10 Compra, Elaboración y Soporte de los Sistemas de Información: Tiene que ver con la forma en se Gestionan los proyectos de desarrollo de software tanto para los proyectos internos como los de outsourcing. Domino 11 Relaciones con Suministradores: Son los diferentes lineamientos dirigidos al control de los proveedores de servicios de la entidad. Domino 12 Gestión de Incidentes en la Seguridad de la Información: Son el conjunto de políticas que la entidad debe implementar para recuperarse frente a los incidentes que se presentan como consecuencia del desarrollo de sus actividades. Domino 13 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio: Tiene que ver con las acciones a tomar luego de presentado un incidente que pone en riesgo la información de la entidad. Domino 14 Cumplimiento: Tiene que ver con las acciones orientadas a la supervisión y cumplimiento de las medidas de seguridad implementadas.

Por otro lado, para el entendimiento teórico de nuestra variable 2 la implementación y estudio de los SGR, recurrimos a lo manifestado por Velásquez, Velásquez, Velásquez y Villa (2017), quienes indican que la implementación de un SGR está claramente normada por la ISO:31000 siendo esta una base sólida para el establecimiento de dichos procesos. También tenemos el caso de Rivero (2017), quien manifiesta que toda implementación de un SGR no debe para nada alejarse de lo establecido universalmente por la respectiva norma ISO. Según Moscoso, Esau y Soto (2018) la implementación de un SGR en nuestro país está regulada por la NTP-ISO 31000:2018. Esto mismo es manifestado por Celi (2016), quien indica que para las implementaciones en nuestro país de un SGR toda organización debe

recurrir a lo establecido por la NTP que es el marco normativo valido en nuestro país según lo establecido por las leyes en el Perú. Según este mismo autor, un SGR se describe como un framework que evalúa, orienta y supervisa el riesgo determinando puntos de control y de acción correctiva que deben ser implementados con el fin de garantizar que se cuente con el tratamiento adecuado según el tipo de riesgo que se pueda presentar en una organización.

Según lo establecido por la NTP, los SGR permiten manejar la incertidumbre respecto una amenaza, mediante un conjunto de acciones que permiten la identificación, el análisis y la evaluación de riesgo, estableciendo sus correctivos respectivos. Estas acciones permiten transferir el riesgo a otra parte, evitándolo o reduciendo el impacto negativo. Además, considera que los SGR son el conjunto de acciones que permiten identificar, analizar y cuantificar un desastre, mediante el uso de acciones de evaluación, orientación y supervisión.

Para la NTP, sus alcances u objetivos están agrupados en 3 dominios de aplicación. Estos dominios o dimensiones son los siguientes según su grado de relevancia: Dimensión 1 Evaluación, considerado como las fases dirigidas a la identificación del riesgo estableciendo su prioridad la ejecución del respectivo correctivo. Dimensión 2 Orientación, La norma la considera como el conjunto de principios que ofrecen una dirección a los riesgos explicando la intención y propósito de los correctivos. Estos principios la razón de la existencia de los SGR y permiten a una organización minimizar la incertidumbre sobre los procesos propios de la organización. Dimensión 3 Supervisión, esta otra parte fundamental de los SGR permitiendo alinear el control sobre los riesgos, en cumplimiento de los objetivos organizacionales. Por otro lado, menciona que en la supervisión deben coexistir el personal y la alta dirección, estableciendo estrategias donde no solo incluyan las dificultades actuales, sino que también las futuras.

Para la fundamentación de nuestra investigación se recurrió a trabajos precedentes que nos permitan entender el comportamiento de estos dos sistemas independientes. Dentro de los antecedentes nacionales tenemos a Moscoso, Esaú y Soto (2018) en su trabajo “Modelo de Gestión de Riesgos de TI que contribuye a la Operación de los procesos de Gestión Comercial de las Empresas del Sector de Saneamiento del Norte del Perú” de diseño descriptivo, tuvo como objetivo mejorar los procesos de gestión comercial a través del desarrollo de un modelo de gestión de riesgos de TI adecuado a las empresas de saneamiento

del norte del Perú. El autor concluye que el modelo de gestión de riesgos de TI propuesto aporto para la identificación de los riegos y categorizarlos para su intervención.

También está el estudio de Baca (2016), cuyo trabajo "Diseño de un Sistema de Gestión de la Seguridad de la Información para la Unidad de Gestión Educativa Local – Chiclayo", con un diseño pre experimental, para implementar un SGSI basándose en la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2013, integrado a COBIT 5. En su investigación el autor concluye un SGSI permite mejorar la situación actual que vive la entidad respecto al uso de la información, debido a la generación de una efectiva administración de la información.

Tenemos también el caso de Seclén (2016), y su trabajo "Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001", descriptivo con enfoque cualitativo, que tuvo por objetivo determinar los niveles de madurez de las entidades públicas que han implementado un SGSI y que factores influyen en su correcto desarrollo. El autor concluye que las entidades enfrentan múltiples desafíos luego de su implementación, recomendando su no implementación cuando no se cuenta con procesos claramente definidos o funciones no perfectamente definidas.

Esta también el estudio de Tarrillo (2015), con su trabajo "Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015", de diseño correlacional descriptivo y de tipo no experimental, que tuvo por objetivo conocer un SGR afecta a los activos informáticos. El autor concluye que existe influencia del SGR sobre los activos de información de forma significativa y positiva.

También tenemos el caso de Córdova, Morales y Samamé (2015), en su trabajo "Desarrollo de un SGSI para los Colegios Profesionales en la Región Lambayeque. Caso de estudio: Colegio de Ingenieros", con diseño pre experimental que tuvo por objetivo usar la norma ISO 27001 para la implementación de un SGSI. Los autores concluyen que la implementación del SGSI les permitió asegurar que en un futuro se podrá actuar de una manera asertiva y proactiva; para tener la capacidad de reaccionar con rapidez ante cualquier

incidente que afecta a los Sistemas de Información, recomendando realizar estudios de impacto sobre los riesgos a los que pueda ser sometidos los activos de información.

Respecto a los antecedentes internacionales tenemos a Casadesús (2018) en su trabajo "La Gestión del Riesgo Aplicada a la Gestión de Documentos y su Impacto en la Rendición de Cuentas Públicas", con diseño correlacional y enfoque cuantitativo, cuyo objetivo fue medir el impacto un SGR en los sistemas de gestión documental en las organizaciones públicas de Barcelona. El autor concluye que existe una estrecha y positiva relación entre el SGR y la rendición publica, demostrando que un SGR mejora considerablemente los activos de información debido a su relación significativa y directamente proporcional.

Valencia y Orozco (2017) que en su trabajo "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000" con diseño descriptivo, tuvo por objetivo proponer una SGSI con énfasis en las ISO 27001, 27002, 27005 y 27003. En este trabajo el autor concluye que, la cantidad de normas de la ISO/IEC 27000 vuelve complejo el proceso de desarrollo un SGR. Por ende, su investigación busco establecer un marco metodológico para su implementación.

Bernal (2017), "Propuesta de un Plan de Gestión de Riesgos y Gestión Ética para el Departamento de Tecnologías en el Sector Educativo", con diseño descriptivo cualitativo, cuyo objetivo fue identificar los principales riesgos de TI para el desarrollo de un SGR basado en la ISO 31000:2011 (ISO, 2017), donde el autor concluye que, es necesario elaborar un plan estratégico previo y único que sirva de base a las organizaciones educativas para minimizar las amenazas a la información y alcanzar los estándares internacionales vinculados a la implementación de un SGR.

También está el caso de De Souza (2016), en su investigación "Guía de Apoyo a la Implementación de la Norma ISO 31000 para la Gestión de Riesgos de TI: Un Caso de Estudio en IFTO", de diseño exploratorio y enfoque cualitativo, cuyo objetivo fue el establecer un marco metodológico para la facilitar el desarrollo de un SGR en TI. El autor concluye que gerenciar y controlar los riesgos relacionados a las actividades de los sectores de TI en las organizaciones públicas del Brasil son un gran reto y su estudio según los

especialistas consultados, cumple con los objetivos y entrega un marco metodológico valido para su implementación.

Esta el caso de Fassheber (2016) y su investigación "Análisis de Madurez de Gestión de Riesgos en el Ministerio de Planeamiento: Proponer y Aplicar un Instrumento de Evaluación Orientada a Procesos de TI", de diseño descriptivo y enfoque cualitativo, cuyo objetivo es diseñar un instrumento para cuantificar la madurez en gestión de riesgos en los procesos de TI. El autor concluye que, en su estudio hacen entrega de un instrumento que parte de un modelo comparativo entre los diversos modelos de madurez existentes, desde los genéricos hasta los frameworks tradicionales para poder establecer un modelo propio de medición que se ha ajustado perfectamente a la realidad de la entidad pública objeto de estudio.

Nuestro trabajo de investigación tiene como justificaciones del estudio lo siguiente: Como Justificación Teórica, tenemos el analizar el SGSI en el MINSA, basándose en la NTP-ISO/IEC 27001:2018 y su relación con el SGR normado por el estándar NTP-ISO 31000:2018, de forma tal que nuestros resultados incorporen nuevos conocimientos a la comunidad científica sobre el aseguramiento de la información y su relación con la gestión de riesgos.

Como Justificación Práctica tenemos que se carece de un estudio que permita corroborar la existencia o no de relación entre nuestras variables, que sirva como marco de referencia para posteriores estudios con el fin analizar el impacto de la implementación de SGSI en las Gestiones del riesgo. Como Justificación Metodológica tenemos que para alcanzar los objetivos de la investigación se aplicó una investigación de nivel correlacional con un diseño no experimental de corte transeccional.

El marco teórico se constituye en el fundamento para la operacionalización de las variables en dimensiones, indicadores y será determinante en la elaboración de un instrumento de medición, que será validado por juicio de expertos y se comprobará su funcionamiento mediante una prueba piloto con la que se medirá su confiabilidad. El cuestionario aplicado permitió la recolección de datos que fueron posteriormente analizados

mediante el programa SPSS v22 para corroborar las hipótesis planteadas en esta investigación.

En nuestra investigación tenemos como problema principal ¿Cuál es la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud, 2019? Asimismo, como problemas secundarios fueron ¿Cuál es la relación que existe entre Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Evaluación, 2019?, ¿Cuál es la relación que existe entre Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Orientación, 2019?, ¿Cuál es la relación que existe entre Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Supervisión, 2019?.

En cuanto a los objetivos tenemos como objetivo principal, Identificar la relación que existe entre el Sistema de Gestión de Seguridad de la Información del Ministerio de Salud y la Gestión del Riesgo, 2019. Asimismo, como objetivos secundarios tenemos: Identificar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Evaluación, 2019, Identificar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Orientación, 2019, Identificar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Supervisión, 2019.

Respecto a las hipótesis tenemos como hipótesis principal, El Sistema de Gestión de Seguridad de la Información está relacionada con la Gestión del Riesgo del Ministerio de Salud, 2019. Asimismo, como hipótesis secundarias tenemos: El Sistema de Gestión de Seguridad de la Información está relacionada con la Gestión del Riesgo del Ministerio de Salud respecto a la dimensión Evaluación, 2019, El Sistema de Gestión de Seguridad de la Información está relacionada con la Gestión del Riesgo del Ministerio de Salud respecto a la dimensión Orientación, 2019, El Sistema de Gestión de Seguridad de la Información está relacionada con la Gestión del Riesgo del Ministerio de Salud respecto a la dimensión Supervisión, 2019.

II. Método

2.1. Tipo y diseño de investigación

Nuestro trabajo está basado en un enfoque cuantitativo, de acuerdo al método deductivo teniendo como variables: Sistema de Gestión de Seguridad de la Información y Gestión del Riesgo, permitiendo establecer nuestras hipótesis respecto a lo que pretendíamos demostrar. Esto debido a que se han utilizado datos para la corroboración de la hipótesis. Según Baptista, Fernández y Hernández (2014), este tipo de estudio se basa en una medición matemática y el estudio de los datos por métodos estadísticos con el fin de establecer los comportamientos que nos permitan demostrar nuestras hipótesis.

Se ha tomado como diseño el Correlacional no experimental con corte transeccional. Es no experimental debido a la falta de manipulación de las variables, las que se analizaron de manera intacta. Es transeccional porque la captura de datos se ejecutó a través de la aplicación de instrumentos en un solo instante de tiempo.

Para Baptista, Hernández y Fernández (2014) los estudios no experimentales son aquellos donde las variables no son alteradas o manipuladas. Para estos mismos autores el diseño transeccional captura los datos en un tiempo único.

2.2. Operacionalización

En este apartado desarrollamos los conceptos o definiciones específicas de los temas o palabras claves que se usaron en la investigación, y que están relacionados con las variables y sus dimensiones según Baptista, Fernández y Hernández (2014).

2.2.1. Definición conceptual

SGSI.

Un SGSI, está definido como un framework normado internacionalmente por la ISO 27001 cuyo enfoque está dirigido a sostener la integridad de la información. En nuestro país está regido por la NTP, que es la base sobre la cual todo SGSI se rige para su implementación a nivel gubernamental y privado. Según la NTP-ISO/IEC 27001:2018, los SGSI permiten “gestionar de forma adecuada los activos de información, para lo cual se debe hacer uso de

un procedimiento único a toda la entidad, con el fin de minimizar los riesgos siendo esto el fundamento de un SGSI" (p. 28).

SGR.

Para la NTP-ISO/IEC 31000:2018, un SGR "permite manejar la incertidumbre respecto una amenaza, mediante un conjunto de acciones que permiten la identificación, el análisis y la evaluación de riesgo, estableciendo sus correctivos respectivos" (p. 20). Esta norma es la rige en nuestro país para, el análisis, implementación y evaluación del riesgo, definiendo un conjunto de estrategias dirigidas a mitigación de todo factor de amenaza. Es bajo este contexto que esta norma sienta las bases para su uso en nuestro país.

2.2.2. Definición operacional

SGSI.

Según la NTP-ISO/IEC 27001:2018, este framework se compone con 14 dominios de aplicación, 34 objetivos y 144 protocolos de control. "Estos dominios abarcan la totalidad de ámbitos organizacionales susceptibles a sufrir algún daño a sus procesos de informáticos" (p. 32). Para el presenta trabajo se han tomado los dominios como dimensiones de la variable SGSI ya es a través de ellos que se define su ámbito de aplicación. Por otro lado, los objetivos que según la NTP estable los alcances que debe de contener toda implementación SGSI, razón por la cual se han tomado los objetivos como indicadores para el presente trabajo.

Gestión del Riesgo.

Según la NTP-ISO/IEC 31000:2018, "los SGR necesitan de una base que permita la gestión de los riesgos, el cual se agrupa en 3 dominios de aplicación que son la Evaluación, Orientación y Supervisión, que están ordenados según su grado de importancia" (p. 6). Estos dominios son los que se han tomado como dimensiones para el estudio de esta variable y sus respectivos objetivos como indicadores.

Tabla 1

Matriz Operacional de la Variable SGSI

Dimensiones	Indicadores	Ítem	Escala de valoración	Niveles y Rangos
Políticas de Seguridad	✓ Directrices de la Dirección en seguridad de la información.	1	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Aspectos Organizativos de la Seguridad de la Información	✓ Organización interna. ✓ Dispositivos para movilidad y teletrabajo.	2-3	Pregunta cerrada politómica Escala ordinal de Likert (4) Nunca. (5) A veces. (6) Con Frecuencia. (7) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Seguridad Ligada a los Recursos Humanos	✓ Antes de la contratación. ✓ Durante la contratación. ✓ Cese o cambio de puesto de trabajo.	4-6	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Gestión de Activos	✓ Responsabilidad sobre los activos. ✓ Clasificación de la información. ✓ Manejo de los soportes de almacenamiento.	7-9	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Control de Accesos	✓ Requisitos de negocio para el control de accesos. ✓ Gestión de acceso de usuario. ✓ Responsabilidades del usuario. ✓ Control de acceso a sistemas y aplicaciones.	10-13	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.

Cifrado de Información	✓ Controles Criptográficos	14	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Seguridad Física y Ambiental	✓ Áreas seguras. ✓ Seguridad de los equipos	15-16	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Seguridad En La Operativa	✓ Responsabilidades y procedimientos de operación. ✓ Protección contra código malicioso. ✓ Copias de seguridad. ✓ Control del software en explotación. ✓ Gestión de la vulnerabilidad técnica. ✓ Consideraciones de las auditorías de los sistemas de información.	17-22	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Seguridad en las Telecomunicaciones	✓ Gestión de la seguridad en las redes. ✓ Intercambio de información con partes externas.	23-24	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	✓ Requisitos de seguridad de los sistemas de información. ✓ Seguridad en los procesos de desarrollo y soporte. ✓ Datos de prueba.	25-27	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.

Relaciones con Suministradores	✓ Seguridad de la información en las relaciones con suministradores. ✓ Gestión de la prestación del servicio por suministradores.	28-29	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Gestión de Incidentes en la Seguridad de la Información.	✓ Gestión de incidentes de seguridad de la información y mejoras.	30	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.	✓ Continuidad de la seguridad de la información. ✓ Redundancias.	31-32	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Cumplimiento.	✓ Cumplimiento de los requisitos legales y contractuales. ✓ Revisiones de la seguridad de la información.	33-34	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.

Fuente: Elaboración Propia

Tabla 2

Matriz Operacional de la Variable SGR

Dimensiones	Indicadores	Ítem	Escala de valoración	Niveles y Rangos
Evaluación	✓ Niveles de riesgo relacionados a las TI. ✓ Umbrales de tolerancia. ✓ Riesgos empresariales. ✓ Decisiones estratégicas. ✓ Valoración según estándares. ✓ Recuperación y tolerancia ante perdidas de TI.	1-6	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Orientación	✓ Oportunidades e impactos potenciales. ✓ Decisiones y operaciones estratégicas. ✓ Elaboración de planes. ✓ Capacidad de respuesta	7-10	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.
Supervisión	✓ Umbrales de apetito. ✓ Metas y métricas clave. ✓ Objetivos identificados. ✓ Consejo o comité de dirección.	11-14	Pregunta cerrada politómica Escala ordinal de Likert (0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	1. Deficiente. 2. Regular. 3. Eficiente.

Fuente: Elaboración Propia

2.3. Población, muestra y muestreo

Población.

Se ha considerado a los 145 trabajadores pertenecientes a la Unidad de Gestión de Inversiones de Reconstrucción con Cambios, que es la dependencia del Ministerio de Salud donde se realizó el estudio. Según Baptista, Fernández y Hernández (2014) una población se define como aquel grupo de fenómenos a examinar, donde los entes de la población tienen una particularidad igualitaria a la cual se investiga.

Muestra.

Estuvo formada por los 145 trabajadores administrativos de la Unidad de Gestión de Inversiones de Reconstrucción con Cambios como técnica censal y tipo no probabilístico intencional. Según Baptista, Fernández y Hernández (2014) es aquel sub grupo de la población sobre los cuales se realizará la captura de datos.

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

Técnica de recolección de datos.

La encuesta fue usada como técnica mediante la aplicación de un cuestionario. Según Baptista, Fernández y Hernández (2014) los cuestionarios son aquel conjunto de preguntas con un número codificado de respuestas para las variables objeto del estudio.

Tabla 3

Tipos de Técnicas e Instrumentos Usados en la Recolección de Datos

Técnicas	Instrumentos
Encuesta	Cuestionario

Fuente: Elaboración Propia

Según se especifica en la Tabla 3, nuestra investigación utilizo como técnica la encuesta y como instrumento un cuestionario para cada variable.

Tabla 4

Ficha Técnica del Instrumento del SGSI

SGSI	
Técnica	Encuesta
Instrumento	Cuestionario
Autor	Oscar Yonatan Huayllani Muñoz
Extensión	Formado por 34 preguntas
Significación	Conformada por 14 dimensiones que capturan las impresiones del observador en cuanto al SGSI. Se cuenta con 34 indicadores y cada indicador consta de un ítem.
Puntuación	Las respuestas que el observador puede obtener ante cada enunciado son: Nunca (0), A veces (1), Con Frecuencia (2), Siempre (3)
Duración	60 minutos.
Aplicación	Trabajadores de la Unidad de Gestión de Inversiones de Reconstrucción con Cambios.
Administración	Única vez.

Fuente: Elaboración Propia

Tabla 5

Ficha Técnica del Instrumento del SGR

SGR	
Técnica	Encuesta
Instrumento	Cuestionario
Autor	Oscar Yonatan Huayllani Muñoz
Extensión	Consta de 14 ítems
Significación	Conformado por 3 dimensiones que capturan las impresiones del observador en cuanto al SGR. Se cuenta con 14 dimensiones y cada indicador consta de un ítem.
Puntuación	Las respuestas que el observador puede obtener ante cada enunciado son: Nunca (0), A veces (1), Con Frecuencia (2), Siempre (3)
Duración	60 minutos.
Aplicación	Trabajadores de la Unidad de Gestión de Inversiones de Reconstrucción con Cambios.
Administración	Única vez.

