ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN GESTIÓN PÚBLICA

Seguridad de la Información y Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Gestión Pública

AUTOR:

Castro Rios, Henry (ORCID: 0000-0003-3554-203X)

ASESOR:

Dr. Candia Menor, Marco Antonio (ORCID: 0000-0002-4661-6228)

LÍNEA DE INVESTIGACIÓN:

Gestión de Políticas Públicas

LIMA – PERÚ

2022

Dedicatoria

El presente trabajo de tesis va dedicado a Dios, quien como guía estuvo presente en el caminar de mi vida, bendiciéndome y dándome fuerzas para continuar con mis metas trazadas sin desfallecer. A mi esposa e hija que con su apoyo incondicional, amor y confianza permitieron que logre culminar esta etapa académica.

Agradecimiento

A Dios, mi Familia, Padres quienes me apoyaron en esta etapa. A la Universidad César Vallejo por haberme brindado la oportunidad en mi desarrollo profesional. Al Dr. Marco Candia Menor asesor del curso diseño y desarrollo del trabajo de investigación por las horas y conocimientos dedicados a la culminación de esta investigación. A mis compañeros de trabajo que participaron del presente.

INDICE

Índice de Tablas

Índice de Figuras

RESUMEN

El presente estudio de investigación tuvo el propósito de determinar la relación entre la seguridad de la información y gestión del riesgo en una entidad del sistema electoral, año 2021. Estuvo regida bajo el enfoque cuantitativo, diseño no experimental correlacional, transversal. La muestra empleada fue de 45 colaboradores de la entidad del sistema electoral, año 2021, con instrumentos validados por expertos y una alta fiabilidad piloto con un indicador de Alfa de Cronbach 0,965 y 0,905. Los resultados nos indicaron la existente de una correlación positiva perfecta entre las variables seguridad de la información y gestión de riesgo: Rho de Spearman de ,924** y una significación bilateral de ,000.

Palabras clave: Seguridad, Información, Gestión, Riesgo.

ABSTRACT

The present research study had the purpose of determining the relationship between information security and risk management in an entity of the electoral system, year 2021. It was governed under the quantitative approach, non-experimental, correlational, cross-sectional design. The sample used was 45 collaborators from the electoral system entity, year 2021, with instruments validated by experts and a high pilot reliability with a Cronbach's Alpha indicator 0.965 and 0.905. The results indicate the existence of a perfect positive correlation between the variables information security and risk management: Spearman's Rho of .924 ** and a bilateral significance of .000.

Keywords: Security, information, Management, Risk.

I. INTRODUCCIÓN

El componente seguridad de la información es importante en el desarrollo empresarial dado que a través de sus medidas permite controlar y salvaguardar la información de la organización, priorizando la protección de sus activos de información como los equipos informáticos, base de datos, entre otros, todo esto aplicando los pilares que son la confidencialidad, integridad y disponibilidad según ISOTools (2017), además Figueroa, Rodríguez, Bone, Saltos (2017) en su investigación hace una comparación entre la seguridad de la información y la seguridad informática, siendo la primera dirigida a proteger los activos de información, utilizando normas, herramientas, técnicas y metodologías, por otro lado tenemos a la seguridad informática, que es parte de la seguridad de la información , es decir , la seguridad informática se encarga de salvaguardar la infraestructura tecnológica y la información digital que esta contenga sin embargo la seguridad de la información busca resguardar la información sin importar el medio en el cual se encuentra almacenada, puede ser almacenamiento físico o digital.

Para Sullivan (2016), gestión del riesgo es un proceso que involucra la identificación, comprensión, evaluación y mitigación de riesgos, si faltara esta gestión puede tener impactos importantes en la organización como perdida de posicionamiento en el mercado altos costos de recuperación de activos y un alto impacto en la pérdida de imagen, como entre otras consecuencias.

Dentro de los escenario internacional, según la encuesta sobre el estado mundial de la seguridad de la información del año 2018, la PriceWaterhouseCoopers (2018) realizó a 9500 ejecutivos de 122 países, de lo cual se obtuvieron los siguientes resultados: a) 44% de las organizaciones no tiene una estrategia de seguridad de la información b) 48% no tiene un plan de concientización y capacitación en ciberseguridad para sus trabajadores.

En el contexto Nacional, según los resultados de la 22° encuesta sobre seguridad de la información por EY Ernst & Young Global Limited – EY Perú (2020) el 51% de las empresas en el Perú manifiestan que no existe relación entre ciberseguridad y su negocio además según la publicación de EY Perú (2021), los

resultados de la Encuesta Global de Seguridad de la Información 2021 de EY – Ernst & Young Global Limited revela que los CISO – líderes de seguridad vienen enfrentando una batalla contra las amenazas del COVID-19 esto fue en base a entrevistas realizadas a directores de seguridad de la información y ejecutivos del mundo, dicen que mayor del 60% del empresariado peruano tiene una preocupación en cómo afrontar los ataques de ciberseguridad, el 47% manifiesta que garantizar cumplir con las normativa de seguridad es la parte estresante del trabajo, el 39% no cuenta con el presupuesto suficiente necesario para afrontar los retos de la ciberseguridad y el 64% considera que su presupuesto es gasto excesivo en Tecnología de la información*.*

El Diario Gestión (2019) dice también que las empresas peruanas invierten en protección de la información por debajo del 0.10% del producto bruto interno (PBI) además el riesgo es grande cuando un colaborador tiene una mala ejecución de los sistemas de información, cuales pueden afectar la continuidad del negocio el articulo también nos indica que para prevenir los riesgos es importante identificar los activos críticos y quienes hagan usos de ellos.

En el contexto local, Latina (2021) realizó una nota periodística en la cual investigan que un grupo de colaboradores de la Superintendencia Nacional de Migraciones utilizaba información personal de personajes públicos para enviarla por chats de whatsapp internos, las razones desconocidas, solo que lo hacían por órdenes del supervisor, el artículo indica que la información es personal de tránsito migratorio de las personas la cual debería ser protegida y el uso de la misma debería estar condicionada solo a la atribución de sus funciones

La Republica (2021) en su artículo periodístico digital señalaron que delincuentes obtienen huellas digitales con el objeto de suplantar identidad y que este supuesto grupo criminal está conformada por funcionarios públicos, gerentes de entidad bancarias y empleados de empresas de telefonía, en dicho artículo entrevistan al PNP Eric Ángeles, jefe de la Investigación de Delitos de Alta Complejidad donde manifiesta que dicha información personal como las huellas dactilares son obtenidas por un grupo criminal instalada en el Registro Nacional de Identificación

y Estado Civil (RENIEC) y luego las otorgan a los delincuentes para elaborar el molde de silicona con la huella impresa por consiguiente se contactan con empleados de las empresas de telefonía y adquieren los chips, el cual es el primer paso para poder acceder a los servicios bancarios digitales y extraer todo el dinero posible.

