ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:

Maestro en ingeniería de sistemas con mención en tecnologías de la información

AUTOR:

Br. Calderón Sánchez Jorge Armando

ASESOR:

Dr. Luis Torres Cabanillas

SECCIÓN:

Ingeniería

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LIMA – PERÚ

2019

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

DICTAMEN DE LA SUSTENTACIÓN DE TESIS

EL / LA BACHILLER (ES): **CALDERON SANCHEZ, JORGE ARMANDO**

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

SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN LOS TRABAJADORES DE LA DIGERE DEL MINISTERIO DE EDUCACIÓN,2018

Fecha: 25 de enero de 2019 Hora: 2:00 p.m.

JURADOS:

PRESIDENTE: Dr. Noel Alcas Zapata **Firma: .....**

SECRETARIO: Dra. Flor de Maria Sanchez Aguirre **Firma: .....**

VOCAL: Mg. Luis Alberto Torres Cabanillas **Firma: .....**

El Jurado evaluador emitió el dictamen de:

..... APROBADO POR MAYORÍA .....

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

.....

..... INCONSISTENCIAS METODOLÓGICAS .....

.....

.....

Recomendaciones sobre el documento de la tesis:

..... APA .....

..... MEJORAR LA DISCUSIÓN .....

.....

.....

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.

Dedicatoria

Dedico el presente trabajo a mi padre Manuel que siempre me cuida, porque no importa que no se encuentre físicamente a mi lado, su cariño siempre permanecerá en mi corazón, a mi madre Ysabel que está a mi lado siempre, a mi familia y a las personas que creyeron en mí, en los momentos más difíciles que me toco afrontar y de alguna forma me alentaron en todo momento para que logre cumplir mis metas profesionales.

Agradecimiento

Mi agradecimiento a los docentes y asesores de la escuela de Posgrado de la “Universidad Cesar Vallejo” que colaboraron con la elaboración de la presente investigación, a los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación por su apoyo durante el desarrollo de la investigación.

A mi padre por esas noches de conversación donde escuchaba atentamente las metas que me trazaba y me daba el respaldo y aliento necesario para seguir, muchas gracias y te puedo decir promesa cumplida.

Presentación

Señores miembros del jurado calificador

De conformidad con el Reglamento de Grados y Títulos de la Universidad César Vallejo, pongo a vuestra consideración la evaluación de la tesis Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018 elaborada con el objetivo general de encontrar la correlación entre las variables seguridad de la información y la gestión de riesgos.

En el presente trabajo, se estudia la relación existente entre las variables seguridad de la información y gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación. El estudio comprende los siguientes capítulos: el capítulo I se refiere a la introducción; el capítulo II se refiere al Marco metodológico; el capítulo IV se refiere a la discusión; el capítulo V a las conclusiones; el capítulo VI a las recomendaciones. Por último, el capítulo VII menciona las referencias bibliográficas y los anexos respectivos.

Los resultados obtenidos en la presente investigación han sido elaborados siguiendo el protocolo de la Escuela de Post grado de la Universidad.

Señores miembros del jurado esperamos que esta investigación sea evaluada y merezca su aprobación.

Los Olivos, 25 de Enero del 2019

Jorge Armando Calderón Sánchez

DNI: 41908330

Declaratoria de autenticidad

Yo, Jorge Armando Calderón Sánchez, estudiante del Programa de Maestría en Ingeniería de Sistemas con mención de Gestión de Tecnologías de la Información de la Escuela de Postgrado de la Universidad César Vallejo, identificado con DNI N° 41908330, respectivamente, con la tesis titulada Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018, declaro bajo juramento que:

1) La tesis es de autoría propia.

2) Se ha respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto, la tesis no ha sido plagiada ni total ni parcialmente.

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

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

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

Los Olivos, 25 de Enero del 2019

Jorge Armando Calderón Sánchez

DNI: 41908330

Índice

Índice de Tablas

Índice de Figuras

Resumen

A continuación se presenta una síntesis de la investigación “Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018"

El objetivo de la investigación estuvo dirigido a reconocer la relación de la seguridad de la información y la gestión de riesgos en la Dirección de Gestión de Recursos Educativos del ministerio de educación, 2018. La investigación fue de tipo de estudio básico, con un diseño no experimental, correlacional y transversal, la población elegida fue de 106 trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, los cuales fueron seleccionados de una manera probabilística y aleatoria simple, muestreo de tipo probabilístico y aleatorio simple; mientras el método de investigación hipotético-deductivo de enfoque cuantitativo; y en el tratamiento de los datos se realizó a través del SPSS; se empleó la prueba no paramétrica de alcance correlacional Rho de Spearman.

Con la presente investigación se espera encontrar la relación entre las dos variables de estudio, y de esta forma los resultados sean tomados en cuenta por la entidad donde se realizó el estudio; para que se establezca una correcta toma de decisiones en temas de seguridad de la información y la correcta gestión de los riesgos y amenazas que puedan producirse en el tratamiento de los activos importantes para la entidad. Así mismo será de utilidad para medir el grado de aprendizaje y conocimiento con el que cuentan los trabajadores de la DIGERE, en temas de seguridad y gestión de riesgos.

Palabras claves (2): *seguridad de la información, gestión de riesgos, disponibilidad.*

Abstract

Below is a summary of the research "Information security and risk management in the workers of the DIGERE of the Ministry of Education, 2018"

The objective of the research was aimed at recognizing the relationship of information security and risk management in the General Directorate of Educational Resources of the Ministry of Education, 2018. The research was of a basic study type, with a non-experimental design , correlational and cross-sectional, the chosen population was 106 workers of the General Directorate of Educational Resources of the Ministry of Education, which were selected in a simple random and probabilistic manner, simple probabilistic and random sampling; while the hypothetico-deductive research method of quantitative approach; and in the treatment of the data was done through the SPSS; the nonparametric test of Spearman's Rho correlation scope was used.

With the present investigation it is expected to find the relationship between the two study variables, and in this way the results are taken into account by the entity where the study was conducted; so that a correct decision-making is established in matters of information security and the correct management of risks and threats that may occur in the treatment of important assets for the entity. Likewise, it will be useful to measure the degree of learning and knowledge that DIGERE workers have, in matters of security and risk management.

Keywords (2): *information security, risk management, availabilit.*

I. Introducción

1.1 Realidad problemática

Internacionalmente, se está tomando a la seguridad de la información con el apelativo de Cyberseguridad según lo estipulado por Giant (2016) esto con relación a los ataques masivos que se pueden producir a través de la redes sociales, del mismo modo en Sudamérica específicamente en Colombia, existe una cantidad elevada de empresas que le brindan poco interés a la gestión de riesgos en el desarrollo de sus procesos, Venegas y Pardo (2014) detallan que a los inicios del nuevo milenio, las empresas cuyo core de trabajo es el desarrollo de software en sus proyectos no realizan la gestión del riesgo, solo se enfocaban en lograr la respuesta ante un problema inmediato sin prevenir posibles riesgos vinculados a los incidentes reportados. Para Burgos Salazar en la actualidad son múltiples los riesgos asociados a que los equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad. Las amenazas en las TIC son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Preocupante es para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

En el Perú según Simich (2016), existe una enorme brecha en el tema de seguridad de la Información debido a una falta de cultura de seguridad de las empresas vinculado a un tema de desconocimiento por parte de los directivos y/o Direcciones encargadas de las entidades, los cuales no toman la importancia debida en los grandes riesgos existentes de ataques que se pueden producir en sus organizaciones.

La Dirección de Gestión de Recursos Educativos del Ministerio de Educación del Perú fue creada bajo Resolución Ministerial 491-2013 y la cual será sujeta al presente estudio cuenta con una población de 106 usuarios. La labor de esta entidad es dotar de recursos tecnológicos y material educativo a todos los colegios del Perú, con la finalidad que los niños puedan aprovecharlos y de esta

manera contribuir con el desarrollo en materia educativa. De esta manera los trabajadores de la DIGERE realizan intercambio de información para ejecutar las labores del día a día y para ello utilizan herramientas informáticas las cuales son susceptibles a posibles ataques informáticos o de ingeniería social con el objetivo de realizar el robo de información. Esta entidad a través de la gestión de la oficina de Tecnologías de la Información viene realizando políticas de seguridad en las etapas de confidencialidad, disponibilidad e integridad basada en norma ISO 27001:2013 con la finalidad de minimizar los riesgos vinculados a los activos de información que maneja, así mismo ha desarrollo programas de capacitación acerca de los activos de información que son primordiales para la entidad con la finalidad de sensibilizar a los trabajadores en el correcto resguardo de los mismos, si bien es el inicio de una etapa de capacitación lo que se tiene proyectado es realizar la implementación de un sistema gestión de la seguridad de la Información el cual establezca las medidas adecuadas y las alertas correspondientes sobre el resguardo de los activos importantes para la entidad, esto con la finalidad de gestionar los riesgos, minimizando las amenazas y riesgos que puedan generarse durante el desarrollo de las actividades de los colaboradores de la entidad.

En la actualidad las entidades públicas vienen tomando conciencia de la importancia de la seguridad de la información y de la gestión de riesgos, por ende se encuentran estableciendo las primeras medidas para proteger la información que se maneja sea física o digital, esto como primer paso para una futura implementación de un sistema de gestión integral de seguridad que permita no solo identificar las vulnerabilidades; sino brindar una solución inmediata a los incidentes que se reporten. Así mismo es fundamental realizar la gestión de riesgos de TI, ya que ella permitirá a las entidades contar con la información adecuada para identificar los activos de información que son relevantes y de suma importancia para minimizar los riesgos a los que se encuentre expuestos la entidad en temas de seguridad.

1.2 Trabajos previos

1.2.1 Trabajos previos internacionales

Arévalo (2017) en su investigación titulada *Elaboración y Plan de Implementación de Políticas de Seguridad de la Información Aplicadas a una Empresa Industrial de Alimentos*, realizó un estudio de tipo básico, con diseño no experimental de corte transversal. La población estuvo conformada por todos los procesos del departamento de producción de la empresa. Este estudio permitió definir las dimensiones de la gestión de riesgos y asentar las bases para la propuesta de implementación de un sistema de seguridad de la información, una de las conclusiones describe la relación de seguridad de la información en base a la gestión de riesgos.

Crespo (2016) en su investigación titulada *Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES,* realizo un estudio de tipo básico, con diseño no experimental de corte transversal. La población del estudio se basó en 50 MPYMES. En esta se tomó una evaluación del estado actual con respecto a la seguridad de la información. Una de las conclusiones acentúa la importancia de la gestión de riesgos dentro de cada organización en base a las dimensiones de evaluación y tratamiento de los riegos para su resolución eficaz.

Muñoz (2016) en su investigación *Diseño de Políticas de Seguridad Informática para la Dirección de Tecnología de la Información y Comunicación (DTIC) de la Universidad de Cuenca*, realizo un estudio de tipo básico, con diseño no experimental de corte transversal. Se tomó como población de estudio la aplicación de los 11 dominios de seguridad de la norma ISO 27002. Una de las conclusiones hace referencia a las dimensiones de disponibilidad, confidencialidad e integridad de la información es de vital importancia para mejorar el cumplimento de las políticas y disminuir el riesgo.

Molina (2015) en su investigación titulada *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica de Litoral*,

realizo un estudio de tipo básico, con diseño no experimental de corte transversal. En esta se tomó en cuenta a todo el personal de la Escuela Superior Politécnica de Litoral. Este estudio permitió obtener las dimensiones e indicadores de la gestión de riesgos basados en las normas internacionales y obtener un marco de referencia a un plan de seguridad de la información y la gestión de los riesgos mediante la metodología MAGERIT, a su vez se denota la relación entre la seguridad de la información y la gestión de riesgos.

Castro (2014) en su investigación *Elaboración de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Empresa Radical CIA. LTDA. En la ciudad de Quito para el año 2014,* realizo un estudio de tipo básico, con diseño no experimental de corte transversal. De esta se pudo obtener las dimensiones de la seguridad de información expuestas por medio de atributos dentro de la misma. Una de las conclusiones denota que la seguridad de la información depende de la disponibilidad de la información de seguridad interna dentro de la organización lo cual disminuye los riesgos.

Maggiore (2014) en su investigación *Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio,* realizo un estudio de tipo básico, con diseño no experimental de corte transversal. En esta se realizó un corte en el año 2009 para un análisis y recopilación de información de modelos de madurez de la gestión de seguridad de la información. Una de las conclusiones muestra como resultado un marco integrado de gestión de riesgos que se tomara como base para la propuesta final. Se evidencia que la aplicación de un correcto sistema de seguridad de la información a partir del control de la gestión de riesgos proporciona un modelo a seguir en una entidad con la finalidad de proteger la información vital que se maneje.

Los antecedentes internacionales han sido de gran importancia para establecer dimensiones de las variables, tipo de estudio, el enfoque utilizado para la obtención de los resultados, que serán parte de estudio en la presente investigación, así como los resultados obtenidos que sin duda brindaran la

información necesaria para verificar el tratamiento que se brinda a cada variable en otros países y la importancia que las empresas o entidades les brindan.

1.2.2 Trabajos previos nacionales

Otoya (2018) en su investigación *Gestión de Riesgos TI en la seguridad de la Información del Programa de Desarrollo Productivo Agrario Rural 2017*, realizo un estudio de tipo básica, con diseño no experimental y de corte transversal. Se empleó el método estadístico causa efecto. La población estuvo conformada por 174 colaboradores de la entidad y se concluyó que existe una influencia significativa de la gestión de riesgos de TI en la seguridad de la información. De esta manera esta investigación fue de ayuda para contar con el marco teórico acerca de las teorías del magerit y su aplicación de los activos de la información.

Tacza (2018) en su *investigación Cumplimiento del plan de seguridad de la información con relación a la norma ISO 27000 en la Universidad Nacional Tecnológica de Lima Sur año 2017*, realizo un estudio de tipo básica, con diseño no experimental y de corte transversal. Se empleó el método estadístico de correlación. La población estuvo conformada por el personal administrativo (100 personas), con una muestra de 80 trabajadores. Una de las conclusiones hace referencia a las dimensiones de disponibilidad, integridad y confidencialidad afirmando que existe relación directa con la norma ISO/IEC 27001:2005 (Seguridad de la Información). Con respecto a la gestión del riesgo denota que existe una relación directa con la distribución de la información.

Pinto (2017) en su investigación *Gestión y riesgos de seguridad de la información en la Escuela de Suboficiales de la Policía Nacional del Perú, Puente Piedra 2016,* realizo un estudio de tipo básica, con diseño no experimental y de corte transversal. Se empleó el método estadístico de correlación. La población estuvo conformada por 117 docentes de la escuela de sub oficiales de la P.N.P. – Puente Piedra, se tomó toda la población como muestra. Una de las conclusiones hace referencia a las dimensiones de la gestión de riesgos y la seguridad de la información, afirmando que existe una relación directa entre ambas.

Mercado (2016) en su investigación *Modelo de gestión de seguridad de la información para el E-Gobierno*, realizo un estudio de tipo básico, con diseño no experimental y de corte transversal. La población estuvo conformada por 69 entidades del sector público con el mismo tamaño de muestra. Esta realizo una revisión de modelos de la seguridad de la información basados en estándares, definiendo la organización y funciones de la seguridad de la información. Una de las conclusiones hace referencia a la relación que existe entre la dimensión de disponibilidad y los controles de seguridad para una gestión de riesgos.

Seclen (2016) en su investigación *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*, realizo un estudio de tipo básico, con diseño no experimental y de corte transversal. Esta nos brinda sustento para la investigación en la entidad pública nacional en la cual se realizó la investigación. Una de las conclusiones hace referencia a la dimensión de análisis de riesgos la cual indica que existe una relación de con la seguridad de la información, con respecto a la seguridad de la información brindo una serie de factores que están relacionados al sistema de seguridad de la información.

Tarrillo (2015) en su investigación *Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba*, realizo un estudio de tipo básico, con diseño experimental y de corte transversal. Se empleó el método estadístico de correlación. La población estuvo conformada por 150 trabajadores de la zona registral III Sede Moyobamba con una muestra de 50 trabajadores. Este trabajo nos brinda como resultado la relación directa entre la seguridad de la información y los activos de información que se encuentra ligado a la gestión de riesgos razón por la cual brinda sustento al presente trabajo de investigación.

Los trabajos previos nacionales han servido al presente trabajo de investigación para determinar la valoración que se brinda por parte de las entidades a las variables de estudio seguridad de la información y gestión de riesgos, así mismo nos permitirá tomar en cuenta los instrumentos de medición utilizados por

los diversos autores a los cuales se les realizar una adaptación propia con la finalidad de utilizar un instrumento aplicable a la realidad de los trabajadores de la Dirección de Gestión de Recursos Educativos

1.3 Teorías relacionados al tema

1.3.1 Teorías relacionadas a la seguridad de la Información

Definición

Solarte (2015), la seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. La información puede presentarse en diversos formatos y medios tanto físicos, como electrónicos. Por lo tanto, las organizaciones deben adoptar y adaptar metodologías para proteger los archivos y registros, mantener en funcionamiento una infraestructura tecnológica adecuada que sirva para la custodia y salvaguarda de la información.

Soriano (2014), define el concepto de seguridad de la información como “La manera de proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados” (p.6).

La información es un activo importante para cualquier empresa y que debe ser tratado bajo un esquema de seguridad y desde esta manera se debe establecer parámetros en los cuales se pueda verificar que no existan amenazas que puedan provocar ataques internos o externos y que manipulen la información. En el año 1992 la OCDE4 desarrollo el concepto de políticas y directivas de seguridad en los sistemas de información los cuales básicamente buscan orientar al personal de la empresa sobre la cultura de la seguridad de la información.

Las directivas utilizadas son la concientización, la responsabilidad, la respuesta adecuada, la ética, la democracia, la evaluación del riesgo, diseño y realización de la seguridad, gestión de la seguridad y la reevaluación. Con el pasar de los años se ha venido estableciendo políticas de seguridad en las empresas a través de sus áreas de tecnologías de la información en los que se brinda

preponderantemente conceptos sobre la implantación de sistemas fiables y seguros basados en un enfoque de desarrollo e integración del personal de la empresa. Los objetivos de la gestión de la seguridad de la información son básicamente la protección de los tres pilares de la información y los cuales son la confidencialidad, integridad de datos y disponibilidad de la información.

Figura 1. Tratamiento de la seguridad de la información

Figura 2. Esquema de la seguridad de la información

Existen algunas directivas que se pueden aplicar como primeras medidas a adoptar para el resguardo de la información y las cuales se detallan a continuación:

- Exponer la información de la empresa ya sea de manera física o digital sin el uso de parámetros de seguridad.
- Modificación de información sin la autorización del personal autorizado y con los permisos correspondientes, esto debe ser establecido por el comité de seguridad de la información.
- Perdida de información debido a manipulación de la misma por personal externo o interno de la empresa, y no pudiendo recuperarla.
- Cortes imprevistos en el acceso a la información necesaria para el desarrollo de las labores del personal de la empresa.