Fuente: Elaboración Propia

Validez.

En la presente investigación, el cuestionario fue certificado por el juicio de tres competentes en metodología de investigación quienes validaron el instrumento que dando como resultado su aplicabilidad. Según Baptista, Fernández y Hernández (2014) "la validez es el nivel en que un instrumento captura las variantes que se procuran valorar" (p.245).

Tabla 6

Resultados del Juicio de Expertos

Expertos	Grado Académico	Especialidad	Juicio
Angel Salvatierra Melgar	Doctor	Matemático Estadístico	Procede
Gustavo Ernesto Zarate Ruiz	Magister	Temático	Procede
Pedro Martin Lezama Gonzales	Doctor	Ing. De Sistemas	Procede

Fuente: Elaboración Propia

Para cuantificar esta validez de contenido se recurrido al juicio de expertos y han realizado las siguientes pruebas estadísticas:

Prueba de Aiken.

Conocida también como coeficiente de validez V, Según Escurra (1987), esta prueba "se computa como la razón de un dato obtenido sobre la suma máxima de la diferencia de los valores posibles" (p. 107).

Teniéndose que: $S =$ $V = \dfrac{S}{(n(c-1))}$

$S_i =$

n = Número de jueces.

C = Número de valores de la escala de valoración.

Para nuestro caso y según nuestro instrumento, tenemos los siguientes valores:

$$V = 3 / (3 * (2-1)) = 1$$

El valor de 1, corresponde al 100%, por lo que podemos afirmar que nuestro instrumento tiene un nivel de validez alto para la prueba de Aiken. Por tenerse los mismos datos para los dos instrumentos de nuestra investigación podemos inferir que ambos instrumentos cumplen con la prueba de Aiken.

Prueba Binomial.

Según Escurra (1988) "es un análisis estadístico, que estudia la probabilidad de obtener x objetos en una categoría y n – x objetos en la otra". (p. 106). Para nuestro estudio se procesaron los datos en el software SPSS obteniéndose los siguientes valores según la Tabla 7.

Tabla 7

Resultados de Prueba Binomial del Instrumento que mide el SGSI y SGR

	Juez	Grupo	Categoría	N	Proporción observada	Prop. de prueba	Sig. exacta (unilateral)
SGSI	1	1	Si	34	1,00	0,85	0,004
		2	No	0	0	0	0
		Total		34	1,00		
	2	1	Si	34	1,00	0,85	0,004
		2	No	0	0	0	0
		Total		34	1,00		
	3	1	Si	34	1,00	0,85	0,004
		2	No	0	0	0	0
		Total		34	1,00		
SGR	1	1	Si	14	1,00	0,85	0,014
		2	No	0	0	0	0
		Total		14	1,00		
	2	1	Si	14	1,00	0,85	0,014
		2	No	0	0	0	0
		Total		14	1,00		
	3	1	Si	14	1,00	0,85	0,014
		2	No	0	0	0	0
		Total		14	1,00		

Fuente: Elaboración Propia

Como se puede apreciar en la Tabla 7 en el caso de la variable SGSI el nivel de sig. Para el p valor es de 0,004 que es menor al $\alpha = 0,15$ por lo que podemos afirmar que se acepta la hipótesis de que el instrumento cuenta con validez a un nivel de confianza del 85%. En el caso de la variable SGR, el nivel de sig. Para el p valor es de 0,014 que es menor al $\alpha = 0,15$ por lo que podemos afirmar que se acepta la hipótesis de que el instrumento cuenta con validez a un nivel de confianza del 85%.

Pruebas de Kaiser-Meyer-Olkin y Esfericidad de Bartlett.

Según Fuente (2011) son pruebas que tratan de validar el constructo de un instrumento, basándose en un análisis factorial para determinar "la varianza común a todas las variables" (p. 2). Para nuestro estudio, se ha procesado los valores de la prueba piloto para determinar mediante el software SPSS v.20 los valores de KMO y Bartlett. Según este análisis se han obtenido los siguientes valores:

Tabla 8

Prueba KMO y Bartlett para el instrumento que mide el SGSI y SGR

SGSI	Medida de adecuación muestral de Kaiser-Meyer-Olkin.		0,787
	Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	21,305
		gl	6
		Sig.	,020
SGR	Medida de adecuación muestral de Kaiser-Meyer-Olkin.		0,670
	Prueba de esfericidad de Bartlett	Chi-cuadrado aproximado	13,574
		gl	3
		Sig.	0,004

Fuente: Elaboración Propia

Como se puede ver en la Tabla 8 para la variable SGSI, la medida de KMO es de 0,787 lo cual es considerado significativamente alto, según Fuente (2011) "los valores KMO > 0,6 son bastante buenos, pero no se puede solo tomar este valor es necesario analizar los resultados de la esfericidad de Bartlett" (p. 85), según este autor el p valor debe ser menor a un $\alpha = 0,05$. Como se puede apreciar en la misma tabla, se obtuvo como resultado un p valor de 0,02 por lo que se aprueba la hipótesis de que existe validez de constructo en el instrumento. En el caso de la variable SGR, la medida de KMO es de 0,670 lo cual es considerado aceptable, con un p valor de 0,004 por lo que se aprueba la hipótesis de que existe validez de constructo en el instrumento. Por otro lado, se pudo analizar las dimensiones mediante el método de Componentes Principales a los instrumentos tanto para la variable SGSI como para la SGR obteniéndose los siguientes resultados:

Tabla 9

Varianza Total Explicada para la SGSI y la SGR

	Componente	Autovalores iniciales			Sumas de las saturaciones al cuadrado de la extracción		
		Total	% de la varianza	% acumulado	Total	% de la varianza	% acumulado
SGSI	1	3,939	65,655	65,655	3,939	65,655	65,655
	2	1,058	17,627	83,283	1,058	17,627	83,283
	3	,416	6,927	90,210			
	4	,262	4,366	94,576			
	5	,226	3,761	98,337			
	6	,100	1,663	100,000			
SGR	1	2,443	81,423	81,423	2,443	81,423	81,423
	2	,405	13,512	94,935			
	3	,152	5,065	100,000			

Fuente: Elaboración Propia

Con los valores mostrados en la Tabla 9 podemos inferir que para la variable SGSI, los datos se explican al 83,283% para los ítems de nuestro instrumento. Por otro lado, para la variable SGR vemos que los datos se explican al 81,423% a los ítems de nuestro instrumento.

Confiabilidad.

Se empleó prueba piloto con el objeto de obtener el valor Alpha de Cronbach y determinar la solidez de los ítems para cada variable que para Baptista, Fernández y Hernández (2014) "este estudio se efectúa con el modelo Alpha de Cronbach para variables con escalas politómicas o de tipo Likert" (p. 167).

Tabla 10

Prueba de Confiabilidad del Instrumento que mide el SGSI y la SGR

Variable	Alpha de Cronbach	N de Elementos
SGSI	,907	34
SGR	,942	14

Fuente: Elaboración Propia

Teniendo en cuenta los valores de la tabla 10, para la variable SGSI se observa que el coeficiente de Alpha de Cronbach obtenido es de 0.907, por lo cual podemos afirmar que el instrumento tiene un excelente de confiabilidad según la Figura 1. Por otro lado, para la

variable SGR el Alpha de Cronbach es igual a 0,942 que también presenta según la figura 1 un grado de confiabilidad excelente.

Coeficiente	Criterio
> 0,9	Excelente
> 0,8	Bueno
> 0,7	Aceptable
> 0,6	Cuestionable
> 0,5	Pobre
< 0,5	Inaceptable

Figura 1

Criterios de Evaluación del Alpha de Cronbach

Fuente: Metodología de correlación estadística de un sistema integrado de gestión de la calidad en el sector salud, Revista Signos vol. 10 Num. 2 (2018).

2.5. Procedimiento

Para realización de la presente investigación se tomó en consideración dos fuentes de información: Teórica y de Campo. En la fuente teórica, la información se obtuvo mediante libros, revistas y artículos científicos búsquedas de forma virtual mediante buscadores especializados. En la fuente de campo, los resultados del cuestionario fueron obtenidos de forma presencial mediante la aplicación de los instrumentos que miden la SGSI y la gestión del riesgo.

2.6. Métodos de análisis de datos

En el análisis de las variables se empleó el SPSS v.22, el cual nos proporcionó las gráficas y porcentajes en las tablas de frecuencia, lo cual nos dio material para exponer los resultados en tablas. Según Baptista, Fernández y Hernández (2014) manifiesta que "para las informaciones obtenidas es esencial transformarlos, para ello se ejecuta una medición matemática" (p. 270).

2.7. Aspectos éticos

La información obtenida dentro de esta investigación no ha sido mostrada a la opinión pública y no será mostrada si la unidad del MINSA en estudio no lo desea, puesto que se ejecutó el estudio para enriquecer el entendimiento que se posee sobre los SGSI y la SGR recientemente implementados. Se ha respetado la propiedad intelectual de los autores

consultados y se ha usado citas estilo APA en los casos en los que se ha tomado ideas de estos.

III. Resultados

3.1. Análisis Descriptivo

Análisis Univariado de las Variables SGSI y SGR.

Tabla 11

Distribución de Frecuencias de la Variable SGSI

Variable	Nivel	Frecuencia	Porcentaje	Porcentaje Acumulado
SGSI	Deficiente	1	0,7	0,7
	Regular	118	81,4	82,1
	Eficiente	26	17,9	100,0
SGR	Deficiente	2	1,4	1,4
	Regular	115	79,3	80,7
	Eficiente	28	19,3	100,0

Fuente: Elaboración Propia

En la tabla 11, se observa de una muestra de 145 trabajadores para el caso del SGSI, el 0,7% considera que es un sistema deficiente, 81,4% lo considera regular y 17,9% lo considera deficiente. Para el caso del SGR el 1,4% lo considera deficiente, el 79,3% lo considera regular y 19% lo considera eficiente.

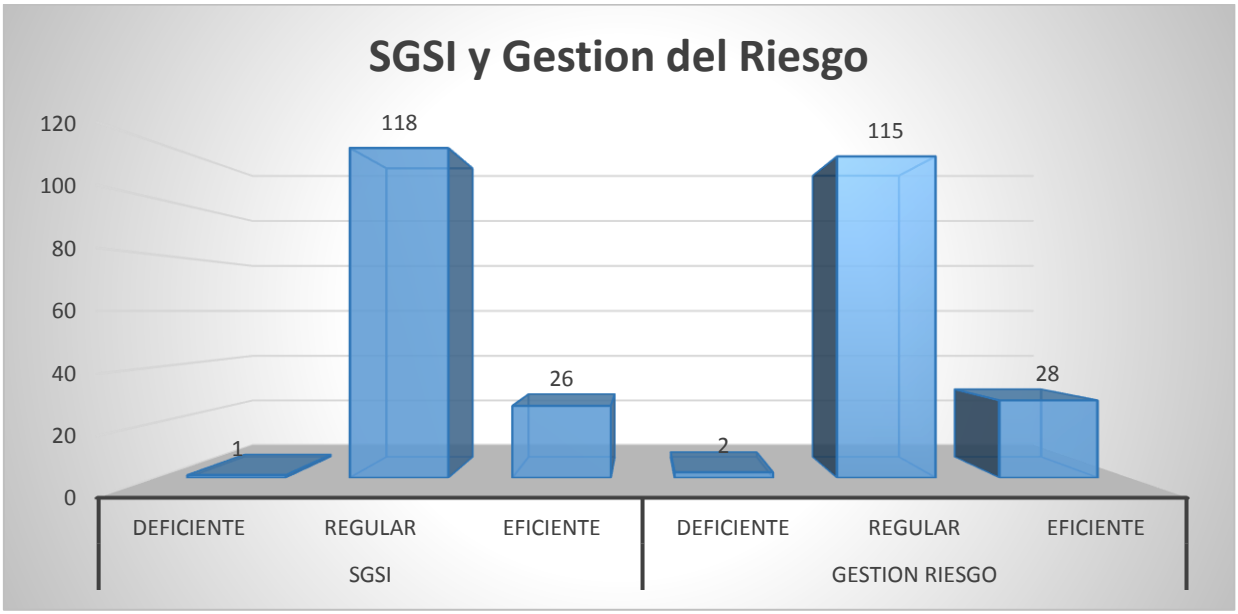


Figura 2

Gráfica de la Distribución de Frecuencias de la Variable SGSI y Gestión del Riesgo

Fuente: Elaboración Propia

En la figura 2, se observa de una muestra de 145 trabajadores, 118 consideran que el SGSI implementado en el MINSA es regular, 1 lo considera deficiente y 26 lo considera eficiente. Para el caso de la Gestión del Riesgo se observa que el 115 la considera regular, 2 dijeron que es deficiente y 28 lo consideran eficiente.

Análisis Bivariado de las Variables SGSI y SGR.

Tabla 12

Tabla Cruzada entre la SGSI y la SGR con sus Dimensiones

Variable y Dimensiones		SGSI		
		Deficiente	Regular	Eficiente
Gestión del Riesgo	Deficiente	1 50,0%	1 50,0%	0 0,0%
	Regular	0 0,0%	115 100,0%	0 0,0%
	Eficiente	0 0,0%	2 7,1%	26 92,9%
Evaluación	Deficiente	1 66,7%	14 8,6%	0 0,0%
	Regular	0 0,0%	100 100,0%	0 0,0%
	Eficiente	0 0,0%	4 13,3%	26 86,7%
Orientación	Deficiente	1 6,3%	15 93,8%	0 0,0%
	Regular	0 0,0%	100 97,1%	3 2,9%
	Eficiente	0 0,0%	3 11,5%	23 88,5%
Supervisión	Deficiente	1 8,3%	11 91,7%	0 0,0%
	Regular	0 0,0%	105 98,1%	2 1,9%
	Eficiente	0 0,0%	2 7,7%	24 92,3%

Fuente: Elaboración Propia

Aquí se puede observar que de la muestra de 145 trabajadores 115 opinan que las políticas de SGSI está en el nivel regular de la Gestión de Riesgos. También se puede observar que 100 opinan que las políticas de SGSI está en el nivel regular de la Gestión de Riesgos respecto a la Evaluación, 100 también opinaron que las políticas de SGSI está en el nivel regular de la Gestión de Riesgos respecto a la Orientación y 105 piensan que las políticas de SGSI está en el nivel regular de la Gestión de Riesgos respecto a la Supervisión. De lo

anteriormente expuesto podemos observar que se tiene una percepción de que la gestión del riesgo está en el nivel regular a eficiente en el desempeño del SGSI.

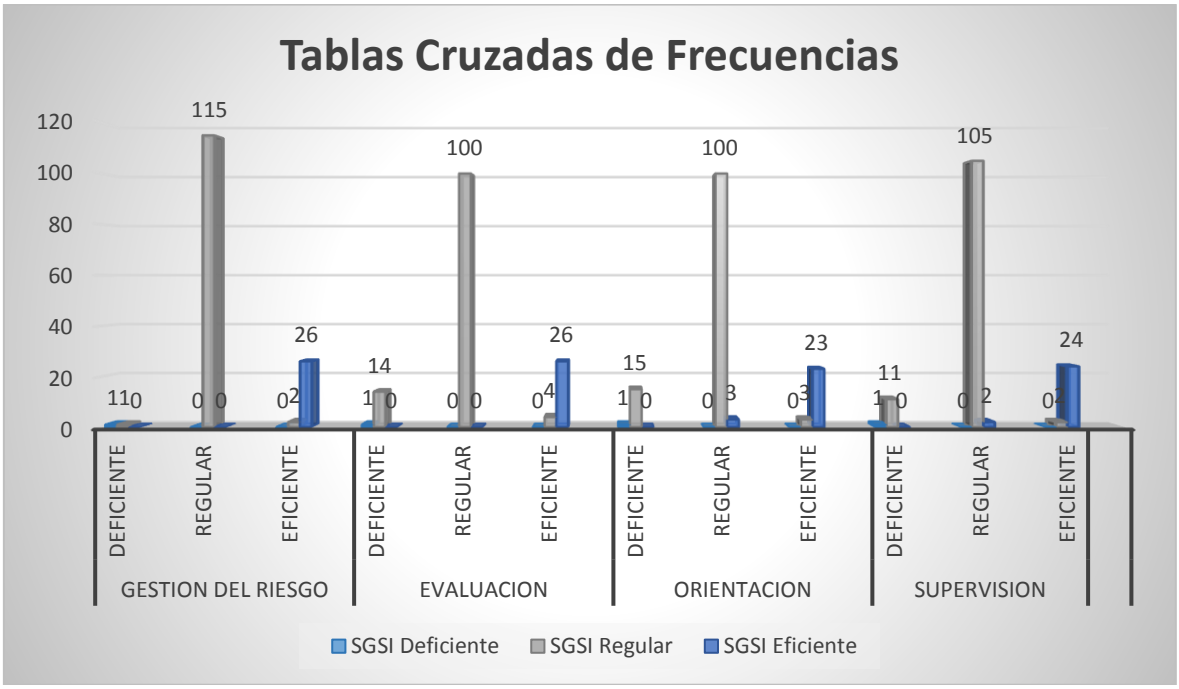


Figura 3

Gráfica Agrupada de SGSI y Gestión del Riesgo con sus Dimensiones

Fuente: Elaboración Propia

Según la Figura 3, de conformidad con los resultados existe una percepción por parte del personal encuestado que la gestión del riesgo está en el nivel regular sobre el SGSI con tendencia a la eficiencia. De igual forma se observa en el análisis por dimensiones tanto para la evaluación como para la orientación y la supervisión.

3.2. Análisis Inferencial.

Para la validación de las hipótesis se asumieron los siguientes supuestos:

Nivel de significación de prueba.

El análisis de la prueba se asume un $\alpha = 0.05$ con una confianza del 95%.

Selección del estadístico de prueba.

Según Baptista, Fernández y Hernández (2014), para las investigaciones donde se hace uso de la escala de Likert, no es necesario realizar una prueba de normalidad (p. 94). Por lo tanto, se utilizó el estadístico no paramétrico de Rho de Spearman.

Decisión de prueba.

Para asumir la decisión de la contrastación se tomó a:

p_valor $< \alpha = 0.05$; rechazar la hipótesis nula.

p_valor $\geq \alpha = 0.05$; No se rechazar la hipótesis nula.

3.2.1. Pruebas de Hipótesis.

Hipótesis General:

Ho: El Sistema de Gestión de Seguridad de la Información del Ministerio de Salud no se relaciona con la Gestión del Riesgo en el Ministerio de Salud, 2019.

Ho: $\rho = 0$

Ha: El Sistema de Gestión de Seguridad de la Información del Ministerio de Salud se relaciona con la Gestión del Riesgo en el Ministerio de Salud, 2019.

Ha: $\mu_2 < \mu_1$

Así mismo se plantearon las siguientes hipótesis específicas:

Hipótesis Específica 1:

Ho: El Sistema de Gestión de Seguridad de la Información del Ministerio de Salud no se relaciona con la Gestión del Riesgo respecto a la dimensión Evaluación, 2019.

Ho: $\rho = 0$

Ha: El Sistema de Gestión de Seguridad de la Información del Ministerio de Salud se relaciona con la Gestión del Riesgo respecto a la dimensión Evaluación, 2019.

Ha: $\rho \neq 0$

Hipótesis Específica 2:

Ha: El Sistema de Gestión de Seguridad de la Información del Ministerio de Salud no se relaciona con la Gestión del Riesgo respecto a la dimensión Orientación, 2019.

Ho: $\rho = 0$

Ha: El Sistema de Gestión de Seguridad de la Información del Ministerio de Salud se relaciona con la Gestión del Riesgo respecto a la dimensión Orientación, 2019.

Ha: $\rho \neq 0$

Hipótesis Específica 3:

Ho: El Sistema de Gestión de Seguridad de la Información del Ministerio de Salud no se relaciona con la Gestión del Riesgo respecto a la dimensión Supervisión, 2019.

Ho: $\rho = 0$

Ha: El Sistema de Gestión de Seguridad de la Información del Ministerio de Salud se relaciona con la Gestión del Riesgo respecto a la dimensión Supervisión, 2019.