Por consiguiente a ello se formuló la siguiente problema general ¿En qué medida se relaciona la seguridad de la información y la gestión del riesgo en una entidad del sistema electoral, año 2021? y los específicos, a) ¿Cuál es la relación que existe entre la Confidencialidad de Seguridad de la Información y la Gestión del Riesgo en una entidad del sistema electoral, año 2021? b)¿Cuál es la relación que existe entre la Integridad de Seguridad de la Información y la Gestión del Riesgo en una entidad del sistema electoral, año 2021? c) ¿Cuál es la relación que existe entre la Disponibilidad de Seguridad de la Información y la Gestión del Riesgo en una entidad del sistema electoral, año 2021?7

Teóricamente podemos justificar que mediante la presente investigación se busca identificar la relación existente entre las variables seguridad de la información y la gestión del riesgo a fin de generar valor interno y externo para la organización y la ciudadanía respectivamente, la cual dará recomendaciones que puedan fortalecer las variables de estudio. En la práctica con esta investigación fue realizado para identificar la situación de las variables de estudio en una entidad del sistema electoral, de tal manera que al saber la relación de ambas variables proponer las recomendaciones que contribuya con la mejora continua y el desarrollo de los procesos todo ello en busca de un estado y una gestión pública moderna. Desde un aspecto social la presente investigación tiene por objeto beneficiar a los ciudadanos, fortaleciendo la confianza y la satisfacción y garantizando que la información que soliciten sea integra y confiable, en conclusión generar de valor público para el ciudadano

Por ello el objetivo general será Identificar la relación que existe entre la Seguridad de la Información y la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021. Los objetivos específicos son: a) Identificar la relación que

existe entre la confidencialidad de Seguridad de la Información y la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021; b) Identificar la relación que existe entre la Integridad de Seguridad de la Información y la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021; c) Identificar la relación que existe entre la disponibilidad de Seguridad de la Información y la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021.

Del problema planteado se formuló la siguiente hipótesis general: La seguridad de la Información se relaciona con la gestión del riesgo en una entidad del sistema electoral, año 2021. De las cuales surgen, las hipótesis específicas: a) La Confidencialidad de la Seguridad de la Información se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021; b) La Integridad de Seguridad de la Información se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021; c) La Disponibilidad Seguridad de la Información se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021.

II. MARCO TEÓRICO

Carlino (2021) nos dice que los antecedentes de una investigación buscan situarla en el mismo nivel de otras investigaciones, es decir investigaciones en similitud dado que estas permitirán ubicarlas en el espacio, contextualizarlas, en ese sentido se detalla antecedentes nacionales relacionados al tema de investigación:

Pinto (2017) en su investigación en la Escuela de Suboficiales de la Policía Nacional del Perú, tiene como objetivo determinar la relación que existe entre las variables de gestión de la información y seguridad de la información para ello su tipo de investigación es básica, con diseño no experimental y transversal, utilizo el método estadístico de correlación, la población que también fue la muestra fue de 117 docentes de la institución del presente estudio. En conclusión afirma que existe una relación inversa entre ambas variables de estudio donde los resultados estadísticos evidencian la relación inversa (r=-0.647) y significativa (p = 0.000) entre la gestión de la información y riesgos de seguridad.

Calderón (2019) en su tesis de investigación en el Ministerio de Educación tiene como objetivo reconocer la relación de las variables de la seguridad de la información y la gestión de riesgos para ello el tipo de investigación fue básico, diseño no experimental, correlacional y transversal, la población fue de 106 colaboradores de la institución del presente estudio, teniendo como resultados un Rho Spearman de 0.886 y una significancia bilateral menor a 0.05 evidenciando una relación directa entre sus variables de estudio seguridad de la información y gestión de riesgos.

Huayllani (2020) en su tesis de investigación en el Ministerio de Salud, estudia que tanto influye la variable Sistema de Gestión de Seguridad de la Información en la Gestión del Riesgo. Para ello utilizo el método hipotético deductivo, de enfoque cuantitativo de tipo aplicada, correlacional y corte longitudinal. Su población y a la vez muestra fue de 145 trabajadores de la institución del presente estudio. El levantamiento de la información fue a través de encuestas las cuales pasaron por análisis estadísticos obteniendo un coeficiente de correlación de

0.856 y con una probabilidad menor al valor critico 0.05, lo cual evidencian una relación positiva y significativa entre las variables de estudio.

Huaura (2019) en su investigación tiene como objetivo determinar en las empresas del sector de telecomunicaciones cómo influye la Norma Técnica Peruana ISO/IEC 31000 en el control de los riesgos para eso la investigación fue de tipo no experimental, diseño transaccional descriptivo, para una población de 104 y una muestras de 85 personas del sector de telecomunicaciones ubicados en Lima Metropolitana, concluye que hay una correlación positiva media de 0.592 entre las variables de estudio.

Tarrillo (2015) en su investigación en la zona Registral III Sede Moyobamba, dicha estudio tiene objetivo conocer como la gestión de riesgos afecta o influye en la seguridad de activos de información. Para esto la investigación fue de tipo básico, diseño experimental de corte transversal, correlacional. La muestra de 50 es parte de una población de 150 trabajadores, las cuales dieron los resultados que efectivamente si hay una relación directa entre las variables de estudio, gestión de riesgos y la seguridad de activos de información.

En relación a los estudios internacionales se ha considerado como antecedentes a lo siguiente:

Aguilar (2020) en su investigación en una institución de educación superior el objetivo es el diseño de un modelo de seguridad de la información que permita el control de proceso en Instituciones de Educación Superior, el tipo de investigación es cuantitativo de alcance descriptivo, la población son todas las instituciones de educación superior del Municipio de Norte de Santander siendo cuatro universidades del sector público y dos privadas, la muestra son los representantes del área de tecnología de la información de las Instituciones de Educación Superior del Norte de Santander, la encuesta fue el instrumento de recolección de data. La conclusión del investigador fue que el modelo de Seguridad de la Información para la Institución de Educación Superior es viable dado que a través de la estadística de las encuestas obtenidas se obtuvo lo siguiente: a) el 33% de las instituciones de educación superior no tienen implementado un sistema de gestión de seguridad de la información, b) un 33% lo tienen definido el cual

permite su monitoreo y seguimiento y c) 34% tienen un sistema de gestión de seguridad de la información implementado apropiadamente, en relación a la gestión de riesgos se obtuvo que el 67% de las universidades tienen implementadas medidas de tratamiento de riesgos eficiente sin embargo el 37% restante no tienen medidas de remediación y/o mitigación del riesgo, finalmente aunado a los juicios de valor de los expertos estos recomendaron su implementación.

Nieves (2017) en su investigación de un diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma IOC/IEC 27001:2013 el cual tiene como finalidad implementar un SGSI ISO 27001:2013 y la metodología de análisis y gestión de riesgos en activos de información del componente de investigación, para ello realizo investigación cuantitativa y cualitativa , los cuestionarios, entrevistas y la observación fueron los instrumentos de recolección de data, el investigador realizó un análisis de cumplimiento de dominios de control en la organización de estudio y estableció el siguiente nivel; a) >=56 y <=100% es valoración Alto, b), >=40% y <=55% valoración Media c) >=0% y <=39 valoración Baja, obtuvo la siguiente información estadística; de catorce dominios que tiene la norma ISO 27001 , seis de ellos tienen un nivel de cumplimiento por debajo del 40% siendo valoración Baja sin embargo los ocho dominios restantes tienen un nivel cumplimiento por encima del 40% considerándose estas con un nivel de valoración Media y Alta; por lo cual el concluye resaltando la importancia del acatamiento de los controles de la norma ISO 27001 el cual permite identificar amenazas y vulnerabilidades a los que están expuestos los activos de información y por consiguiente desarrollar un plan de tratamiento de riesgos con el objetivo de mitigarlos o desplazarlos a un nivel donde la organización lo acepte.

Bermúdez y Bailón (2015) en su investigación en una empresa de servicios financieros cuyo objetivo fue analizar los procesos referente a seguridad y garantizar la confidencialidad, integridad y disponibilidad de la información, para ello el tipo de investigación fue no experimental -descriptivo teniendo como base la observación de un hecho o evento, la población fue de 230 empleados y una muestra de 23, el levantamiento de la información se realizó a través de encuestas y entrevistas por ejemplo el 100% de los entrevistados indica que no

existe un repositorio de incidencias de seguridad además que no existe un bloqueo automático de equipos desatendidos el cual afecta directamente a la confidencialidad además que el 91.30% no ha recibido capacitación lo cual es una debilidad para la seguridad de la información, finalmente en su conclusión manifiesta que existe un alto riesgo de modificación, daño y perdidas de los activos de información con respecto a la seguridad de la información.