De acuerdo a lo que establece Soriano (2014) existen deficiencias y vulnerabilidades que brindan la capacidad de desarrollo de los problemas descritos anteriormente, a continuación detallaremos las siguientes:

Las Deficiencias tecnológicas: Con el pasar de los años la tecnología avanza de una manera exponencial y se dan a conocer nuevas tecnologías y equipamiento necesarios poder enfrentar los posibles ataques o amenazas informáticas referentes a la información que maneje la empresa. Pero se debe tener presente que depende en gran manera la importancia que cada empresa le brinde al resguardo de su información y así mismo el presupuesto que se destine para la adquisición y renovación del equipamiento y así mismo las licencias de los software que se encargaran del monitoreo de la red interna de la empresa necesario para afrontar los ataques que se puedan producir.

Deficiencias de la política de seguridad: Cada empresa tiene la responsabilidad de adecuarse a la política de seguridad de la información que fuese aprobada y así mismo cumplirla de manera estricta. Pero esto no se realiza debido quizás a una mala práctica de los usuarios, a la falta de criterio del personal técnico responsable, a la falta de supervisión por parte de los oficiales o encargados de la seguridad de la información de cada empresa, a la falta de la distribución de la política de la seguridad de la información al personal de la empresa y la debida capacitación,

ausencia de un plan de contingencia ante un desastre, en suma a diversos factores que deben ser evaluados constantemente.

Deficiencias de configuración: El personal técnico de cada empresa debe realizar una correcta configuración de los equipos informáticos, esta configuración debe estar ligada a la política de accesos del personal a los equipos y a bloquear los accesos no autorizados

NTP-ISO/IEC 17799 (2014), es la Norma Técnica Peruana la cual establece que la seguridad de la información está ligada a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, además de otras muchas propiedades como puede ser la autenticidad, la falta de rechazo, la contabilidad y la confiabilidad. Esta norma provee un modelo para implementar los principios en las pautas que gobiernan la evaluación del riesgo, el diseño e implementación de la seguridad, la gestión de seguridad y la reevaluación de la información en una institución. De acuerdo a esta resolución, se especifica que la implementación deberá realizarse en un plazo máximo de dos (02) años a partir de su publicación.

Dimensiones de la Seguridad de la Información

Dimensión 1: Disponibilidad

Soriano (2014), establece que la disponibilidad es contar con acceso a la información cuando se requiere ya que cualquier retardo superior al establecido según los niveles de servicio puede ser descrito como una violación de la disponibilidad.

De esta manera si un sistema de información no está disponible cuando se necesita es, como mínimo, tan malo como no disponer de dicho sistema. La disponibilidad, de la misma forma que otros aspectos vinculados a la seguridad, de la información puede verse afectada por cuestiones puramente técnicas por ejemplo, una parte mal funcionamiento de una computadora o dispositivo de comunicaciones, fenómenos naturales como por ejemplo, el viento el agua, etc o causas humanas ya sea de manera accidental o deliberada.

Dimensión 2: Confidencialidad

Soriano (2014), hace referencia a la protección de la información frente a su divulgación a entidades o individuos no autorizados (organizaciones, personas, máquinas, procesos). Nadie debe poder leer los datos a excepción de las entidades específicas previstas.

Dimensión 3: Integridad de datos

Soriano (2014), La integridad de datos es la protección de los datos frente a la modificación, supresión, duplicación o reordenación realizada por entidades no autorizadas (organizaciones, personas, máquinas, procesos). Más concretamente, la integridad se refiere a la fiabilidad de los recursos de información. Una violación de la integridad se debe siempre a un ataque activo.

La integridad de datos es la garantía de la no alteración: se garantiza la detección de cualquier alteración de los datos (ya sea en tránsito por la red o en almacenamiento en un disco duro, por accidente o deliberadamente). Es evidente que esta garantía es esencial en cualquier tipo de entorno empresarial o comercio electrónico, y es más que deseable en muchos otros entornos. La integridad de un sistema de información implica garantizar que no ha habido ninguna corrupción en los datos que han sido transmitidos o almacenados en el sistema, detectando cualquier posible manipulación. Para ello, es necesario el uso de técnicas criptográficas.

1.3.2 Teorías relacionadas a la gestión de riesgos

Definición

Westerman (2006), menciona que la gestión de riesgos en TI tiene un trasfondo en la actualidad ya que no solo se evalúan riesgos técnicos; sino que se ha expandido a riesgos en todos los niveles que pueden ocasionar graves pérdidas a la empresa o entidades que no tomen conciencia de realizar supervisión del incremento de los niveles de riesgo. Hoy en día el jefe encargado de una empresa valora las pérdidas que se podrían generar y brinda una visión tanto presupuestal para la adquisición de equipamiento de minimice los riesgos ante incidentes que

afecten la información que maneje la empresa.

Por ende contar con un política que regule la seguridad de la información y la gestión de riesgos podrá generar rápidas medidas de contingencia a la alta dirección en la toma de decisiones a efectos de subsanar cualquier incidente que esto provoque. Esto se ve reflejado en la disposición que tiene la alta dirección en brindar un alto presupuesto al área de tecnologías de la Información a la espera que esto será un “gasto” sino una inversión con un tiempo de retorno mínimo, ya que no tener disponible los servicios supone grandes pérdidas para las empresas.

Muchas empresas ven como un gasto innecesario invertir en la adquisición de equipos informáticos sofisticados, que podrían impedir ataques de robo de información, esto es tener una visión anticuada sobre la realidad tecnológica que se vive hoy en día sobre gestionar sus riesgos:

Cabe señalar que los riesgos no son solo a través de medios virtuales sino físicamente y para ello se deben establecer controles de seguridad internos que permitan supervisar los accesos de personal no autorizado a sectores de la empresa cuyo acceso es restringido.

Magerit (2012) denominó proceso de gestión de riesgos a la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores: (1) la gravedad del impacto y/o del riesgo, (2) las obligaciones a las que por ley esté sometida la organización, (3) las obligaciones a las que por reglamentos sectoriales esté sometida la Organización, (4) las obligaciones a las que por contrato esté sometida la Organización. (p. 84).

Es necesario tener muy en claro cuál es la definición del riesgo y su análisis. Dentro del contexto de un análisis de riesgos, es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

Figura 3. Esquema de la gestión de riesgos

Establecer un marco de evaluación de riesgos

El marco se encarga de definir cuestiones como la capacidad de riesgo y la cultura de la empresa, las escalas de riesgo que se van a utilizar, así como la metodología a seguir a la hora de evaluar riesgos de seguridad de la información.

Identificar los riesgos

Posiblemente es la parte más difícil y la que mayor tiempo del proceso consume. Puede encontrarse más fácilmente tras una evaluación del riesgo basada en activos, de tal modo que se identifiquen todos y cada uno de los riesgos que pueden afectar a los activos de información. También resulta de gran utilidad el libre acceso a una biblioteca o registro de riesgos y amenazas que puedan afectar a la organización.

Analizar y evaluar los riesgos

El análisis y la evaluación de los riesgos conllevan un proceso de asignación de

valores concretos para determinar la probabilidad y el impacto en la empresa de los distintos riesgos, y para definir cómo encajan estos en el umbral de aceptación del riesgo. Se debe ser capaz de concretar cuáles de los riesgos son prioridades que requieren medidas urgentes y cuáles tienen un nivel de prioridad medio o aceptable.

Seleccione las opciones de gestión de riesgos

Cuando se hayan determinado los riesgos, se debe establecer si se desean gestionar, admitir, eliminar o transferir. Para gestionar los riesgos debemos hacer uso de los controles de seguridad de la información adecuados. Es de gran utilidad tener acceso a los controles establecidos bajo la norma ISO 27001 2013, sobre todo basándonos en las políticas fijadas según la norma e incorporadas previamente a cada uno de los controles.

Revisión, informe y mantenimiento

Una cuestión de gran importancia respecto a la realización de la evaluación de riesgos para el cumplimiento de la norma ISO 27001 es, naturalmente, el posterior desarrollo del conjunto de informes donde se recogen cuáles son los riesgos, las medidas que se van a llevar a cabo para gestionarlos, cada uno de los plazos para la implementación de los controles, y las distintas acciones accesorias. Respecto a esto, aparecen en la norma ISO 27001 dos documentos de relevancia, como son la Declaración de Aplicabilidad (SOA) y el plan de gestión de riesgos.

ISO 31000. Esta norma fue publicada en noviembre del 2009 por la Organización Internacional de Normalización (ISO) en colaboración con IEC, y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos en la empresa de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Como complemento a esta norma se ha desarrollado otro estándar: la ISO 31010 “Gestión del riesgo. Técnicas de evaluación de riesgos”. Esta norma provee

de una serie de técnicas para la identificación y evaluación de riesgos, tanto positivos como negativos.

Dimensión 1: Proceso de gobernanza del riesgo

Según Westerman (2006) son “políticas completas y eficaces relacionadas al riesgo, combinado con un proceso maduro y consistente para identificar, evaluar, priorizar y supervisar los riesgos oportunamente, el cual incluye políticas y procedimientos para identificar y evaluar los riesgos y prevenir conductas de riesgo”.

Dimensión 2: Cultura consciente sobre riesgos

Según Westerman (2006) “Personas cualificadas que saben cómo identificar y evaluar las amenazas e implementar la mitigación efectiva del riesgo. La conciencia de riesgos ayuda a todos en la empresa a comprender las amenazas y las oportunidades de mitigación”.

Dimensión 3: Implantación eficaz de TI

Según Westerman (2006) son la “Infraestructura y las aplicaciones de TI que tienen riesgos inherentemente inferiores a los tolerables, debido a que están bien gestionados y tienen una buena arquitectura. Una TI bien estructurada y bien administrada es inherentemente menos riesgosa que una más compleja”.

1.4 Formulación del problema

1.4.1 Problema general

¿Qué relación existe entre la seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018?

1.4.2 Problemas específicos

Problema específico 1

¿Qué relación existe entre la dimensión disponibilidad de la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018?

Problema específico 2

¿Qué relación existe entre la dimensión confidencialidad de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018?

Problema específico 3

¿Qué relación existe entre la dimensión integridad de datos de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018?

Problema específico 4

¿Qué relación existe entre la dimensión proceso de gobernanza del riesgo y la seguridad de la información en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018?

Problema específico 5

¿Qué relación existe entre la dimensión cultura consciente sobre riesgos y la seguridad de la información en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018?

Problema específico 6

¿Qué relación existe entre la dimensión implantación eficaz de TI y la seguridad de la información en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018?

1.5 Justificación del estudio

1.5.1 Justificación teórica

Al buscar la relación entre las variables seguridad de la información y gestión de riesgos, se aplica el estándar ISO 27001 promovido por una organización internacional para mejorar el proceso de gestión del riesgo, así mismo los resultados de la investigación incorporaran conocimientos a la Dirección de Gestión de Recursos Educativos en seguridad de la información, lo cual permitirá su aprovechamiento en los procesos que genera la entidad.

1.5.2 Justificación practica

La justificación práctica se centra en determinar las variables que nos proporcionan información diseñada a la medida de las necesidades, esta estructura tiene como parte fundamental y alimentadora a la retroalimentación, ya que con ella se podrá mejorar los puntos identificados como débiles y mejorar aquellos que ya estén ofreciendo resultados positivos dentro de la entidad donde se realiza el estudio.

1.5.3 Justificación metodológica

Metodológicamente la investigación se justifica porque se realizó una encuesta al personal de la Dirección de Gestión de Recursos Educativos, a los cuales se les consulto acerca de su conocimiento acerca de las variables de estudio y de esta manera se obtuvieron datos con los cuales se pudo proponer indicadores de mejora para lograr resultados eficientes.

Según lo que define la investigación correlacional; con los resultados de las encuestas realizadas, se pudo concretar la relación entre las variables de estudio.

1.6 Hipótesis

1.6.1 Hipótesis General

Existe una relación directa entre la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018.

1.6.2 Hipótesis Específicas

Hipótesis específica 1

Existe una relación directa entre la dimensión disponibilidad de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018.

Hipótesis específica 2

Existe una relación directa entre la dimensión confidencialidad de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección de Gestión

de Recursos Educativos del Ministerio de Educación, 2018.

Hipótesis específica 3

Existe una relación directa entre la dimensión integridad de datos de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018.

Hipótesis específica 4

Existe una relación directa entre la dimensión proceso de gobernanza del riesgo y la seguridad de la información en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018.

Hipótesis específica 5

Existe una relación directa entre la dimensión cultura consciente sobre riesgos y la seguridad de la información en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018.

Hipótesis específica 6

Existe una relación directa entre la dimensión implantación eficaz de TI y la seguridad de la información en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018.

1.7 Objetivos

1.7.1 Objetivo General

Determinar la relación que existe entre la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018.

1.7.2 Objetivos Específicos

Objetivo específico 1

Determinar la relación que existe entre la dimensión disponibilidad de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018.

Objetivo específico 2

Determinar la relación que existe entre la dimensión confidencialidad de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018.

Objetivo específico 3

Determinar la relación que existe entre la dimensión integridad de datos de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018.

Objetivo específico 4

Determinar la relación que existe entre la dimensión proceso de gobernanza del riesgo y la seguridad de la información en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018.

Objetivo específico 5

Determinar la relación que existe entre la dimensión cultura consciente sobre riesgos y la seguridad de la información en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018.

Objetivo específico 6

Determinar la relación que existe entre la dimensión implantación eficaz de TI y la seguridad de la información en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018.

II. Método

2. Método

El estudio aplicó el método hipotético - deductivo, De acuerdo a lo que expone Lorezano (2010), este método se basa en la observación y generación de hipótesis acerca de las variables Seguridad de la Información y gestión de riesgos de TI, asimismo esto se complementó con el aporte de la estadística a través de los resultados consignados en los cuestionarios.

2.1 Enfoque

En base a lo expuesto por Fernández y Baptista (2010), la presente investigación se desarrolló bajo un enfoque cuantitativo pues fundamentalmente se realizó la recolección de datos para probar la hipótesis, en función de una medida numérica y el respectivo análisis estadístico. De esta manera se podrá determinar las interacciones entre las variables, así mismo se estipula que un enfoque cuantitativo es secuencial y probatorio ya que existen varias etapas y estas no pueden ser eludidas sino que se realiza un avance secuencial.

2.2 Diseño de investigación

El diseño de investigación empleado es no experimental, según Hernández, Fernández y Baptista (2010), este diseño de investigación consiste en “observar fenómenos tal como se dan en un contexto natural, para posteriormente analizarlos”. (p. 149)

Es transversal, según Hernández, Fernández y Baptista (2010), pues se trata de “recolectar datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado (p. 151).

Por lo dicho, se sostiene que la investigación fue de diseño no experimental y de corte transversal, pues no se manipularon las variables Seguridad de la Información y Gestión de riesgos en TI y solo se describió sus características e importancia; asimismo la recolección de los datos a los clientes se realizó en un solo momento.

2.3 Tipo de estudio

El tipo de investigación es básica teniendo en cuenta lo indicado por Sánchez y Reyes (2002, p.13), que este tipo de investigación nos lleva a la búsqueda de nuevos conocimientos y campos de investigación, manteniendo como propósito recoger información de la realidad para enriquecer el conocimiento científico, en esta investigación el propósito es recoger información y determinar la relación que existe entre la variable Seguridad de la Información y la variable Gestión de riesgos en TI.

2.4 Operacionalización de variables

En la presente investigación se establecerán como variables de estudio la seguridad de la información y la gestión de riesgos.

Tabla 1

Operacionalización de la variable Seguridad de la Información

DIMENSIONES	INDICADORES	ITEMS	ESCALA DE MEDICIÓN	NIVELES Y RANGOS
Disponibilidad	Tiempo que tarda en obtener la información que se requiere.	1-4	1) Nunca 2) Casi nunca 3) Algunas veces 4) Casi siempre 5) Siempre	1) Malo 2) Regular 3) Bueno
	Copias de respaldo de información.	5-6		
Confidencialidad	Clasificación de activos de Información.	7-8		
	Políticas de Seguridad de la Información.	9-12		
	Encriptación de la información	13		
Integridad de datos	Cantidad de incidentes reportados por manipulación de datos.	14-18		

Nota: Elaboración propia

Tabla 2

Operacionalización de la variable Gestión de Riesgos de TI

DIMENSIONES	INDICADORES	ITEMS	ESCALA DE MEDICIÓN	NIVELES Y RANGOS
Proceso de gobernanza del riesgo	Grado de Planeamiento	1-2	1) Nunca 2) Casi nunca 3) Algunas veces 4) Casi siempre 5) Siempre	1) Malo 2) Regular 3) Bueno
	Efectividad en la definición de los riesgos de TI según las categorías de información.	3-6		
Cultura consciente sobre riesgos	Grado de concientización.	7-9		
	Efectividad del monitoreo de las actividades de gestión de riesgos de TI.	10-12		
Implantación eficaz de TI	Efectividad de la implantación de controles y seguimiento de las brechas de seguridad.	13-14		
	Efectividad en los niveles de riesgos inherentes de TI.	15-18		

Nota: Elaboración propia

2.5 Población y muestra

Población:

Según Sánchez y Reyes (2002, p.111) población, “comprende a todos los miembros de cualquier clase bien definida de personas, eventos u objetos”.
La población está conformada por 106 trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación.

Muestreo:

Según Hernandez (2010) en las muestras probabilísticas todos los elementos de la población tienen la misma posibilidad de ser escogidos y se obtienen definiendo las características de la población y el tamaño de la muestra, y por medio de una selección aleatoria o mecánica de las unidades de análisis.

Probabilística y aleatorio simple

N	Universo	106
P	Probabilidad de éxito	10%
q = (1-p)	Probabilidad de fracaso	90%
Z	Nivel de confianza	1.96
E	Error de estimación	0.05
n	Muestra	

Formula de muestreo con población finita

$$\frac{Z2 \times p \times q \times N}{(N-1) \times e2 + Z2 \times p \times q}$$

n = 83

Muestra:

Según Sánchez y Reyes (2002, p.111), denominamos muestra, al "grupo con el que se trabaja, la muestra debe ser representativa de la población".

De esta manera según los cálculos realizados la muestra está conformada por 83 trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación.

Para la presente investigación se contó con la colaboración de 83 usuarios de la Dirección de Gestión de Recursos Educativos del Minedu según el siguiente cuadro:

Tabla 3

Número de usuarios que fueron parte de la muestra de estudio, según las Oficinas a las que pertenecen.