Ha: $\rho \neq 0$

Luego de aplicar los estadísticos respectivos a las variables se obtuvieron los siguientes resultados:

Tabla 13

Resultados de la Prueba de Hipótesis

			SGSI
Rho de Spearman	SGR	Coeficiente de correlación	0,856**
		Sig. (bilateral)	0,000
		N	145
	Evaluación	Coeficiente de correlación	0,794**
		Sig. (bilateral)	0,000
		N	145
	Orientación	Coeficiente de correlación	0,747**
		Sig. (bilateral)	0,000
		N	145
	Supervisión	Coeficiente de correlación	0,553**
		Sig. (bilateral)	0,000
		N	145

**. La correlación es significativa al nivel 0,01 (bilateral).

Fuente: Elaboración Propia

En la tabla superior se observa que existe un nivel de correlación significativa entre la SGSI y la SGR, ya que el coeficiente de correlación es de 0,856 y como el valor de probabilidad (p=0,000) es mucho menor que el valor critico 0,05 se toma la decisión de rechazar la hipótesis nula y aceptar la hipótesis alterna.

También se observa que existe un nivel de correlación positiva y significativa entre el SGSI y la Evaluación de la SGR, ya que el valor de probabilidad es igual a 0,000 es menor que 0,05 y el coeficiente de correlación es de 0,794 cercano a uno, por lo que se rechaza la hipótesis nula y se aceptar la hipótesis alterna. Por otro lado, se observa que existe un nivel de correlación positiva y significativa entre el SGSI y la Orientación de la SGR, ya que el valor de probabilidad es igual a 0,000 es menor que 0,05 y el coeficiente de correlación es de 0,747 cercano a uno, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alterna y por último se observa también que existe un nivel de correlación positiva y significativa entre el SGSI y la Supervisión de la SGR, con un coeficiente de correlación de 0,553 y con el valor de probabilidad es igual 0,000 y es menor que 0,05 por lo que se rechaza la hipótesis nula y aceptar la hipótesis alterna.

IV. Discusión

Nuestra investigación permitió alcanzar los objetivos planteados, en los cuales se buscó determinar la relación que existe entre el Sistema de Gestión de Seguridad de la Información del Ministerio de Salud y la Gestión del Riesgo, 2019. Como parte de la revisión de investigaciones precedentes, tenemos la investigación realizada por Moscoso, Esaú y Soto (2018), quienes estudiaron la implementación de un SGR basándose en la NTC- ISO 31000 en una empresa de saneamiento. Si bien durante esta investigación no se estudia la relación existente entre las variables de nuestra investigación, si logran intuir la existencia de una relación entre la gestión del riesgo y los SGSI recomendando profundizar en investigaciones futuras la relación entre estas variables con la intención de evitar posibles interferencias entre las implementaciones de estos sistemas en las organizaciones. De conformidad con nuestra investigación hemos podido determinar que las intuiciones establecidas por Moscoso, Esaú y Soto (2018) respecto a la existencia de una relación entre nuestras variables de estudio son reales. Mediante la comprobación de nuestra hipótesis hemos podido demostrar la existencia una relación significativa y positiva entre la gestión del riesgo y los SGSI lo que permitirá en el MINSA evaluar el desempeño de las implementaciones realizadas bajo este enfoque.

En el caso de Baca (2016), quien realiza una investigación basada en la implementación de un SGSI y establece vínculos con la gestión del riesgo en los modelos MAGERIT 3.0 que existían a pesar de la falta de interés en la implementación del SGSI debido a que se consideraba que no todos los controles en la gestión del riesgo permitían establecer de forma clara si existía una mitigación en los riesgo o si existía un efecto cruzado en el SGSI y la gestión del riesgo a pesar de haber cumplido con lo establecido por la norma técnica. Por lo anteriormente expuesto este investigador recomienda al igual que Moscoso, Esaú y Soto (2018) en profundizar estudios que determinen la relación existente entre las variables que han sido motivo de estudio en nuestra investigación. Sin embargo, Baca (2016) determina que en implementaciones de SGSI se debe considerar la identificación de los activos críticos de información de una institución que es uno de los puntos considerados en la implementación de la gestión de riesgos según la norma técnica peruana. Estas recomendaciones han sido corroboradas con nuestra investigación mediante nuestra prueba de hipótesis al determinarse que efectivamente existe una relación entre los SGSI y la gestión del riesgo sobre todo en la gestión de los activos críticos de información.

Por otro lado, tenemos la investigación de Seclén (2016). Este investigador logra mediante su trabajo determinar los factores que afectan la implementación de SGSI en las entidades del estado clasificándolas en tres categorías donde su primera categoría es referente al nivel estratégico y considera que la falta de políticas estratégicas de seguridad de la información con planes bien elaborados y con sus objetivos claramente identificados, es uno de los factores primordiales que impiden una adecuada implementación de SGSI en el estado. Este factor considerado por Seclén (2016) es coincidente con las dimensiones que tenemos en nuestra investigación respecto a la evaluación y las decisiones estratégicas, la orientación y la elaboración de planes, así como la supervisión y la identificación de objetivos. De lo anteriormente mencionado podemos ver que Seclén (2016) logra identificar que los factores que definen los SGR son también los factores que afectan a la implementación de los SGSI en las entidades del estado. Todas estas conclusiones establecidas por Seclén (2016) han sido corroboradas por nuestra investigación debido a que nosotros hemos podido determinar que existe una relación entre los SGSI y la gestión del riesgo.

En este punto de nuestra discusión debemos de considerar también el trabajo de Tarrillo (2015), este investigador concluye que existe una influencia alta entre la gestión del riesgo y la seguridad de los activos de información. También debemos mencionar que los activos son una dimensión de los SGSI en cuanto a la gestión de activos que consideran la responsabilidad, su clasificación y el manejo de los niveles de soporte. Este dimensionamiento trabajado en nuestra investigación es muy similar al dimensionamiento que Tarrillo (2015) emplea al dimensionar la seguridad de los activos concluyendo que existe una influencia entre ellos. Esto es corroborado en nuestra investigación mediante nuestra hipótesis que ha concluido que efectivamente existe una relación entre los SGSI y la gestión del riesgo en las implementaciones basadas en la NTP respecto a la evaluación. Otro aspecto resaltante en la investigación de Tarrillo (2015) es que considera que el SGR implementado es un macro conjunto donde la seguridad de la información debe estar siempre incluida.

También está el caso de Ayala (2017), cuya investigación buscaba determinar cómo la implementación de un SGSI mejora el SGR en un hospital estatal. Este investigador logra demostrar que la utilización de un modelo SGSI adecuado a la realidad de la organización, mejora sustancialmente el rendimiento del SGR. Esto lo hemos podido corroborar mediante

nuestra investigación debido a que hemos concluido que existe una relación nuestras variables, siendo así que podemos decir que las afirmaciones establecidas por Ayala (2017) son del todo acertadas a las luces de nuestros resultados. Sin embargo, creemos que se deben realizar más investigaciones que permitan confirmar definitivamente nuestras afirmaciones.

Pero es necesario validar nuestras afirmaciones con estudios internacionales que evidencien la relación que hemos encontrado entre los SGSI y la gestión del riesgo. En este contexto debemos mencionar el trabajo de Casadesús (2018), quien en su investigación utiliza nueve factores para la identificación de los riesgos a partir de la utilización de un cuadro de amenazas e identificación de riesgos. En él se puede apreciar como el investigador identifica 49 riesgos muy vinculados a la seguridad de la información que van desde la perdida de información hasta la falta de definición de procedimientos para la gestión de repositorios de esta información. Es necesario mencionar que de conformidad con la NTP/ISO 27001 estos son aspectos que implementan en un SGSI según esta norma. Casadesús (2018) logra determinar a partir de su estudio que la perdida de información es el riesgo más importante y recurrente en las entidades públicas. A pesar que su investigación se centra en la identificación de riesgos documentales para posterior fiscalización, este investigador concluye que el 86% de los riesgos identificados están asociados a la gestión de las aplicaciones informáticas. De los 60 riesgos identificados, 49 corresponden a los informáticos y los clasifica como riesgos que van de 1 a 9, donde 9 es el valor más malo. Luego de la aplicación de sus instrumentos Casadesús (2018) concluye que los 49 riesgos informáticos están dentro de las valoraciones más altas. A este punto, podemos decir que las conclusiones de Casadesús (2018) se deben a la relación existente entre los SGSI y la gestión de los riegos.

Otra experiencia es la realizada por Bernal (2017), este autor en su investigación basada en la implementación de la gestión de riesgos para una oficina informática, recomienda mejorar la estructura organizativa de las organizaciones donde se pretende implementar una gestión de riesgos. Así mismo al existir alta rotación de personal en las organizaciones donde se realizó el estudio, recomienda la implementación de SGSI para mejorar la gestión de riesgos. Este investigador de manera intuitiva encuentra cierta relación entre el SGSI implementado y los SGR, por ello sugiere la implementación de un SGSI como mecanismo para el mejoramiento del SGR sobre todo en aquellos aspectos que conciernen a

la supervisión cuyo objetivo es el monitoreo de posibles riesgos vinculados a la perdida de información. Estos resultados son bastante congruentes con nuestra investigación, donde encontramos que la dimensión Supervisión respecto al SGSI del MINSA se ubica en una posición entre regular y eficiente con un 92,3% respecto a las demás dimensiones confirmándose las afirmaciones de Bernal (2017).

Es el mismo caso de De Souza (2016) y Fassheber (2016), estos investigadores en sus trabajos para la implementación de modelos de gestión de riesgos en entidades públicas y áreas de TI respectivamente concluyen que para poder realizar una implementación perfecta hay que considerar dos factores, primero lo establecido por la norma ISO 31000 y como segundo aspecto los SGSI que para Fassheber (2016) se podría entender como un subconjunto de la gestión de riesgos. Para estos investigadores (Bernal, De Souza y Fassheber) los SGSI son elementos a considerar en un diseño de gestión de riesgos y contiene elementos que ya no deben ser considerados al momento de diseñar modelos con MAGERIT 3.0 en la gestión de riesgos. Esto definitivamente nos hace pensar que estos investigadores de alguna manera están intuyendo la existencia de una relación entre la gestión de riesgos con MAGERIT 3.0 y los SGSI. Mencionamos MEGERIT 3.0 debido a que este es el modelo implementado en MINSA y fue nuestro objeto de estudio.

También podemos mencionar el caso de Rivero (2017), quien considera que la implementación de un SGR debe preceder a la implementación de un SGSI con el fin de evitar incongruencias en los procesos asumidos por estos sistemas. Este autor incluso llega a asumir que un SGR debe ser el macro modelo de un SGSI recomendando una evolución en las ISO con el fin de que se unifiquen y así se pueda establecer un marco de referencia más integral que facilita las implementaciones de estos sistemas en las organizaciones. En su investigación Rivero (2017) diseña un modelo basado en las ISOs pero unificadas lo que le permitió optimizar los resultados en la implementación y evolución de estos sistemas. En nuestro caso, a partir de los resultados de nuestra investigación podemos coincidir con este investigador puesto que a pesar de que ambos sistemas son independientes entre sí poseen una relación que puede afectar el desempeño de los mismos y entorpecer su operatividad.

Por todo lo anteriormente expuesto, consideramos que estamos en la capacidad de afirmar que lo manifestado por estos investigadores son afirmaciones validas, basándonos

en la comprobación de las hipótesis de nuestra investigación. También debemos afirmar que es necesaria una revisión de la NTP siendo responsabilidad de INDECOPI el mejoramiento de esta para que no existan políticas contradictorias que mermen el buen desempeño de estos sistemas. Sin embargo, consideramos que es necesario realizar estudios de tipo pre experimentales bajo modelos integrales que permitan crear un modelo base de aplicación general en nuestro país.

V. Conclusiones

Primera

El Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión del Riesgo del Ministerio de Salud para el año 2019, analizado en la Unidad de Gestión de Inversión de Reconstrucción con Cambios. Luego de la aplicación de los instrumentos y el estudio estadístico respectivo, podemos concluir que existe una correlación entre nuestras variables de estudio de forma significativa y positiva.

Segunda

El Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión del Riesgo del Ministerio de Salud respecto a la dimensión Evaluación 2019, analizado en la Unidad de Gestión de Inversión de Reconstrucción con Cambios. Luego de la aplicación de los instrumentos y el estudio estadístico respectivo, podemos concluir que existe una correlación entre nuestras variables de estudio de forma significativa y positiva.

Tercera

El Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión del Riesgo del Ministerio de Salud respecto a la dimensión Orientación 2019, analizado en la Unidad de Gestión de Inversión de Reconstrucción con Cambios. Luego de la aplicación de los instrumentos y el estudio estadístico respectivo, podemos concluir que existe una correlación entre nuestras variables de estudio de forma significativa y positiva.

Cuarta

El Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión del Riesgo del Ministerio de Salud respecto a la dimensión Supervisión en el año 2019, analizado en la Unidad de Gestión de Inversión de Reconstrucción con Cambios. Luego de la aplicación de los instrumentos y el estudio estadístico respectivo, podemos concluir que existe una correlación entre nuestras variables de estudio de forma significativa y positiva.

VI. Recomendaciones

Primera

En las entidades del estado, se recomienda alinear a la Gerencia de TI con las estrategias del negocio (es decir lo que quiere el negocio). Se debe mantener información de calidad para apoyar las decisiones empresariales, para ello es necesario que la institución tenga mapeando todos sus activos y a cada activo se le debe gestionar sus riesgos (amenazas y vulnerabilidades), de tal manera se pueda aplicar un adecuado control y mantener los riesgos en un nivel aceptable. En caso de que se implemente un SGSI de forma paralela, se debe considerar que existen procesos que requieren suficiente flexibilidad para que los sistemas sean eficientes debido a la influencia que pueda existir entre ambos sistemas. Para ello recomendamos una implementación integral que combine ambos sistemas.

Segunda

Se recomienda realizar evaluaciones periódicas de los niveles de riesgo, de tal manera se pueda monitorear correctamente la efectividad de los controles aplicados, a su vez se puede usar varias metodologías para salvaguardar los activos de información. Siendo la NTP un estándar en nuestro país, creemos que es necesario realizar una revisión de la misma y mediante nuevos estudios poder definir claramente una NTP que permita la integración de ambas ISOs.

Tercera

Se recomienda que los responsables de la seguridad de la información (oficial de seguridad) formulen los planes de acción o mejora de controles necesarios para el tratamiento de los riesgos según su criticidad, para el caso de la Ministerio de Salud se recomienda Gestionar los riesgos, para evaluar los riesgos, impactos. Deben de seguir un procedimiento de tratamiento de los riesgos, de tal manera la gerencia pueda definir la opción de tratamiento a implementar (transferir, evitar, reducir o asumir el riesgo).

Cuarta

Consideramos necesario profundizar en el estudio de los SGSI y los de gestión de riesgo respecto a la relación que puedan tener ambos en nuestro país. Por otro lado, consideramos a partir de nuestra investigación que se debe realizar una revisión de las implementaciones normadas en nuestro país para estos sistemas, para que se puedan alinear a las necesidades

de cada organización y no exista merma en sus tiempos de respuesta frente a incidentes o inconsistencias procedimentales que inhabiliten su uso y práctica.

Referencias

Avalos. C. (2012). *Análisis. diseño e implementación del sistema de riesgo operacional para entidades financieras – SIRO (Tesis para Maestría*). Pontificia Universidad Católica Del Perú. Perú. Recuperada de: http://tesis.pucp.edu.pe/repositorio/handle/123456789/4454

Alvizuri. G. (2014). *Implementación de ITIL v3.0 y su influencia en el proceso de gestión de incidencias y cambios en el área de ti de la consultora ESPROTEC (Tesis de Maestría)*. Universidad Peruana Unión. Perú. Recuperada de: http://repositorio.upeu.edu.pe/handle/UPEU/359?show=full

Areitio, J. (2008). *Seguridad de la información Redes, informática y sistemas de información*. (C. L. Carmona, Ed.) Madrid España: Ediciones Paraninfo. Recuperado de: https://books.google.com.pe/books?id=_z2GcBD3deYC&printsec=frontcover#v=onepage&q&f=false

Arias Y., Díaz M. y Vargas, J. (2014). *Elaboración De Una Guía De Gestión De Riesgos Basados En La Norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia*. Tesis, Universidad Católica de Colombia, Colombia. Recuperado de: https://repository.ucatolica.edu.co/bitstream/10983/1758/1/Trabajo%20de%20Grado%20Especializacion%20Auditoria%20de%20Sistemas.pdf

Ayala, M. (2017). *Sistema de gestión de seguridad de información Para mejorar el proceso de gestión del riesgo En un hospital nacional, 2017*. Tesis, Universidad César Vallejo, Lima Perú. Recuperado de: http://repositorio.ucv.edu.pe/bitstream/handle/UCV/13753/Ayala_MMA.pdf?sequence=1&isAllowed=y

Bernaldo, N. (2016). *Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC.* San Borja. Lima 2016. Tesis, Universidad César Vallejo, Lima. Recuperado de: http://repositorio.ucv.edu.pe/bitstream/handle/UCV/13753/Ayala_MMA.pdf?sequence=1&isAllowed=y

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

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

Betacourt A. (2018). *Metodología de correlación estadística de un sistema integrado de gestión de la calidad en el sector salud*. Revista Signos, 10 (1), 10. Recuperado de: http://revistas.usantotomas.edu.co/index.php/signos/rt/printerFriendly/4681/html

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

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

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

Celí. E. (2016). *La gestión de riesgo TI y la efectividad de los sistemas de seguridad de información: caso de procesos críticos en las pequeñas entidades financieras de Lambayeque. Pueblo Cont*. 27(1). 73-84. Recuperado de: http://journal.upao.edu.pe/PuebloContinente/article/download/395/360

Cordova M. (2003). *Estadistica Descriptiva e Inferencias*. Perú. Editorial: Moshera. Edicion: 5ta. Recuperado de: http://repositorio.ucv.edu.pe/handle/UCV/30663

Córdova C, Morales G y Samamé J (2015). *Desarrollo de un SGSI para los Colegios Profesionales en la Región Lambayeque. Caso de estudio: Colegio de Ingenieros.* Recuperado de: http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.EF23EAC4&lang=es&site=eds-live

De La cruz, R. (2016). *Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la municipalidad provincial de Paita; 2016*. Tesis, Universidad Católica Los Ángeles Chimbote, Piura. Recuperado de: http://repositorio.uladech.edu.pe/handle/123456789/885

Díaz, R. (2015). *Apoyo al proceso de implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001:2013 en la alcaldía de Pasto*. Tesis, Universidad de Nariño, Colombia. 86. Recuperado de: http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/91046.pdf

Díaz, A. (2010). *System of Management of Security Information*. Magazine Clarity, (IV), 18–20. Recuperado de: http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.EF23EAC4&lang=es&site=eds-live

Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*. Madrid: Ministerio de Hacienda y Administraciones Públicas, Ed.

Duque, A. C. (2017). *Methodology for risk management. How to integrate security into strategic business objectives in a cost-effective way*. Retrieved abril 10, 2017,

Recuperado de: http://www.ridsso.com/documents/ muro/207_1469148692_57916e1488c74.pdf

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

Freixo, J., y Rocha, Á. (2014). *Arquitetura de informação de suporte à gestão da qualidade em unidades hospitalares*. *RISTI* - Revista Ibérica de Sistemas e Tecnologías de Informação, (14), 1-15. http://dx.doi.org/10.17013/risti.14.1-15.

Granados R. (2012) *Auditoria del Desarrollo de Sistemas de Información en el Gobierno Regional de Cajamarca*. De la Universidad Privada del Norte. Recuperado de: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=4c561103-d180-4b5f-9baa-4c12a14e149d%40sessionmgr4008

Hernández R., Fernández C. y Baptista L. (2014). *Metodología de la investigación científica*. (6.ª ed.). México: Mc Graw-Hill. Recuperado de http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

ICONTEC. (2009). *Norma Técnica Colombiana. NTC-ISO/IEC 27005. Tecnología de Información. Técnicas de Seguridad. Gestión del riesgo en la seguridad de la información.* Recuperado de: https://tienda.icontec.org/wp-content/uploads/ pdfs/NTC-ISO-IEC27005.pdf.

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

ISO. (2018). I*SO/IEC 27002:2018. Information technology — Security techniques — Code of practice for information security controls*. Revisión marzo 17, 2015, Recuperado de: http://www.iso.org/iso/catalogue_detail?csnumber=54533

ISO. (2017). *ISO Survey 2015*. Retrieved March 15, 2017, Recuperado de: https://www.iso.org/ the-iso-survey.html

ISO/IEC. (2014). *INTERNATIONAL STANDARD ISO / IEC 27000. Information technology Security techniques Information security management systems Overview and vocabulary* (Vol. 2014). ISO/IEC. Recuperado de: http://www.iso.org/iso/catalogue_detail?csnumber=54533

Jiménez-Martín, A., Vicente, E., & Mateos, A. (2015). *Selection of safeguards in risk management in information systems: a blurred approach*. RISTI - Magazine System and Technology Information, (15), 83–100. http:// doi.org/10.17013/risti.15.83-100

López, N. (2011). *Gestion de Riesgos Corporativos de Tecnologías de Información en Guatemala.* Tesis, Guatemala, Guatemala. 49.