Guaman (2015) en su investigación tuvo como objetivo modernizar las instituciones militares (Quito, Ecuador) a través del diseño e implementación de un Sistema de Gestión de Seguridad de la Información incorporando tecnología de información y comunicación. El instrumento de recolección de datos fue la encuesta con un confiabilidad Alpha de Cronbach de 0.96 y la población-muestra de 51 colaboradores del área de tecnología y a través de la estadística descriptiva se obtuvieron resultados para las dimensiones y/o controles de seguridad, donde concluye que las instituciones militares tienen un riesgo de vulnerabilidad en el resguardo de los activos de información por una falta de un Sistema de Gestión de Seguridad de la Información, para lo cual recomienda en su estudio la factibilidad de la implementación a fin de asegurar la confidencialidad, integridad , disponibilidad y mitigar los riesgos de la seguridad de la información.

Castro (2014) en su investigación en la Empresa Radical CIA. LTDA (Quito, Ecuador) siendo el objetivo de desarrollar e implementar un SGSI, el estudio fue de tipo básico, con diseño no experimental de corte transversal, el instrumento de recolección de datos fue las entrevistas y la población compuesta por 15 colaboradores de la empresa de estudio, el análisis descriptivo dio los resultados bajo el calificativo de cumplimiento en ese sentido el autor nos dice que el dominio: a) Política de Seguridad tiene un nivel de cumplimiento de 50%, b) Organización de la Seguridad de la Información de 19%, c) Gestión de Activos de 46%, d) Seguridad en los recursos humanos de 56%, e) Seguridad física y ambienta de 21%,f) Gestión de comunicaciones y operaciones de 20%, g) Control de Acceso de 32%, h) Adquisición, desarrollo y mantenimiento de sistemas de información de 10%, i) Gestión de incidentes de 43%, j) Gestión de continuidad de negocio de 0% y k) cumplimiento 0%; una de las conclusiones que la empresa de estudio tiene vulnerabilidad en los activos de información como la fuga de

información a través de los colaboradores siendo un riesgo muy alto valorizado entre el 30% y 60%, también concluye que la falta de un SGSI ha ocasionado pérdidas económicas en la empresa dado que no existe una correcta gestión de la información.

Desde un aspecto normativo y legal el estado peruano ha aportado y estos es con diferentes normas como la Resolución Ministerial (RM) N° 129-2012-PCM (23MAY2012) bajo este último se les exhorta a las organizaciones que pertenecen al Sistema nacional de Informática que deberán implementar un SGSI bajo la norma ISO 27001:2008 también con la RM N° 0004-2016- PCM aprueba el uso obligatorio e implemente un SGSI bajo la norma ISO 27001:2014 además con el Decreto Supremo N° 081-2013-PCM, se establecen directrices estratégicas para un Gobierno Peruano con enfoque electrónico resalando cumplir con la confidencialidad, integridad y disponibilidad y establecer procedimientos a fin de minimizar los impactos de los riesgos de la información sensible del ciudadano

Con la Ley N° 27658 – Ley Marco de Modernización de la Gestión del Estado, el del Perú entra a un proceso de modernización esto con el objeto de dar mejorar la administración pública, tener un estado moderno, usando tecnología que oferte servicios de calidad a la ciudadanía por la RM N° 00087-2019-PCM crea el comité de Gobierno Digital con el objeto de implementar acciones de fortalecimiento de las competencias del comité y la seguridad de la información.

Según Ley N°29733 – Ley de Protección de Datos Personales en su principio de Seguridad, donde el titular del banco de dato debe implementar los controles necesarios de seguridad además con el DU N° 0007-2020 aprueba el Marco de Confianza Digital y Dispone medidas para su fortalecimiento la cual busca garantizar que las transacciones en un entorno digital entre personas, empresas privadas o públicas sean confiables y seguras que garanticen la protección de datos, transparencias, seguridad digital y protección del consumidor en un entorno digital.

En este punto se detallan las teorías y conceptos fundamentados relacionados a la primera variable Seguridad de la Información, lo cual podemos indicar lo siguiente, al respecto:

Soriano (2014) autor base de la primera variable de estudio nos dice sobre seguridad de la información que es salvaguardar la información de amenazas de modificarlas, divulgarlas, alterarlas, destruirlas acceder a ellos sin tener los permisos y accesos de autorización para ello se tienen las pilares como la confidencialidad, la disponibilidad e integridad, las cuales para el presente estudio fueron consideradas como las dimensiones de la primera variable primera estos tres pilares Soriano los defines como: a) La confidencialidad es proteger la información, evitar su divulgación con entidades o individuos no autorizados, solo pueden acceder a ella los que tengas los permisos respectivos. b) La integridad es proteger los datos de modificaciones, eliminaciones, duplicados, entre otros de personas o entidades no autorizadas. c) La disponibilidad es acceder a la información en el momento que se requiere, garantizar a los usuarios el acceso a la información.

Alvarado (2021) dice que la seguridad de la información son las políticas, procedimientos, recursos, talento humano que tiene como misión la salvaguardar los activos de información.

Según el estudio de Rojas (2019) nos dice que implementar la Norma ISO /IEC 27001 Seguridad de la Información da efectos positivos en la gestión de seguridad de la información también manifestó que se debe tener un ambiente con las condiciones adecuadas donde se gestione los riesgos, la seguridad, se implemente políticas y prácticas.

Solarte, Rosero, Benavides (2015) en su artículo de investigación dice que la seguridad de la información es la prevención adoptando medidas en protección de la información, en ese sentido la infraestructura tecnológica o técnica tiene que ser la adecuada que garantice la gestión de riesgos y el aseguramiento de la seguridad de la organización.

Aenor (2015), manifiesta que la seguridad de la información como una secuencia de procedimientos que se deben implementar, hacer su seguimiento y aplicar la mejora continua a los activos de información teniendo como marco referencial la identificación de los riesgos que tenga una organización y sus principios son 1) Confidencialidad, quien da garantía de acceso autorizados para tal fin, 2)

Integridad, quien da preservación de la información completa y exacta y 3) Disponibilidad, quien es da garantía de que el usuario accede a la información que necesita en ese preciso momento.

Por otra parte tenemos las normas ISO referente a la seguridad de la información (SI) como la ISO 27000:2021 (2021) la cual nos brinda los términos y definiciones comunes en un sistema de gestión de seguridad de la información (SGSI) aplicado a nivel mundial. La ISO 27001 (2017) es una norma de cumplimiento en organizaciones públicas o privadas que tiene como objetivo salvaguardar los activos de información a través de controles y políticas. La 27002:2017 (2017) nos brinda información de buenas prácticas y controles que se podrían implementar en la gestión de la SI. La 27003:2017 (2017) norma guía que orienta a una efectiva implementación de un SGSI. La 27004:2010 (2010) norma que brinda los parámetros de medición y evaluación la eficacia de la SI. La ISO 27005 (2018) norma proporcione información de la gestión de riesgos de la SI.