Oficinas	Sexo Masculino	Sexo Femenino	Cantidad de Encuestados
Unidad de Administración	15	5	20
Unidad de Adquisición de Recursos Educativos	20	8	28
Unidad de Almacenamiento y Distribución	19	6	25
Unidad de Planeamiento Presupuesto y Monitoreo	7	3	10
Total			**83**

Nota: Elaboración propia

2.6 Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Técnicas de recolección: La técnica que se aplicará en la presente investigación será la Encuesta.
Instrumentos de recolección: El instrumento que se aplicará en la presente investigación será el Cuestionario con escala de tipo Likert modificado.

Variable 1: Seguridad de la Información

Se aplicó el cuestionario de Seguridad de Información, considerando su ficha técnica con las siguientes características:
Instrumento: Cuestionario de Seguridad de la Información
Autor y Año: Esteban Crespo Martínez (2017).
Adaptado y Año: Jorge Armando Calderón Sánchez (2018)
Escala de medición: Escala Likert (politómica)

Significación: El cuestionario de Seguridad de Información tiene 3 dimensiones que son los siguientes:

- Disponibilidad
- Confiabilidad
- Integridad de datos

Extensión: El cuestionario consta de 18 ítems.
Administración: Individual o colectiva
Ámbito de Aplicación: Trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación.
Duración: El tiempo de duración para desarrollar el cuestionario es de aproximadamente 20 minutos.
Puntuación: El cuestionario de Seguridad de la Información utiliza la escala de Likert:

1 = Nunca
2 = Casi nunca
3 = Algunas veces
4 = Casi siempre
5 = Siempre

Variable 2: Gestión de riesgos de TI

Se aplicó el cuestionario de Gestión de riesgos de TI, considerando su ficha técnica con las siguientes características:

Instrumento: Cuestionario de Gestión de riesgos de TI

Autor y Año: Esteban Crespo Martínez (2017).

Adaptado y Año: Jorge Armando Calderón Sánchez (2018)

Escala de medición: Escala Likert (politómica)

Significación: El cuestionario de la Gestión de riesgos de TI tiene 3 dimensiones que son los siguientes:

- Proceso de gobernanza del riesgo
- Cultura consciente sobre riesgos
- Implantación eficaz de TI

Extensión: El cuestionario consta de 18 ítems.

Administración: Individual o colectiva

Ámbito de Aplicación: Trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación.

Duración: El tiempo de duración para desarrollar el cuestionario es de aproximadamente 20 minutos.

Puntuación: El cuestionario de la Gestión de riesgos de TI utiliza la escala de Likert:

1 = Nunca
2 = Casi nunca
3 = Algunas veces
4 = Casi siempre
5 = Siempre

Validez

La validez de un instrumento según lo que afirma el autor Hernández, Fernández y Baptista (1998), consiste en determinar el grado real en que el instrumento mide las variables que son objeto de la investigación.

Tabla 4

Juicio de Expertos

	Aplicabilidad					
	Seguridad de la Información			Gestión de Riesgos		
Expertos	Pertinencia	Relevancia	Claridad	Pertinencia	Relevancia	Claridad
Dr. Luis Torres Cabanillas	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable
Dr. Edward José Flores Masías	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable
Mg. Orleans Moises Galvez Tapia	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable

En la Tabla 4, se presenta el resumen del juicio de expertos aplicado a la presente investigación en donde en su totalidad se expone que el instrumento es aplicable en pertinencia, relevancia y claridad a las variables seguridad de la información y gestión de riesgos.

2.7 Métodos de análisis de datos

Para el análisis de datos se utilizará el software de reporte de datos estadístico SPSS en su versión 22.0 y para la prueba de hipótesis se utilizará la prueba Coeficiente de Correlación de Spearman, por medio de la cual se realizará la contrastación de la hipótesis y determinar conclusiones.

2.8 Aspectos éticos

La presente investigación no está excluida del aspecto ético debido a ello, se realizó una estricta toma de datos a través de las encuestas a los trabajadores de la Dirección de Gestión de Recursos Educativos con la finalidad de contar con datos

reales y transparentes sin ningún tipo de manipulación.

III. Resultados

Tabla de Frecuencias

Tabla 5

Seguridad de la información V1

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Malo	3	3,6	3,6
	Regular	44	53,0	56,6
	Bueno	36	43,4	100,0
	Total	83	100,0	

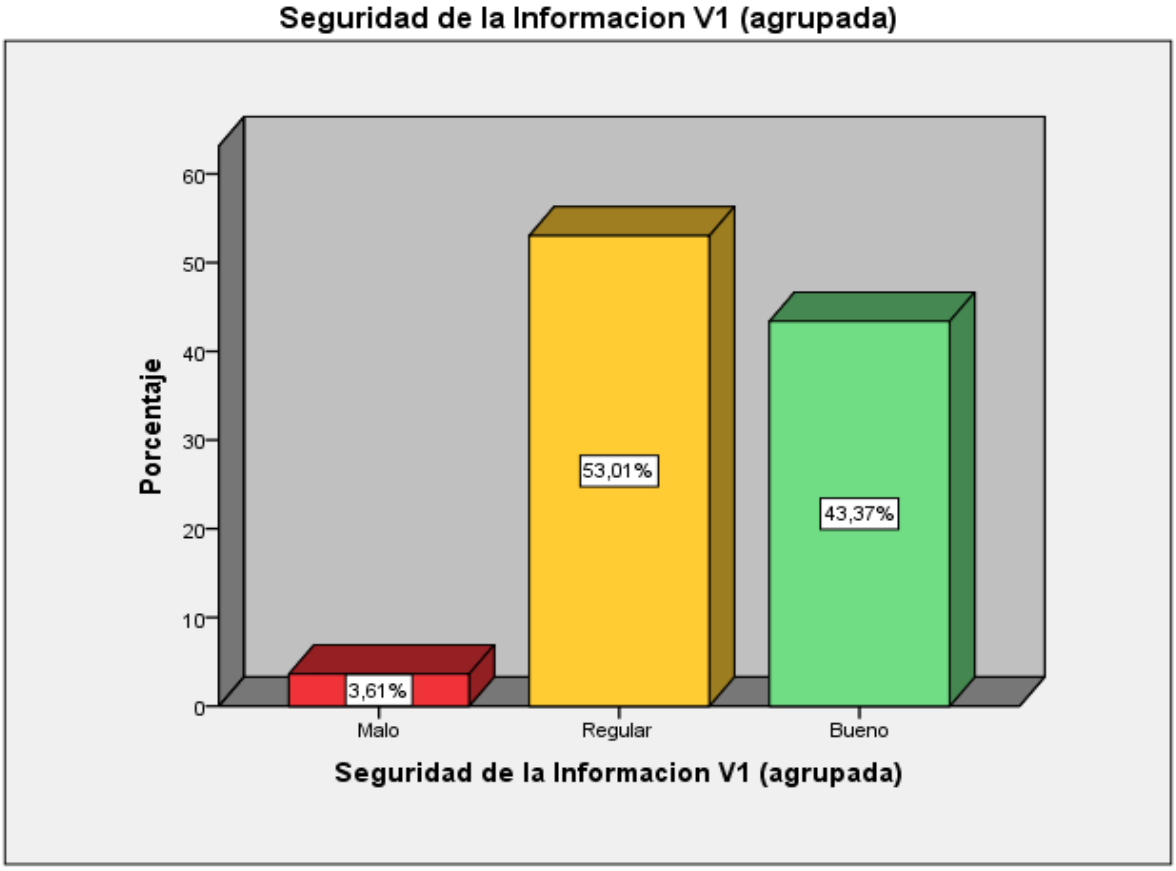


Figura 4. Seguridad de la Información V1 (agrupada)

Interpretación:

De acuerdo a la Tabla 5 y Figura 4, los resultados de los entrevistados consideran que el 53,01% es Bueno, el 43.37% es regular y el 3.61% es malo, respecto a la Seguridad de la Información de la DIGERE del Ministerio de Educación.

Tabla 6

Dimensión disponibilidad D1V1 (Agrupado)

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Malo	3	3,6	3,6
	Regular	44	53,0	56,6
	Bueno	36	43,4	100,0
	Total	83	100,0	

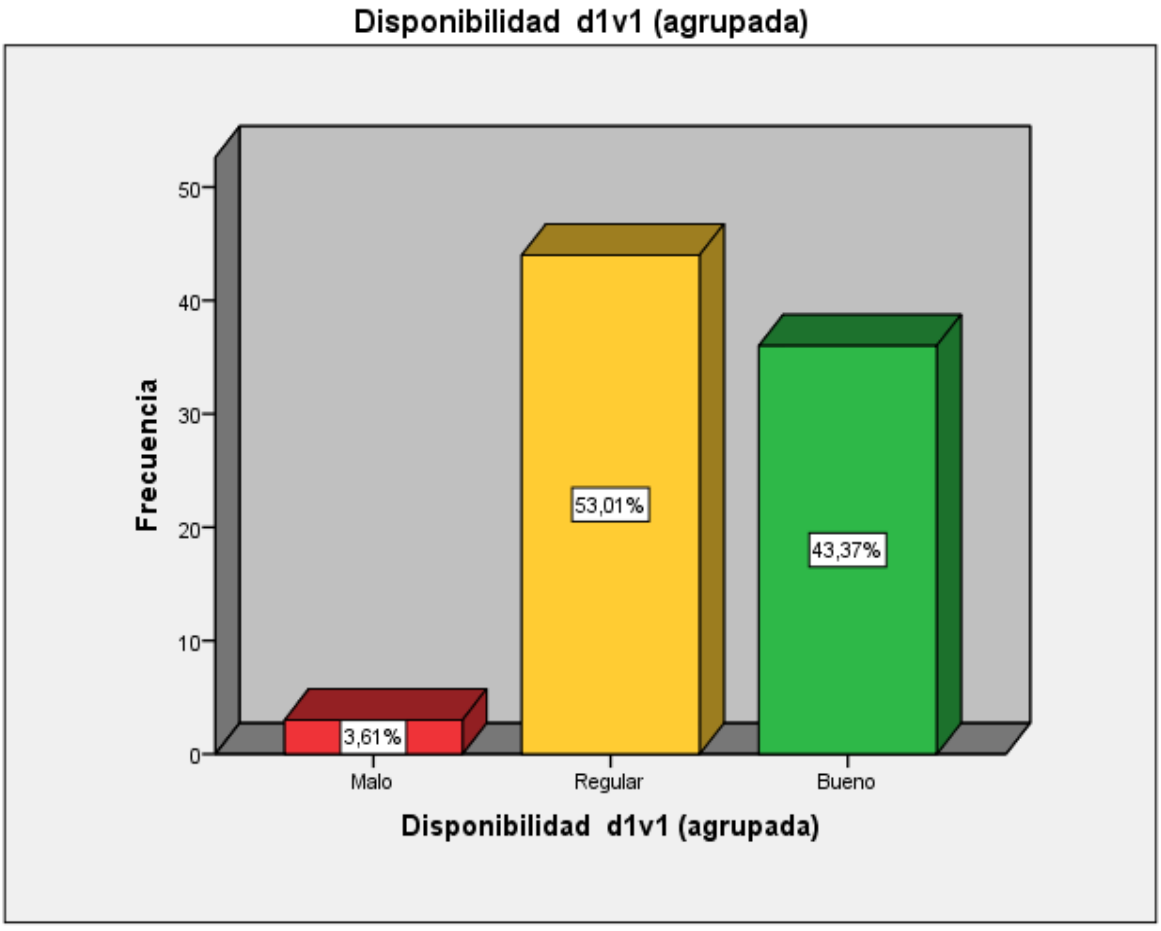


Figura 5. Dimensión disponibilidad D1V1 (agrupada)

Interpretación:

De acuerdo a la Tabla 6 y Figura 5, los resultados de los entrevistados consideran que el 53,01% es Bueno, el 43.37% es regular y el 3.61% es malo, respecto a la dimensión disponibilidad de la variable seguridad de la Información de la DIGERE

del Ministerio de Educación.

Tabla 7

Dimensión Confidencialidad D2V1 (Agrupado)

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Malo	3	3,6	3,6
	Regular	44	53,0	56,6
	Bueno	36	43,4	100,0
	Total	83	100,0	

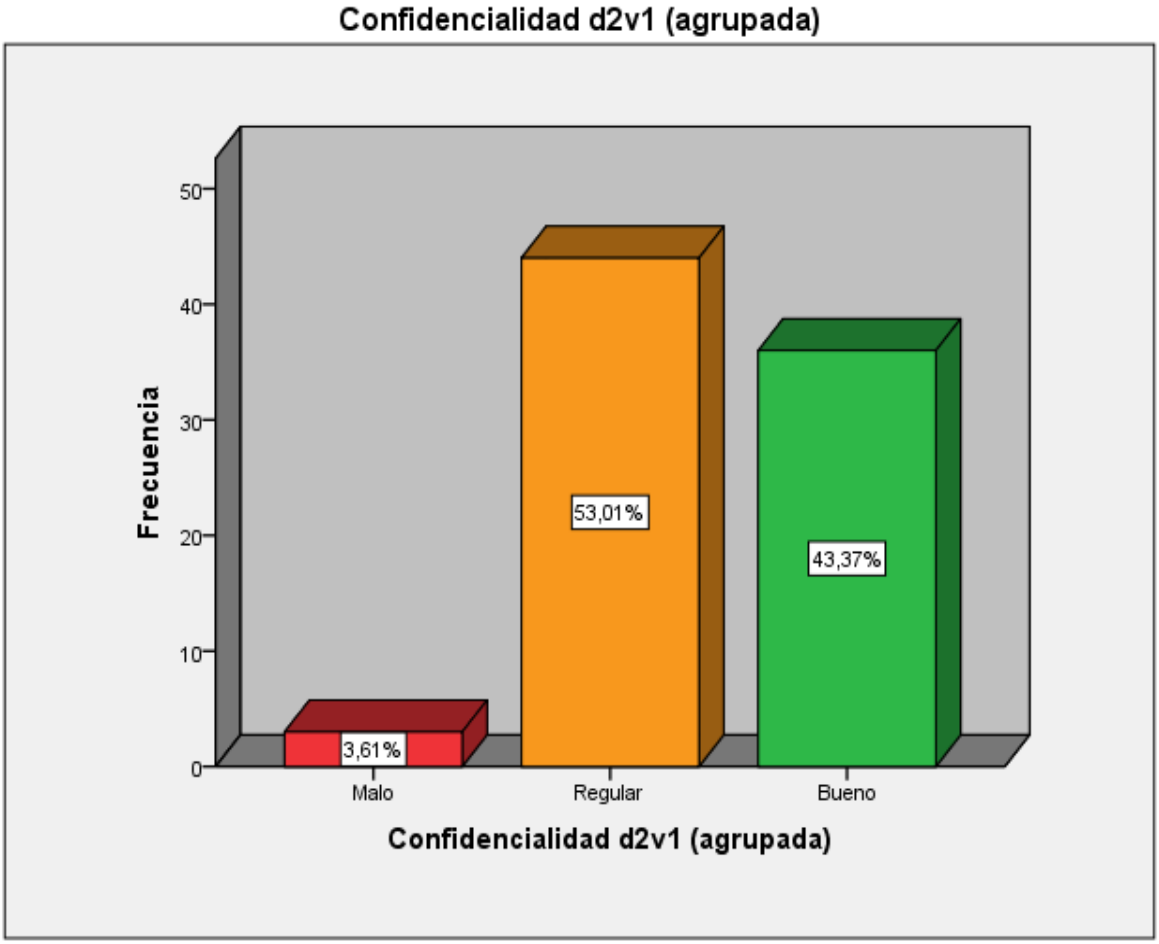


Figura 6. Dimensión confidencialidad D2V1 (agrupada)

Interpretación:

De acuerdo a la Tabla 7 y Figura 6, los resultados de los entrevistados consideran que el 53,01% es Bueno, el 43.37% es regular y el 3.61% es malo, respecto a la dimensión confidencialidad de la variable seguridad de la Información de la

DIGERE del Ministerio de Educación.

Tabla 8

Dimensión integridad de datos D3V1 (Agrupado)

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Malo	3	3,6	3,6
	Regular	44	53,0	56,6
	Bueno	36	43,4	100,0
	Total	83	100,0	

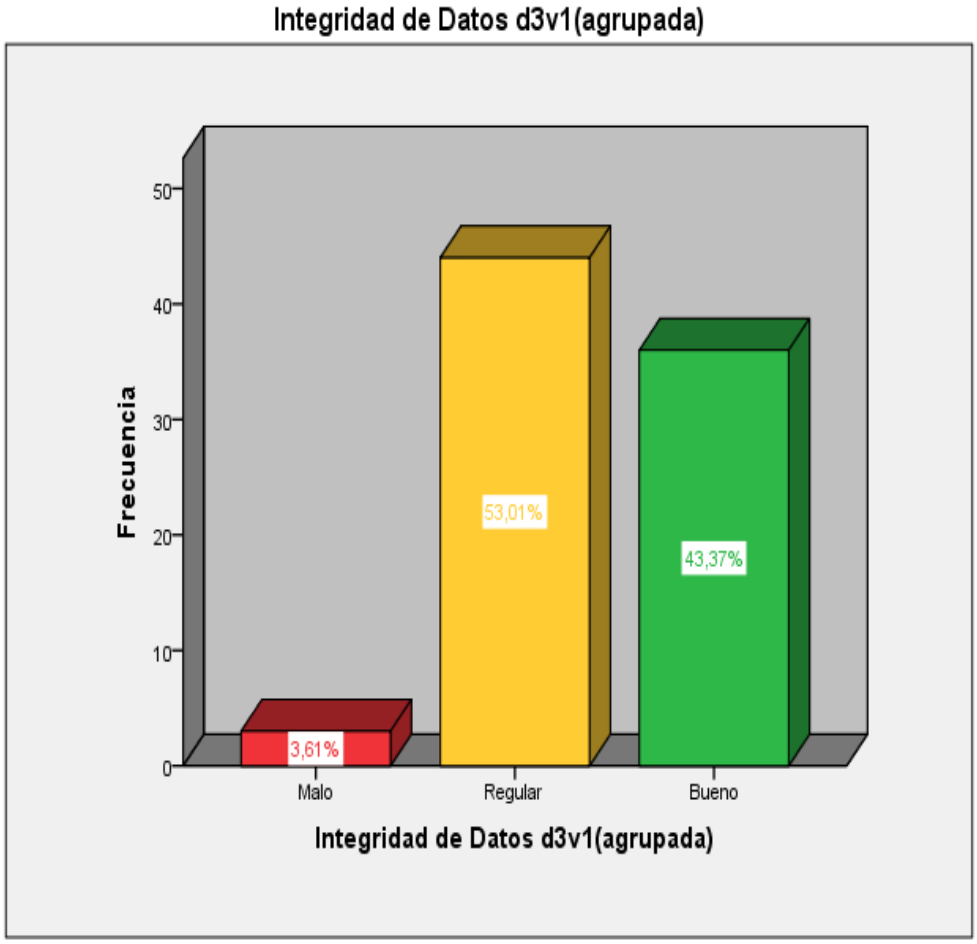


Figura 7. Dimensión integridad de datos D3V1 (agrupada)

Interpretación:

De acuerdo a la Tabla 8 y Figura 7, los resultados de los entrevistados consideran que el 53,01% es Bueno, el 43.37% es regular y el 3.61% es malo, respecto a la dimensión integridad de datos de la variable seguridad de la Información de la

DIGERE del Ministerio de Educación.