NTP-27001:2009. (2009). *Tecnología de la Informacion-Tecnicas de Seguridad -Gestion de riesgos de seguridad de la información.* Primera edición.

Méndez E, Aguilar M (2006). *Proyecto Sanitas: Sistema de Gestión de Seguridad de la Información y certificación UNE 71502 e ISO 27001*. Del Grupo Sanitas.

Mera. A. (2014). *Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP PETROECUADOR de acuerdo a norma ISO/IEC 27002 y COBIT 5*. (Tesis de Maestría). Universidad. Ecuador. Recuperado de: http://repositorio.espe.edu.ec/bitstream/21000/8073/1/T-ESPE-047641.pdf

Mesquida A, Mas A y Amengual A (2008), *Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001*. REICIS Revista Española de Innovación, Calidad e Ingeniería del Software, vol. 6, núm. 3, noviembre, 2010, pp. 25-34, Asociación de Técnicos de Informática España.

Moscoso L, Esau E y Soto C (2018). *Modelo de gestión de riesgos de TI que contribuye a la operación de los procesos de gestión comercial de las empresas del sector de*

saneamiento del norte del Perú. Recuperado de: http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.6EDBFCEC&lang=es&site=eds-live

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

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

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

Perafan, J. (2014). *Análisis de Riesgo de la Seguridad de la Información para la institución Universitaria Colegia Mayor del Cauca.*

Ramos C. (2018). *Paradigmas de la Investigación Científica, Revista de Psicología,* 1(1), 10 Recuperado de: http://www.unife.edu.pe/publicaciones/revistas/psicologia/2015_1/Carlos_Ramos.pdf

Ricoy C. (2006). *Contribución sobre los paradigmas de investigación. Revista do Centro de Educação,* 31 (1), 11-22. Recuperado de: http://www.unife.edu.pe/publicaciones/revistas/psicologia/2015_1/Carlos_Ramos.pdf

Ríos J. (2014). *Diseño de un Sistema de Gestión De Seguridad de Información para una Central Privada de Información de riesgos*. Tesis, Pontificia Universidad Católica del Perú, Lima Perú. Recuperado de: http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/5555

Rivero, P. (2017). *Diseño de un modelo de gestión del riesgo aplicado a una empresa manufacturera de autopartes*. Tesis, Instituto Politécnico Nacional, México.

Recuperado de: http://vitela.javerianacali.edu.co/bitstream/handle/11522/11277/Dise%C3%B1o_sistema_Gestión.pdf?sequence=1&isAllowed=y

Rodríguez, Y. (2016). *Diseño y formulación de un sistema de gestión de riesgos basados en los lineamientos establecidos por la norma NTC- ISO 31000 versión 2011 para la empresa Simma Ltda*. Tesis, Universidad Industrial de Santander, Colombia. Recuperado de: http://tangara.uis.edu.co/biblioweb/tesis/2016/163435.pdf

Ramírez. A. y Ortiz. Z. (2011). *Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios*. Ingeniería. 16 (2). 56- 66. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/4797252.pdf

Ramírez. G. y Álvarez. E. (2003). *Auditoría a la gestión de las Tecnologías y sistemas de Información. Industrial Data*. 6(1). 99-102. Recuperado de: http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/indata/Vol6_n1/pf/auditoria.pdf

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

Romeral, L. (2008). *Gestion de Riesgos Tecnológicas.* Madrid: Asociación Española para la Gobernanza, la Gestion y la medición de las Tecnologías de la Información.

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

Tarrillo, E. (2016). *Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015*. Tesis, Universidad César Vallejo, Tarapoto. Recuperado de: http://repositorio.ucv.edu.pe/handle/UCV/1286

Valencia, H. (2016). *Metodología del SGSI Según La Norma ISO/IEC 27001 para el gobierno autónomo descentralizado de San Miguel de Urcuquí*. Tesis, Universidad Técnica Del Norte, Ibarra- Ecuador. Recuperado de: http://repositorio.utn.edu.ec/handle/123456789/5714

Velásquez P, Velásquez S, Velásquez M y Villa J (2017). *Implementación de la gestión de riesgo en los procesos misionales de la Sección de Dermatología de la Universidad de Antioquia (Medellín, Colombia) siguiendo las directrices de la norma ISO 9001:2015*. Revista Gerencia y Políticas de Salud, 16(33), 78–101. http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=4c561103-d180-4b5f-9baa-4c12a14e149d%40sessionmgr4008

Anexos

Anexo 1: Matriz de consistencia

MATRIZ DE CONSISTENCIA

Título: Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo en el Ministerio de Salud, 2019.

Autor: Oscar Yonatan Huayllani Muñoz.

<table>
<tr><th>Problema</th><th>Objetivos</th><th>Hipótesis</th><th colspan="5">Variables e indicadores</th></tr>
<tr><td rowspan="2">Problema General:

¿Cuál es la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud, 2019?

Problemas Específicos:

¿Cuál es la relación que existe entre Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Evaluación, 2019?

¿Cuál es la relación que existe entre Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Orientación, 2019?

¿Cuál es la relación que existe entre Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Supervisión, 2019?</td><td rowspan="2">Objetivo general:

Identificar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud, 2019.

Objetivos específicos:

Identificar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Evaluación, 2019.

Identificar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Orientación, 2019.

Identificar la relación que existe entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo del Ministerio de Salud respecto a la Supervisión, 2019.</td><td rowspan="2">Hipótesis general:

El Sistema de Gestión de Seguridad de la Información del Ministerio de Salud se relaciona con la Gestión del Riesgo en el ministerio de Salud, 2019

Hipótesis específicas:

El Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión del Riesgo del Ministerio de Salud respecto a la dimensión Evaluación, 2019

El Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión del Riesgo del Ministerio de Salud respecto a la dimensión Orientación, 2019

El Sistema de Gestión de Seguridad de la Información se relaciona con la Gestión del Riesgo del Ministerio de Salud respecto a la dimensión Supervisión, 2019</td><td colspan="5">Variable 1: Sistema de Gestión de Seguridad de la Información</td></tr>
<tr><td>Dimensiones</td><td>Indicadores</td><td>Ítems</td><td>Escala de medición</td><td>Niveles y rangos</td></tr>
<tr><td>1. POLITICAS DE SEGURIDAD</td><td>✓ Directrices de la Dirección en seguridad de la información.</td><td>1</td><td rowspan="6">(0) Nunca.
(1) A veces.
(2) Con Frecuencia.
(3) Siempre.</td><td rowspan="6">(1) Deficiente
(2) Regular
(3) Eficiente</td></tr>
<tr><td>2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.</td><td>✓ Organización interna.
✓ Dispositivos para movilidad y teletrabajo.</td><td>2
3</td></tr>
<tr><td>3. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.</td><td>✓ Antes de la contratación.
✓ Durante la contratación.
✓ Cese o cambio de puesto de trabajo.</td><td>4
5
6</td></tr>
<tr><td>4. GESTIÓN DE ACTIVOS.</td><td>✓ Responsabilidad sobre los activos.
✓ Clasificación de la información.
✓ Manejo de los soportes de almacenamiento.</td><td>7
8
9</td></tr>
<tr><td>5. CONTROL DE ACCESOS.</td><td>✓ Requisitos de negocio para el control de accesos.
✓ Gestión de acceso de usuario.
✓ Responsabilidades del usuario.
✓ Control de acceso a sistemas y aplicaciones.</td><td>10
11
12
13</td></tr>
<tr><td>6. CIFRADO DE INFORMACION.</td><td>✓ Controles criptográficos.</td><td>14</td><td></td></tr>
</table>

			7. SEGURIDAD FÍSICA Y AMBIENTAL.	✓ Áreas seguras. ✓ Seguridad de los equipos.	15 16	(0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	(1) Deficiente (2) Regular (3) Eficiente
			8. SEGURIDAD EN LO OPERATIVO.	✓ Responsabilidades y procedimientos de operación. ✓ Protección contra código malicioso. ✓ Copias de seguridad. ✓ Control del software en explotación. ✓ Gestión de la vulnerabilidad técnica. ✓ Consideraciones de las auditorías de los sistemas de información.	17 18 19 20 21 22		
			9. SEGURIDAD EN LAS TELECOMUNICACIONES.	✓ Gestión de la seguridad en las redes. ✓ Intercambio de información con partes externas.	23 24		
			10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	✓ Requisitos de seguridad de los sistemas de información. ✓ Seguridad en los procesos de desarrollo y soporte. ✓ Datos de prueba.	25 26 27		
			11. RELACIONES CON SUMINISTRADORES.	✓ Seguridad de la información en las relaciones con suministradores. ✓ Gestión de la prestación del servicio por suministradores.	28 29		
			12. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	✓ Gestión de incidentes de seguridad de la información y mejoras.	30		

			13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	✓ Continuidad de la seguridad de la información. ✓ Redundancias.	31 32	(0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	(1) Deficiente (2) Regular (3) Eficiente
			14. CUMPLIMIENTO.	✓ Cumplimiento de los requisitos legales y contractuales. ✓ Revisiones de la seguridad de la información.	33 34		
			Variable 2: Gestión del Riesgo				
			Dimensiones	**Indicadores**	**Ítems**	**Escala de medición**	**Niveles y rangos**
			1. EVALUACIÓN.	✓ Niveles de riesgo relacionados a las TI. ✓ Umbrales de tolerancia. ✓ Riesgos empresariales. ✓ Decisiones estratégicas. ✓ Valoración según estándares. ✓ Recuperación y tolerancia ante perdidas de TI.	1 2 3 4 5 6	(0) Nunca. (1) A veces. (2) Con Frecuencia. (3) Siempre.	(1) Deficiente (2) Regular (3) Eficiente
			2. ORIENTACIÓN.	✓ Oportunidades e impactos potenciales. ✓ Decisiones y operaciones estratégicas. ✓ Elaboración de planes. ✓ Capacidad de respuesta.	7 8 9 10		
			3. SUPERVISIÓN.	✓ Umbrales de apetito. ✓ Metas y métricas clave. ✓ Objetivos identificados. ✓ Consejo o comité de dirección.	11 12 13 14		

Nivel - diseño de investigación	Población y muestra	Técnicas e instrumentos	Estadística a utilizar
Enfoque: Cuantitativo. **Método:** Hipotético – Deductivo. **Diseño:** No experimental. **Tipo de estudio:** Aplicada. **Nivel de estudio:** Correlacional. **Corte:** Transversal o Transeccional.	**Población:** La población está comprendida por los trabajadores de la Unidad de Gestión de Inversiones de Reconstrucción con Cambios del Ministerio de Salud 2019 **Tipo de Muestra:** Censal **Tamaño de Muestra:** 145	**Variable 1:** Sistema de Gestión de Seguridad de la Información. **Técnica:** Encueta. **Instrumento:** Cuestionario. **Autor:** Oscar Yonatan Huayllani Muñoz. **Año:** 2019. **Monitoreo:** Oscar Yonatan Huayllani Muñoz. **Ámbito de Aplicación:** Unidad de Gestión de Inversiones de Reconstrucción con Cambios del Ministerio de Salud. **Forma de Administración:** Individual. **Variable 2:** Gestión del Riesgo. **Técnica:** Encueta. **Instrumento:** Cuestionario. **Autor:** Oscar Yonatan Huayllani Muñoz. **Año:** 2019. **Monitoreo:** Oscar Yonatan Huayllani Muñoz **Ámbito de Aplicación:** Unidad de Gestión de Inversiones de Reconstrucción con Cambios del Ministerio de Salud. **Forma de Administración:** Individual.	**Descriptiva:** Para el análisis estadístico respectivo, se utilizará el paquete estadístico SPSS Versión 22 con licencia de la UCV. Los datos obtenidos serán presentados en tablas y gráficos de acuerdo a las variables y dimensiones, para luego analizarlo e interpretarlos considerando el marco teórico. **Inferencial:** En base a los instrumentos de recolección de datos tenemos que la variable es cualitativa ordinal en ese sentido, Para la prueba de hipótesis se aplicará la prueba de la estadística no paramétrica Rho de Spearman con un ($\alpha = 0.05$), el cual se realiza para variables cualitativas ordinales, con la finalidad de inferir los resultados dentro de lo que circunscribirá este estudio. Para Suarez (2013), la inferencia estadística, consiste en llegar a obtener conclusiones o generalizaciones que sobrepasan los límites de los conocimientos aportados por un conjunto de datos. Busca obtener información sobre la población basándose en el estudio de los datos de una muestra tomada a partir de ella (p. 67).

Anexo 2: Validación de instrumentos

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Nº	Dimensiones / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Políticas de Seguridad							
	Directrices de la Dirección en Seguridad de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Los colaboradores cumplen las directrices establecidas en cuanto a la seguridad de la información?	✓		✓		✓		
	Aspectos Organizativos de la Seguridad de la Información							
	Organización Interna	**Si**	**No**	**Si**	**No**	**Si**	**No**	
2	¿Se organiza de forma coherente la seguridad de la información por parte de los colaboradores de la empresa?	✓		✓		✓		
	Dispositivos para movilidad y teletrabajo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Se cumple con las políticas para la salida de equipos informáticos de la entidad?	✓		✓		✓		
	Seguridad Ligada a los Recursos Humanos							
	Antes de la Contratación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	¿Cuándo ingresa un nuevo personal se le capacita en las políticas de seguridad de la información de la entidad?	✓		✓		✓		
	Durante la Contratación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
5	¿Se capacita constantemente sobre las políticas de seguridad de la información asumidas por la entidad?	✓		✓		✓		
	Cese o Cambio de Puesto de Trabajo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	¿Se respeta las políticas establecidas respecto a la rotación de personal?	✓		✓		✓		
	Gestión de Activos							
	Responsabilidad Sobre los Activos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Se usan actas de confidencialidad de información y cargos de asignación de equipos que son firmados por los colaboradores?	✓		✓		✓		
	Clasificación de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
8	¿Se clasifica la información según las necesidades de la entidad?	✓		✓		✓		
	Manejo de los Soportes de Almacenamiento	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	¿Se controla la forma en que los colaboradores usan el almacenamiento de información en medios externos como USB, discos externos u otros?	✓		✓		✓		

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

	Control de Accesos							
	Requisitos de Negocio para el Control de Accesos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	¿Para ingresar a la red de la entidad cuenta un usuario y contraseña?	✓		✓		✓		
	Gestión de acceso de usuario	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	¿Se cambia periódicamente la contraseña de su usuario en la red de la entidad?	✓		✓		✓		
	Responsabilidades del Usuario	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	¿Ha tenido ocasiones en la que por motivos de trabajo ha tenido que entregar a un compañero su usuario y contraseña para ingresar a la red de la entidad?	✓		✓		✓		
	Control de Acceso a Sistemas y Aplicaciones	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Usa las credenciales entregados por sistemas para el uso de los sistemas de la entidad?	✓		✓		✓		
	Cifrado de Información							
	Control de Acceso a Sistemas y Aplicaciones	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	¿Usa las credenciales entregados por sistemas para el uso de los sistemas de la entidad?	✓		✓		✓		
	Seguridad Física y Ambiental							
	Áreas Seguras	**Si**	**No**	**Si**	**No**	**Si**	**No**	
15	¿Han existido ocasiones en las que haya tenido que pedir acceso a las áreas restringidas de la entidad?	✓		✓		✓		
	Seguridad de los Equipos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	¿Se colocan los equipos de cómputo en lugares seguros para su correcto uso?	✓		✓		✓		
	Seguridad en lo Operativo							
	Responsabilidades y Procedimientos de Operación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	¿Se realizan instrucciones para indicar las responsabilidades del mal uso de los equipos informáticos mal utilizados?	✓		✓		✓		
	Protección Contra Código Malicioso	**Si**	**No**	**Si**	**No**	**Si**	**No**	
18	¿Usa los programas para protección de su información como antivirus o repositorios en línea?	✓		✓		✓		
	Copias de seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Utiliza los recursos en línea para compartir la información y realiza copias de su información como respaldo?	✓		✓		✓		
	Control del Software en Explotación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
20	¿Se siguen procedimientos para la instalación de software que haya requerido?	✓		✓		✓		

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

	Gestión de la Vulnerabilidad Técnica	**Si**	**No**	**Si**	**No**	**Si**	**No**	
21	¿Se tiene control del uso de algún software para fines personales?	✓		✓		✓		
	Consideraciones de las Auditorías de los Sistemas de Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
22	¿Se realizan auditorías a los equipos asignados para verificar su correcto uso?	✓		✓		✓		
	Seguridad en las Telecomunicaciones							
	Gestión de la Seguridad en las Redes	**Si**	**No**	**Si**	**No**	**Si**	**No**	
23	¿Ha solicitado al área de sistemas acceso a información que está restringida?	✓		✓		✓		
	Intercambio de Información con Partes Externas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
24	¿Se usan protocolos para enviar información de la entidad a colaboradores de otras entidades?	✓		✓		✓		
	Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información							
	Requisitos de Seguridad de los Sistemas de Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Se conecta a los sistemas de la entidad desde su domicilio u otra conexión a internet?	✓		✓		✓		
	Seguridad en los Procesos de Desarrollo y Soporte	**Si**	**No**	**Si**	**No**	**Si**	**No**	
26	¿Cambia usted libremente el software que está instalado en su equipo de cómputo?	✓		✓		✓		
	Datos de Prueba	**Si**	**No**	**Si**	**No**	**Si**	**No**	
27	¿Cuándo se pone a disposición un nuevo software se realizan pruebas con data de la entidad para verificar su usabilidad?	✓		✓		✓		
	Relaciones con Suministradores							
	Seguridad de la Información en las Relaciones con Suministradores	**Si**	**No**	**Si**	**No**	**Si**	**No**	
28	¿Existen protocolos para la elección proveedores de consumibles como tintas, papel, etc.?	✓		✓		✓		
	Gestión de la Prestación del Servicio por Suministradores	**Si**	**No**	**Si**	**No**	**Si**	**No**	
29	¿Se realiza una evaluación previa para poder suministrar servicios a la entidad?	✓		✓		✓		
	Gestión de Incidentes en la Seguridad de la Información							
	Gestión de Incidentes de Seguridad de la Información y Mejoras	**Si**	**No**	**Si**	**No**	**Si**	**No**	
30	¿Ha reportado a TI incidentes que pongan en riesgo la seguridad de la información de la entidad?	✓		✓		✓		
	Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio							
	Continuidad de la Seguridad de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

31	¿Hace uso de TI cuando ha perdido algún tipo de información?	✓		✓		✓		
	Redundancias	**Si**	**No**	**Si**	**No**	**Si**	**No**	
32	¿Hace uso mecanismos para tener copias de la información que usa en su equipo de cómputo?	✓		✓		✓		
	Cumplimiento							
	Cumplimiento de los Requisitos Legales y Contractuales	**Si**	**No**	**Si**	**No**	**Si**	**No**	
33	¿Cumple el personal las actividades según lo descrito en el MOF para su cargo?	✓		✓		✓		
	Revisiones de la Seguridad de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
34	¿Hace TI revisiones periódicas de como usan los colaboradores los equipos y servicios de red de la entidad?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA

Opinión de aplicabilidad: **Aplicable** [✓] **Aplicable después de corregir** [ ] **No aplicable** [ ]

Apellidos y nombres del juez validador. Dr/ Mg: ANGEL SOLUNTERNO MILEAN **DNI:** 19873533

Especialidad del validador: METODOLOGO - ESTADISTICO

14 de 11 del 2019

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

UCV
UNIVERSIDAD CESAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE GESTION DEL RIESGO

Nº	Dimensiones / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Evaluar la Gestión del Riesgo							
	Niveles de Riesgo Relacionados a las TI	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Determina la empresa el nivel de riesgos relacionados con las TI que está dispuesta a asumir para cumplir con sus objetivos?	✓		✓		✓		
	Umbrales de Tolerancia	**Si**	**No**	**Si**	**No**	**Si**	**No**	
2	¿Frente a los niveles de riesgo y oportunidad aceptables, la entidad evalúa y aprueba propuestas de umbrales de tolerancia al riesgo de TI?	✓		✓		✓		
	Riesgos Empresariales	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Determina la empresa el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales?	✓		✓		✓		
	Decisiones Estratégicas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	¿Se evalúa con frecuencia los factores de riesgo de TI con anterioridad a las decisiones estratégicas de la empresa pendientes y se asegura que las decisiones de la empresa se toman conscientes de los riesgos?	✓		✓		✓		
	Valoración según estándares	**Si**	**No**	**Si**	**No**	**Si**	**No**	
5	¿Con que frecuencia determina si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes?	✓		✓		✓		
	Recuperación y tolerancia ante perdidas de TI	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	¿Con que frecuencia la empresa evalúa las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos?	✓		✓		✓		
	Orientar en la Gestión de Riesgos							
	Oportunidades e Impactos Potenciales	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Se promueve una cultura consciente de los riesgos TI que impulse a la identificación proactiva de riesgos, oportunidades e impactos potenciales en el negocio?	✓		✓		✓		
	Decisiones y Operaciones Estratégicas	**Si**	**No**	**Si**	**No**	**Si**	**No**	