La ISO 27006 (2015) a través de esta norma se establece los requisitos de acreditación y certificación de entidades para auditorías. La ISO 27032 (2012) la presente norma busca cerrar las brechas en SI y fortalecer la ciberseguridad de las organizaciones para ello considera la seguridad en la redes, seguridad en internet, seguridad en aplicaciones. La ISO 17799 (2007) dice que la información debido a la interconectividad de los negocios están expuestos amenazas por consiguiente requieren de una protección adecuada, por ello la SI protege a la organización de estas amenazas para garantizar la continuidad del negocio

La teoría de la segunda variable gestión de riesgos según Westerman (2006) el cual es el autor base de esta investigación indicó que una organización están en la capacidad de gestionar riesgos que dan como beneficio una gestión de forma efectiva, considerando que influyen en los riesgos técnicos así como riesgos de tecnología de información, en ese sentido el autor habla de tres disciplinas las cuales son: 1) Proceso de gobernanza del riesgo, políticas completas y efectivas afines con el riesgo, combinadas con un proceso maduro y consistente para identificar, evaluar, priorizar y monitorear los riesgos a lo largo del tiempo. 2) Cultura consciente sobre riesgos, talento humano capacitado que saben cómo identificar y evaluar amenazas e implementar una mitigación de riesgos efectiva.

3) Base de la Tecnología de información eficaz: Infraestructura de TI y aplicaciones que tienen un riesgo inherentemente menor porque están bien diseñadas y bien administradas.

Gerber y Von (2005) adopta un enfoque al análisis de riesgos tradicional, con el cual se analizar los riesgos de los activos tangibles como los intangibles, al respecto Alexander (2007) indica que analizar riesgos es identificar sus amenazas vulnerabilidades basados en los activos, Peltier (2014) define el presente proceso en identificar los riesgos, evaluar la probabilidad de que sucedan y tener medidas para reducirlas.

La Norma ISO 31000 (2018) es un estándar internacional la cual brinda alcances técnicos y metodológicos para la gestión de riesgos la cuales son aplicable en cualquier organización.

Cardona (2008) en su estudio resalta que una gestión de riesgos es un proceso social teniendo como objetivo el de controlar y mitigar el riesgo existentes en la sociedad, además de tomar accione frente amenazas y vulnerabilidad.

Lavado (2020) nos dice que la epistemología estudia los procesos del conocimiento científico y sus resultados.

INCIBE (2015) nos dice que la preocupación por la seguridad inicia con la aparición de los humanos los cuales buscaban seguridad física , ahora la protección y seguridad de la información es relevante para la para nosotros mimos y las organizaciones, se puede resumir que en la etapa Prehistoria cuando aparece el ser humano la protección y seguridad de ellos mismos era en base al uso de armas, en la edad Antigua se dice que a través de la información cifrada llamada jeroglíficos protegían su información, edad Media aparecen las armas, ballestas a fin de dar seguridad de las mercancías, Edad Moderna surgen las armas de fuego y se profesionalizan los ejércitos a fin de dar seguridad a un estado y en la contemporánea puntualmente a finales del siglo XX la seguridad física se va quedando relegada por la importancia de dar seguridad y protección a la información, esto debido a la alta demanda de tecnología, siendo esto un pilar de crecimiento y desarrollo de las organizaciones.

Rosales (2021) en su investigación manifiesta que la gestión de riesgo es comprender eventos simples hasta entender que el humano es la influencia principal de construir escenarios de riesgos, desde que se tiene claro lo mencionado la Asamblea General de la Organización de las Naciones Unidas hace 40 años ha desarrollado documentación para atender las consecuencias de eventos adversos y menciona también que desde inicios del siglo XXI es importante fortalecer la educación y formación en un pensamiento basado en gestión de riesgos.

III. METODOLOGÍA

Según Bernal (2010), manifiesta que en una investigación o estudio la metodología es un conjunto de aspectos operativos indispensables.

3.1. Tipo y diseño de investigación

Tipo de investigación: Para Concytec (2018) la investigación es de tres tipos: básica, aplicada y experimental, la básica se enfoca al entender las características principales de los fenómenos, hechos observables o relaciones entre sujetos.

Hernández, Fernández, y Baptista (2014), investigar científicamente es un proceso organizado que tiene como objeto generar conocimiento o teorías esto en base a la investigación básica y dar solución a conflictos a través de la investigación aplicada.

Gallardo (2017) indica que la investigación es de pura o básica el cual tiene el propósito de desarrollar teoría.

En ese sentido la presente investigación fue básica, dado que la finalidad es generar conocimiento, tomando como base la información o hechos en una entidad del sistema electoral, la cual servirá para la comprobación de la hipótesis planteada.

Diseño de investigación: Según Hernández et. al (2014), diseño de investigación es un curso de acción que el investigador ejecuta para tener información, analizarla y obtener una respuesta al problema de investigación. Los diseños de investigación pueden ser de tipo experimental y no experimental, el experimental involucra manipulación de las variables y analizar los resultados y/o consecuencias estas se extienden con tipo transversal, longitudinal o evolutivo, sin embargo el diseño no experimental transeccional o transversal nos dice que a través de la observación se estudia el comportamiento de las variables sin manipularlas o modificarlas, la recolección de información es la fotografía del momento, se inicia la

descripción de las variables y análisis de incidencias y la interrelación de las mismas. Respecto al enfoque cuantitativo nos dice que mediante la recolección de datos se obtendrá medición numérica y estadística la cual servirá para contrastar la hipótesis y validar la teoría y respecto al alcance correlacional indica que esta busca saber la magnitud de asociación entre variables.

En ese sentido el presente trabajo de investigación fue realizado con las siguientes características: tipo de investigación básica, diseño no experimental transeccional, alcance descriptivo – correlacional, enfoque cuantitativo.

3.2. Variables y operacionalización

Para la variable uno se definió lo siguiente:

- **Definición conceptual**:

  Var1 - Seguridad de la información para Soriano (2014) define que son medios preventivos aplicados a salvaguardar, resguardar la información y los sistemas utilizando los principios básicos como la confidencialidad, integridad y disponibilidad.

- **Definición operacional:** En ese sentido del concepto del autor se definieron las dimensiones: a) La confidencialidad es proteger la información, evitar su divulgación con entidades o individuos no autorizados, solo pueden acceder a ella los que tengas los permisos respectivos. b) La integridad es proteger los datos de modificaciones, eliminaciones, duplicados, entre otros de personas o entidades no autorizadas. c) La disponibilidad es acceder a la información en el momento que se requiere, garantizar a los usuarios el acceso a la información.

- **Indicadores:** Para la dimensión confidencialidad se establecieron los siguientes indicadores: 1. Protección de la Información, 2. Accesos, 3. Redes, 4.Técnicas Criptográficas, 5. Información Crítica, 6. Claves y/o Contraseñas.

Para la dimensión integridad se establecieron los siguientes indicadores: 1. Protección de Datos, 2. Fiabilidad de Recursos. 3. Ataque, 4. Almacenamiento, 5. Sistemas de Información, 6.Técnicas Criptográficas. Para la dimensión disponibilidad se establecieron los siguientes indicadores: 1. Acceso a la Información, 2. Sistemas de Información, 3.Aspectos Técnicos, 4. Fenómenos Naturales, 5. Causas Humanas, 6. Voluntad.