Tabla 9

Gestión de riesgos V2 (Agrupado)

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Malo	4	4,8	4,8
	Regular	42	50,6	55,4
	Bueno	37	44,6	100,0
	Total	83	100,0	

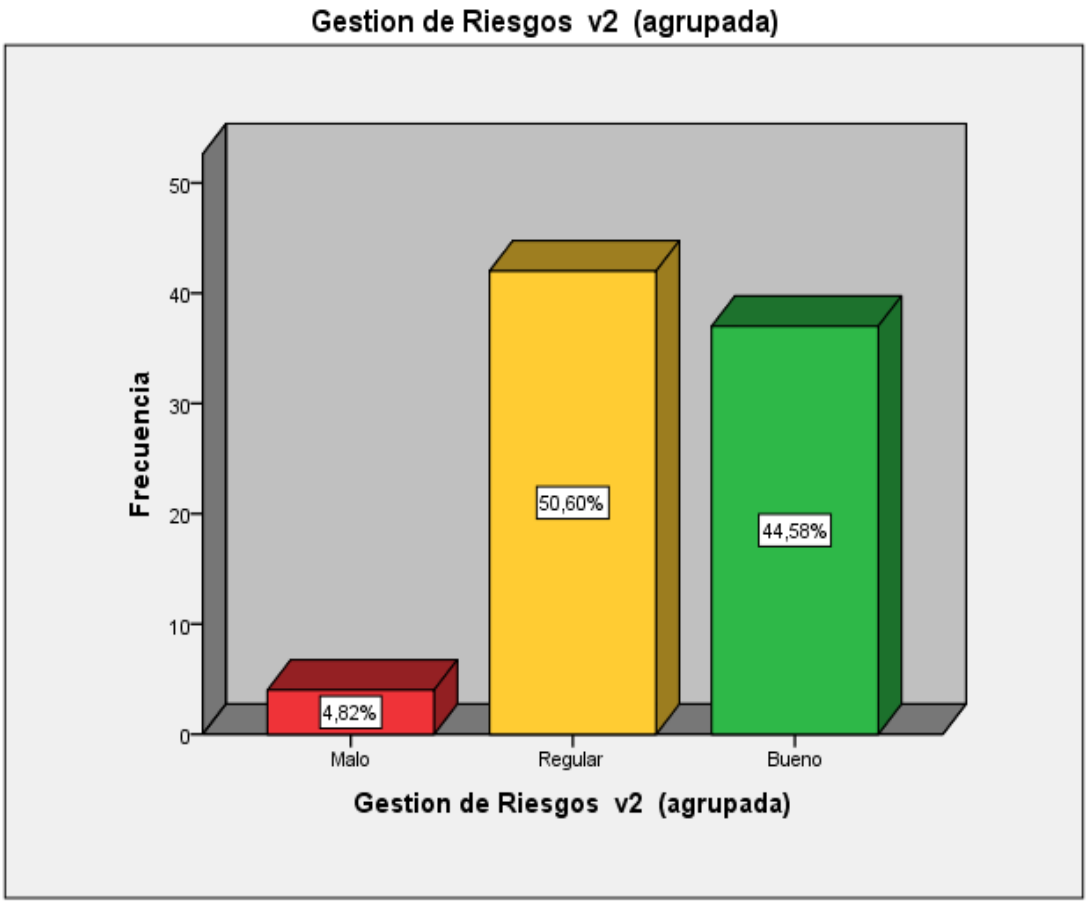


Figura 8. Gestión de riesgos V2 (agrupada)

Interpretación:

De acuerdo a la Tabla 9 y Figura 8, los resultados de los entrevistados consideran que el 50,60% es Bueno, el 44.58% es regular y el 4.62% es malo, respecto a la Seguridad de la Información de la DIGERE del Ministerio de Educación.

Tabla 10

*Tabla Cruzada Seguridad de la Información V1 (agrupada)*Gestión de Riesgos v2 (agrupada)*

			Gestión de Riesgos v2 (agrupada)			
			Malo	Regular	Bueno	Total
Seguridad de la Información V1 (agrupada)	Malo	Recuento	3	0	0	3
		% del total	3,6%	0,0%	0,0%	3,6%
	Regular	Recuento	1	40	3	44
		% del total	1,2%	48,2%	3,6%	53,0%
	Bueno	Recuento	0	2	34	36
		% del total	0,0%	2,4%	41,0%	43,4%
Total		Recuento	4	42	37	83
		% del total	4,8%	50,6%	44,6%	100,0%

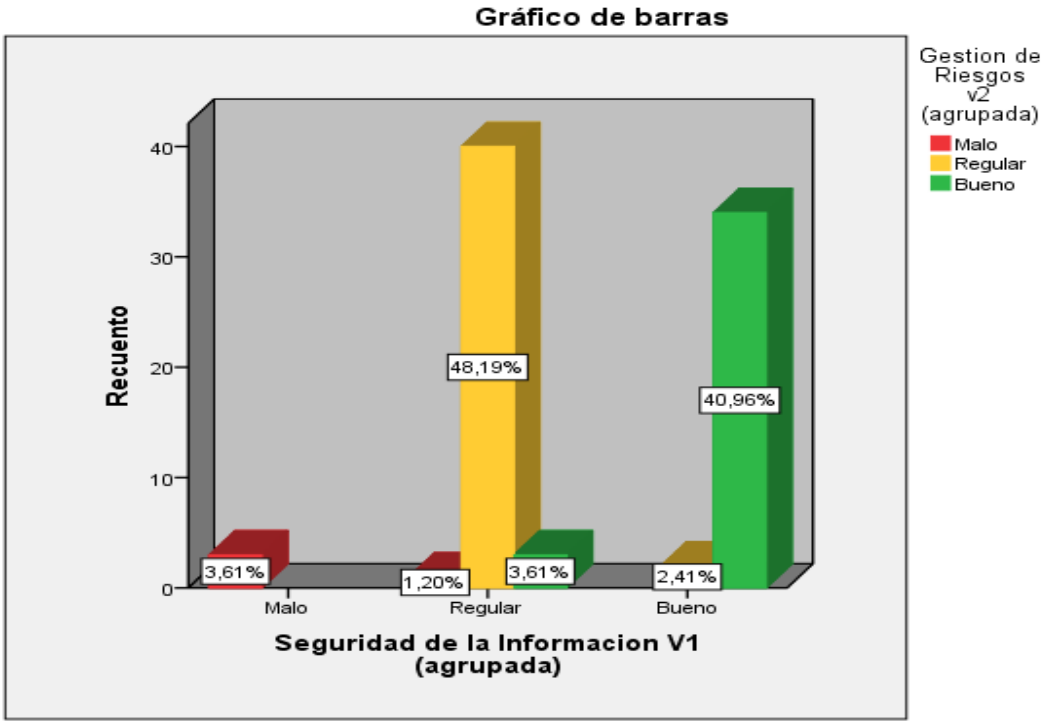


Figura 9. Seguridad de la información por gestión de riesgos

Interpretación:

De acuerdo a la tabla 10 y figura 9, muestran los resultados desde la percepción de los encuestados, que el 40.96% de la seguridad de la información y la gestión de

riesgos tienen un nivel bueno, el 48,19% de la seguridad de la información y la gestión de riesgos tiene un nivel regular, y solamente el 3.61% de la seguridad de la información y la gestión de riesgos tienen un nivel malo, respecto a los trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación.

Correlaciones no paramétricas - Hipótesis General

Ho= No Existe una relación directa entre la seguridad de la información no tiene relación significativa con la gestión de riesgos.

Ha= Existe una relación directa entre La seguridad de la información tiene relación significativa con la gestión de riesgos.

Regla Teórica para Toma de Decisiones

Se utilizó la Regla de Decisión, comparando el Valor p calculado por la data con el Valor p teórico de tabla = 0.05. Si el Valor p calculado ≥ 0.05, se Aceptará Ho. Pero, si el Valor p calculado < 0.05, se Aceptará Ha.

Prueba de estadística: Debido a que las variables tienen escala ordinal utilizamos el procedimiento estadístico Rho de Spearman de la estadística no paramétrica, para determinar el grado de relación que tiene ambas variables.

Tabla 11

Correlación de la seguridad de información y la gestión de riesgos

			Seguridad de la Información V1 (agrupada)	Gestión de Riesgos v2 (agrupada)
Rho de Spearman	Seguridad de la Información V1 (agrupada)	Coeficiente de correlación	1,000	,886**
		Sig. (bilateral)	.	,000
		N	83	83
	Gestión de Riesgos v2 (agrupada)	Coeficiente de correlación	,886**	1,000
		Sig. (bilateral)	,000	.
		N	83	83

En la tabla 11 se observa .que la correlación es significativa en el nivel 0,01 (2 colas).

Según la Tabla 11, dado que en la prueba el valor p=0,000 es menor que el nivel de confianza p=0,01, es decir, que existe una relación altamente significativa entre seguridad de la información y la gestión de riesgos, siendo esta relación alta, entre las variables, con un Rho de Spearman de (0.886), se concluye que existe una relación directa entre la seguridad de la información y la gestión de riesgos de los trabajadores de la DIGERE del Minedu.

Prueba de hipótesis especifica 1 de la investigación

Ho= No existe una relación directa entre la dimensión disponibilidad de la variable seguridad de la información y la gestión de riesgos.

Ha= Existe una relación significativa y positiva entre la dimensión disponibilidad de la variable seguridad de la información y la gestión de riesgos.

Regla Teórica para Toma de Decisiones

Se utilizó la Regla de Decisión, comparando el Valor p calculado por la data con el Valor p teórico de tabla = 0.05. Si el Valor p calculado ≥ 0.05, se Aceptará Ho. Pero, si el Valor p calculado < 0.05, se Aceptará Ha.

Prueba de estadística: Debido a que las variables tienen escala ordinal utilizamos el procedimiento estadístico Rho de Spearman de la estadística no paramétrica, para determinar el grado de relación que tiene ambas variables.

Tabla 12

Correlación de la dimensión disponibilidad de la variable seguridad de la información y la gestión de riesgos

			Disponibilidad d1v1 (agrupada)	Gestión de Riesgos v2 (agrupada)
Rho de Spearman	Disponibilidad d1v1 (agrupada)	Coeficiente de correlación	1,000	,886**
		Sig. (bilateral)	.	,000
		N	83	83
	Gestion de Riesgos v2 (agrupada)	Coeficiente de correlación	,886**	1,000
		Sig. (bilateral)	,000	.
		N	83	83

En la tabla 12 se observa que la correlación es significativa en el nivel 0,01 (2 colas).

Según la Tabla 12, dado que en la prueba el valor p=0,000 es menor que el nivel de confianza p=0,01, es decir, que existe una relación altamente significativa entre seguridad de la información y la gestión de riesgos, siendo esta relación alta, entre las variables, con un Rho de Spearman de (0.886), se concluye que existe una relación directa entre la seguridad de la información y la gestión de riesgos de los trabajadores de la DIGERE del Minedu.

Prueba de hipótesis especifica 2 de la investigación

Ho= No existe una relación directa entre la dimensión confidencialidad de la variable seguridad de la información y la gestión de riesgos.

Ha= Existe una relación directa entre la dimensión confidencialidad de la variable seguridad de la información y la gestión de riesgos.

Regla Teórica para Toma de Decisiones

Se utilizó la Regla de Decisión, comparando el Valor p calculado por la data con el Valor p teórico de tabla = 0.05. Si el Valor p calculado ≥ 0.05, se Aceptará Ho. Pero, si el Valor p calculado < 0.05, se Aceptará Ha.

Tabla 13

Correlación de la dimensión confidencialidad de la variable seguridad de la información y la gestión de riesgos

			Confidencialidad d2v1 (agrupada)	Gestión de Riesgos v2 (agrupada)
Rho de Spearman	Confidencialidad d2v1 (agrupada)	Coeficiente de correlación	1,000	,886**
		Sig. (bilateral)	.	,000
		N	83	83
	Gestion de Riesgos v2 (agrupada)	Coeficiente de correlación	,886**	1,000
		Sig. (bilateral)	,000	.
		N	83	83

En la tabla 13 se observa que la correlación es significativa en el nivel 0,01 (2 colas).

Según la Tabla 13, dado que en la prueba el valor p=0,000 es menor que el nivel de confianza p=0,01, es decir, que existe una relación altamente significativa entre seguridad de la información y la gestión de riesgos, siendo esta relación alta, entre las variables, con un Rho de Spearman de (0.886), se concluye que existe una relación directa entre la dimensión confidencialidad de la variable seguridad de la información y la gestión de riesgos de los trabajadores de la DIGERE del Minedu.

Prueba de hipótesis especifica 3 de la investigación

Ho= No existe una relación directa entre la dimensión integridad de datos de la variable seguridad de la información y la gestión de riesgos.

Ha= Existe una relación directa entre la dimensión integridad de datos de la variable seguridad de la información y la gestión de riesgos.

Regla Teórica para Toma de Decisiones

Se utilizó la Regla de Decisión, comparando el Valor p calculado por la data con el Valor p teórico de tabla = 0.05. Si el Valor p calculado ≥ 0.05, se Aceptará Ho. Pero, si el Valor p calculado < 0.05, se Aceptará Ha.

Tabla 14

Correlación de la dimensión integridad de datos de la variable seguridad de la información y la gestión de riesgos

			Integridad de Datos d3v1(agrupada)	Gestión de Riesgos v2 (agrupada)
Rho de Spearman	Integridad de Datos d3v1(agrupada)	Coeficiente de correlación	1,000	,886**
		Sig. (bilateral)	.	,000
		N	83	83
	Gestion de Riesgos v2 (agrupada)	Coeficiente de correlación	,886**	1,000
		Sig. (bilateral)	,000	.
		N	83	83

En la tabla 14 se observa que la correlación es significativa en el nivel 0,01 (2 colas).

Según la Tabla 14, dado que en la prueba el valor p=0,000 es menor que el nivel de confianza p=0,01, es decir, que existe una relación altamente significativa entre seguridad de la información y la gestión de riesgos, siendo esta relación alta, entre las variables, con un Rho de Spearman de (0.886), se concluye que existe una relación directa entre la dimensión integridad de datos de la variable seguridad de la información y la gestión de riesgos de los trabajadores de la DIGERE del MINEDU.

IV. Discusión

En el presente etapa y después de obtener los resultados, se compararan con los antecedentes de la presente investigación, los cuales confirmaran las hipótesis planteadas, pudiendo determinar que la hipótesis general, cuyo planteamiento ha sido de que “Existe relación entre la seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018”, las pruebas estadísticas utilizadas nos indican que la correlación no paramétrica de Spearman de 0,886**, representando ésta una alta asociación de las variables y siendo positivo con un valor $p = 0.000$ ($p < 0.01$).

Así mismo, las dimensiones descritas en el presente trabajo de investigación, toman una alta relación con las variables de estudio, esto confirma que si se capacita al personal de la Dirección de Gestión de Recursos Educativos acerca de temas vinculados a la seguridad de la información y gestión de riesgos, este podrá tomar decisiones adecuadas a fin de salvaguardar los activos importantes para la entidad. Al respecto para Seclén (2016) para salvaguardar los activos es importante cubrir la necesidad de establecer la creación de un Departamento de Gobierno de Seguridad de la Información del más alto nivel compuesto por un grupo de especialistas en seguridad de la información que opere como un solo grupo de trabajo nacional el cual tenga como principal función un monitoreo permanente de avance y ejecución del avance de la implementación del SGSI en todas las entidades públicas peruanas, lo que podría darse a través de la potenciación funcional y técnica de la Secretaria de Gobierno Digital del Perú..

En la misma línea Otoya (2018), concluyó que los profesionales alegan estar preocupados por la seguridad y en transmitir a los clientes la sensación de seguridad pero admiten no conocer en profundidad los procesos que la aumentan tangiblemente y no poder ponerlas en práctica a sus proyectos en TI; concordante con todo ello la Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico e Informático (ONGEI) hoy conocida como Secretaria de Gobierno digital, dispone de uso obligatorio de la Norma Técnica Peruana: “NTP – ISO 17999:2014 EDI para la Gestión de la Seguridad de la Información, dicha norma se basa en el estándar internacional ISO 17799 que es una compilación de recomendaciones para las prácticas exitosas de seguridad

que toda organización puede aplicar independientemente de su tamaño o sector. Tal como se precisó, existe una relación directa entre la seguridad de la información y la gestión de riesgos, ya que si la seguridad de la información mejora la gestión de riesgos también lo hará, por ello para Arévalo (2017) no solo basta con implementar capacitaciones constantes, sino que precisa que es vital establecer políticas de seguridad, las cuales deberán ser aplicadas bajo responsabilidad por todo el personal de la empresa. Para Tarrillo (2015) como primer paso es de vital importancia que se implemente la metodología MAGERIT como punto base para determinar que activos son los preponderantes para la entidad ya que con ello el personal de la entidad podrá identificar los posibles riesgos que atenten en contra de los intereses de la entidad.

El presente trabajo de investigación coincide con lo mencionado por Guevara (2013) es fundamental el apoyo tanto humano como financiero de la Alta Dirección y el compromiso del personal de la entidad para poder aplicar la seguridad de la información y la gestión de riesgos en la entidad donde se apliquen los conceptos antes estudiados.

V. Conclusiones

Primera

Existe una relación directa entre la seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del MINEDU, ya que se obtuvo un valor de significancia igual a 0 con un Rho de Spearman de (0.886**).
Al ser el valor de sigma bilateral menor al 0,05 o 5,00% se manifiesta que se ha probado la hipótesis de estudio del investigador que para este caso seria “Existe una relación directa entre la seguridad de la información y la gestión de riesgos.