UCV Universidad César Vallejo

ESCUELA DE POSTGRADO

8	¿Se orientan la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas?	✓		✓		✓		
	Elaboración de Planes	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	¿Con que frecuencia comunican los planes de acción frente a un riesgo?	✓		✓		✓		
	Capacidad de Respuesta	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	¿Con que periodicidad se capacita en la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y se notifica a los niveles adecuados de gestión?	✓		✓		✓		
	Supervisar en la Gestión de Riesgos							
	Umbrales de Apetito.	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	¿Se supervisa con regularidad, hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo?	✓		✓		✓		
	Metas y Métricas Clave	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	¿Se supervisa con regularidad las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos?	✓		✓		✓		
	Objetivos Identificados	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Se facilita la revisión por las partes interesadas del progreso de la empresa hacia el control de los riesgos identificados?	✓		✓		✓		
	Consejo o Comité de Dirección	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	¿Se Informa cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección?	✓		✓		✓		

UCV
UNIVERSIDAD CESAR VALLEJO
ESCUELA DE POSTGRADO

Observaciones (precisar si hay suficiencia): Si HAY SUFICIENCIA

Opinión de aplicabilidad: **Aplicable** [✓] **Aplicable después de corregir** [ ] **No aplicable** [ ]

Apellidos y nombres del juez validador. Dr/ Mg: ANGEL SOLORZANO MEJIA **DNI:** 19873523

Especialidad del validador: METODOLOGO - ESTADISTICO

14 de 11 del 20 19

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Nº	Dimensiones / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Políticas de Seguridad							
	Directrices de la Dirección en Seguridad de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Los colaboradores cumplen las directrices establecidas en cuanto a la seguridad de la información?	✓		✓		✓		
	Aspectos Organizativos de la Seguridad de la Información							
	Organización Interna	**Si**	**No**	**Si**	**No**	**Si**	**No**	
2	¿Se organiza de forma coherente la seguridad de la información por parte de los colaboradores de la empresa?	✓		✓		✓		
	Dispositivos para movilidad y teletrabajo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Se cumple con las políticas para la salida de equipos informáticos de la entidad?	✓		✓		✓		
	Seguridad Ligada a los Recursos Humanos							
	Antes de la Contratación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	¿Cuándo ingresa un nuevo personal se le capacita en las políticas de seguridad de la información de la entidad?	✓		✓		✓		
	Durante la Contratación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
5	¿Se capacita constantemente sobre las políticas de seguridad de la información asumidas por la entidad?	✓		✓		✓		
	Cese o Cambio de Puesto de Trabajo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	¿Se respeta las políticas establecidas respecto a la rotación de personal?	✓		✓		✓		
	Gestión de Activos							
	Responsabilidad Sobre los Activos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Se usan actas de confidencialidad de información y cargos de asignación de equipos que son firmados por los colaboradores?	✓		✓		✓		
	Clasificación de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
8	¿Se clasifica la información según las necesidades de la entidad?	✓		✓		✓		
	Manejo de los Soportes de Almacenamiento	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	¿Se controla la forma en que los colaboradores usan el almacenamiento de información en medios externos como USB, discos externos u otros?	✓		✓		✓		

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

	Control de Accesos							
	Requisitos de Negocio para el Control de Accesos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	¿Para ingresar a la red de la entidad cuenta un usuario y contraseña?	✓		✓		✓		
	Gestión de acceso de usuario	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	¿Se cambia periódicamente la contraseña de su usuario en la red de la entidad?	✓		✓		✓		
	Responsabilidades del Usuario	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	¿Ha tenido ocasiones en la que por motivos de trabajo ha tenido que entregar a un compañero su usuario y contraseña para ingresar a la red de la entidad?	✓		✓		✓		
	Control de Acceso a Sistemas y Aplicaciones	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Usa las credenciales entregados por sistemas para el uso de los sistemas de la entidad?	✓		✓		✓		
	Cifrado de Información							
	Control de Acceso a Sistemas y Aplicaciones	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	¿Usa las credenciales entregados por sistemas para el uso de los sistemas de la entidad?	✓		✓		✓		
	Seguridad Física y Ambiental							
	Áreas Seguras	**Si**	**No**	**Si**	**No**	**Si**	**No**	
15	¿Han existido ocasiones en las que haya tenido que pedir acceso a las áreas restringidas de la entidad?	✓		✓		✓		
	Seguridad de los Equipos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	¿Se colocan los equipos de cómputo en lugares seguros para su correcto uso?	✓		✓		✓		
	Seguridad en lo Operativo							
	Responsabilidades y Procedimientos de Operación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	¿Se realizan instrucciones para indicar las responsabilidades del mal uso de los equipos informáticos mal utilizados?	✓		✓		✓		
	Protección Contra Código Malicioso	**Si**	**No**	**Si**	**No**	**Si**	**No**	
18	¿Usa los programas para protección de su información como antivirus o repositorios en línea?	✓		✓		✓		
	Copias de seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Utiliza los recursos en línea para compartir la información y realiza copias de su información como respaldo?	✓		✓		✓		
	Control del Software en Explotación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
20	¿Se siguen procedimientos para la instalación de software que haya requerido?	✓		✓		✓		

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

	Gestión de la Vulnerabilidad Técnica	**Si**	**No**	**Si**	**No**	**Si**	**No**	
21	¿Se tiene control del uso de algún software para fines personales?	✓		✓		✓		
	Consideraciones de las Auditorías de los Sistemas de Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
22	¿Se realizan auditorías a los equipos asignados para verificar su correcto uso?	✓		✓		✓		
	Seguridad en las Telecomunicaciones							
	Gestión de la Seguridad en las Redes	**Si**	**No**	**Si**	**No**	**Si**	**No**	
23	¿Ha solicitado al área de sistemas acceso a información que está restringida?	✓		✓		✓		
	Intercambio de Información con Partes Externas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
24	¿Se usan protocolos para enviar información de la entidad a colaboradores de otras entidades?	✓		✓		✓		
	Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información							
	Requisitos de Seguridad de los Sistemas de Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Se conecta a los sistemas de la entidad desde su domicilio u otra conexión a internet?	✓		✓		✓		
	Seguridad en los Procesos de Desarrollo y Soporte	**Si**	**No**	**Si**	**No**	**Si**	**No**	
26	¿Cambia usted libremente el software que está instalado en su equipo de cómputo?	✓		✓		✓		
	Datos de Prueba	**Si**	**No**	**Si**	**No**	**Si**	**No**	
27	¿Cuándo se pone a disposición un nuevo software se realizan pruebas con data de la entidad para verificar su usabilidad?	✓		✓		✓		
	Relaciones con Suministradores							
	Seguridad de la Información en las Relaciones con Suministradores	**Si**	**No**	**Si**	**No**	**Si**	**No**	
28	¿Existen protocolos para la elección proveedores de consumibles como tintas, papel, etc.?	✓		✓		✓		
	Gestión de la Prestación del Servicio por Suministradores	**Si**	**No**	**Si**	**No**	**Si**	**No**	
29	¿Se realiza una evaluación previa para poder suministrar servicios a la entidad?	✓		✓		✓		
	Gestión de Incidentes en la Seguridad de la Información							
	Gestión de Incidentes de Seguridad de la Información y Mejoras	**Si**	**No**	**Si**	**No**	**Si**	**No**	
30	¿Ha reportado a TI incidentes que pongan en riesgo la seguridad de la información de la entidad?	✓		✓		✓		
	Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio							
	Continuidad de la Seguridad de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	

UCV
UNIVERSIDAD CESAR VALLEJO
ESCUELA DE POSTGRADO

31	¿Hace uso de TI cuando ha perdido algún tipo de información?	✓		✓		✓		
	Redundancias	**Si**	**No**	**Si**	**No**	**Si**	**No**	
32	¿Hace uso mecanismos para tener copias de la información que usa en su equipo de cómputo?	✓		✓		✓		
	Cumplimiento							
	Cumplimiento de los Requisitos Legales y Contractuales	**Si**	**No**	**Si**	**No**	**Si**	**No**	
33	¿Cumple el personal las actividades según lo descrito en el MOF para su cargo?	✓		✓		✓		
	Revisiones de la Seguridad de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
34	¿Hace TI revisiones periódicas de como usan los colaboradores los equipos y servicios de red de la entidad?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Si hay Suficiencia

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: ZARATE RUIZ GUSTAVO ERNESTO **DNI:** 09870134

Especialidad del validador: TEMATICO

14 de 11 del 20 15

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE GESTION DEL RIESGO

Nº	Dimensiones / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Evaluar la Gestión del Riesgo							
	Niveles de Riesgo Relacionados a las TI	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Determina la empresa el nivel de riesgos relacionados con las TI que está dispuesta a asumir para cumplir con sus objetivos?	✓		✓		✓		
	Umbrales de Tolerancia	**Si**	**No**	**Si**	**No**	**Si**	**No**	
2	¿Frente a los niveles de riesgo y oportunidad aceptables, la entidad evalúa y aprueba propuestas de umbrales de tolerancia al riesgo de TI?	✓		✓		✓		
	Riesgos Empresariales	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Determina la empresa el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales?	✓		✓		✓		
	Decisiones Estratégicas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	¿Se evalúa con frecuencia los factores de riesgo de TI con anterioridad a las decisiones estratégicas de la empresa pendientes y se asegura que las decisiones de la empresa se toman conscientes de los riesgos?	✓		✓		✓		
	Valoración según estándares	**Si**	**No**	**Si**	**No**	**Si**	**No**	
5	¿Con que frecuencia determina si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes?	✓		✓		✓		
	Recuperación y tolerancia ante perdidas de TI	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	¿Con que frecuencia la empresa evalúa las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos?	✓		✓		✓		
	Orientar en la Gestión de Riesgos							
	Oportunidades e Impactos Potenciales	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Se promueve una cultura consciente de los riesgos TI que impulse a la identificación proactiva de riesgos, oportunidades e impactos potenciales en el negocio?	✓		✓		✓		
	Decisiones y Operaciones Estratégicas	**Si**	**No**	**Si**	**No**	**Si**	**No**	

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

8	¿Se orientan la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas?	✓		✓		✓		
	Elaboración de Planes	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	¿Con que frecuencia comunican los planes de acción frente a un riesgo?	✓		✓		✓		
	Capacidad de Respuesta	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	¿Con que periodicidad se capacita en la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y se notifica a los niveles adecuados de gestión?	✓		✓		✓		
	Supervisar en la Gestión de Riesgos							
	Umbrales de Apetito.	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	¿Se supervisa con regularidad, hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo?	✓		✓		✓		
	Metas y Métricas Clave	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	¿Se supervisa con regularidad las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos?	✓		✓		✓		
	Objetivos Identificados	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Se facilita la revisión por las partes interesadas del progreso de la empresa hacia el control de los riesgos identificados?	✓		✓		✓		
	Consejo o Comité de Dirección	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	¿Se Informa cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección?	✓		✓		✓		

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

Observaciones (precisar si hay suficiencia): Si hay suficiencia

Opinión de aplicabilidad: **Aplicable** [X] **Aplicable después de corregir** [ ] **No aplicable** [ ]

Apellidos y nombres del juez validador. Dr/ Mg: ZARATE RUIZ GUSTAVO ERNESTO **DNI:** 09870134

Especialidad del validador: TEMATICO

14 **de** 11 **del 20** 19

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Nº	Dimensiones / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Políticas de Seguridad							
	Directrices de la Dirección en Seguridad de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Los colaboradores cumplen las directrices establecidas en cuanto a la seguridad de la información?	✓		✓		✓		
	Aspectos Organizativos de la Seguridad de la Información							
	Organización Interna	**Si**	**No**	**Si**	**No**	**Si**	**No**	
2	¿Se organiza de forma coherente la seguridad de la información por parte de los colaboradores de la empresa?	✓		✓		✓		
	Dispositivos para movilidad y teletrabajo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Se cumple con las políticas para la salida de equipos informáticos de la entidad?	✓		✓		✓		
	Seguridad Ligada a los Recursos Humanos							
	Antes de la Contratación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	¿Cuándo ingresa un nuevo personal se le capacita en las políticas de seguridad de la información de la entidad?	✓		✓		✓		
	Durante la Contratación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
5	¿Se capacita constantemente sobre las políticas de seguridad de la información asumidas por la entidad?	✓		✓		✓		
	Cese o Cambio de Puesto de Trabajo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	¿Se respeta las políticas establecidas respecto a la rotación de personal?	✓		✓		✓		
	Gestión de Activos							
	Responsabilidad Sobre los Activos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Se usan actas de confidencialidad de información y cargos de asignación de equipos que son firmados por los colaboradores?	✓		✓		✓		
	Clasificación de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
8	¿Se clasifica la información según las necesidades de la entidad?	✓		✓		✓		
	Manejo de los Soportes de Almacenamiento	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	¿Se controla la forma en que los colaboradores usan el almacenamiento de información en medios externos como USB, discos externos u otros?	✓		✓		✓		

UCV UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSTGRADO

	Control de Accesos							
	Requisitos de Negocio para el Control de Accesos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	¿Para ingresar a la red de la entidad cuenta un usuario y contraseña?	✓		✓		✓		
	Gestión de acceso de usuario	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	¿Se cambia periódicamente la contraseña de su usuario en la red de la entidad?	✓		✓		✓		
	Responsabilidades del Usuario	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	¿Ha tenido ocasiones en la que por motivos de trabajo ha tenido que entregar a un compañero su usuario y contraseña para ingresar a la red de la entidad?	✓		✓		✓		
	Control de Acceso a Sistemas y Aplicaciones	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Usa las credenciales entregados por sistemas para el uso de los sistemas de la entidad?	✓		✓		✓		
	Cifrado de Información							
	Control de Acceso a Sistemas y Aplicaciones	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	¿Usa las credenciales entregados por sistemas para el uso de los sistemas de la entidad?	✓		✓		✓		
	Seguridad Física y Ambiental							
	Áreas Seguras	**Si**	**No**	**Si**	**No**	**Si**	**No**	
15	¿Han existido ocasiones en las que haya tenido que pedir acceso a las áreas restringidas de la entidad?	✓		✓		✓		
	Seguridad de los Equipos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	¿Se colocan los equipos de cómputo en lugares seguros para su correcto uso?	✓		✓		✓		
	Seguridad en lo Operativo							
	Responsabilidades y Procedimientos de Operación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	¿Se realizan instrucciones para indicar las responsabilidades del mal uso de los equipos informáticos mal utilizados?	✓		✓		✓		
	Protección Contra Código Malicioso	**Si**	**No**	**Si**	**No**	**Si**	**No**	
18	¿Usa los programas para protección de su información como antivirus o repositorios en línea?	✓		✓		✓		
	Copias de seguridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
19	¿Utiliza los recursos en línea para compartir la información y realiza copias de su información como respaldo?	✓		✓		✓		
	Control del Software en Explotación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
20	¿Se siguen procedimientos para la instalación de software que haya requerido?	✓		✓		✓		

UCV UNIVERSIDAD CESAR VALLEJO

ESCUELA DE POSTGRADO

	Gestión de la Vulnerabilidad Técnica	**Si**	**No**	**Si**	**No**	**Si**	**No**	
21	¿Se tiene control del uso de algún software para fines personales?	✓		✓		✓		
	Consideraciones de las Auditorías de los Sistemas de Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
22	¿Se realizan auditorías a los equipos asignados para verificar su correcto uso?	✓		✓		✓		
	Seguridad en las Telecomunicaciones							
	Gestión de la Seguridad en las Redes	**Si**	**No**	**Si**	**No**	**Si**	**No**	
23	¿Ha solicitado al área de sistemas acceso a información que está restringida?	✓		✓		✓		
	Intercambio de Información con Partes Externas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
24	¿Se usan protocolos para enviar información de la entidad a colaboradores de otras entidades?	✓		✓		✓		
	Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información							
	Requisitos de Seguridad de los Sistemas de Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
25	¿Se conecta a los sistemas de la entidad desde su domicilio u otra conexión a internet?	✓		✓		✓		
	Seguridad en los Procesos de Desarrollo y Soporte	**Si**	**No**	**Si**	**No**	**Si**	**No**	
26	¿Cambia usted libremente el software que está instalado en su equipo de cómputo?	✓		✓		✓		
	Datos de Prueba	**Si**	**No**	**Si**	**No**	**Si**	**No**	
27	¿Cuándo se pone a disposición un nuevo software se realizan pruebas con data de la entidad para verificar su usabilidad?	✓		✓		✓		
	Relaciones con Suministradores							
	Seguridad de la Información en las Relaciones con Suministradores	**Si**	**No**	**Si**	**No**	**Si**	**No**	
28	¿Existen protocolos para la elección proveedores de consumibles como tintas, papel, etc.?	✓		✓		✓		
	Gestión de la Prestación del Servicio por Suministradores	**Si**	**No**	**Si**	**No**	**Si**	**No**	
29	¿Se realiza una evaluación previa para poder suministrar servicios a la entidad?	✓		✓		✓		
	Gestión de Incidentes en la Seguridad de la Información							
	Gestión de Incidentes de Seguridad de la Información y Mejoras	**Si**	**No**	**Si**	**No**	**Si**	**No**	
30	¿Ha reportado a TI incidentes que pongan en riesgo la seguridad de la información de la entidad?	✓		✓		✓		
	Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio							
	Continuidad de la Seguridad de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

31	¿Hace uso de TI cuando ha perdido algún tipo de información?	✓		✓		✓		
	Redundancias	**Si**	**No**	**Si**	**No**	**Si**	**No**	
32	¿Hace uso mecanismos para tener copias de la información que usa en su equipo de cómputo?	✓		✓		✓		
	Cumplimiento							
	Cumplimiento de los Requisitos Legales y Contractuales	**Si**	**No**	**Si**	**No**	**Si**	**No**	
33	¿Cumple el personal las actividades según lo descrito en el MOF para su cargo?	✓		✓		✓		
	Revisiones de la Seguridad de la Información	**Si**	**No**	**Si**	**No**	**Si**	**No**	
34	¿Hace TI revisiones periódicas de como usan los colaboradores los equipos y servicios de red de la entidad?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Si hay Suficiencia

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: PEDRO MARTIN LEZAMA GONZALES **DNI:** 09656793

Especialidad del validador: ING. DE SISTEMAS

14 de 11 del 2019

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE GESTION DEL RIESGO

Nº	Dimensiones / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	Evaluar la Gestión del Riesgo							
	Niveles de Riesgo Relacionados a las TI	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Determina la empresa el nivel de riesgos relacionados con las TI que está dispuesta a asumir para cumplir con sus objetivos?	✓		✓		✓		
	Umbrales de Tolerancia	**Si**	**No**	**Si**	**No**	**Si**	**No**	
2	¿Frente a los niveles de riesgo y oportunidad aceptables, la entidad evalúa y aprueba propuestas de umbrales de tolerancia al riesgo de TI?	✓		✓		✓		
	Riesgos Empresariales	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Determina la empresa el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales?	✓		✓		✓		
	Decisiones Estratégicas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	¿Se evalúa con frecuencia los factores de riesgo de TI con anterioridad a las decisiones estratégicas de la empresa pendientes y se asegura que las decisiones de la empresa se toman conscientes de los riesgos?	✓		✓		✓		
	Valoración según estándares	**Si**	**No**	**Si**	**No**	**Si**	**No**	
5	¿Con que frecuencia determina si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes?	✓		✓		✓		
	Recuperación y tolerancia ante perdidas de TI	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	¿Con que frecuencia la empresa evalúa las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos?	✓		✓		✓		
	Orientar en la Gestión de Riesgos							
	Oportunidades e Impactos Potenciales	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿Se promueve una cultura consciente de los riesgos TI que impulse a la identificación proactiva de riesgos, oportunidades e impactos potenciales en el negocio?	✓		✓		✓		
	Decisiones y Operaciones Estratégicas	**Si**	**No**	**Si**	**No**	**Si**	**No**	

UCV UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSTGRADO

8	¿Se orientan la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas?	✓		✓		✓		
	Elaboración de Planes	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	¿Con que frecuencia comunican los planes de acción frente a un riesgo?	✓		✓		✓		
	Capacidad de Respuesta	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	¿Con que periodicidad se capacita en la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y se notifica a los niveles adecuados de gestión?	✓		✓		✓		
	Supervisar en la Gestión de Riesgos							
	Umbrales de Apetito.	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	¿Se supervisa con regularidad, hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo?	✓		✓		✓		
	Metas y Métricas Clave	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	¿Se supervisa con regularidad las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos?	✓		✓		✓		
	Objetivos Identificados	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Se facilita la revisión por las partes interesadas del progreso de la empresa hacia el control de los riesgos identificados?	✓		✓		✓		
	Consejo o Comité de Dirección	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	¿Se Informa cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección?	✓		✓		✓		