Para la variable dos se definió lo siguiente:

- **Definición conceptual:**

  Var2 - Gestión del riesgo, según Westerman (2006) indica que a través de la globalización las organizaciones deberían estar en la capacidad de gestionar riesgos que dan como beneficio una gestión de forma efectiva, considerando que actualmente son atacados por riesgos técnicos y de tecnología de información. En ese sentido una gestión eficaz del riesgo es la aplicación coordinada del Proceso de Gobernanza de Riesgos, Cultura Consciente del Riesgo y Base de la Tecnología de la Información Eficaz.
- **Definición operacional:**

  Por ello se determinaron las siguientes dimensiones: 1) Proceso de gobernanza del riesgo, políticas completas y efectivas afines con el riesgo, combinadas con un proceso maduro y consistente para identificar, evaluar, priorizar y monitorear los riesgos a lo largo del tiempo. 2) Cultura consciente sobre riesgos, talento humano capacitado que saben cómo identificar y evaluar amenazas e implementar una mitigación de riesgos efectiva. 3) Base de la Tecnología de información eficaz: Infraestructura de TI y aplicaciones que tienen un riesgo inherentemente menor porque están bien diseñadas y bien administradas.
- **Indicadores:**

  Para la dimensión Proceso de gobernanza del riesgo se establecieron los siguientes indicadores: 1. Política de Riesgo, 2. Eficacia 3. Proceso, 4.Identificar Riesgos, 5. Evaluar Riesgos, 6. Prioriza Riesgos, 7.Monitorea Riesgos.

Para la dimensión Cultura consciente sobre riesgos se establecieron los siguientes indicadores: 1. Capacitación, 2. Conocimiento 3. Identificar Amenazas, 4. Evaluar Amenazas, 5.Implementación Eficaz.

Para la dimensión Base de la Tecnología de la información eficaz se establecieron los siguientes indicadores: 1. Infraestructura, 2. Aplicaciones, 3.Riesgo, 4. Diseño, 5. Administrar.

- **Escala de medición:** Para ambas variables Según Bernal (2010) se tienen cuatro niveles de medición ordinal, nominal, de proporción e intervalos, siendo la ordinal un ordenamiento por prioridades siendo ascendente o descendente, para la presente investigación todos los indicadores (diecisiete) y sus items y/o preguntas (dieciocho) son de tipo de medición ordinal y su codificación fue de la siguiente manera: Nunca y su código 1, Casi nunca y su código 2, A veces y su código 3, Casi siempre y su código 4, Siempre y su código 5.

3.3. Población , muestra y muestreo

Población: Para Hernández et. al (2014) la población y su delimitación se caracteriza por que sus componentes tienen los mismos atributos y especificaciones. Es por consiguiente que para la presente investigación se estableció como población a los cuarenta y cinco (45) colaboradores de una Dirección de una entidad del sistema electoral que según ROF RENIEC (2021) en su artículo 49 se les da atribuciones en materia electoral entre ellas coordinar con los organismos del Sistema Electoral.

Definido la población en el párrafo precedente se consideró los siguientes Criterios:

- **Criterios de inclusión:** Los servidores de diferentes modalidades contractual o régimen laboral, supervisores, abogados, verificadores de firmas, técnicos, asistentes administrativos, analistas.
- **Criterios de exclusión:** Para el personal de soporte seguridad y limpieza dado que el enfoque de las preguntas o items están relacionados al uso y acceso de tecnología utilizada a diario por los colaboradores.

Muestra: Bernal (2010) la muestra representa a la población siempre y cuando los elementos de estas tengan las mismas características En ese sentido para la presente investigación la muestra será el total de la población, dado que la población es pequeña, por ello se aplicará el instrumento de medición a los cuarenta y cinco (45) servidores civiles de una entidad del sistema electoral

Según Hernández, Fernández y Baptista (2014) dice que no necesariamente se realizan estudios con una muestra, también es necesario, si el escenario lo requiere realizar censo a toda la población además la unidad de análisis son los componentes de la misma.

Muestreo : Arias (2006) nos dice que tenemos dos tipos de muestreo, en el probabilístico o aleatorio cualquier integrante de la población puede ser seleccionado dado que este integrante tiene características en común y representativa de la población sin embargo en un muestreo no probabilístico es un proceso de selección sin probabilidad donde la elección es arbitraria, muestreo intencional donde el investigador tiene un previo conocimiento y la decisión de juicio si el elemento forma de la parte de la muestra o no y el muestreo por cuotas donde la elección es a través de la conformación de grupos proporcionales de características similares.

En ese sentido se utilizó el muestreo censal, porque la población en su totalidad está conformado por cuarenta y cinco servidores civiles todos con los mismos atributos o características a los cuales se les aplicó un instrumento de medición, y que su aplicación en su totalidad era más certera que al aplicar una muestra, dado que se están considerando todas los datos de los componentes.

3.4. Técnicas e instrumentos de recolección de datos

La técnica utilizada en esta investigación fue la encuesta, que para Gallardo (2017), nos dice que la encuesta sirve para recolectar información de algún componente de la muestra o de la población en su totalidad, las cuales pueden ser orales o escritas. Se recolectó información de los servidores civiles respecto al tema de estudio, está encuesta consto de 18 preguntas por cada variable, relacionados a sus dimensiones e indicadores.

Hernández et al. (2014), dice que los instrumentos de medición deben cumplir algunos requisitos como la confiabilidad que significa si se aplica en forma repetida el instrumento de medición al componente de la muestra o población, estos resultados no pueden variar, debiendo ser coherentes y consistentes, respecto a la validez también dice que el instrumento debe garantizar que fue diseñado para medir la variable de estudio y evitar desviación en su medida y la objetividad está más enfocada al investigador donde sus tendencias o creencias no afectan al instrumento en su etapa de recolección y análisis de datos , por consiguiente el instrumento de medición debe cumplir los tres requisitos en mención, para ello en la práctica de la investigación se recurrió a la validación de expertos que según Hernández et al. (2014), dice que es el grado que un instrumente mide la variables de investigación de acuerdo a opiniones calificadas llamados expertos en la materia o a fin de la investigación.

Bernal (2010), dice que la encuesta tiene como base a los cuestionarios y/o preguntas. Sánchez, Reyes y Mejía (2018) coincide en el concepto de confiabilidad siendo su sinónimo la fiabilidad es decir un instrumentos que se aplique varias veces al mismo componente de la muestra o población dará el mismo resultado, por ello dicen que el alfa de Cronbach es un formula o procedimiento estadístico que tiene un rango de medición de -1 a +1 y el cual estima el nivel de confiabilidad por consistencia interna de un instrumento de recolección de datos, esto siendo aplicable en respuestas politónicas es decir que admiten dos o más respuestas.

En ese sentido el cuestionario fue procesada por un software estadístico SPPS a fin de obtener su alfa Cronbach que para Celina y Campo Arias (2005) es un indicador que mide la fiabilidad de consistencia interna a través de la correlación de las preguntas del instrumento recolector de datos, por ello de una prueba piloto de obtuvo el resultado de 0,965 para el cuestionario de la variable Seguridad de la Información y 0,905 para el cuestionario de la variable Gestión del Riesgo, evidenciando un alto grado de confiabilidad.

3.5. Procedimientos

La presente investigación dio a conocer a la entidad a través de una Carta de Presentación N° Carta P.262-2021-II EPG-UCV LE con fecha 20 de Octubre del 2021 la cual fue recibida el 17 de Noviembre del 2021 en ella se solicitó a la entidad las facilidades para la recolección de la información la cual fue aprobada, responde con la Carta N° 00627-2021/GRE/RENIEC con fecha 16 de Diciembre del 2021.

Por consiguiente se procedió a realizar el levantamiento de información con los cuarenta y cinco colaboradores parte de la muestra censal, se les explico la finalidad de la investigación la justificación práctica y social de la misma.