Segunda

Se puede concluir para la Hipótesis Especifica 1 que para la correlación se uso Rho de Spearman, para este caso se presenta que el coeficiente de correlación es de 0,866** y un valor de sigma bilateral o p-valor de 0,000. Al ser el valor de sigma bilateral menor al 0,05 o 5,00% se manifiesta que se ha probado la hipótesis de estudio del investigador que para este caso seria “Existe una relación directa entre la dimensión disponibilidad de la seguridad de la información y la gestión de riesgos”. Es importante precisar que los valores obtenidos por el SPSS han sido considerando el nivel de 0,01 o 1,00% bilateral o a dos colas, lo que indica que para cada cola el error es de 0,005 y hay un nivel de aceptación de 99,0%.

Tercera

Se puede concluir para la Hipótesis Especifica 2 que para la correlación se uso Rho de Spearman, para este caso se presenta que el coeficiente de correlación es de 0,866** y un valor de sigma bilateral o p-valor de 0,000. Al ser el valor de sigma bilateral menor al 0,05 o 5,00% se manifiesta que se ha probado la hipótesis de estudio del investigador que para este caso seria “Existe una relación directa entre la dimensión confidencialidad de la seguridad de la información y la gestión de riesgos”. Es importante precisar que los valores obtenidos por el SPSS han sido considerando el nivel de 0,01 o 1,00% bilateral o a dos colas, lo que indica que para cada cola el error es de 0,005 y hay un nivel de aceptación de 99,0%.

Cuarta

Se puede concluir para la Hipótesis Especifica 2 que para la correlación se uso Rho de Spearman, para este caso se presenta que el coeficiente de correlación es de 0,866** y un valor de sigma bilateral o p-valor de 0,000. Al ser el valor de sigma bilateral menor al 0,05 o 5,00% se manifiesta que se ha probado la hipótesis de estudio del investigador que para este caso seria “Existe una relación directa entre la dimensión integridad de datos de la seguridad de la información y la gestión de riesgos”. Es importante precisar que los valores obtenidos por el SPSS han sido considerando el nivel de 0,01 o 1,00% bilateral o a dos colas, lo que indica que para cada cola el error es de 0,005 y hay un nivel de aceptación de 99,0%.

Quinta

Existe una relación directa entre la seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del MINEDU, ya que según lo observado en los resultados de la Tabla 12; las variables seguridad de la información y gestión de riesgos fueron cruzadas obteniendo un 40.96% de nivel bueno, así mismo se cuenta con un valor de significancia 0 el cual corrobora la dependencia de ambas variables.

V. Recomendaciones

Primera

La seguridad de la información tiene una relación directa con la gestión de riesgos, (en las instituciones pública como la nuestra entiéndase logro de objetivos) motivo por el cual la DIGERE a través del área de Tecnologías de la información debe reforzar la importancia de lograr los objetivos estratégicos correspondientes a la seguridad de la información por ende se debe realizar constantes coordinaciones con el Ministerio de Educación con la finalidad de que se brinde el Presupuesto necesario para la adquisición de equipamiento tecnológico e informático; los cuales servirán para reforzar y actualizar las medidas de seguridad impartidas de acuerdo a la política de seguridad de la información con la que se cuente.

Segunda

La disponibilidad tiene relación directa con la gestión de riesgos, motivo por el cual la Dirección de Gestión de Recursos Educativos del MINEDU, a través del área de Tecnologías de la Información deberá tener planificado medidas de contingencia ante posibles riesgos que afecten la continuidad de los servicios que tengan involucrado la información que maneje la entidad.

Tercera

La confidencialidad tiene relación directa con la gestión de riesgos, por ende la Dirección de Gestión de Recursos Educativos del MINEDU a través de las áreas de Tecnologías de la Información y Recursos Humanos debe establecer constantes capacitaciones a los trabajadores donde se debe sensibilizar a los trabajadores de la DIGERE sobre la información confidencial que maneja la entidad y cuáles son las medidas de asegurar la no filtración de la misma.

Cuarta

La integridad de datos tiene relación directa con la gestión de riesgos, de esta manera el área de tecnologías de la información debe implementar políticas de acceso a la información, así mismo deberá solicitar la adquisición o de ser el caso de la renovación de las licencias del software de análisis de vulnerabilidades de los sistemas para prevenir cualquier ataque que perjudique la continuidad de los procesos que se ejecuten en la entidad.

Quinta

Luego de establecer que existe una relación entre las variables de estudio, es recomendable continuar con la implementación de un sistema de gestión de seguridad de la información, ya que se cuenta con la base de conocimiento de los activos de información que son sensibles y los riesgos a los que están expuestas, por ende se debe conformar un comité de seguridad en donde se establezcan los roles y pasos a seguir para la implementación del sistema recomendado.

VI. Referencias

Arevalo F. (2017). Elaboración y plan de implementación de política de seguridad de la información aplicada a una empresa nacional de alimentos. (Tesis de Maestría).Universidad de Cuenca Ecuador. Recuperado de: file:///C:/Users/jorge/Downloads/Trabajo%20de%20titulaci%C3%B3n%20(2).pdf

Alba. J. (2011). Planeación de la seguridad de la información corporativa sensible contra amenazas internas (Tesis de Maestría). Instituto Politécnico Nacional. México. Recuperada de: http://www.repositoriodigital.ipn.mx/bitstream/123456789/12642/1/Trabajo%20de%20Investigaci%C3%B3n%20-%20Jorge%20Alba%20Cruz.pdf

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

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

Banda H. (2014).Elaboración de un sistema de gestión de la seguridad de la información (SGSI) para la empresa radical CIA LTDA en la ciudad de quito para el año 2014. (Tesis de Maestría).Universidad de las Américas Ecuador. Recuperado de: file:///C:/Users/jorge/Downloads/UDLA-EC-TMGSTI-2014-28(S)%20(2).pdf

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

Galicia. L. (2016). *Propuesta de modelo de gestión para la prevención del riesgo operacional en el sector financiero caso: grupo financiero X. S.A. de C.V*. (Tesis de Maestría). Instituto Politécnico Nacional. México. Recuperada de: http://tesis.ipn.mx/bitstream/handle/123456789/18694/1.%20Liliana%20Gali cia%20Palacios.pdf?sequence=1

Guevra T (2013). Modelo de gestión de seguridad de la información para la corporación financiera nacional basado en gestión de riesgos.(Tesis de Maestría). Escuela Politecnica Nacional. Ecuador. Recuperado de: http://bibdigital.epn.edu.ec/bitstream/15000/8052/4/CD-5084.pdf

Guzmán. G. (2015). *Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica ortega*. (Tesis para Maestría). Universidad Nacional del Centro del Perú. Recuperada de: http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/1478/Tes Goyo%20Francisco%20Guzman%20Pacheco.pdf?sequence is- =1&isAllowed=

Maggiore M. (2014). Modelo de evaluación de madurez para la gestión de seguridad de la información integrada en los procesos de negocio.(Tesis de Maestría).Universidad de Buenos Aires. Argentina. Recuperado de:

http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0550_MaggioreML.pdf

Llontop G. (2018). Gestión de riesgos de Tecnologías de Información de las Empresas de Nephila Networks. Universidad Cesar Vallejo Lima Perú. Recuperado de: file:///C:/Users/jorge/Downloads/Llotop_DGC%20(4).pdf

Magerit (2012). Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro I Método - versión 3.0. Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Mercado J. (2016). Modelo de gestión de seguridad de la información para el E-Gobierno. Universidad Nacional Mayor de San Marcos Perú. Recuperado de: http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/6414/Mercado_rj.pdf?sequence=1&isAllowed=y

Muñoz J. (2016) Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (dtic) de la Universidad de Cuenca. (Tesis de Maestría). Recuperado de:http://dspace.ucuenca.edu.ec/bitstream/123456789/25646/1/Tesis.pdf

Otoya M. (2018). Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Universidad Cesar Vallejo. Lima Perú. Recuperado de: file:///C:/Users/jorge/Downloads/Otoya_VM.pdf

Tarrillo E. (2016). Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015. Universidad Cesar Vallejo Tarapoto Perú. Recuperado de:

http://repositorio.ucv.edu.pe/bitstream/handle/UCV/1286/tarrillo_se.pdf?sequence=1&isAllowed=y

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

Soriano M. (2014) Seguridad en redes y seguridad de la información 23-58 Recuperado de: http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

VII. ANEXOS

Anexo 01
ARTÍCULO CIENTÍFICO

1. TÍTULO

Seguridad de la información y la gestión de riesgos de la DIGERE del Ministerio de Educación, 2018.

2. AUTOR (A, ES, AS)

Jorge Armando Calderón Sánchez

Correo electrónico: Jcalderons2000@gmail.com

Analista en sistemas de información de la DIGERE.

3. RESUMEN

El objetivo de la investigación estuvo dirigido a reconocer la relación de la seguridad de la información y la gestión de riesgos en la Dirección de Gestión de Recursos Educativos del ministerio de educación, 2018. La investigación fue de tipo de estudio básico, con un diseño no experimental, correlacional y transversal, la población elegida fue de 106 trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, los cuales fueron seleccionados de una manera probabilística y aleatoria simple, muestreo de tipo probabilístico y aleatorio simple; mientras el método de investigación hipotético-deductivo de enfoque cuantitativo; y en el tratamiento de los datos se realizó a través del SPSS; se empleó la prueba no paramétrica de alcance correlacional Rho de Spearman.

Con la presente investigación se espera encontrar la relación entre las dos variables de estudio, y de esta forma los resultados sean tomados en cuenta por la entidad donde se realizó el estudio; para que se establezca una correcta toma de decisiones en temas de seguridad de la información y la correcta gestión de los riesgos y amenazas que puedan producirse en el tratamiento de los activos importantes para la entidad. Así mismo será de utilidad para medir el grado de aprendizaje y conocimiento con el que cuentan los trabajadores de la DIGERE, en temas de seguridad y gestión de riesgos.

4. PALABRAS CLAVE

seguridad de la información, gestión de riesgos

5. ABSTRACT

Below is a summary of the research "Information security and risk management in the workers of the DIGERE of the Ministry of Education, 2018"

The objective of the research was aimed at recognizing the relationship of information security and risk management in the General Directorate of Educational Resources of the Ministry of Education,

2018. The research was of a basic study type, with a non-experimental design , correlational and cross-sectional, the chosen population was 106 workers of the General Directorate of Educational Resources of the Ministry of Education, which were selected in a simple random and probabilistic manner, simple probabilistic and random sampling; while the hypothetico-deductive research method of quantitative approach; and in the treatment of the data was done through the SPSS; the nonparametric test of Spearman's Rho correlation scope was used.

With the present investigation it is expected to find the relationship between the two study variables, and in this way the results are taken into account by the entity where the study was conducted; so that a correct decision-making is established in matters of information security and the correct management of risks and threats that may occur in the treatment of important assets for the entity. Likewise, it will be useful to measure the degree of learning and knowledge that DIGERE workers have, in matters of security and risk management.

6. KEYWORDS

information security, risk management

7. INTRODUCCIÓN

Internacionalmente, se está tomando a la seguridad de la información con el apelativo de Cyberseguridad según lo estipulado por Giant (2016) esto con relación a los ataques masivos que se pueden producir a través de la redes sociales, del mismo modo en Sudamérica específicamente en Colombia, existe una cantidad elevada de empresas que le brindan poco interés a la gestión de riesgos en el desarrollo de sus procesos, Venegas y Pardo (2014) detallan que a los inicios del nuevo milenio, las empresas cuyo core de trabajo es el desarrollo de software en sus proyectos no realizan la gestión del riesgo, solo se enfocaban en lograr la respuesta ante un problema inmediato sin prevenir posibles riesgos vinculados a los incidentes reportados. Para Burgos Salazar en la actualidad son múltiples los riesgos asociados a que los equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad. Las amenazas en las TIC son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Preocupante es para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

En el Perú según Simich (2016), existe una enorme brecha en el tema de seguridad de la Información debido a una falta de cultura de seguridad de las empresas vinculado a un tema de desconocimiento por parte de los directivos y/o Direcciones encargadas de las entidades, los cuales no toman la importancia debida en los grandes riesgos existentes de ataques que se

pueden producir en sus organizaciones.

La Dirección de Gestión de Recursos Educativos del Ministerio de Educación del Perú fue creada bajo Resolución Ministerial 491-2013 y la cual será sujeta al presente estudio cuenta con una población de 106 usuarios. La labor de esta entidad es dotar de recursos tecnológicos y material educativo a todos los colegios del Perú, con la finalidad que los niños puedan aprovecharlos y de esta manera contribuir con el desarrollo en materia educativa. De esta manera los trabajadores de la DIGERE realizan intercambio de información para ejecutar las labores del día a día y para ello utilizan herramientas informáticas las cuales son susceptibles a posibles ataques informáticos o de ingeniería social con el objetivo de realizar el robo de información. Esta entidad a través de la gestión de la oficina de Tecnologías de la Información viene realizando políticas de seguridad en las etapas de confidencialidad, disponibilidad e integridad basada en norma ISO 27001:2013 con la finalidad de minimizar los riesgos vinculados a los activos de información que maneja, así mismo ha desarrollo programas de capacitación acerca de los activos de información que son primordiales para la entidad con la finalidad de sensibilizar a los trabajadores en el correcto resguardo de los mismos, si bien es el inicio de una etapa de capacitación lo que se tiene proyectado es realizar la implementación de un sistema gestión de la seguridad de la Información el cual establezca las medidas adecuadas y las alertas correspondientes sobre el resguardo de los activos importantes para la entidad, esto con la finalidad de gestionar los riesgos, minimizando las amenazas y riesgos que puedan generarse durante el desarrollo de las actividades de los colaboradores de la entidad.

En la actualidad las entidades públicas vienen tomando conciencia de la importancia de la seguridad de la información y de la gestión de riesgos, por ende se encuentran estableciendo las primeras medidas para proteger la información que se maneja sea física o digital, esto como primer paso para una futura implementación de un sistema de gestión integral de seguridad que permita no solo identificar las vulnerabilidades; sino brindar una solución inmediata a los incidentes que se reporten. Así mismo es fundamental realizar la gestión de riesgos de TI, ya que ella permitirá a las entidades contar con la información adecuada para identificar los activos de información que son relevantes y de suma importancia para minimizar los riesgos a los que se encuentre expuestos la entidad en temas de seguridad.

8. METODOLOGÍA

El estudio aplicó el método hipotético - deductivo, porque a través de los conocimientos de las variables Seguridad de la Información y gestión de riesgos de TI se buscó el conocimiento de su

relación, asimismo esto se complementó con el aporte de la estadística a través de los resultados consignados en los cuestionarios. De esta manera el estudio se desarrolló bajo un enfoque cuantitativo pues se realizó con el fin de validar la relación que existen entre las variables (investigación correlacional) bajo un tipo de investigación básica.

Población:

Según Sánchez y Reyes (2002, p.111) población, "comprende a todos los miembros de cualquier clase bien definida de personas, eventos u objetos".

La población está conformada por 106 trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación.

Muestreo:

Según Hernandez (2010) en las muestras probabilísticas todos los elementos de la población tienen la misma posibilidad de ser escogidos y se obtienen definiendo las características de la población y el tamaño de la muestra, y por medio de una selección aleatoria o mecánica de las unidades de análisis.

Probabilística y aleatorio simple

N	Universo	106
P	Probabilidad de éxito	10%
q = (1-p)	Probabilidad de fracaso	90%
Z	Nivel de confianza	1.96
E	Error de estimación	0.05
N	Muestra	

Formula de muestreo con población finita

$$\frac{Z2 \times p \times q \times N}{(N-1) \times e2 + Z2 \times p \times q}$$

n = 83

Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Técnicas de recolección: La técnica que se aplicará en la presente investigación será la Encuesta.

Instrumentos de recolección: El instrumento que se aplicará en la presente investigación será el Cuestionario con escala de tipo Likert modificado.

Variable 1: Seguridad de la Información

Se aplicó el cuestionario de Seguridad de Información, considerando su ficha técnica con las siguientes características:

Instrumento: Cuestionario de Seguridad de la Información

Autor y Año: Esteban Crespo Martínez (2017).

Adaptado y Año: Jorge Armando Calderón Sánchez (2018)

Escala de medición: Escala Likert (politómica)

Significación: El cuestionario de Seguridad de Información tiene 3 dimensiones que son los siguientes:

- Disponibilidad
- Confiabilidad
- Integridad de datos

Extensión: El cuestionario consta de 18 ítems.

Administración: Individual o colectiva

Ámbito de Aplicación: Trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación.

Duración: El tiempo de duración para desarrollar el cuestionario es de aproximadamente 20 minutos.

Puntuación: El cuestionario de Seguridad de la Información utiliza la escala de Likert:

1 = Nunca
2 = Casi nunca
3 = Algunas veces
4 = Casi siempre
5 = Siempre

Variable 2: Gestión de riesgos de TI

Se aplicó el cuestionario de Gestión de riesgos de TI, considerando su ficha técnica con las siguientes características:

Instrumento: Cuestionario de Gestión de riesgos de TI

Autor y Año: Esteban Crespo Martínez (2017).

Adaptado y Año: Jorge Armando Calderón Sánchez (2018)

Escala de medición: Escala Likert (politómica)

Significación: El cuestionario de la Gestión de riesgos de TI tiene 3 dimensiones que son los siguientes:

- Proceso de gobernanza del riesgo
- Cultura consciente sobre riesgos
- Implantación eficaz de TI

Extensión: El cuestionario consta de 18 ítems.

Administración: Individual o colectiva

Ámbito de Aplicación: Trabajadores de la Dirección de Gestión de Recursos

Educativos del Ministerio de Educación.

Duración: El tiempo de duración para desarrollar el cuestionario es de aproximadamente 20 minutos.

Puntuación: El cuestionario de la Gestión de riesgos de TI utiliza la escala de Likert:

1 = Nunca

2 = Casi nunca

3 = Algunas veces

4 = Casi siempre

6 = Siempre

Validez

La validez de un instrumento según lo que afirma el autor Hernández, Fernández y Baptista (1998), consiste en determinar el grado real en que el instrumento mide las variables que son objeto de la investigación el cual fue realizado a través de un juicio de expertos.

Métodos de análisis de datos

Para el análisis de datos se utilizara el software de reporte de datos estadístico SPSS en su versión 22.0 y para la prueba de hipótesis se utilizará la prueba Coeficiente de Correlación de Spearman, por medio de la cual se realizará la contrastación de la hipótesis y determinar conclusiones.

Aspectos éticos

La presente investigación no está excluida del aspecto ético debido a ello, se realizó un estricta toma de datos a través de las encuestas a los trabajadores de la Dirección de Gestión de Recursos Educativos con la finalidad de contar con datos reales y transparentes sin ningún tipo de manipulación.