UCV
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

Observaciones (precisar si hay suficiencia): Si hay Suficiencia

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: PEDRO MARTIN LEZAMA GONZALES **DNI:** 09656793

Especialidad del validador: ING DE SISTEMAS

14, de 11 del 20 19.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---

Firma del Experto Informante

Anexo 3: Data para procesar

SUJETOS	Variable SGSI																																	
	D1	D2		D3			D4			D5				D6	D7		D8						D9		D10			D11		D12	D13		D14	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
1	1	1	2	2	1	2	2	1	2	1	2	2	1	1	1	2	1	1	1	1	2	1	2	2	3	1	1	2	1	2	2	1	1	1
2	1	2	1	1	2	1	1	1	1	1	2	2	1	1	2	1	1	2	1	2	1	1	2	1	2	1	1	1	1	2	2	1	1	2
3	1	2	1	1	2	2	2	2	1	2	2	2	1	1	1	1	1	2	1	2	1	1	1	1	2	1	2	1	2	2	2	1	1	1
4	1	2	2	2	1	2	1	2	1	1	2	2	1	1	1	2	1	2	1	2	1	1	1	1	2	1	2	1	1	2	2	1	1	1
5	2	1	2	1	1	2	1	2	1	2	1	1	1	2	2	1	1	2	1	2	1	1	1	1	2	2	2	1	2	1	1	1	2	2
6	2	1	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	1	2	2	2	1	1	2	2	2	1	1	2	2	1	1	2	2
7	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3	3	3	2	3	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3
8	3	3	2	3	3	3	3	2	2	2	3	3	3	3	3	3	2	3	3	3	3	3	3	2	2	3	2	3	3	3	3	3	3	3
9	3	3	3	2	2	3	3	3	3	3	2	3	3	3	3	3	3	2	3	3	3	2	3	3	3	2	3	3	3	3	3	3	3	3
10	3	3	3	3	3	3	2	3	2	3	3	2	2	3	3	2	3	3	3	2	3	3	3	3	2	3	3	3	3	3	3	3	3	3
11	3	3	2	3	2	3	2	3	3	2	3	3	3	2	3	3	3	3	3	1	2	2	2	3	3	2	2	3	3	3	3	3	3	3
12	2	3	2	3	3	2	2	1	1	1	2	2	2	3	2	3	2	3	3	2	2	2	2	1	1	1	1	1	1	2	2	2	3	2
13	1	1	1	1	1	1	2	2	2	1	1	1	2	2	2	1	2	1	2	3	2	2	2	1	1	2	2	2	1	1	1	2	2	2
14	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
15	1	1	1	1	1	2	2	2	3	3	3	3	3	3	3	3	3	3	3	2	2	2	1	2	1	2	2	3	3	3	3	3	3	3
16	2	2	2	2	1	1	1	1	2	2	2	1	2	2	2	2	1	1	1	1	1	2	2	2	1	1	1	2	2	2	1	2	2	2
17	3	3	3	3	3	3	3	3	1	1	1	1	1	1	3	2	2	2	3	3	3	2	2	1	1	2	3	1	1	1	1	1	1	3
18	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
19	1	1	1	1	1	2	2	2	1	1	1	1	2	2	1	2	1	2	1	2	1	2	1	1	1	2	2	1	1	1	1	2	2	1
20	2	2	2	1	2	2	2	2	3	2	2	2	1	1	1	2	2	1	2	1	2	1	2	1	1	1	2	3	2	2	2	1	1	1
21	1	1	1	1	2	1	1	2	2	1	1	1	1	2	1	2	1	2	1	2	1	1	2	2	2	2	2	2	1	1	1	1	2	1
22	2	2	2	2	2	3	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	3	2	2	3	3	2	3	2	3	2	3	2	3
23	3	2	3	3	3	2	2	3	2	3	2	3	3	2	2	3	3	2	3	2	3	3	3	3	3	2	3	2	3	2	3	3	2	2
24	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
25	3	3	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	2	2	2	2	3	3	3	3	2	2	3	3	3	3	3	3
26	2	3	2	3	2	3	2	3	3	2	3	2	3	2	2	2	2	2	3	3	3	3	3	3	2	1	3	3	2	3	2	3	2	2
27	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

28	1	2	2	1	1	1	2	1	1	1	2	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	2	2
29	1	2	2	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	2	3	2	2	1	1	1	1	1	1	1
30	1	2	2	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	2	1	1	1
31	1	2	1	1	2	1	1	2	1	2	1	1	1	2	1	1	1	1	1	1	2	1	2	1	1	1	2	1	2	1	1	1	2	1
32	1	3	1	1	1	1	1	2	1	2	1	1	1	1	1	2	1	1	2	1	1	1	1	2	2	2	2	1	2	1	1	1	1	1
33	1	2	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	3	1	2	1	1	1	1	1	1
34	1	3	1	2	3	1	1	1	1	2	1	1	1	1	3	1	1	1	1	2	1	1	1	1	2	3	1	1	2	1	1	1	1	3
35	1	2	1	2	1	1	1	1	1	1	2	1	1	2	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	2	1	1	2	1
36	1	3	1	2	2	2	2	1	1	1	1	2	1	1	2	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1	2	1	1	2
37	2	2	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	
38	1	3	1	1	1	1	2	1	1	1	1	1	1	2	2	1	1	1	2	1	2	2	1	1	1	2	1	1	1	1	1	1	2	2
39	1	3	1	1	2	1	2	1	1	1	2	1	1	1	2	1	1	1	1	1	1	2	1	1	1	2	1	1	1	2	1	1	1	2
40	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	2	2	1	1	1	2	1	1	1	1	1	1	1	1	1
41	3	2	1	1	2	1	3	1	1	1	2	1	1	1	1	1	2	2	1	1	2	1	1	2	1	1	1	1	1	2	1	1	1	1
42	3	3	1	1	1	1	2	1	1	1	2	1	3	3	3	1	1	2	2	1	1	1	2	1	1	2	1	1	1	2	1	3	3	3
43	2	3	1	1	1	1	1	2	1	1	3	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	2	1	1	3	1	1	1
44	2	3	1	2	1	1	3	1	1	1	1	1	2	2	3	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	2	3
45	2	3	3	1	2	1	1	2	1	1	2	1	1	1	2	1	1	1	1	2	1	1	1	2	2	2	2	1	1	2	1	1	1	2
46	2	3	3	1	1	1	2	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	2	2	2
47	2	3	3	1	2	1	1	3	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	3	1	1	1	1	1	1	1
48	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1
49	1	2	3	3	1	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1
50	1	2	3	3	1	1	1	2	1	1	2	1	2	2	2	1	1	1	1	1	1	2	2	1	3	1	2	1	1	2	1	2	2	2
51	1	2	3	1	1	1	2	1	1	1	2	1	1	1	3	1	1	1	2	1	1	1	1	1	2	2	1	1	1	2	1	1	1	3
52	1	2	3	2	1	1	1	1	1	1	2	1	1	1	3	3	2	1	2	2	2	2	1	1	2	1	1	1	1	2	1	1	1	3
53	1	2	3	2	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	2	1	1	1	1
54	1	2	3	2	1	1	1	2	1	1	1	1	1	2	1	3	1	2	1	2	1	3	1	1	2	2	1	1	1	1	1	1	1	2
55	1	3	3	1	1	1	1	2	1	2	2	1	1	2	1	1	1	1	1	1	2	1	3	2	1	1	2	1	2	2	1	1	2	1
56	1	3	3	2	1	1	2	1	2	2	1	1	1	1	2	1	3	1	1	2	2	1	3	1	1	2	1	2	2	1	1	1	1	2
57	1	3	3	2	1	1	1	2	1	1	1	1	2	1	1	1	1	1	2	1	1	2	1	2	2	2	2	1	1	1	1	2	1	1
58	1	3	2	2	1	1	1	1	3	1	1	1	1	1	1	1	3	1	1	2	1	2	2	1	2	1	1	3	1	1	1	1	1	1
59	1	3	2	2	1	1	2	1	1	1	2	1	1	1	2	1	2	1	2	2	1	2	1	1	1	2	1	1	1	2	1	1	1	2
60	1	3	2	2	1	1	2	1	1	1	1	1	1	1	2	2	2	1	1	2	1	2	1	1	2	3	1	1	1	1	1	1	1	2
61	2	3	2	2	1	1	2	1	1	2	1	1	1	3	1	2	2	1	1	3	1	1	2	2	2	1	1	1	2	1	1	1	3	1

62	2	1	2	1	1	1	2	1	1	1	1	1	1	1	1	2	2	1	2	2	1	1	1	2	1	2	1	1	1	1	1	1	1	1
63	2	1	2	1	1	2	1	1	1	1	1	1	1	2	1	1	1	3	1	2	1	1	2	1	2	1	1	1	1	1	1	1	2	1
64	3	1	2	2	1	1	2	1	1	2	2	1	2	1	2	1	1	3	1	2	1	1	1	2	1	1	1	1	2	2	1	2	1	2
65	1	1	2	2	1	2	2	1	2	1	2	2	1	1	1	2	1	1	1	1	2	1	2	2	3	1	1	2	1	2	2	1	1	1
66	1	2	1	1	2	1	1	1	1	1	2	2	1	1	2	1	1	2	1	2	1	1	2	1	2	1	1	1	1	2	2	1	1	2
67	1	2	1	1	2	2	2	2	1	2	2	2	1	1	1	1	1	2	1	2	1	1	1	1	2	1	2	1	2	2	2	1	1	1
68	1	2	2	2	1	2	1	2	1	1	2	2	1	1	1	2	1	2	1	2	1	1	1	1	2	1	2	1	1	2	2	1	1	1
69	2	1	2	1	1	2	1	2	1	2	1	1	1	2	2	1	1	2	1	2	1	1	1	1	2	2	2	1	2	1	1	1	2	2
70	2	1	2	1	1	2	2	1	1	2	2	1	1	2	2	1	1	1	2	2	2	1	1	2	2	2	1	1	2	2	1	1	2	2
71	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3
72	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
73	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
74	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
75	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3
76	2	3	2	3	3	2	2	1	1	1	2	2	2	3	2	3	2	3	3	2	2	2	2	1	1	1	1	1	1	2	2	2	3	2
77	1	1	1	1	1	1	2	2	2	1	1	1	2	2	2	1	2	1	2	3	2	2	2	1	1	2	2	2	1	1	1	2	2	2
78	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
79	1	1	1	1	1	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	2	2	2	1	2	1	2	2	3	3	3	3	3	3	3	3
80	2	2	2	2	1	1	1	1	2	2	2	1	2	2	2	2	1	1	1	1	1	2	2	2	1	1	1	2	2	2	1	2	2	2
81	3	3	3	3	3	3	3	3	1	1	1	1	1	1	3	2	2	2	3	3	3	2	2	1	1	2	3	1	1	1	1	1	1	3
82	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
83	1	1	1	1	1	2	2	2	1	1	1	1	2	2	1	2	1	2	1	2	1	2	1	2	1	1	1	2	2	1	1	1	1	2	2	1
84	2	2	2	1	2	2	2	2	3	2	2	2	1	1	1	2	2	1	2	1	2	1	2	1	2	1	1	1	2	3	2	2	2	1	1	1
85	1	1	1	1	2	1	1	2	2	1	1	1	1	2	1	2	1	2	1	2	1	1	2	2	2	2	2	2	1	1	1	1	2	1
86	2	2	2	2	2	3	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	3	2	2	3	3	2	3	2	3	2	3	2	3
87	3	2	3	3	3	2	2	3	2	3	2	3	3	2	2	3	3	2	3	2	3	3	3	3	3	2	3	2	3	2	3	3	2	2
88	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
89	3	3	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	2	2	2	2	3	3	3	3	2	2	3	3	3	3	3	3	3
90	2	3	2	3	2	3	2	3	3	2	3	2	3	2	2	2	2	2	3	3	3	3	3	3	2	1	3	3	2	3	2	3	2	2
91	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
92	1	2	2	1	1	1	2	1	1	1	2	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	2	2
93	1	2	2	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	2	3	2	2	1	1	1	1	1	1	1	1	1
94	1	2	2	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1
95	1	2	1	1	2	1	1	2	1	2	1	1	1	2	1	1	1	1	1	1	2	1	2	1	1	1	2	1	2	1	1	1	2	1	1	1

96	1	3	1	1	1	1	1	2	1	2	1	1	1	1	1	2	1	1	2	1	1	1	1	2	2	2	2	1	2	1	1	1	1	1
97	1	2	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	3	1	2	1	1	1	1	1
98	1	3	1	2	3	1	1	1	1	2	1	1	1	1	3	1	1	1	1	2	1	1	1	1	2	3	1	1	2	1	1	1	1	3
99	1	2	1	2	1	1	1	1	1	1	2	1	1	2	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	2	1	1	2	1
100	1	3	1	2	2	2	2	1	1	1	1	2	1	1	2	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1	2	1	1	2
101	2	2	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	1	1
102	1	3	1	1	1	1	2	1	1	1	1	1	1	2	2	1	1	1	2	1	2	2	1	1	1	2	1	1	1	1	1	1	2	2
103	1	3	1	1	2	1	2	1	1	1	2	1	1	1	2	1	1	1	1	1	1	2	1	1	1	2	1	1	1	2	1	1	1	2
104	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	2	2	1	1	1	2	1	1	1	1	1	1	1	1	1
105	3	2	1	1	2	1	3	1	1	1	2	1	1	1	1	1	2	2	1	1	2	1	1	2	1	1	1	1	1	2	1	1	1	1
106	3	3	1	1	1	1	2	1	1	1	2	1	3	3	3	1	1	2	2	1	1	1	2	1	1	2	1	1	1	2	1	3	3	3
107	2	3	1	1	1	1	1	2	1	1	3	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	2	1	1	3	1	1	1	1
108	2	3	1	2	1	1	3	1	1	1	1	1	2	2	3	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	2	3
109	2	3	3	1	2	1	1	2	1	1	2	1	1	1	2	1	1	1	1	2	1	1	1	2	2	2	2	1	1	2	1	1	1	2
110	2	3	3	1	1	1	2	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	2	2	2
111	2	3	3	1	2	1	1	3	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	3	1	1	1	1	1	1	1
112	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1
113	1	2	3	3	1	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1
114	1	2	3	3	1	1	1	2	1	1	2	1	2	2	2	1	1	1	1	1	1	2	2	1	3	1	2	1	1	2	1	2	2	2
115	1	2	3	1	1	1	2	1	1	1	2	1	1	1	3	1	1	1	2	1	1	1	1	1	2	2	1	1	1	2	1	1	1	3
116	1	2	3	2	1	1	1	1	1	1	2	1	1	1	3	3	2	1	2	2	2	2	1	1	2	1	1	1	1	2	1	1	1	3
117	1	2	3	2	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	2	1	1	1	1
118	1	2	3	2	1	1	1	2	1	1	1	1	1	1	2	1	3	1	2	1	2	1	3	1	1	2	2	1	1	1	1	1	1	2
119	1	3	3	1	1	1	1	2	1	2	2	1	1	2	1	1	1	1	1	1	2	1	3	2	1	1	2	1	2	2	1	1	2	1
120	1	3	3	2	1	1	2	1	2	2	1	1	1	1	2	1	3	1	1	2	2	1	3	1	1	2	1	2	2	1	1	1	1	2
121	1	3	3	2	1	1	1	2	1	1	1	1	2	1	1	1	1	1	2	1	1	2	1	2	2	2	2	1	1	1	1	2	1	1
122	1	3	2	2	1	1	1	1	3	1	1	1	1	1	1	1	3	1	1	2	1	2	2	1	2	1	1	3	1	1	1	1	1	1
123	1	3	2	2	1	1	2	1	1	1	2	1	1	1	2	1	2	1	2	2	1	2	1	1	1	2	1	1	1	2	1	1	1	2
124	1	3	2	2	1	1	2	1	1	1	1	1	1	1	2	2	2	1	1	2	1	2	1	1	2	3	1	1	1	1	1	1	1	2
125	2	3	2	2	1	1	2	1	1	2	1	1	1	3	1	2	2	1	1	3	1	1	2	2	2	1	1	1	2	1	1	1	3	1
126	2	1	2	1	1	1	2	1	1	1	1	1	1	1	1	2	2	1	2	2	1	1	1	2	1	2	1	1	1	1	1	1	1	1
127	2	1	2	1	1	2	1	1	1	1	1	1	1	2	1	1	1	3	1	2	1	1	2	1	2	1	1	1	1	1	1	1	2	1
128	3	1	2	2	1	1	2	1	1	2	2	1	2	1	2	1	1	3	1	2	1	1	1	2	1	1	1	1	2	2	1	2	1	2
129	1	2	3	3	1	1	1	2	1	1	2	1	2	2	2	1	1	1	1	1	1	2	2	1	3	1	2	1	1	2	1	2	2	2

130	1	2	3	1	1	1	2	1	1	1	2	1	1	1	3	1	1	1	2	1	1	1	1	1	2	2	1	1	1	2	1	1	1	3
131	1	2	3	2	1	1	1	1	1	1	2	1	1	1	3	3	2	1	2	2	2	2	1	1	2	1	1	1	1	2	1	1	1	3
132	1	2	3	2	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	2	1	1	1	1
133	1	2	3	2	1	1	1	2	1	1	1	1	1	1	2	1	3	1	2	1	2	1	3	1	1	2	2	1	1	1	1	1	1	2
134	1	3	3	1	1	1	1	2	1	2	2	1	1	2	1	1	1	1	1	1	2	1	3	2	1	1	2	1	2	2	1	1	2	1
135	1	3	3	2	1	1	2	1	2	2	1	1	1	1	2	1	3	1	1	2	2	1	3	1	1	2	1	2	2	1	1	1	1	2
136	1	3	3	2	1	1	1	2	1	1	1	1	2	1	1	1	1	1	2	1	1	2	1	2	2	2	2	1	1	1	1	2	1	1
137	1	3	2	2	1	1	1	1	3	1	1	1	1	1	1	1	3	1	1	2	1	2	2	1	2	1	1	3	1	1	1	1	1	1
138	1	3	2	2	1	1	2	1	1	1	2	1	1	1	2	1	2	1	2	2	1	2	1	1	1	2	1	1	1	2	1	1	1	2
139	1	3	2	2	1	1	2	1	1	1	1	1	1	1	2	2	2	1	1	2	1	2	1	1	2	3	1	1	1	1	1	1	1	2
140	2	3	2	2	1	1	2	1	1	2	1	1	1	3	1	2	2	1	1	3	1	1	2	2	2	1	1	1	2	1	1	1	3	1
141	2	1	2	1	1	1	2	1	1	1	1	1	1	1	1	2	2	1	2	2	1	1	1	2	1	2	1	1	1	1	1	1	1	1
142	2	1	2	1	1	2	1	1	1	1	1	1	2	1	1	1	3	1	2	1	1	2	1	2	1	1	1	1	1	1	1	1	2	1
143	3	1	2	2	1	1	2	1	1	2	2	1	2	1	2	1	1	3	1	2	1	1	1	2	1	1	1	1	2	2	1	2	1	2
144	2	3	3	1	1	1	2	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	2	2	2
145	2	3	3	1	2	1	1	3	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	3	1	1	1	1	1	1	1