3.6. Método de análisis de datos

Bernal (2010) nos dice que el procesamiento de la información consiste en la organización de la data recolectada de los componentes a través de herramientas estadísticas y con la ayuda del computador, para que el caso del presente estudio se hizo lo siguiente:

Una vez obtenido los antecedentes de investigación y autores bases teóricos de nuestras variables se estableció las dimensiones e indicadores de medición ordinal que para Bernal (2010) es un ordenamiento por prioridades, se realizó la validación y la confiabilidad, la confiablidad se aplicó el alfa de Cronbach que para Celina y Campo Arias (2005) lo define

de un indicador que mide la fiabilidad de consistencia interna a través de la correlación de las interrogantes del instrumento recolector de datos; también indica que el valores aceptables para el coeficiente de alfa de Cronbach es de 0,70 a 0.90, debajo de ese rango se considera que existe una consistencia interna baja y por encima del valor redundancia en los items o preguntas; y la validación se realizó con tres expertos con maestría y experiencia en la Gestión Pública como son el Dr. Marco Antonio Candia Menor el Dr. Javier Fernando Díaz Molinari y el Magister Luis Enrique León Alvarado.

El cuestionario se realizó en el formato Google Form y fue completado por encuestados en forma virtual, se trasladó esta la información al aplicativo estadístico IBM SPSS STASTICS versión 26 para su procesamiento estadístico descriptivo e inferencial, sin embargo previamente con la ayuda de la hoja de cálculo de Microsoft Excel se aplicó el Baremos para las variables y sus dimensiones bajo un enfoque ordinal se estableció los siguientes niveles:

Para la Variable Seguridad de la Información, nivel bajo en el rango de 18 a 41, medio en el rango de 42 a 65, nivel alto en el rango de 66 a 90 y sus dimensiones confidencialidad, nivel bajo en el rango de 6 a 13, medio en el rango de 14 a 21, nivel alto en el rango de 22 a 30; para la dimensión integridad , nivel bajo en el rango de 6 a 13, medio en el rango de 14 a 21, nivel alto en el rango de 22 a 30; para la dimensión disponibilidad , nivel bajo en el rango de 6 a 13, medio en el rango de 14 a 21, nivel alto en el rango de 22 a 30.

En la variable Gestión del Riesgo, nivel bajo en el rango de 18 a 41, medio en el rango de 42 a 65, nivel alto en el rango de 66 a 90 y sus dimensiones, Proceso de gobernanza del riesgo, nivel bajo en el rango de 8 a 18, medio en el rango de 19 a 29, nivel alto en el rango de 30 a 40; para la dimensión Cultura consciente sobre riesgos, nivel bajo en el rango de 5 a 11, medio en el rango de 12 a 18, nivel alto en el rango de 19 a 25; para la dimensión

Base de la Tecnología de la información eficaz , nivel bajo en el rango de 6 a 13, medio en el rango de 14 a 21, nivel alto en el rango de 22 a 30.
Con la información en SPSS y los niveles ya establecidos se procedió a realizar la estadística descriptiva que según Hernández et al. (2014) es la representación de los tablas y gráficos de frecuencia de datos agrupados por cada variable con dimensión (univariado) y variable con dimensión (Bivariado), en ese sentido Echaiz (2018) nos dice que un análisis univariado es cuando las variables se analizan por separado por ejemplo realizando tabla de frecuencias, y para el análisis Bivariado previamente se elaboran tablas cruzadas es decir la relación de la variable 1 con la variable 2 o las dimensiones de la variable 1 con la variable 2.

Luego se procedió a realizar la prueba de normalidad de Shapiro Wilk que para Flores y Flores (2021) la prueba de normalidad es un procedimiento que busca garantizar que los resultados estadísticos mantengan una distribución normal de los datos que significa que la moda, mediana, y media aritmética tengan el misma valor, además que gráficamente el pico de la campana se encuentre en la parte central y la data se desplace de manera uniforme por los lados, respecto a la prueba de normalidad de Shapiro Wilk es una prueba que se utilizó para verificar la normalidad cuando la muestra es menor a 50 registros , esto inicia con el ordenamiento de la data y se rechaza la hipótesis nula de normalidad, si el estadístico Shapiro Wilk es menor que el valor 0.05 para el tamaño de la muestra y el nivel de significancia dado se tiene que aplicar Correlación Rho de Spearman o Pearson que para Mondragón (2014) son técnicas estadísticas bivariadas de la estadística inferencial que para Hernández et al. (2014), es la estadística que permite probar las hipótesis y determinar los parámetros o la distribución de la data.

La contratación de la hipótesis se aplicó la correlación que para Mondragón (2014) es la correspondencia recíproca de intensidad y relación entre dos variables.

Según analizando los valores obtenidos de la prueba de normalidad de Shapiro Wilk la presente investigación correspondió aplicar Rho de spearman que para Mondragón (2014) es determinar el sentido y nivel de relación entre dos variables cuantitativas según los rangos establecido por el autor como:

Correlación Negativa: Rango de -0.91 a 1.00 es una Correlación negativa perfecta; Rango de -0.76 a 0.90 es una Correlación negativa muy fuerte; Rango de -0.51 a -0.75 es una Correlación negativa considerable; Rango de -0.11 a -0.50 es una Correlación negativa media; Rango de -0.01 a -0.10 es una Correlación negativa débil.

Sin Correlación: Rango 0.00 es sin Correlación.

Correlación Positiva: Rango de +0.01 a 0.10 es una Correlación positiva débil; Rango de +0.11 a 0.50 es una Correlación positiva media; Rango de +0.51 a + 0.75 es una Correlación positiva considerable; Rango de +0.76 a +0.90 es una positiva muy fuerte; Rango de +0.91 a + 1.00 es una positiva perfecta.

3.7. Aspectos éticos

Millan (2017) nos dice que la No Maleficencia es la no generación de daño a los participantes en la investigación tales como los encuestados, asesores, investigadores, entre otros asimismo indica que el daño no solamente es de un aspecto físico sino también desde un enfoque intangible es decir el obstaculizar, impedir la personas ejerzan su legítimo derecho, respecto a Beneficencia indica que prima el comportamiento ético con los sujetos de la investigación, la investigación va dirigida al grupo de personas o el colectivo social que lo enmarca, una principio de la investigación es la priorización del ser humano ante el contexto o fin de la investigación.

En ese sentido como investigador se ha tenido el mayor cuidado con las acciones al levantamiento de la información y la redacción de la tesis

además que existe una justificación social de la presente investigación, donde prima la creación del valor público.

Martin (2013) respecto a la autonomía es la capacidad de decisión del investigar de desarrollar libremente sin coacción o manipulación externa, respecto a la justicia manifiesta que es un principio de igualdad en ese sentido, se respetó el derecho de autor y su propiedad intelectual, usando como referencias las normas APA, y como soporte tecnológico se utilizara el aplicativo Turnitin para encontrar y prevenir posibles similitudes y copias, además a todos el proceso de la investigación primó la igualdad y respeto y se evitó poner en riesgo y/o mostrar su identidad.