9. RESULTADOS

Regla Teórica para Toma de Decisiones

Se utilizó la Regla de Decisión, comparando el Valor p calculado por la data con el Valor p teórico de tabla = 0.05. Si el Valor p calculado ≥ 0.05, se Aceptará Ho. Pero, si el Valor p calculado < 0.05, se Aceptará Ha.

Prueba de estadística: Debido a que las variables tienen escala ordinal utilizamos el procedimiento estadístico Rho de Spearman de la estadística no paramétrica, para determinar el grado de relación que tiene ambas variables.

De esta manera luego del análisis estadístico se obtuvo un valor de rho de spearman de 0.886 ** y un p=0 por lo que se acepta la Hipótesis General del presente trabajo de investigación y lo cual

demuestra que existe una relación entre las variables seguridad de la información y la gestión de riesgos tal como se determinó al inicio del presente trabajo.

Ha= Existe una relación directa entre La seguridad de la información tiene relación significativa con la gestión de riesgos.

10. DISCUSIÓN

En el presente etapa y después de obtener los resultados, se compararan con los antecedentes de la presente investigación, los cuales confirmaran las hipótesis planteadas, pudiendo determinar que la hipótesis general, cuyo planteamiento ha sido de que "Existe relación entre la seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018", las pruebas estadísticas utilizadas nos indican que la correlación no paramétrica de Spearman de 0,886**, representando ésta una alta asociación de las variables y siendo positivo con un valor $p = 0.000$ ($p < 0.01$).

Así mismo, las dimensiones descritas en el presente trabajo de investigación, toman una alta relación con las variables de estudio, esto confirma que si se capacita al personal de la Dirección de Gestión de Recursos Educativos acerca de temas vinculados a la seguridad de la información y gestión de riesgos, este podrá tomar decisiones adecuadas a fin de salvaguardar los activos importantes para la entidad. Al respecto para Seclén (2016) para salvaguardar los activos es importante cubrir la necesidad de establecer la creación de un Departamento de Gobierno de Seguridad de la Información del más alto nivel compuesto por un grupo de especialistas en seguridad de la información que opere como un solo grupo de trabajo nacional el cual tenga como principal función un monitoreo permanente de avance y ejecución del avance de la implementación del SGSI en todas las entidades públicas peruanas, lo que podría darse a través de la potenciación funcional y técnica de la Secretaria de Gobierno Digital del Perú..

En la misma línea Otoya (2018), concluyó que los profesionales alegan estar preocupados por la seguridad y en transmitir a los clientes la sensación de seguridad pero admiten no conocer en profundidad los procesos que la aumentan tangiblemente y no poder ponerlas en práctica a sus proyectos en TI; concordante con todo ello la Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico e Informático (ONGEI) hoy conocida como Secretaria de Gobierno digital, dispone de uso obligatorio de la Norma Técnica Peruana: "NTP – ISO 17999:2014 EDI para la Gestión de la Seguridad de la Información, dicha norma se basa en el estándar internacional ISO 17799 que es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector.

Tal como se precisó existe una relación directa entre la seguridad de la información y la gestión de

riesgos, ya que si la seguridad de la información mejora la gestión de riesgos también lo hará, por ello para Arévalo (2017) no solo basta con implementar capacitaciones constantes, sino que precisa que es vital establecer políticas de seguridad, las cuales deberán ser aplicadas bajo responsabilidad por todo el personal de la empresa. Para Tarrillo (2015) como primer paso es de vital importancia que se implemente la metodología MAGERIT como punto base para determinar que activos son los preponderantes para la entidad ya que con ello el personal de la entidad podrá identificar los posibles riesgos que atenten en contra de los intereses de la entidad.

El presente trabajo de investigación coincide con lo mencionado por Guevara (2013) es fundamental el apoyo tanto humano como financiero de la Alta Dirección y el compromiso del personal de la entidad para poder aplicar la seguridad de la información y la gestión de riesgos en la entidad donde se apliquen los conceptos antes estudiados.

11. CONCLUSIONES

Se concluye que existe una relación directa entre la seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del MINEDU, ya que se obtuvo un valor de significancia igual a 0 con un Rho de Spearman de (0.886**).

Al ser el valor de sigma bilateral menor al 0,05 o 5,00% se manifiesta que se ha probado la hipótesis de estudio del investigador que para este caso seria “Existe una relación directa entre la seguridad de la información y la gestión de riesgos.

12. REFERENCIAS

La uniformidad de las referencias bibliográficas tendrá como patrón las normas internacionales para que el artículo sea publicado y sea sometido a arbitraje.

Arevalo F. (2017). Elaboración y plan de implementación de política de seguridad de la información aplicada a una empresa nacional de alimentos. (Tesis de Maestría).Universidad de Cuenca Ecuador. Recuperado de: file:///C:/Users/jorge/Downloads/Trabajo%20de%20titulaci%C3%B3n%20(2).pdf

Alba. J. (2011). Planeación de la seguridad de la información corporativa sensible contra amenazas internas (Tesis de Maestría). Instituto Politécnico Nacional. México. Recuperada de: http://www.repositoriodigital.ipn.mx/bitstream/123456789/12642/1/Trabajo%20de%20Investigaci%C3%B3n%20%20Jorge%20Alba%20Cruz.pdf

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

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

Banda H. (2014).Elaboración de un sistema de gestión de la seguridad de la información (SGSI) para la empresa radical CIA LTDA en la ciudad de quito para el año 2014. (Tesis de Maestría).Universidad de las Américas Ecuador. Recuperado de: file:///C:/Users/jorge/Downloads/UDLA-EC-TMGSTI-2014-28(S)%20(2).pdf

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

Galicia. L. (2016). Propuesta de modelo de gestión para la prevención del riesgo operacional en el sector financiero caso: grupo financiero X. S.A. de C.V. (Tesis de Maestría). Instituto Politécnico Nacional. México. Recuperada de: http://tesis.ipn.mx/bitstream/handle/123456789/18694/1.%20Liliana%20Gali cia%20Palacios.pdf?sequence=1

Guevara T (2013). Modelo de gestión de seguridad de la información para la corporación financiera nacional basado en gestión de riesgos.(Tesis de Maestría). Escuela Politecnica Nacional. Ecuador. Recuperado de: http://bibdigital.epn.edu.ec/bitstream/15000/8052/4/CD-5084.pdf

Guzmán. G. (2015). Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica ortega. (Tesis para Maestría). Universidad Nacional del Centro del Perú. Recuperada de: http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/1478/Tes Goyo%20Francisco%20Guzman%20Pacheco.pdf?sequenceis-=1&isAllowed=

Maggiore M. (2014). Modelo de evaluación de madurez para la gestión de seguridad de la información integrada en los procesos de negocio.(Tesis de Maestría).Universidad de Buenos Aires. Argentina. Recuperado de:

http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0550_MaggioreML.pdf

Llontop G. (2018). Gestión de riesgos de Tecnologías de Información de las Empresas de Nephila Networks. Universidad Cesar Vallejo Lima Perú. Recuperado de: file:///C:/Users/jorge/Downloads/Llotop_DGC%20(4).pdf

Magerit (2012). Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro I Método - versión 3.0. Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Mercado J. (2016). Modelo de gestión de seguridad de la información para el E-Gobierno. Universidad Nacional Mayor de San Marcos Perú. Recuperado de: http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/6414/Mercado_rj.pdf?sequence=1&isAllowed=y

Muñoz J. (2016) Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (dtic) de la Universidad de Cuenca. (Tesis de Maestría). Recuperado de:http://dspace.ucuenca.edu.ec/bitstream/123456789/25646/1/Tesis.pdf

Otoya M. (2018). Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Universidad Cesar Vallejo. Lima Perú. Recuperado de: file:///C:/Users/jorge/Downloads/Otoya_VM.pdf

Tarrillo E. (2016). Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015. Universidad Cesar Vallejo Tarapoto Perú. Recuperado de: http://repositorio.ucv.edu.pe/bitstream/handle/UCV/1286/tarrillo_se.pdf?sequence=1&isAllowed=y

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

Soriano M. (2014) Seguridad en redes y seguridad de la información 23-58 Recuperado de: http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

13.RECONOCIMIENTOS

Se agradece el apoyo de los docentes Mg. Luis Torres Cabanillas (Asesor de Tesis) y Dr. Yolvi Ocaña Fernández (Revisor de Tesis) quienes bridaron el apoyo necesario para la elaboración del presente trabajo de investigación.

DECLARACIÓN JURADA

DECLARACIÓN JURADA DE AUTORÍA Y AUTORIZACIÓN PARA LA PUBLICACIÓN DEL ARTÍCULO CIENTÍFICO

Yo, Jorge Armando Calderon Sanchez estudiante (x), egresado ( ), docente ( ), del Programa Maestría de Ingeniería de Sistemas con mención en Tecnologías de la Información de la Escuela de Postgrado de la Universidad César Vallejo, identificado(a) con DNI 41908330, con el artículo titulado

"Seguridad de la Información y Gestión de Riesgos en los trabajadores de la DIGERE del MINEDU, 2018"

declaro bajo juramento que:

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

Lima 25 de Enero del 2019

Jorge Armando Calderón Sánchez

ANEXO 2

MATRIZ DE CONSISTENCIA

Titulo: Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018

Autor: Jorge Armando Calderon Sanchez

Problema	Objetivo	Hipótesis	Variables e Indicadores				
Problema General: ¿Qué relación existe entre la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018? **Problemas Especificos:** ¿Qué relación existe entre la dimensión disponibilidad de seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018? ¿Qué relación existe entre la dimensión confidencialidad de la seguridad de información y la gestión de riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018? ¿Qué relación existe entre la dimensión integridad de datos de la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018?	**Objetivo general:** Determinar la relación que existe entre la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. **Objetivos especificos:** Determinar la relación que existe entre la dimensión disponibilidad de seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. Determinar la relación que existe entre la dimensión confidencialidad de la seguridad de información y la gestión de riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. Determinar la relación que existe entre la dimensión integridad de datos de la seguridad de información y la gestión de riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018.	**Hipótesis general:** Existe una relación directa entre la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. **Hipótesis especificas:** Existe una relación directa entre la dimensión disponibilidad de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. Existe una relación directa entre la dimensión disponibilidad de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. Existe una relación directa entre la dimensión integridad de datos de la seguridad de la información y la gestión de riesgos en los trabajadores en la Dirección General de Recursos Educativos del Ministerio de Educación, 2018.	**Variable 1: Seguridad de la Información**				
			Dimensiones	**Indicadores**	**Ítems**	**Escala de medición**	**Niveles o rangos**
			Disponibilidad	• Tiempo que tarda en obtener la información que se requiere. • Copias de respaldo de información.	1-4 5-6	1) Nunca 2) Casi nunca 3) Algunas veces 4) Casi siempre 5) Siempre	1) No aceptable 2) Aceptable 3) Bueno
			Confidencialidad	• Clasificación de activos de información. • Politicas de Seguridad de la información.	7-8 9-12		
			Integridad de datos	• Encriptación de la información. • Cantidad de incidentes reportados por manipulación de datos.	13 14-18		

Fuente: Elaboración propia

Problema General:	Objetivo general:	Hipótesis general:	Variable 2: Gestión de riesgos				
¿Qué relación existe entre la seguridad de la información y la gestión por riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación 2018? Problemas Específicos: ¿Qué relación existe entre la dimensión proceso de gobernanza del riesgo de la gestión de riesgos y la seguridad de la información en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018? ¿Qué relación existe entre la dimensión cultura consciente sobre riesgos de la gestión de riesgos y la seguridad de la información en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018? ¿Qué relación existe entre la dimensión implantación eficaz de TI de la gestión de riesgos y la seguridad de la información en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018?	Determinar la relación que existe entre la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. **Objetivos específicos:** Determinar la relación que existe entre la dimensión proceso de gobernanza del riesgo de la gestión de riesgos y la seguridad de la información en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. Determinar la relación que existe entre la dimensión cultura consciente sobre riesgos de la gestión de riesgos y la seguridad de la información en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018 Determinar la relación que existe entre la dimensión implantación eficaz de TI de la gestión de riesgos y la seguridad de la información en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018.	Existe una relación directa entre la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. **Hipótesis específicas:** Existe una relación directa entre la dimensión proceso de gobernanza del riesgo de la gestión de riesgos y la seguridad de la información en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018. Existe una relación directa entre la dimensión cultura consciente sobre riesgos de la gestión de riesgos y la seguridad de la información en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018 Existe una relación directa entre la dimensión implantación eficaz de TI de la gestión de riesgos y la seguridad de la información en los trabajadores de la Dirección General de Recursos Educativos del Ministerio de Educación, 2018.					
	Dimensiones	**Indicadores**	**Ítems**	**Escala de valores**	**Niveles o rangos**
	Proceso de gobernanza del riesgo	• Grado de Planeamiento • Efectividad en la definición de los riesgos de TI según las categorías de información.	1-2 3-6	1) Nunca 2) Casi nunca 3) Algunas veces 4) Casi siempre 5) Siempre	1) No aceptable 2) Aceptable 3) Bueno
	Cultura consciente sobre riesgos	• Grado de concientización. • Efectividad del monitoreo de las actividades de gestión de riesgos de TI.	7-9 10-12		
	Implantación eficaz de TI	• Efectividad de la implantación de controles y seguimiento de las brechas de seguridad. • Efectividad en los niveles de riesgos inherentes de TI.	13-14 15-18		

Fuente: Elaboración propia

Tipo y diseño de investigación	Población y muestra	Técnicas e instrumentos	Estadística a utilizar
Tipo: Básica **Alcance:** Encontrar la relación entre la seguridad de la información y la gestión de riesgos. **Diseño:** No experimental de corte transversal **Método:** Hipotético - deductivo	**Población:** 106 **Tipo de muestreo:** No probabilística **Nivel de confianza: 95%** **Margen de error: 0.05%** **Tamaño de muestra:** 83	**Variable 1: Seguridad de la Información** **Técnicas:** Encuesta **Instrumentos:** Cuestionario Autor: Bach. Jorge Armando Calderon Sanchez Año: 2018 Monitoreo: Seguimiento Ambito de Aplicación: Personal de la Dirección de Gestión de Recursos Educativos **Variable 2: Gestión de riesgos** **Técnicas:** Encuesta **Instrumentos:** Cuestionario Autor: Bach. Jorge Armando Calderon Sanchez Año: 2018 Monitoreo: Jorge Armando Calderon Sanchez Ambito de Aplicación: Personal de la Dirección de Gestión de Recursos Educativos	**DESCRIPTIVA:** Estadistica descriptiva **INFERENCIAL:** Prueba estadistica de Rho de Spearman

Variable 1: **Seguridad de la Información**

Variable 2: **Gestión de riesgos**

Fuente: Elaboración propia

PERÚ | Ministerio de Educación | Viceministerio de Gestión Pedagógica | Dirección de Gestión de Recursos Educativos

Lima 04 de Setiembre del 2018

CARTA DE AUTORIZACIÓN

Por medio del presente documento el Jefe de la Unidad de Administración de la Dirección de Gestión de Recursos Educativos, autoriza al Sr. Jorge Armando Calderón Sánchez, a que realice las encuestas necesarias al personal de la DIGERE, dichas encuestas solo deberán ser utilizadas como medio de recolección de datos para la Tesis de Maestría que el personal solicitante realice.

Atentamente,

Anexo 04
Matriz de datos

VARIABLE 1: SEGURIDAD DE LA INFORMACION

	V1 SEGURIDAD DE LA INFORMACION																	
	DISPONIBILIDAD						CONFIDENCIALIDAD						INTEGRIDAD DE DATOS					
	d1xV1						d2x1						d3x1					
Nro.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	5	5	5	5	5	5	4	4	4	5	5	4	4	5	4	5	4	4
2	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
3	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
4	2	2	3	2	2	4	3	2	3	2	2	3	4	2	3	2	4	2
5	2	4	2	5	4	4	4	4	4	4	4	4	4	4	2	4	4	2
6	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
7	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
8	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4
9	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
10	2	5	1	2	5	5	3	5	3	2	3	5	5	5	5	2	3	5
11	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	4	4
12	5	4	3	5	4	4	3	5	3	3	5	4	4	4	4	3	4	4
13	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	5	4
14	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
15	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4
16	5	4	5	5	4	4	5	4	5	5	5	4	4	4	4	3	4	4
17	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
18	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
19	4	4	4	4	4	4	4	4	3	4	4	3	4	4	3	4	4	4
20	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
21	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
22	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
23	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
24	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
25	5	4	4	5	5	4	3	5	3	4	5	3	4	5	3	5	4	5
26	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
27	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
28	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
29	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4
30	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
31	4	5	4	4	5	5	4	5	4	4	4	5	5	5	3	2	3	4
32	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	4	4
33	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
34	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3

	V1 SEGURIDAD DE LA INFORMACION																	
	DISPONIBILIDAD						CONFIDENCIALIDAD						INTEGRIDAD DE DATOS					
	d1xV1						d2x1						d3x1					
Nro.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
35	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
36	5	4	3	4	4	4	3	4	3	4	4	3	4	4	3	3	4	3
37	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
38	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
39	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
40	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4
41	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
42	2	5	1	2	5	5	3	5	3	2	3	5	5	5	3	2	3	3
43	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	4	4
44	2	2	3	2	2	4	3	2	3	2	2	3	4	2	3	2	4	2
45	2	4	2	2	4	4	2	4	2	2	2	4	4	4	2	2	4	2
46	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
47	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
48	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
49	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
50	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
51	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
52	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
53	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
54	4	5	4	4	5	5	4	5	4	4	4	5	5	5	4	2	4	4
55	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	4	4
56	4	4	3	3	4	4	4	4	3	3	3	4	4	4	3	4	4	4
57	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	5	4
58	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
59	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4
60	5	4	5	5	5	5	5	5	5	5	5	4	4	4	5	4	4	4
61	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
62	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
63	4	4	4	4	4	4	3	4	4	4	4	5	4	5	5	5	4	4
64	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
65	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
66	4	5	4	3	5	5	4	5	4	4	4	5	5	5	4	4	4	4
67	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	4	4
68	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

	V1 SEGURIDAD DE LA INFORMACION																	
	DISPONIBILIDAD						CONFIDENCIALIDAD						INTEGRIDAD DE DATOS					
	d1xV1						d2x1						d3x1					
Nro.	**1**	**2**	**3**	**4**	**5**	**6**	7	8	9	10	11	12	**13**	**14**	**15**	**16**	**17**	**18**
69	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
70	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
71	4	4	4	4	4	4	4	4	4	4	4	5	4	5	3	4	4	4
72	4	4	4	4	4	4	5	4	3	4	5	4	4	4	4	4	4	4
73	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
74	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
75	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4
76	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	4	4
77	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
78	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
79	4	5	3	4	4	4	3	4	3	4	4	3	4	4	3	5	4	4
80	5	4	4	4	4	4	4	4	3	4	3	4	4	4	4	4	4	4
81	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
82	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
83	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4