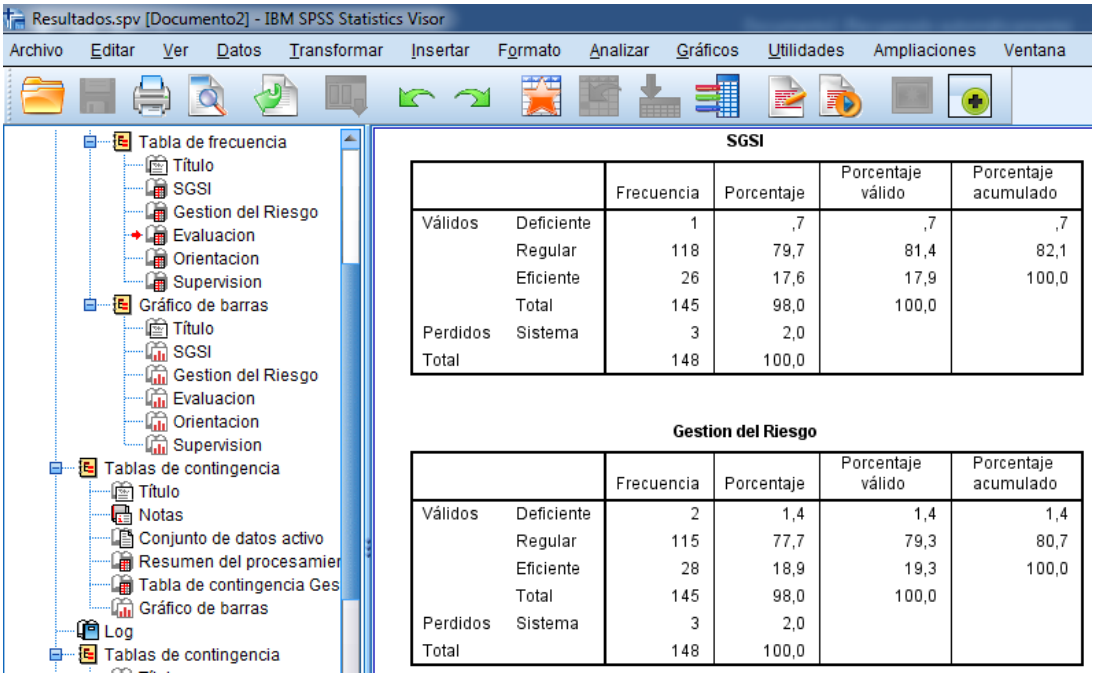
SUJETOS	Variable Gestión del Riesgo													
	D1						D2				D3			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1	2	1	1	1	1	2	1	2	2	3	1	1
2	1	2	1	1	2	1	2	1	1	2	1	2	1	1
3	1	1	1	1	2	1	2	1	1	1	1	2	1	2
4	1	1	2	1	2	1	2	1	1	1	1	2	1	2
5	2	2	1	1	2	1	2	1	1	1	1	2	2	2
6	2	2	1	1	1	2	2	2	1	1	2	2	2	1
7	3	3	3	3	2	3	3	3	3	3	3	3	3	2
8	3	3	3	2	3	3	3	3	3	3	2	2	3	2
9	3	3	3	3	2	3	3	3	2	3	3	3	2	3
10	3	3	2	3	3	3	2	3	3	3	3	2	3	3
11	2	3	3	3	3	3	1	2	2	2	3	3	2	2
12	3	2	3	2	3	3	2	2	2	2	1	1	1	1
13	2	2	1	2	1	2	3	2	2	2	1	1	2	2
14	3	3	3	3	3	3	3	3	3	3	3	3	3	3
15	3	3	3	3	3	3	2	2	2	1	2	1	2	2
16	2	2	2	1	1	1	1	1	2	2	2	1	1	1
17	1	3	2	2	2	3	3	3	2	2	1	1	2	3
18	3	3	3	3	3	3	3	3	3	3	3	3	3	3
19	2	1	2	1	2	1	2	1	2	1	1	1	2	2
20	1	1	2	2	1	2	1	2	1	2	1	1	1	2
21	2	1	2	1	2	1	2	1	1	2	2	2	2	2
22	2	3	2	3	2	3	2	3	3	2	2	3	3	2
23	2	2	3	3	2	3	2	3	3	3	3	3	2	3
24	3	3	3	3	3	3	3	3	3	3	3	3	3	3
25	3	3	3	3	3	2	2	2	2	3	3	3	3	2
26	2	2	2	2	2	3	3	3	3	3	3	2	1	3
27	1	1	1	1	1	1	1	1	1	1	1	1	1	1
28	2	2	2	1	1	1	1	1	1	1	1	1	1	1
29	1	1	1	1	1	1	1	2	1	1	2	3	2	2
30	1	1	1	1	1	1	2	1	1	1	1	1	2	1
31	2	1	1	1	1	1	1	2	1	2	1	1	1	2
32	1	1	2	1	1	2	1	1	1	1	2	2	2	2
33	1	1	1	1	1	1	1	1	1	1	1	2	3	1
34	1	3	1	1	1	1	2	1	1	1	1	2	3	1
35	2	1	1	1	1	1	1	2	1	1	1	2	1	1
36	1	2	1	2	1	1	2	1	1	1	1	1	1	1
37	1	1	1	1	1	1	1	1	2	1	1	1	1	1
38	2	2	1	1	1	2	1	2	2	1	1	1	2	1

39	1	2	1	1	1	1	1	1	2	1	1	1	2	1
40	1	1	2	1	1	1	2	2	1	1	1	2	1	1
41	1	1	1	2	2	1	1	2	1	1	2	1	1	1
42	3	3	1	1	2	2	1	1	1	2	1	1	2	1
43	1	1	1	1	1	1	2	1	2	1	1	1	1	2
44	2	3	1	1	1	1	1	2	1	1	1	1	1	1
45	1	2	1	1	1	1	2	1	1	1	2	2	2	2
46	2	2	1	1	1	1	1	1	1	2	2	1	1	1
47	1	1	1	1	1	2	1	1	1	1	1	1	2	3
48	1	1	1	2	2	1	1	1	2	2	2	1	1	1
49	1	1	2	1	1	1	1	1	1	1	1	1	2	2
50	2	2	1	1	1	1	1	1	2	2	1	3	1	2
51	1	3	1	1	1	2	1	1	1	1	1	2	2	1
52	1	3	3	2	1	2	2	2	2	1	1	2	1	1
53	1	1	1	1	1	1	1	2	1	1	1	2	1	1
54	1	2	1	3	1	2	1	2	1	3	1	1	2	2
55	2	1	1	1	1	1	1	2	1	3	2	1	1	2
56	1	2	1	3	1	1	2	2	1	3	1	1	2	1
57	1	1	1	1	1	2	1	1	2	1	2	2	2	2
58	1	1	1	3	1	1	2	1	2	2	1	2	1	1
59	1	2	1	2	1	2	2	1	2	1	1	1	2	1
60	1	2	2	2	1	1	2	1	2	1	1	2	3	1
61	3	1	2	2	1	1	3	1	1	2	2	2	1	1
62	1	1	2	2	1	2	2	1	1	1	2	1	2	1
63	2	1	1	1	3	1	2	1	1	2	1	2	1	1
64	1	2	1	1	3	1	2	1	1	1	2	1	1	1
65	1	1	2	1	1	1	1	2	1	2	2	3	1	1
66	1	2	1	1	2	1	2	1	1	2	1	2	1	1
67	1	1	1	1	2	1	2	1	1	1	1	2	1	2
68	1	1	2	1	2	1	2	1	1	1	1	2	1	2
69	2	2	1	1	2	1	2	1	1	1	1	2	2	2
70	2	2	1	1	1	2	2	2	1	1	2	2	2	1
71	3	3	3	3	2	3	3	3	3	3	3	3	3	2
72	3	3	3	3	3	3	3	3	3	3	3	3	3	3
73	3	3	3	3	3	3	3	3	3	3	3	3	3	3
74	3	3	3	3	3	3	3	3	3	3	3	3	3	3
75	3	3	3	3	3	3	3	3	3	3	3	3	2	3
76	3	2	3	2	3	3	2	2	2	2	1	1	1	1
77	2	2	1	2	1	2	3	2	2	2	1	1	2	2
78	3	3	3	3	3	3	3	3	3	3	3	3	3	3
79	3	3	3	3	3	3	2	2	2	1	2	1	2	2
80	2	2	2	1	1	1	1	1	2	2	2	1	1	1

81	1	3	2	2	2	3	3	3	2	2	1	1	2	3
82	3	3	3	3	3	3	3	3	3	3	3	3	3	3
83	2	1	2	1	2	1	2	1	2	1	1	1	2	2
84	1	1	2	2	1	2	1	2	1	2	1	1	1	2
85	2	1	2	1	2	1	2	1	1	2	2	2	2	2
86	2	3	2	3	2	3	2	3	3	2	2	3	3	2
87	2	2	3	3	2	3	2	3	3	3	3	3	2	3
88	3	3	3	3	3	3	3	3	3	3	3	3	3	3
89	3	3	3	3	3	2	2	2	2	3	3	3	3	2
90	2	2	2	2	2	3	3	3	3	3	3	2	1	3
91	1	1	1	1	1	1	1	1	1	1	1	1	1	1
92	2	2	2	1	1	1	1	1	1	1	1	1	1	1
93	1	1	1	1	1	1	1	2	1	1	2	3	2	2
94	1	1	1	1	1	1	2	1	1	1	1	1	2	1
95	2	1	1	1	1	1	1	2	1	2	1	1	1	2
96	1	1	2	1	1	2	1	1	1	1	2	2	2	2
97	1	1	1	1	1	1	1	1	1	1	1	2	3	1
98	1	3	1	1	1	1	2	1	1	1	1	2	3	1
99	2	1	1	1	1	1	1	2	1	1	1	2	1	1
100	1	2	1	2	1	1	2	1	1	1	1	1	1	1
101	1	1	1	1	1	1	1	1	2	1	1	1	1	1
102	2	2	1	1	1	2	1	2	2	1	1	1	2	1
103	1	2	1	1	1	1	1	1	2	1	1	1	2	1
104	1	1	2	1	1	1	2	2	1	1	1	2	1	1
105	1	1	1	2	2	1	1	2	1	1	2	1	1	1
106	3	3	1	1	2	2	1	1	1	2	1	1	2	1
107	1	1	1	1	1	1	2	1	2	1	1	1	1	2
108	2	3	1	1	1	1	1	2	1	1	1	1	1	1
109	1	2	1	1	1	1	2	1	1	1	2	2	2	2
110	2	2	1	1	1	1	1	1	1	2	2	1	1	1
111	1	1	1	1	1	2	1	1	1	1	1	1	2	3
112	1	1	1	2	2	1	1	1	2	2	2	1	1	1
113	1	1	2	1	1	1	1	1	1	1	1	1	2	2
114	2	2	1	1	1	1	1	1	2	2	1	3	1	2
115	1	3	1	1	1	2	1	1	1	1	1	2	2	1
116	1	3	3	2	1	2	2	2	2	1	1	2	1	1
117	1	1	1	1	1	1	1	2	1	1	1	2	1	1
118	1	2	1	3	1	2	1	2	1	3	1	1	2	2
119	2	1	1	1	1	1	1	2	1	3	2	1	1	2
120	1	2	1	3	1	1	2	2	1	3	1	1	2	1
121	1	1	1	1	1	2	1	1	2	1	2	2	2	2
122	1	1	1	3	1	1	2	1	2	2	1	2	1	1

123	1	2	1	2	1	2	2	1	2	1	1	1	2	1
124	1	2	2	2	1	1	2	1	2	1	1	2	3	1
125	3	1	2	2	1	1	3	1	1	2	2	2	1	1
126	1	1	2	2	1	2	2	1	1	1	2	1	2	1
127	2	1	1	1	3	1	2	1	1	2	1	2	1	1
128	1	2	1	1	3	1	2	1	1	1	2	1	1	1
129	2	2	1	1	1	1	1	1	2	2	1	3	1	2
130	1	3	1	1	1	2	1	1	1	1	1	2	2	1
131	1	3	3	2	1	2	2	2	2	1	1	2	1	1
132	1	1	1	1	1	1	1	2	1	1	1	2	1	1
133	1	2	1	3	1	2	1	2	1	3	1	1	2	2
134	2	1	1	1	1	1	1	2	1	3	2	1	1	2
135	1	2	1	3	1	1	2	2	1	3	1	1	2	1
136	1	1	1	1	1	2	1	1	2	1	2	2	2	2
137	1	1	1	3	1	1	2	1	2	2	1	2	1	1
138	1	2	1	2	1	2	2	1	2	1	1	1	2	1
139	1	2	2	2	1	1	2	1	2	1	1	2	3	1
140	3	1	2	2	1	1	3	1	1	2	2	2	1	1
141	1	1	2	2	1	2	2	1	1	1	2	1	2	1
142	2	1	1	1	3	1	2	1	1	2	1	2	1	1
143	1	2	1	1	3	1	2	1	1	1	2	1	1	1
144	2	2	1	1	1	1	1	1	1	2	2	1	1	1
145	1	1	1	1	1	2	1	1	1	1	1	1	2	3

Anexo 4: Pantalla SPSS

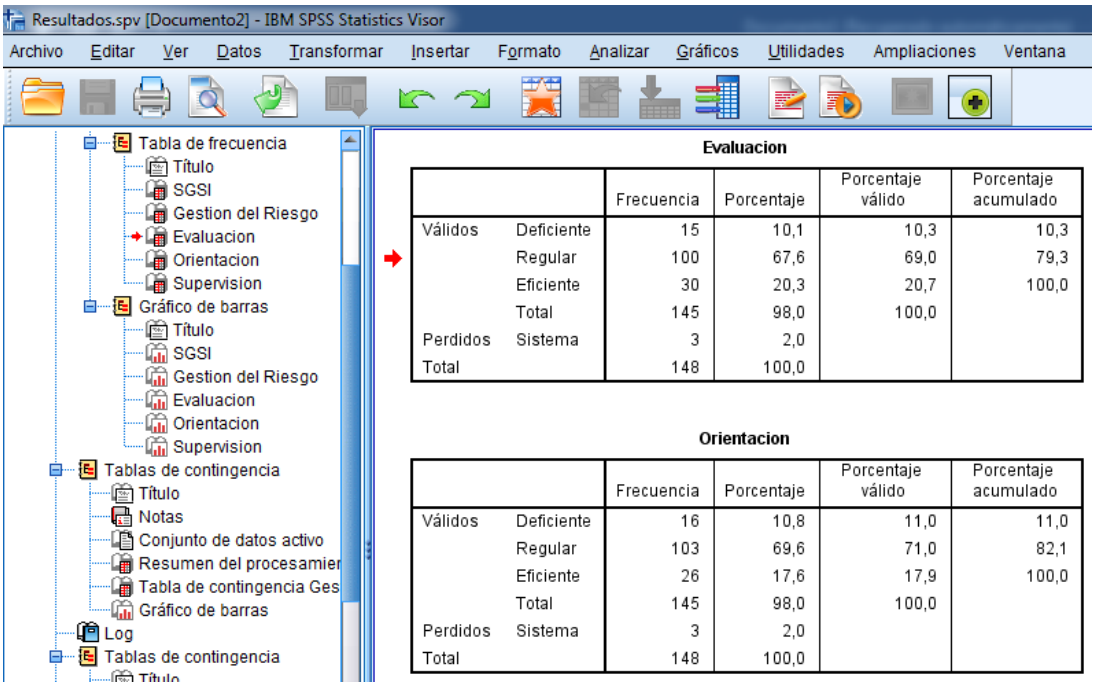


SGSI

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Deficiente	1	,7	,7	,7
	Regular	118	79,7	81,4	82,1
	Eficiente	26	17,6	17,9	100,0
	Total	145	98,0	100,0	
Perdidos	Sistema	3	2,0		
Total		148	100,0		

Gestion del Riesgo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Deficiente	2	1,4	1,4	1,4
	Regular	115	77,7	79,3	80,7
	Eficiente	28	18,9	19,3	100,0
	Total	145	98,0	100,0	
Perdidos	Sistema	3	2,0		
Total		148	100,0		

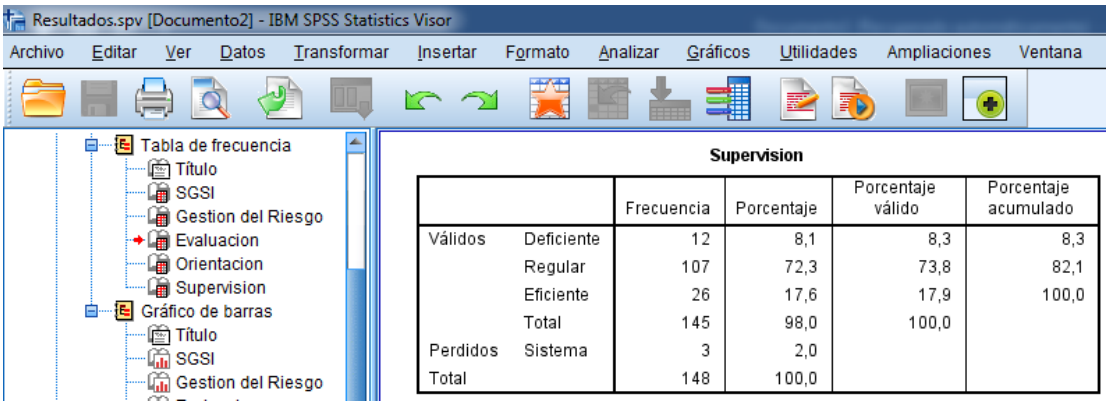


Evaluacion

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Deficiente	15	10,1	10,3	10,3
	Regular	100	67,6	69,0	79,3
	Eficiente	30	20,3	20,7	100,0
	Total	145	98,0	100,0	
Perdidos	Sistema	3	2,0		
Total		148	100,0		

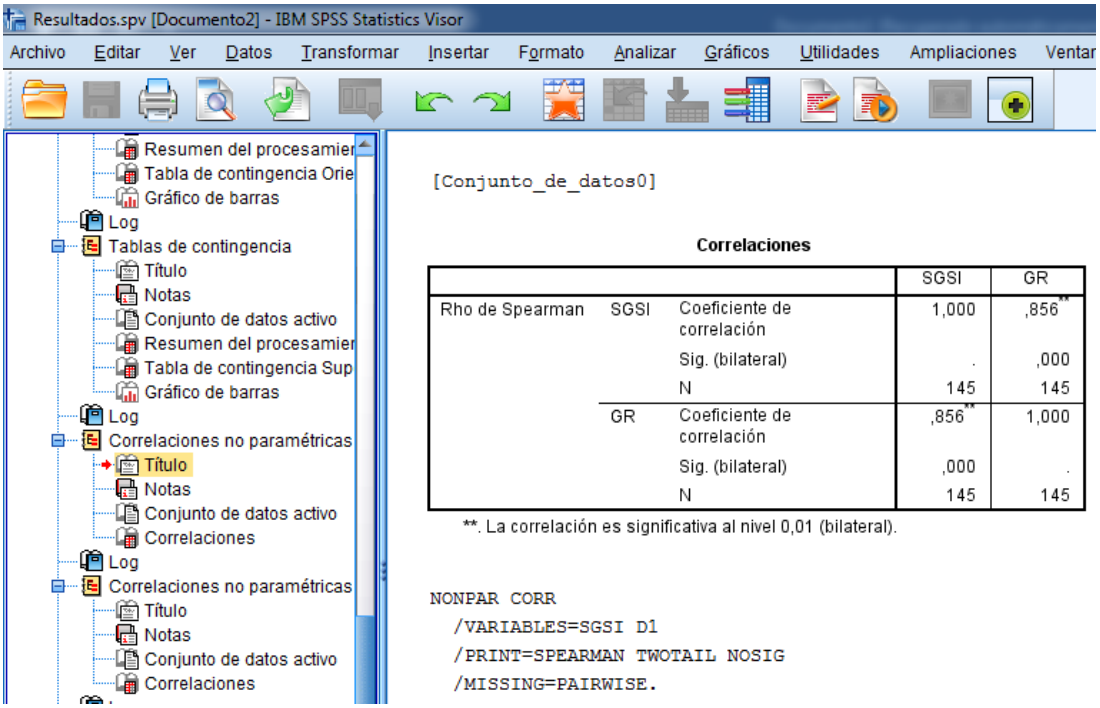
Orientacion

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Deficiente	16	10,8	11,0	11,0
	Regular	103	69,6	71,0	82,1
	Eficiente	26	17,6	17,9	100,0
	Total	145	98,0	100,0	
Perdidos	Sistema	3	2,0		
Total		148	100,0		



Supervision

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Deficiente	12	8,1	8,3	8,3
	Regular	107	72,3	73,8	82,1
	Eficiente	26	17,6	17,9	100,0
	Total	145	98,0	100,0	
Perdidos	Sistema	3	2,0		
Total		148	100,0		



[Conjunto_de_datos0]

Correlaciones

			SGSI	GR
Rho de Spearman	SGSI	Coeficiente de correlación	1,000	,856**
		Sig. (bilateral)	.	,000
		N	145	145
	GR	Coeficiente de correlación	,856**	1,000
		Sig. (bilateral)	,000	.
		N	145	145

**. La correlación es significativa al nivel 0,01 (bilateral).

```
NONPAR CORR
  /VARIABLES=SGSI D1
  /PRINT=SPEARMAN TWOTAIL NOSIG
  /MISSING=PAIRWISE.
```

Anexo 5: Carta presentación UCV

UNIVERSIDAD CÉSAR VALLEJO

Escuela de Posgrado

"Año de la lucha contra la corrupción y la impunidad"

MINISTERIO DE SALUD
SECRETARÍA GENERAL
OFICINA DE GESTIÓN DOCUMENTAL Y ATENCIÓN AL CIUDADANO
16 DIC. 2019
RECIBIDO
Exp. N°:
FIRMA: HORA:

Lima, 13 de diciembre de 2019

Carta P. 573–2019–EPG–UCV–LN

ING. CÉSAR JOSUÉ MORENO TOLEDO
COORDINADOR TÉCNICO ADMINISTRATIVO DE EXPEDIENTES TÉCNICOS
UNIDAD DE GESTIÓN DE INVERSIÓN DE RECONSTRUCCIÓN CON CAMBIOS
MINISTERIO DE SALUD

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a **OSCAR YONATAN HUAYLLANI MUÑOZ** identificado con DNI N.° **44030405** y código de matrícula N.° **7001256167;** estudiante del Programa de **MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN** quien se encuentra desarrollando el Trabajo de Investigación (Tesis):

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DEL RIESGO EN EL MINISTERIO DE SALUD, 2019

En ese sentido, solicito a su digna persona otorgar el permiso y brindar las facilidades a nuestro estudiante, a fin de que pueda desarrollar su trabajo de investigación en la institución que usted representa. Los resultados de la presente serán alcanzados a su despacho, luego de finalizar la misma.