IV. RESULTADOS

Análisis Univariado

Tabla 1

Variable1 : Seguridad de la Información

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Medio	7	15,6	15,6
	Alto	38	84,4	100,0
	Total	45	100,0	

Fuente: Cuestionario Seguridad de la Información

Figura 1

Variable 1: Seguridad de la Información

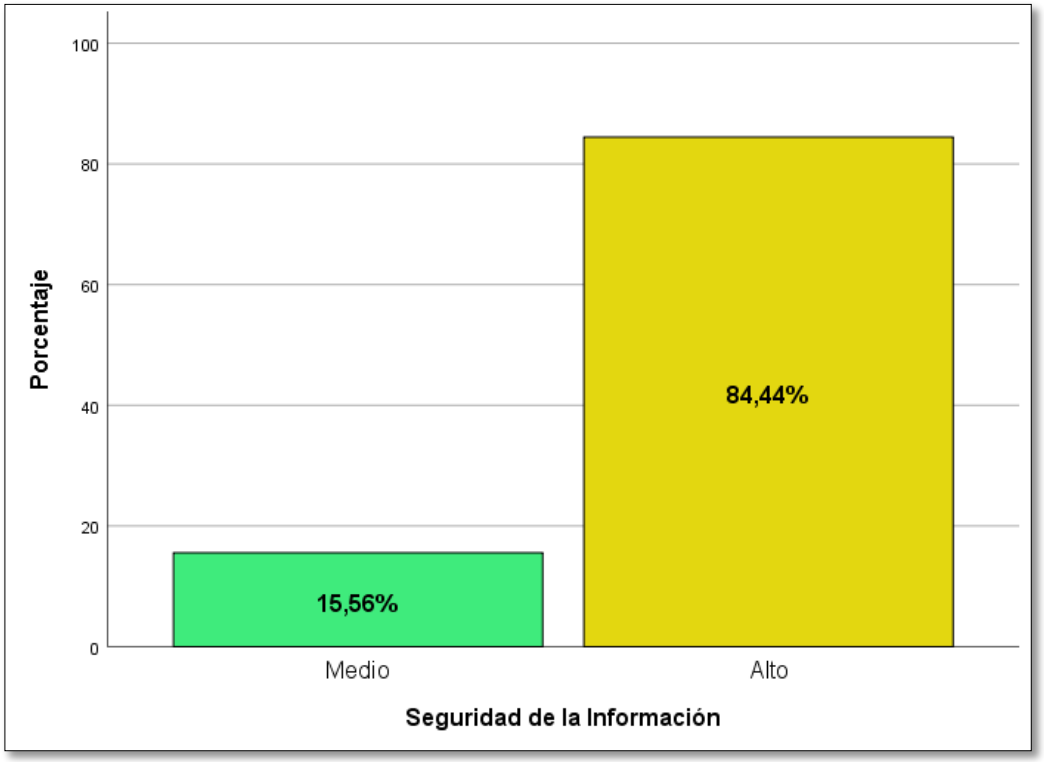


Figura 1 Seguridad de la Información

Se determina de la Tabla 1 y Figura 1 que los colaboradores encuestados de una entidad del sistema electoral, expresan que la Seguridad de la Información tiene un nivel Alto de 84.44% y un nivel medio de 15.56%.

Tabla 2

Dimensión 1 Confidencialidad de la Variable Seguridad de la información

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Medio	18	40,0	40,0
	Alto	27	60,0	100,0
	Total	45	100,0	

Fuente: Cuestionario Seguridad de la Información

Figura 2

Dimensión 1 Confidencialidad de la Variable Seguridad de la información

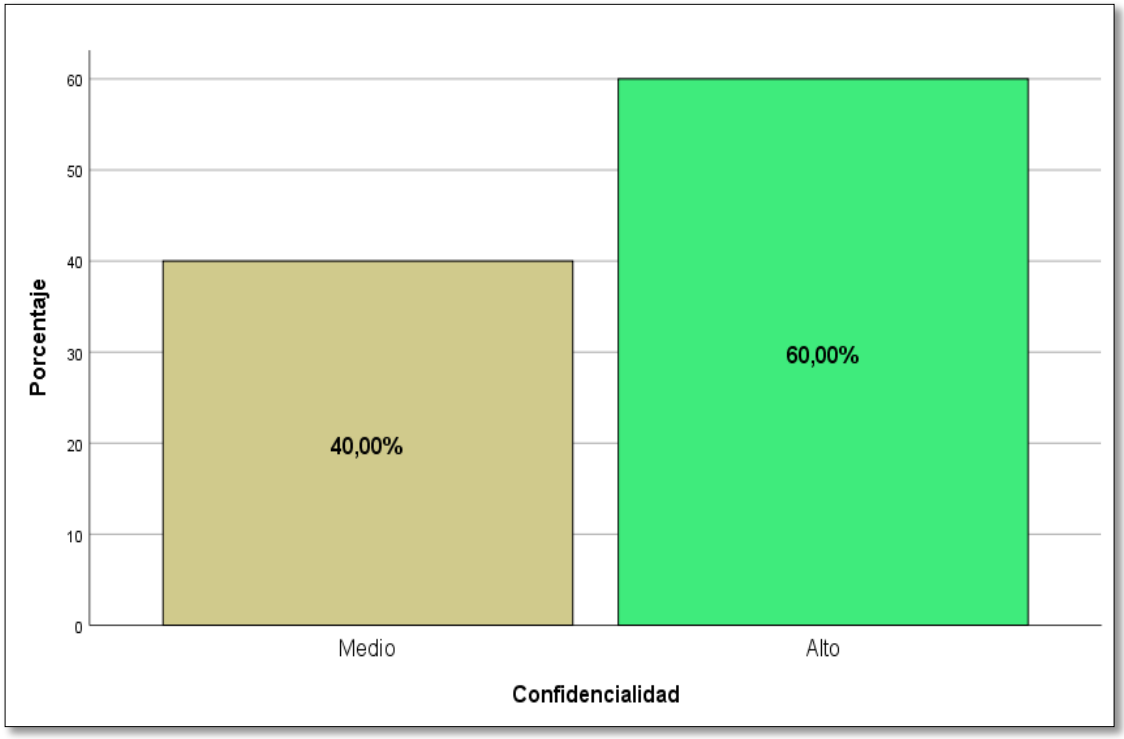


Figura 2 Confidencialidad

Se determina de la Tabla 2 y Figura 2, que los colaboradores encuestados de una entidad del sistema electoral consideran que la dimensión Confidencialidad de la variable Seguridad de la Información es Alto con un 60% y Medio con 40%.

Tabla 3

Dimensión 2 Integridad de la Variable Seguridad de la Información

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Medio	12	26,7	26,7
	Alto	33	73,3	100,0
	Total	45	100,0	