VARIABLE 2: GESTION DE RIESGOS

	V2 Gestion de riesgos																	
	Proceso de gobernanza del riesgo						Cultura consciente sobre riesgos						Implantación eficaz de TI					
	d1x2						d2x2						d3x2					
Nro.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
2	5	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	3	4
3	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
4	4	5	4	2	3	3	4	3	4	4	2	3	3	3	3	2	2	3
5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
6	5	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4
7	4	4	4	4	4	4	4	3	4	4	4	5	4	5	4	4	5	4
8	4	5	5	2	5	4	5	4	3	3	3	3	4	2	3	3	4	3
9	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
10	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
11	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
12	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4
13	5	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4
14	5	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4
15	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
16	5	4	4	4	4	4	4	4	4	4	4	5	4	4	5	4	4	4
17	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5
18	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
19	4	3	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4
20	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4
21	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
22	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	2	4	4
23	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
24	4	4	3	3	4	4	3	4	4	4	4	4	4	4	3	3	4	4
25	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	5	4
26	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3
27	5	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4
28	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	5
29	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
30	4	3	4	4	3	4	4	3	4	4	4	5	4	3	4	4	3	4
31	5	5	4	4	4	4	4	4	4	4	5	5	4	4	4	5	5	5
32	5	4	4	4	4	4	4	4	4	5	4	4	5	4	4	4	4	4
33	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
34	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

	V2 Gestion de riesgos																	
	Proceso de gobernanza del riesgo						Cultura consciente sobre riesgos						Implantación eficaz de TI					
	d1x2						d2x2						d3x2					
Nro.	**1**	**2**	**3**	**4**	**5**	**6**	7	8	9	10	11	**12**	**13**	**14**	**15**	**16**	**17**	**18**
35	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
36	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
37	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4
38	5	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	4	5
39	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5
40	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
41	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4
42	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
43	5	5	5	4	5	5	4	5	4	4	4	5	5	5	4	4	3	4
44	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
45	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4	3
46	5	4	4	4	4	4	4	5	4	4	4	4	4	5	4	4	4	4
47	5	5	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4
48	4	4	3	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4
49	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
50	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
51	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
52	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
53	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3
54	5	5	4	4	5	5	4	5	4	4	4	5	5	5	4	4	4	4
55	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	4	4
56	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
57	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	5	4
58	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
59	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4
60	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5	5	5
61	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	5	4
62	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
63	4	4	3	4	4	4	4	4	4	4	4	4	4	5	4	5	4	5
64	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
65	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
66	4	5	4	4	5	5	4	4	4	4	4	5	5	5	4	2	3	4
67	4	4	5	4	4	5	5	4	5	4	4	4	5	4	5	4	4	4
68	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

	V2 Gestion de riesgos																	
	Proceso de gobernanza del riesgo						Cultura consciente sobre riesgos						Implantación eficaz de TI					
	d1x2						d2x2						d3x2					
Nro.	**1**	**2**	**3**	**4**	**5**	**6**	7	8	9	10	11	**12**	**13**	**14**	**15**	**16**	**17**	**18**
69	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
70	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
71	5	5	3	5	5	4	5	5	5	5	5	5	4	5	5	5	4	5
72	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
73	5	5	4	4	4	4	4	5	4	5	4	4	4	4	4	4	5	4
74	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
75	5	4	4	4	4	4	5	4	4	4	4	5	4	4	4	5	4	4
76	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
77	3	3	4	3	3	4	4	3	4	3	3	4	4	3	4	3	4	3
78	4	3	4	4	3	2	4	3	4	4	4	5	2	3	4	4	3	4
79	2	2	3	2	2	4	3	2	3	2	2	3	4	2	3	2	4	3
80	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4
81	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4
82	4	5	4	4	5	4	4	5	4	4	4	4	4	5	4	4	5	4
83	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	3	4

Anexo 05:

Instrumentos de recolección de datos

ENCUESTA

Para medir la relación entre la seguridad de la información y la gestión de riesgos de TI dirigido al personal de la Dirección General de Recursos Educativos del Ministerio de Educación.

DATOS GENERALES:

Área: ……..

Cargo: ……

Edad: [ ]

Sexo: Femenino [ ] Masculino [ ]

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

1) Nunca
2) Casi nunca
3) Algunas veces
4) Casi siempre
5) Siempre

	DIMENSIONES	**ESCALA**				
		1	**2**	**3**	**4**	**5**
Ítem	**Disponibilidad**					
1	¿Se encuentra disponible la información que requiere?					
2	¿Los sistemas con que cuenta la DIGERE son rápidos?					
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?					
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?					
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores?					
6	¿La página web de la institución se encuentra activa en todo momento?					

	DIMENSIONES	ESCALA				
		1	2	3	4	5
	Confidencialidad					
7	¿La DIGERE cuenta con políticas de seguridad de la información?					
8	¿La DIGERE distribuye y capacita a los trabajadores sobre la política de información con que cuenta?					
9	¿La DIGERE capacita a los trabajadores acerca de la clasificación de los activos de información y su importancia?					
10	¿Usted resguarda la información de la entidad en medios seguros?					
11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?					
12	¿Existen accesos restringidos al área de redes y comunicaciones?					
	Integridad de datos					
13	¿Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de su ubicación?					
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?					
15	¿La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave?					
16	¿Los antivirus instalados en su equipo son actualizados continuamente?					
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?					
18	¿La DIGERE realiza capacitaciones acerca de ataques virus en sus diversas modalidades?					

Instrumentos de recolección de datos

ENCUESTA

Para medir la relación entre la seguridad de la información y la gestión de riesgos de TI dirigido al personal de la Dirección General de Recursos Educativos del Ministerio de Educación.

DATOS GENERALES:

Área:……..

Cargo:……

Edad: [ ]

Sexo: Femenino [ ] Masculino [ ]

Se ha diseñado el presente cuestionario con el objeto de tener un buen procedimiento de medición sobre la gestión de riesgos de TI, por lo que necesitamos de su colaboración. Marcar con una equis (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

1) Nunca
2) Casi nunca
3) Algunas veces
4) Casi siempre
5) Siempre

	DIMENSIONES	**ESCALA**				
		1	**2**	**3**	**4**	**5**
Ítem	**Cultura consciente sobre riesgos**					
1	¿Ha recibido capacitación referente a seguridad de la información?					
2	¿La DIGERE implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?					
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?					
4	¿La DIGERE recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?					
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información que maneja?					
6	¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza?					

	DIMENSIONES	ESCALA				
		1	2	3	4	5
Ítem	**Proceso de gobernanza del riesgo**					
7	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?					
8	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?					
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?					
10	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?					
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?					
12	¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?					
	Implantación eficaz de TI					
13	¿Se ha implantado políticas para minimizar posibles riesgos vinculados a la seguridad de la Información referente a las Tecnologías de la Información?					
14	¿El área de TI de la DIGERE cuenta con una plataforma virtual en las cuales se actualizan las buenas prácticas vinculados a los activos de la información de la empresa?					
15	¿Han sido efectivos los controles aplicados a los probables riesgos en TI?					
16	¿Se da seguimiento a las brechas entorno a la seguridad de la información?					
17	¿La institución invierte en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para una mayor seguridad de la información y lo comunica a su personal?					
18	¿La entidad renueva continuamente los equipos informáticos en su entidad?					

Anexo 6
Formato de validación

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION Y LA GESTION DE RIESGOS EN LOS TRABAJADORES DE LA DIGERE DEL MINEDU, 2018

VARIABLE: SEGURIDAD DE LA INFORMACION

	DIMENSIONES	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	Disponibilidad	SI	NO	SI	NO	SI	NO	
1	¿Se encuentra disponible la información que requiere para realizar sus labores?	X		X		X		
2	¿Los sistemas con que cuenta la DIGERE son rápidos?	X		X		X		
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?	X		X		X		
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?	X		X		X		
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores a través de los sistemas?	X		X		X		
6	¿La página web de la institución se encuentra activa en todo momento?.	X		X		X		

	DIMENSIONES	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	**Confidencialidad**	SI	NO	SI	NO	SI	NO	
7	¿La DIGERE cuenta con políticas de seguridad de la información?	X		X		X		
8	¿La DIGERE distribuye y capacita a los trabajadores sobre la política de información con que cuenta?	X		X		X		
9	¿Está capacitado acerca de cuáles son los activos de información que son confidenciales para la DIGERE?	X		X		X		
10	¿Usted resguarda la información de la entidad en medios seguros?	X		X		X		
11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?	X		X		X		
12	¿Existen accesos restringidos al área de redes y comunicaciones?	X		X		X		
N°	**Integridad de datos**	SI	NO	SI	NO	SI	NO	
13	¿Ha encontrado una base de datos modificada sin su autorización?	X		X		X		
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?	X		X		X		
15	¿La documentación en físico que usted maneja se encuentra accesible para otras personas?	X		X		X		
16	¿Los antivirus instalados en su equipo son actualizados continuamente?	X		X		X		
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?	X		X		X		
18	¿La DIGERE realiza capacitaciones acerca de ataques virus en sus diversas modalidades?	X		X		X		

Observaciones (precisar si hay suficiencia): _____

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

Apellidos y nombres del juez validador. Dr/ Mg: Dr. Ing. Flores Masías, Edward José **DNI:** 09536323

Especialidad del validador: Dr. en Ing. de Sistemas

....24....de....1....del 20.23

Edw

Firma del Experto Informante.

[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:** No se encuentra dificultad alguna en el enunciado del ítem, es conciso, exacto y directo.

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

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION Y LA GESTION DE RIESGOS EN LOS TRABAJADORES DE LA DIGERE DEL MINEDU, 2018

VARIABLE: GESTION DE RIESGOS

	DIMENSIONES / ITEMS	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
Item	Cultura consciente sobre riesgos	SI	NO	SI	NO	SI	NO	
1	¿Ha recibido capacitación referente a seguridad de la información?	X		X		X		
2	¿La DIGERE implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?	X		X		X		
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?	X		X		X		
4	¿La DIGERE recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?	X		X		X		
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información?	X		X		X		
6	Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza.	X		X		X		

	DIMENSIONES / ITEMS	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	**Proceso de gobernanza del riesgo**	SI	NO	SI	NO	SI	NO	
7	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?	X		X		X		
8	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?	X		X		X		
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?	X		X		X		
10	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?	X		X		X		
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?	X		X		X		
12	¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados	X		X		X		
	Implantación eficaz de TI	SI	NO	SI	NO	SI	NO	
13	¿Se ha implantado políticas para minimizar posibles riesgos vinculados a la seguridad de la información referente a las Tecnologías de la Información?	X		X		X		
14	¿El área de TI de la DIGEIRE cuenta con una plataforma virtual en la cual se detallen las buenas prácticas vinculados a los activos de la información de la empresa?	X		X		X		
15	¿Han sido efectivos los controles aplicados a los probables riesgos en TI?	X		X		X		
16	¿Se da seguimiento a las brechas entorno a la seguridad?	X		X		X		
17	¿La institución invierte en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para una mayor seguridad de la información y lo comunica a su personal?	X		X		X		
18	¿La entidad renueva continuamente los equipos informáticos en su entidad?	X		X		X		

Observaciones (precisar si hay suficiencia: _____

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

Apellidos y nombres del juez validador. Dr/ Mg: Dr. Ing. Flores Masías, Edward José **DNI:** 09536323

Especialidad del validador: Dr. en ling de Sistemas

[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:** No se encuentra dificultad alguna en el enunciado del ítem, es conciso, exacto y directo

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

24 de 11 del 2023

Firma del Experto Informante.

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION Y LA GESTION DE RIESGOS EN LOS TRABAJADORES DE LA DIGERE DEL MINEDU, 2018

VARIABLE: SEGURIDAD DE LA INFORMACION

	DIMENSIONES	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	Disponibilidad	SI	NO	SI	NO	SI	NO	
1	¿Se encuentra disponible la información que requiere para realizar sus labores?	X		X		X		
2	¿Los sistemas con que cuenta la DIGERE son rápidos?	X		X		X		
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?	X		X		X		
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?	X		X		X		
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores a través de los sistemas?	X		X		X		
6	¿La página web de la institución se encuentra activa en todo momento?.	X		X		X		

	DIMENSIONES	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	**Confidencialidad**	SI	NO	SI	NO	SI	NO	
7	¿La DIGERE cuenta con políticas de seguridad de la información?	X		X		X		
8	¿La DIGERE distribuye y capacita a los trabajadores sobre la política de información con que cuenta?	X		X		X		
9	¿Está capacitado acerca de cuáles son los activos de información que son confidenciales para la DIGERE?	X		X		X		
10	¿Usted resguarda la información de la entidad en medios seguros?	X		X		X		
11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?	X		X		X		
12	¿Existen accesos restringidos al área de redes y comunicaciones?	X		X		X		
N°	**Integridad de datos**	SI	NO	SI	NO	SI	NO	
13	¿Ha encontrado una base de datos modificada sin su autorización?	X		X		X		
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?	X		X		X		
15	¿La documentación en físico que usted maneja se encuentra accesible para otras personas?	X		X		X		
16	¿Los antivirus instalados en su equipo son actualizados continuamente?	X		X		X		
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?	X		X		X		
18	¿La DIGERE realiza capacitaciones acerca de ataques virus en sus diversas modalidades?	X		X		X		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [4] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Gálvez Tapia Orleans Moises **DNI:** 16798332

Especialidad del validador: Magister en Ingeniería de Sistemas

30 de 11 del 20 18

[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:** No se encuentra dificultad alguna en 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.

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION Y LA GESTION DE RIESGOS EN LOS TRABAJADORES DE LA DIGERE DEL MINEDU, 2018

VARIABLE: GESTION DE RIESGOS

	DIMENSIONES / ITEMS	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
Item	**Cultura consciente sobre riesgos**	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	
1	¿Ha recibido capacitación referente a seguridad de la información?	X		X		X		
2	¿La DIGERE implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?	X		X		X		
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?	X		X		X		
4	¿La DIGERE recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?	X		X		X		
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información?	X		X		X		
6	Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza.	X		X		X		

	DIMENSIONES / ITEMS	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	**Proceso de gobernanza del riesgo**	SI	NO	SI	NO	SI	NO	
7	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?	X		X		X		
8	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?	X		X		X		
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?	X		X		X		
10	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?	X		X		X		
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?	X		X		X		
12	¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados	X		X		X		
	Implantación eficaz de TI	SI	NO	SI	NO	SI	NO	
13	¿Se ha implantado políticas para minimizar posibles riesgos vinculados a la seguridad de la Información referente a las Tecnologías de la Información?	X		X		X		
14	¿El área de TI de la DIGEIRE cuenta con una plataforma virtual en la cual se detallen las buenas prácticas vinculados a los activos de la información de la empresa?	X		X		X		
15	¿Han sido efectivos los controles aplicados a los probables riesgos en TI?	X		X		X		
16	¿Se da seguimiento a las brechas entorno a la seguridad?	X		X		X		
17	¿La institución invierte en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para una mayor seguridad de la información y lo comunica a su personal?	X		X		X		
18	¿La entidad renueva continuamente los equipos informáticos en su entidad?	X		X		X		

Observaciones (precisar si hay suficiencia: _____

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

Apellidos y nombres del juez validador. Dr/ Mg: Gálvez Tapia Orleans Moisés **DNI:** 16798332

Especialidad del validador: Magister en Ingeniería de Sistemas.

30 de 11 del 2018.

[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: No se encuentra dificultad alguna en 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.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION Y LA GESTION DE RIESGOS EN LOS TRABAJADORES DE LA DIGERE DEL MINEDU, 2018

VARIABLE: SEGURIDAD DE LA INFORMACION

	DIMENSIONES	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	Disponibilidad	SI	NO	SI	NO	SI	NO	
1	¿Se encuentra disponible la información que requiere para realizar sus labores?	X		X		X		
2	¿Los sistemas con que cuenta la DIGERE son rápidos?	X		X		X		
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?	X		X		X		
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?	X		X		X		
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores a través de los sistemas?	X		X		X		
6	¿La página web de la institución se encuentra activa en todo momento?.	X		X		X		

	DIMENSIONES	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	**Confidencialidad**	SI	NO	SI	NO	SI	NO	
7	¿La DIGERE cuenta con políticas de seguridad de la información?	X		X		X		
8	¿La DIGERE distribuye y capacita a los trabajadores sobre la política de información con que cuenta?	X		X		X		
9	¿Está capacitado acerca de cuáles son los activos de información que son confidenciales para la DIGERE?	X		X		X		
10	¿Usted resguarda la información de la entidad en medios seguros?	X		X		X		
11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?	X		X		X		
12	¿Existen accesos restringidos al área de redes y comunicaciones?	X		X		X		
N°	**Integridad de datos**	SI	NO	SI	NO	SI	NO	
13	¿Ha encontrado una base de datos modificada sin su autorización?	X		X		X		
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?	X		X		X		
15	¿La documentación en físico que usted maneja se encuentra accesible para otras personas?	X		X		X		
16	¿Los antivirus instalados en su equipo son actualizados continuamente?	X		X		X		
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?	X		X		X		
18	¿La DIGERE realiza capacitaciones acerca de ataques virus en sus diversas modalidades?	X		X		X		

Observaciones (precisar si hay suficiencia): Es suficiente

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

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Luis Toro Caballero **DNI:** 08404630

Especialidad del validador: Ing. Estadístico CIP 49863

16 de DIC del 2018

[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:** No se encuentra dificultad alguna en 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.

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFORMACION Y LA GESTION DE RIESGOS EN LOS TRABAJADORES DE LA DIGERE DEL MINEDU, 2018

VARIABLE: GESTION DE RIESGOS

	DIMENSIONES / ITEMS	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
Item	Cultura consciente sobre riesgos	SI	NO	SI	NO	SI	NO	
1	¿Ha recibido capacitación referente a seguridad de la información?	X		X		X		
2	¿La DIGERE implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?	X		X		X		
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?	X		X		X		
4	¿La DIGERE recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?	X		X		X		
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información?	X		X		X		
6	Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza.	X		X		X		

	DIMENSIONES / ITEMS	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
N°	**Proceso de gobernanza del riesgo**	SI	NO	SI	NO	SI	NO	
7	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?	X		X		X		
8	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?	X		X		X		
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?	X		X		X		
10	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?	X		X		X		
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?	X		X		X		
12	¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados	X		X		X		
	Implantación eficaz de TI	SI	NO	SI	NO	SI	NO	
13	¿Se ha implantado políticas para minimizar posibles riesgos vinculados a la seguridad de la Información referente a las Tecnologías de la Información?	X		X		X		
14	¿El área de TI de la DIGERE cuenta con una plataforma virtual en la cual se detallen las buenas prácticas vinculados a los activos de la información de la empresa?	X		X		X		
15	¿Han sido efectivos los controles aplicados a los probables riesgos en TI?	X		X		X		
16	¿Se da seguimiento a las brechas entorno a la seguridad?	X		X		X		
17	¿La institución invierte en nuevas tecnologías de información (servidores, PC, antivirus, etc.) para una mayor seguridad de la información y lo comunica a su personal?	X		X		X		
18	¿La entidad renueva continuamente los equipos informáticos en su entidad?	X		X		X		

Observaciones (precisar si hay suficiencia: Es Suficiente

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

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Luis Tovar Cabanillas **DNI:** 08404690

Especialidad del validador: Ing. Estadística CIP 45863.