Con este motivo, le saluda atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dr. Carlos Venturo Orbegoso
Jefe de la Escuela de Posgrado
Universidad César Vallejo - Campus Lima Norte

Ing. César Josué Moreno Toledo
CIP 96202
COORDINADOR TÉCNICO ADMINISTRATIVO
DE EXPEDIENTES TÉCNICOS

RCQA

Somos la universidad de los
que quieren salir adelante.

ucv.edu.pe

Anexo 6: Consentimiento informado

PERÚ | Ministerio de Salud | Viceministerio de Prestaciones y Aseguramiento en Salud

"Año de la lucha contra la corrupción y la impunidad"

Consentimiento Informado para Participantes de Investigación

Yo Oscar Yonatan Huayllani Muñoz estudiante del programa de Maestría de Sistemas con Mencion en Tecnologías de la Información de la Universidad César Vallejo vengo realizando en las oficinas de la Unidad de Gestión de Inversiones de Reconstrucción con Cambios un estudio cuyo objetivo pretende Determinar la Relación Existente entre el Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo en el Ministerio de Salud, 2019. Por lo consiguiente, me presento ante usted y le solicito amablemente participar en este estudio que tomará aproximadamente 60 minutos de su tiempo. Durante el desarrollo de este estudio tendrá que responder a dos cuestionarios. La participación en este estudio es estrictamente voluntaria, siendo la información recogida de carácter confidencial que no podrá ser usada para ningún otro propósito fuera de esta investigación. Sus respuestas al cuestionario serán codificadas usando un número de identificación y por lo tanto, serán anónimas. Si tiene alguna duda sobre este proyecto, puede hacer preguntas en cualquier momento durante su participación en él. Igualmente, puede retirarse del proyecto en cualquier momento sin que eso lo perjudique en ninguna forma. Si alguna de las preguntas durante el cuestionario le parece incómoda, tiene usted el derecho de hacérselo saber al investigador o de no responderlas.

Desde ya le agradecemos su gentil participación.

	NOMBRES Y APELLIDOS	DNI	FIRMA
1	ALFREDO ESCARATE COBEÑAS	32798188	
2	ANGELA YESLI BRAVO HUAMAN	47765301	
3	ANGHELO DOANIN CENTENO DURAND	73658222	
4	ANTHONY YAFEC CABRERA SANDOVAL	70265447	
5	ARLETTE LUNA VALLE	44055119	
6	ARTURO MIGUEL GAMBOA SANCHEZ	20050625	
7	BENNY ABEL CANCHUMANYA SURICHAQUI	42201133	

8	BERLY ANDRES BRAVO DIPAS	43859408	
9	BRENDA JULISSA CARBAJO HUAMAN	73109195	
10	BRIAN JOSE BERRIO HUAMAN	48056270	
11	BRUNO GONZALES ILIZARBE	10107271	
12	BRYAN SAIDEM CASTILLO DAVILA	70651979	
13	CARLOS ANTONIO ACUÑA ALEGRE	08569103	
14	CARLOS ANTONIO ARMAS GAMARRA	40330504	
15	CARLOS ROLANDO SANCHEZ FARFAN	45621812	
16	CARLOS VIDAL SUAREZ CHAVEZ	07249679	
17	CAROLINA CARRASCO RIVERA	77589936	
18	CAROLINA VICTORIA CARRASCO RIVERA	44325078	
19	CELIA ANGELICA CABRERA CERNA	07878185	
20	CESAR ALFREDO CHILETT LEON	07370135	
21	CESAR ARTURO GIRON SANCHEZ	07284841	
22	CESAR AUGUSTO BEGAZO LEON	2153604	
23	CESAR GARCIA AGUIRRE	07494910	
24	CESAR JOSUE MORENO TOLEDO	41033001	
25	CLAUDIA AIME SALAS FLORES	42459415	
26	CLAUDIA LUCIA FUENTES GAMBOA	72927631	
27	CRISTIAN CARLOS ALVARADO RIOS	40004517	
28	CRISTINA MIRANDA FIGUEROA	42642040	
29	CYNTHIA ISABEL CONTRERAS LAZO	47580089	
30	DANI FRANK ATENCIA NEVADO	40325705	
31	DANIEL ANGEL LOPEZ ARMILLON	47609613	
32	DANIEL ZACARIAS CORONEL MOREYRA	25683924	
33	DAVID HECTOR TORRES PUENTE	09593523	

34	DEBORA FABIOLA BARAYBAR MINAYA	10173178	
35	DEYVI ERICK CASTRO ORTEGA	71329984	
36	DIANA ELIZABETH MEDINA URBINA	47400279	
37	DIANA ELVIRA CORNEJO ORZERO	41042115	
38	DIANA ROCIO YUPANQUI ZEVALLOS	45048640	
39	DIANA ROSALINDA MONTES ZEVALLOS	72978863	
40	DIEGO LUIS FERNANDO ROJAS LUDEÑA	47463933	
41	EDDY CHARLIE CONDEZO CHUQUIJAJAS	40860092	
42	EDUARDO AGÜERO MENDEZ	40774609	
43	EDUARDO FREDDY AYALA SOLIS	10153518	
44	EDUARDO MAURICIO GRACEY ORRILLO	41384297	
45	EDWAR WILSOR GONZALES BRICEÑO	44251438	
46	EDWARD CALDERON CALIENES	07500734	
47	EDWIN MOISES YANAC REYES	40129434	
48	ELIOT MANOLO CASAÑO PORTUGAL	08690030	
49	ENRIQUE EDUARDO QUISPE TINTAYA	42872579	
50	*ERICK ADOLFO CASTRO ORTEGA*	21568426	
51	ERIKA MACARENA LAZABARA SHERON	25790867	
52	ERNESTO ALONSO VEGAS CARBONEL	44752216	
53	ERNESTO TALAVERA GELDRES	41495322	
54	FERNANDO ERNESTO PEREZ VALLADARES	15669309	
55	FRANCO AMERICO CANCHOS CUPE	46037409	
56	FRANKLIN CIRILO CUBA HUAMANI	45207997	
57	GINNA PAOLA VARGAS VASQUEZ	42816934	
58	GLADYS REBECA RUBIO MADRID	10143784	
59	GONZALO FELIPE HUAMAN MENDOZA	45242347	

60	HERSON COLLANTES SANTILLAN	70860835	
61	IVAN MIXAN ALVAREZ	18071133	
62	JACQUELINE BARAHONA CUADROS	47960657	
63	JAVIER CARRASCO ASCURRA	08493092	
64	JESSICA CLORINDA QUILICHE AGUIRRE	47378986	
65	JHON FREDY PINEDA COSME	40159156	
66	JHON RICHARD ACERO ROSALES	40644109	
67	JHOSVEL JOSE VELIZ CANO	45483015	
68	JILBER OROSCO TORRES	43988990	
69	JOEL ALFREDO CASTILLA MATEO	10307156	
70	JOHN CRISTIAN NECIOSUP NECIOSUP	47568943	
71	JORGE LEANDRO ALBITES ESPICHAN	06642584	
72	JORGE RAUL MALDONADO HUATUCO	09955522	
73	JOSE ANTONIO CORONADO DIAZ	40669988	
74	JOSE LUIS PACHECO URIBE	15748847	
75	JOSE MANUEL ROJAS DURAND	70000183	
76	JOSE MIGUEL YAURI PASTRANA	42717357	
77	JUAN CARLOS GAPURA CASTILLO	40147716	
78	JUAN CARLOS SOTO DELGADO	09861569	
79	JUAN JESUS AVILA FERNANDEZ	40744944	
80	JUAN LUIS VEGA PINO	10689209	
81	JUAN MANUEL SANABRIA VALVERDE	44657076	
82	JUAN MANUEL SIFUENTES ORTECHO	06225159	
83	KARINA DEL PILAR CASTRO PINEDA	40293511	
84	KATHELLEN LIZZIE CASTILLO PAZ	42525038	
85	KENYI ABEL GAMEROS DUEÑAS	72517127	

86	KRIKOR JHORGAN ALARCON ALVINO	10734936	
87	LEDDY MARGARITA CHIRINOS VARGAS MACHUCA	40806243	
88	LESLIE ALINA ZARATE DAMIAN	45581210	
89	LORENA MAYTTE BARBOZA CALDERON	48320057	
90	LUIS ALBERTO BELLODAS PAREDES	08330725	
91	LUIS ALBERTO SANCHEZ MANSILLA	74021797	
92	LUIS EDMUNDO REYMUNDO HUGO	73738295	
93	LUIS ENRIQUE AGUILAR PEREA	47481979	
94	LUIS ENRIQUE RAMOS OSTOS	41120223	
95	LUIS ENRIQUE ROCA BENDAYAN	09828255	
96	LUIS FERNANDO ALFARO PORTOCARRERO	42291077	
97	LUIS LAGONES LLANQUI	20074076	
98	MANUEL EUSEBIO CALIENES SANTANA	10136475	
99	MARIA DEL PILAR GRETZZEL REYES VASSALLO	06156104	
100	MARIA LORENA CHAVEZ MACA	25713687	
101	MARIA PAOLA VARGAS VASQUEZ	47422599	
102	MICHAEL JONATHAN LUCIANO SOLIS	40761444	
103	MIGUEL ANGEL ROMERO GUERRERO	06707422	
104	MIGUEL RAUL GOMEZ MASIAS	07555585	
105	MIGUEL SLIM ACERO ROSALES	41653652	
106	MIRELLA LISETH TRUJILLO LUCANO	72870176	
107	NANCI AIDEE DIAZ DIAZ	06080079	
108	NATALIE ROXANA PINTO MIRANDA	41908106	
109	NILTON JOHN RIOS TAMAYO	71553045	
110	NILTON WILFREDO DELGADILLO ALANYA	40738035	
111	OLENKA TUESTA DEL AGUILA	47083241	

112	OLINDA VICTORIA ECHEANDIA HEREDIA	10812115	
113	PABLO FRANCISCO LA ROSA SANCHEZ PAREDES	10617029	
114	PAMELA GIANIRA GOMEZ GUERRERO	42986498	
115	PAOLA BELLIDO VALLEJO	42299393	
116	PEDRO PABLO MEJIA MATIAS	06775541	
117	RAFAEL ANTONIO HOYOS GONZALES	40234556	
118	RALPH OSCAR DEL VALLE AZCARZA	44211613	
119	RAUL ALEXIS OJEDA SALCEDO	47329642	
120	RICARDO CORNEJO PASTOR	06793713	
121	RICARDO RAUL LEON ANGOMA	10293453	
122	RICHARD MAMANI APAZA	40386685	
123	RICK GEORGE ORTIZ VELASQUEZ	70366384	
124	ROLANDO ROMERO DELGADO	09326386	
125	ROSALIA MARILIN ROMAN DELGADO	74688537	
126	RUBI XIOMARA ANDIA INCA	73150021	
127	SANDRA FLOR LEON CABRERA	40439606	
128	SANDRA ISSELA CARDENAS MARTINEZ	40058860	
129	SANDRA MABEL OROPEZA MORA	41581606	
130	SOFIA ISABEL FERNANDEZ MEDINA	46411541	
131	SONIA MORENO CUADROS	40541991	
132	STEFANY JAZMIN LOPEZ SOTOMAYOR	75658323	
133	VICTOR ANTONIO SICCHA PEREZ	44741512	
134	VICTOR HUGO CABRERA PERALTA	42730849	
135	VICTOR MILLONES MASIAS	43557865	
136	VIRGINIA LOURDES VELIZ ZAVALA	09157165	
137	VITO MORE VALENTIN DAMAS	47082843	

138	WALTER ATILIO FUENTES CHUQUITAPA	06742100	
139	WENDY HUAMAN TICONA	10712739	
140	WILBER AMAO CALSIN	42062971	
141	WILDER IVAN CABRERA PERALTA	40317444	
142	WILLY RICARDO ZAMALLOA NUÑEZ	41984180	
143	YASER MOHAMMAD HOSSINZADEH SAIRE	43583771	
144	YAZMIN KAREN CACERES SOLIS	23963527	
145	YDA MARIA ELENA DIAZ RODRIGUEZ	47474721	Yda Diaz Rodrig.

Los que suscribimos, dejamos constancia de nuestra participación y dejamos nuestra firma en señal de conformidad.

Lima, 16 de diciembre de 2019

Ing. César Josué Moreno Toledo
CIP 96202
COORDINADOR TÉCNICO ADMINISTRATIVO
DE EXPEDIENTES TÉCNICOS

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

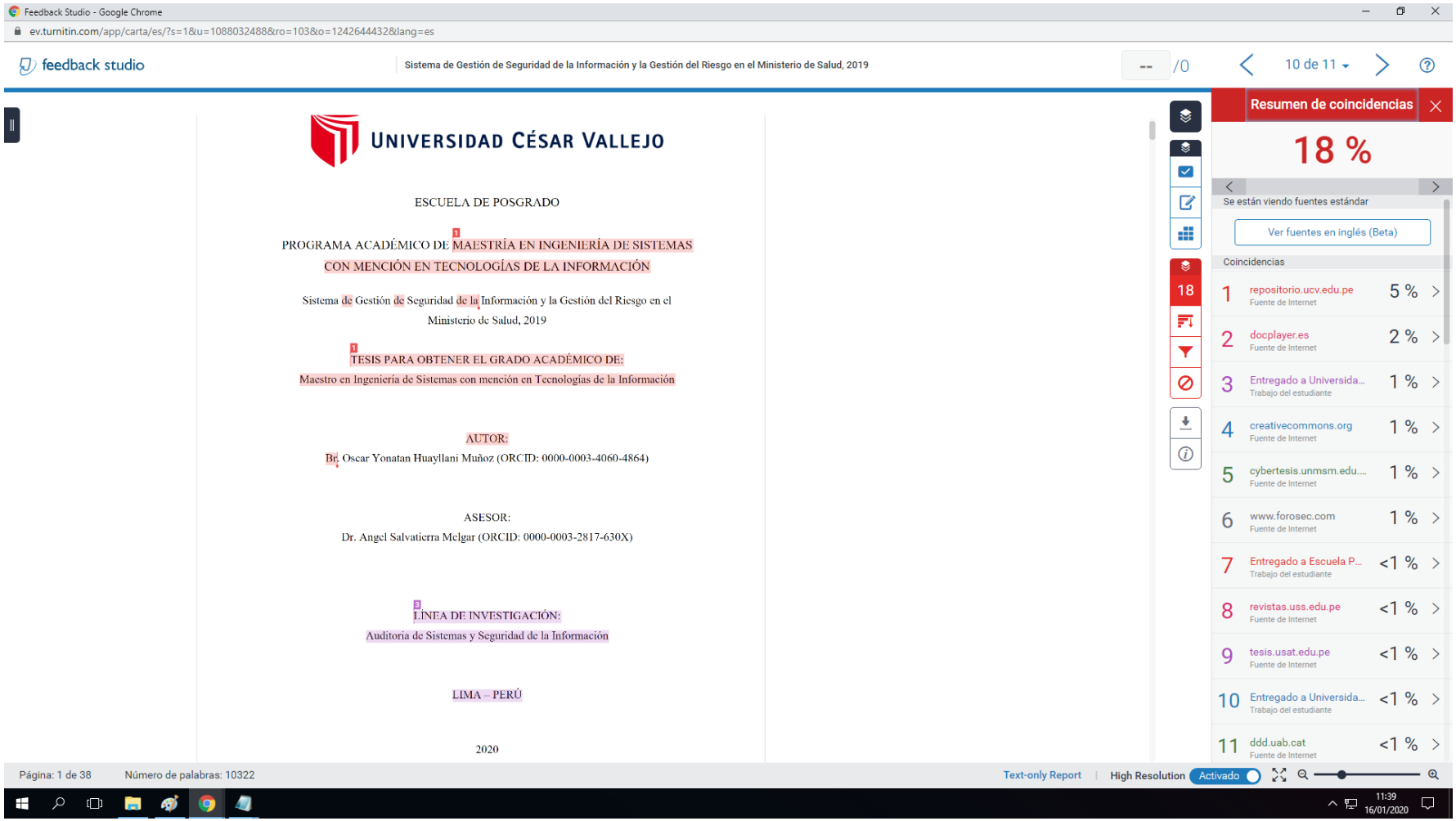
ACTA DE APROBACIÓN DE ORIGINALIDAD DE TRABAJO ACADÉMICO

Yo, Angel Salvatierra Melgar, docente de la Escuela de Posgrado de la Universidad César Vallejo filial Lima Norte. La tesis titulada "**Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo en el Ministerio de Salud, 2019**" del estudiante **Oscar Yonatan Huayllani Muñoz,** constato que la investigación tiene un índice de similitud de 18% verificable en el reporte de originalidad del programa Turnitin.

La suscrita analizó 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, 17 de enero del 2020

Angel Salvatierra Melgar
DNI:19873533


Feedback Studio - Google Chrome
ev.turnitin.com/app/carta/es/?s=1&u=1088032488&ro=103&o=1242644432&lang=es
feedback studio
Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo en el Ministerio de Salud, 2019
-- /0
10 de 11
UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSGRADO
PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN
Sistema de Gestión de Seguridad de la Información y la Gestión del Riesgo en el Ministerio de Salud, 2019
TESIS PARA OBTENER EL GRADO ACADÉMICO DE:
Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información
AUTOR:
Br. Oscar Yonatan Huayllani Muñoz (ORCID: 0000-0003-4060-4864)
ASESOR:
Dr. Angel Salvatierra Melgar (ORCID: 0000-0003-2817-630X)
LÍNEA DE INVESTIGACIÓN:
Auditoría de Sistemas y Seguridad de la Información
LIMA – PERÚ
2020
Resumen de coincidencias
18 %
Se están viendo fuentes estándar
Ver fuentes en inglés (Beta)
Coincidencias
1 repositorio.ucv.edu.pe 5 %
2 docplayer.es 2 %
3 Entregado a Universida... 1 %
4 creativecommons.org 1 %
5 cybertesis.unmsm.edu.... 1 %
6 www.forosec.com 1 %
7 Entregado a Escuela P... <1 %
8 revistas.uss.edu.pe <1 %
9 tesis.usat.edu.pe <1 %
10 Entregado a Universida... <1 %
11 ddd.uab.cat <1 %
Página: 1 de 38
Número de palabras: 10322
Text-only Report
High Resolution
Activado
11:39
16/01/2020

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)

HUAYLLANI MUÑOZ OSCAR YONATAN

D.N.I. : 44030405

Domicilio : JR. HUANTA 540 DPTO. 2 - LIMA

Teléfono : Fijo : ..... Móvil : 997630814

E-mail : oscar.huayllani@t4a.com.pe

2. **IDENTIFICACIÓN DE LA TESIS**
Modalidad:

☐ Tesis de Pregrado
Facultad : .....
Escuela : .....
Carrera : .....
Título : .....

☒ Tesis de Posgrado

☒ Maestría ☐ Doctorado

Grado : MAESTRO

Mención : TECNOLOGÍAS DE LA INFORMACIÓN

3. **DATOS DE LA TESIS**
Autor (es) Apellidos y Nombres:

HUAYLLANI MUÑOZ OSCAR YONATAN

Título de la tesis:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DEL RIESGO EN EL MINISTERIO DE SALUD, 2019

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 : 13/02/2020

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:

OSCAR YONATAN HUAYLLANI MUÑOZ

INFORME TÍTULADO:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DEL RIESGO EN EL MINISTERIO DE SALUD, 2019

PARA OBTENER EL TÍTULO O GRADO DE:

MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

SUSTENTADO EN FECHA: 19 DE ENERO DE 2020

NOTA O MENCIÓN: APROBADO POR UNANIMIDAD

ESCUELA DE POSGRADO UCV INVESTIGACIÓN CAMPUS LIMA NORTE

FIRMA DEL ENCARGADO DE INVESTIGACIÓN