[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:** No se encuentra dificultad alguna en el enunciado del ítem, es conciso, exacto y directo

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

16 de Dic del 20 18

Firma del Experto Informante.

Anexo 7
Inprpant de resultados

Análisis descriptivo de frecuencias de la variable seguridad de la información

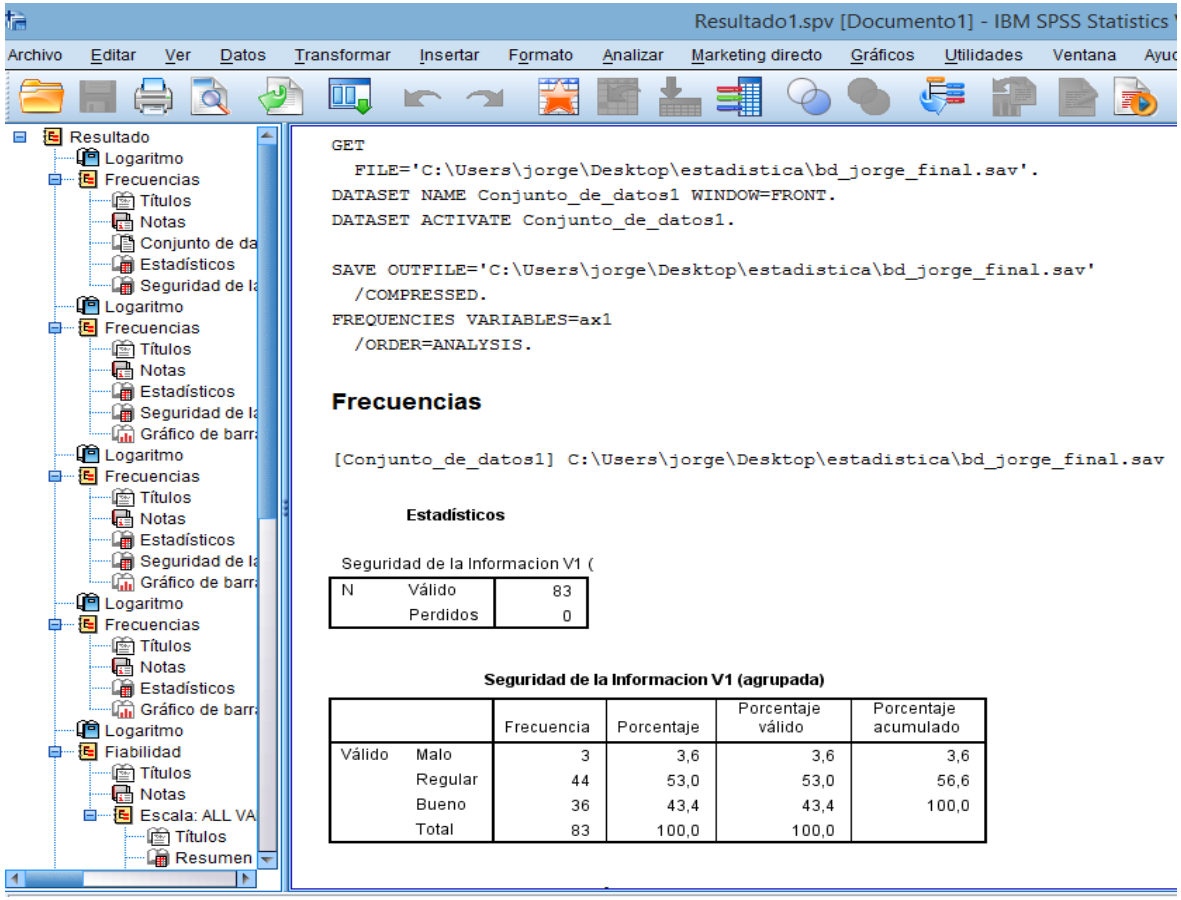
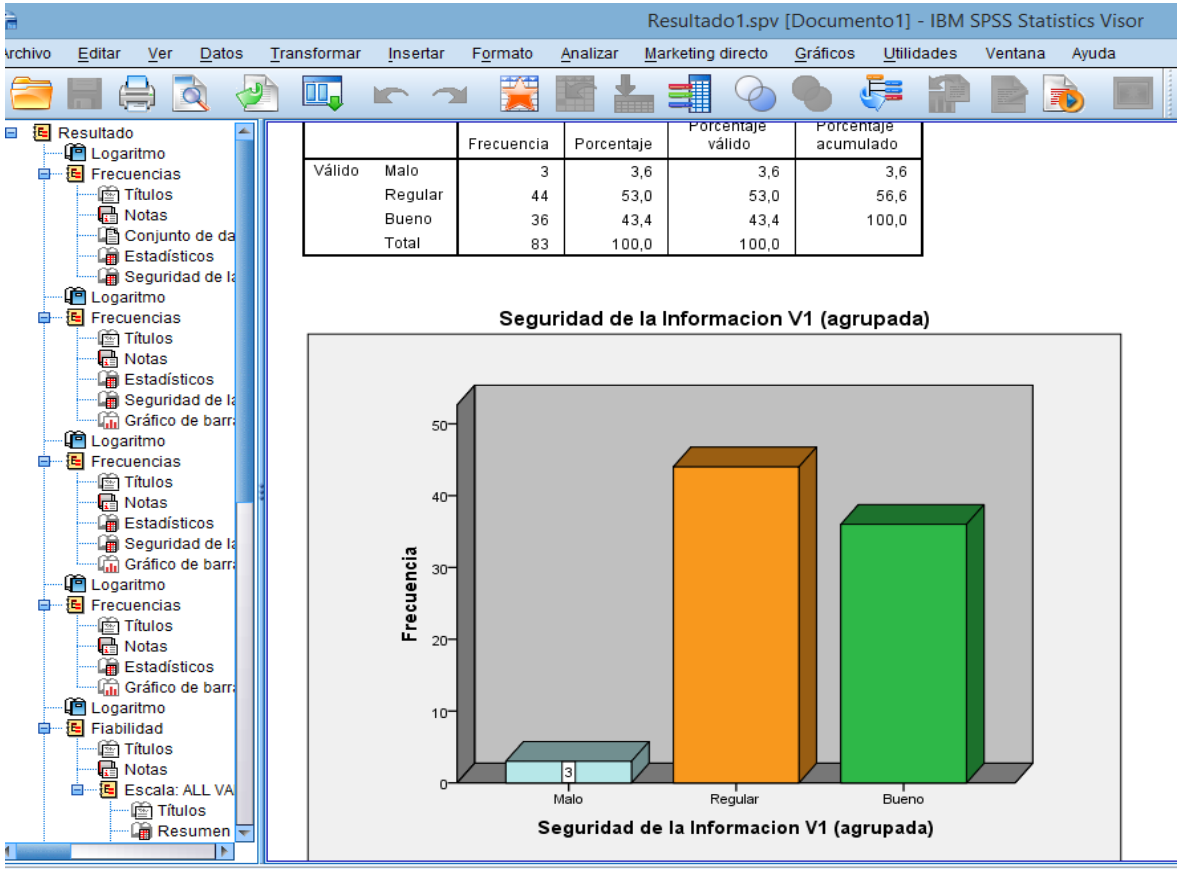
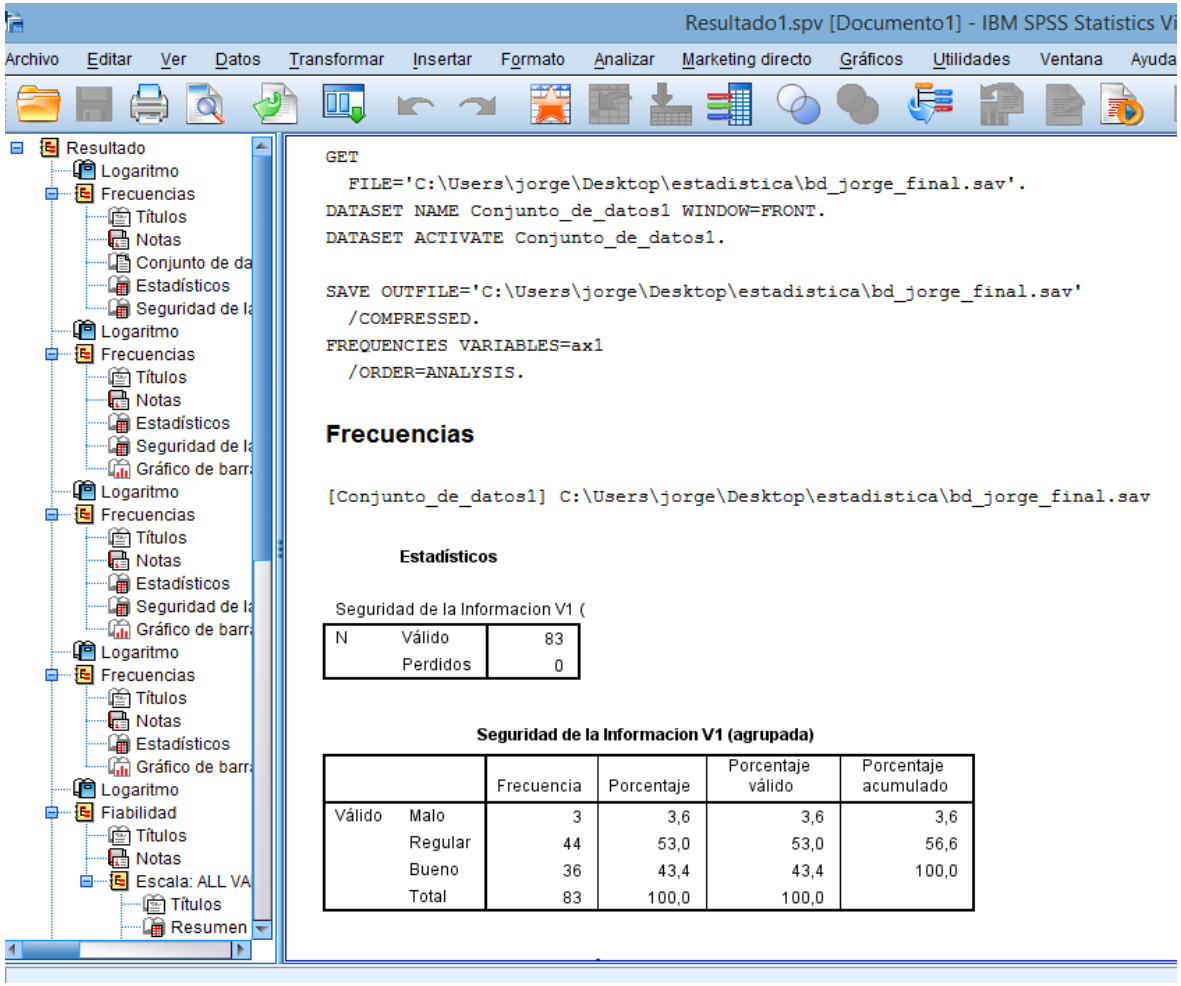


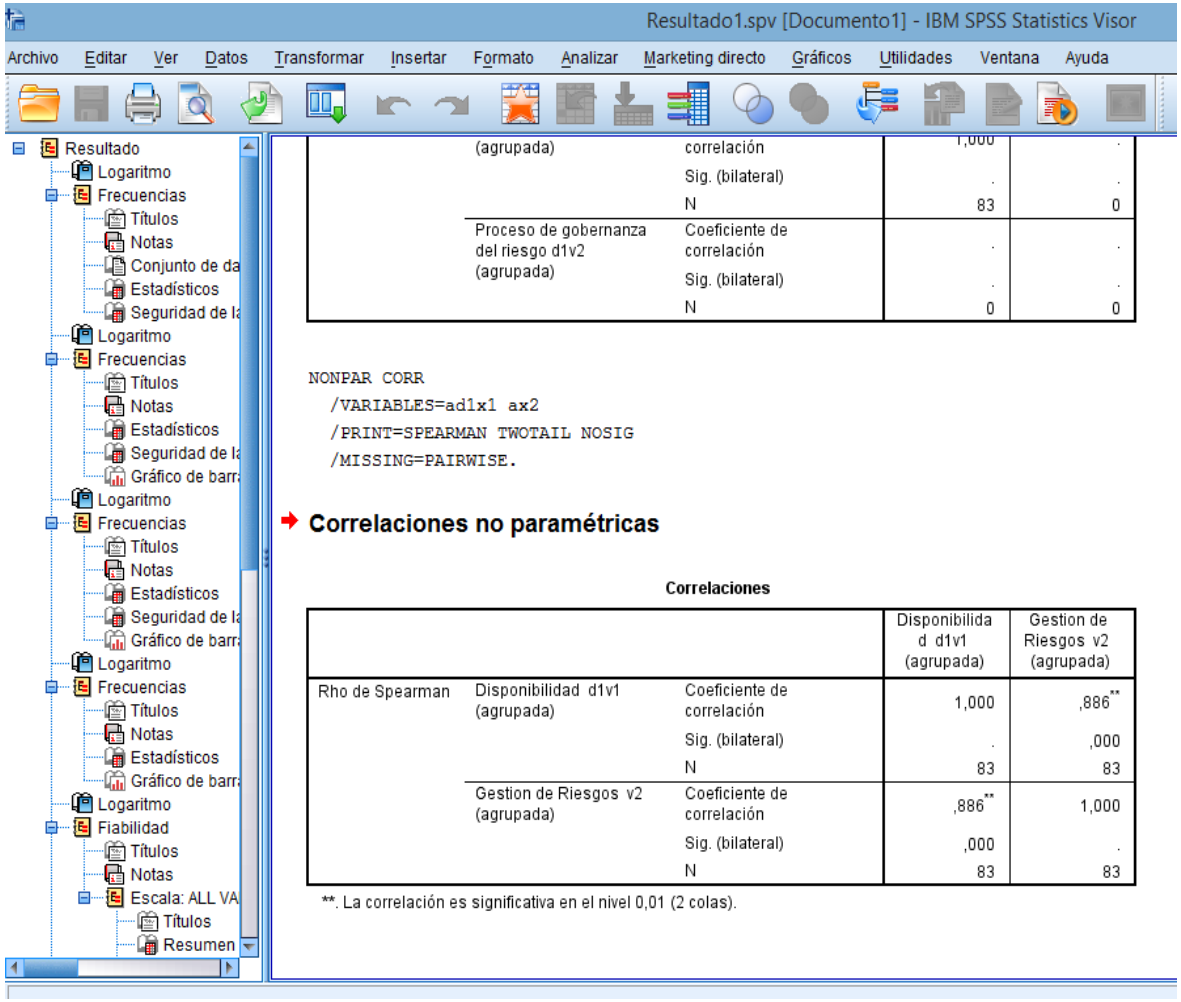
Gráfico de frecuencias de la variable seguridad de la información



Análisis de datos de la muestra



Análisis correlacional entre las variables seguridad de la información y la gestión de riesgos



ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

ACTA DE APROBACIÓN DE ORIGINALIDAD DE LOS TRABAJOS ACADÉMICOS DE LA UCV

Yo, Luis Torres Cabanillas, docente de la Escuela de Posgrado de la UCV y revisor del trabajo académico titulado "Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018" del estudiante: Jorge Armando Calderón Sánchez; y habiendo sido capacitado e instruido en el uso de la herramienta Turnitin, he constatado lo siguiente: Que el citado trabajo académico tiene un índice de similitud constato 25% verificable en el reporte de originalidad del programa turnitin, grado de coincidencia mínimo que convierte el trabajo en aceptable y no constituye plagio, en tanto cumple con todas las normas del uso de citas y referencias establecidas por la universidad César Vallejo.

Lima, 20 de enero del 2019

ESCUELA DE POSGRADO UCV UNIVERSIDAD CÉSAR VALLEJO INVESTIGACIÓN CAMPUS LIMA

Luis Torres Cabanillas
DNI: 08404690

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:

Maestro en ingeniería de sistemas con mención en gestión de tecnologías de la información

AUTOR:

Br. Calderón Sánchez Jorge Armando

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)
CALDERON SANCHEZ JORGE ARMANDO

D.N.I. : 41908330
Domicilio : Av. Juan Velasco Alvarado 455
Teléfono : Fijo : 3621444 Móvil : 959661984
E-mail : Jcalderons2000@gmail.com

2. IDENTIFICACIÓN DE LA TESIS

Modalidad:

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

☐ Tesis de Posgrado
☒ Maestría ☐ Doctorado
Grado : MAESTRO EN Ingeniería de Sistemas
Mención : Tecnologías de la Información

3. DATOS DE LA TESIS

Autor (es) Apellidos y Nombres:
CALDERON SANCHEZ JORGE ARMANDO

Título de la tesis:
SEGURIDAD DE LA Información y la gestion de riesgos en los Trabajadores de la DIGERE del Ministerio de Educación, 2018

Año de publicación : 2019

4. AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN VERSIÓN ELECTRÓNICA:

A través del presente documento,
Si autorizo a publicar en texto completo mi tesis. ☒
No autorizo a publicar en texto completo mi tesis. ☐

Firma :

Fecha : 23/03/19

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:

CALDERÓN SÁNCHEZ JORGE ARMANDO

INFORME TÍTULADO:

SEGURIDAD DE LA Información y la gestión de riesgos en los Trabajadores de la DIGERE del Ministerio de Educación, 2018.

PARA OBTENER EL TÍTULO O GRADO DE:

MAESTRO EN Ingeniería de Sistemas con Mención en Tecnologías de la Información

SUSTENTADO EN FECHA: 25 de enero del 2019

NOTA O MENCIÓN: Aprobado por mayoría

ESCUELA DE POSGRADO UCV UNIVERSIDAD CÉSAR VALLEJO INVESTIGACIÓN CAMPUS LIMA

FIRMA DEL ENCARGADO DE INVESTIGACIÓN