Fuente: Cuestionario Seguridad de la Información

Figura 3

Dimensión 2 Integridad de la Variable Seguridad de la Información

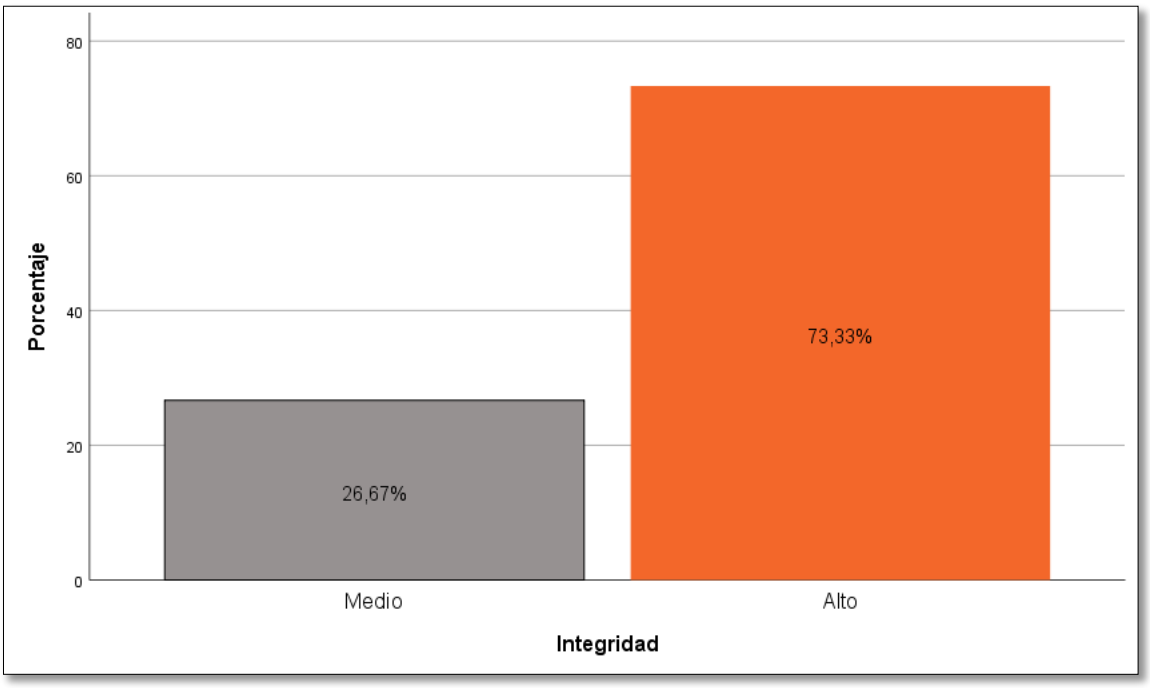


Figura 3 Integridad

Se determina de la Tabla 3 y Figura 3, que los colaboradores encuestados de una entidad del sistema electoral consideran que la dimensión Integridad de la variable Seguridad de la Información es Alto con un 73.33% y Medio con 26.67%.

Tabla 4

Dimensión 3 Disponibilidad de la variable Seguridad de la Información

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Medio	8	17,8	17,8
	Alto	37	82,2	100,0
	Total	45	100,0	

Fuente: Cuestionario Seguridad de la Información

Figura 4

Dimensión 3 Disponibilidad de la variable Seguridad de la Información

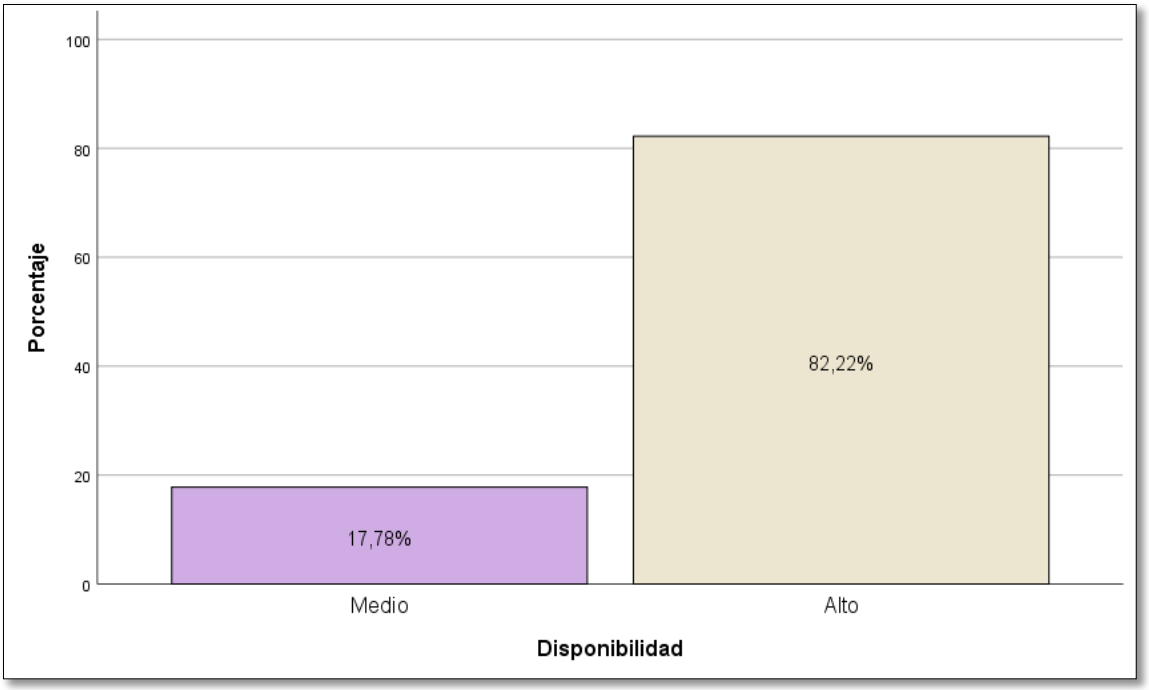


Figura 4 Integridad

Se determina de la Tabla 4 y Figura 4, que los colaboradores encuestados de una entidad del sistema electoral consideran que la dimensión Disponibilidad de la variable Seguridad de la Información es Alto con un 82.22% y Medio con 17.78%.

Tabla 5

Variable 2 Gestión del Riesgo

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Medio	9	20,0	20,0
	Alto	36	80,0	100,0
	Total	45	100,0	

Fuente: Cuestionario Gestión del Riesgo

Figura 5

Variable 2 Gestión del Riesgo

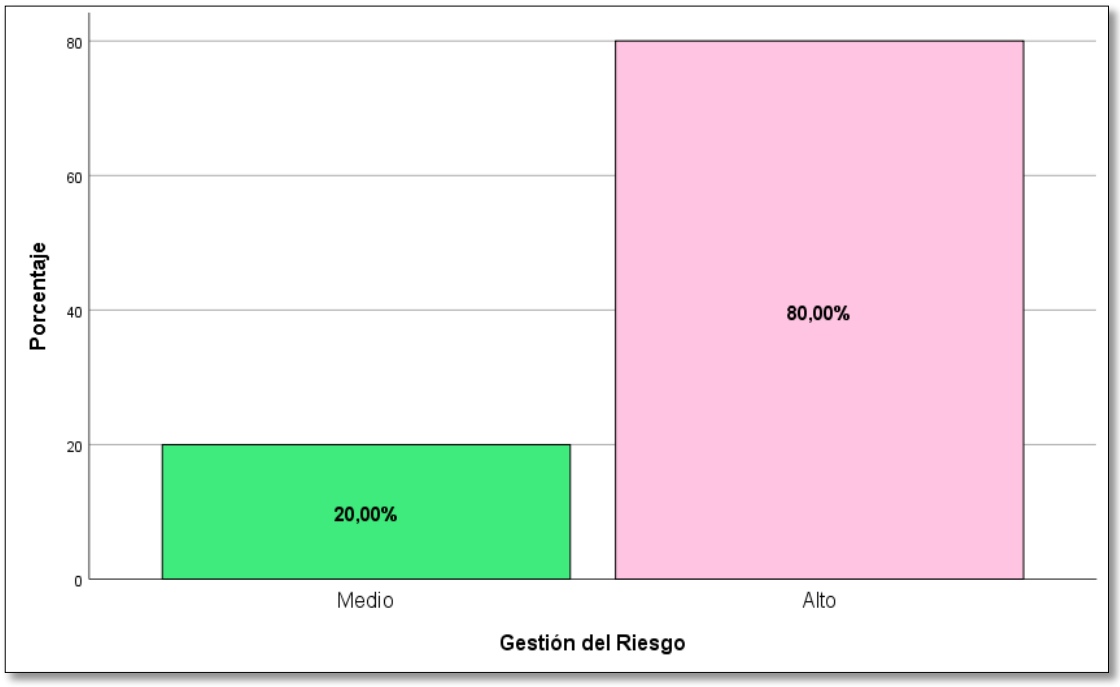


Figura 5 Gestión del Riesgo

Se determina de la Tabla 5 y Figura 5, que los colaboradores encuestados de una entidad del sistema electoral consideran que la variable Gestión del Riesgo es Alto con un 80 % y Medio con 20%.

Tabla 6

Dimensión 1 Proceso de Gobernanza de Riesgos de la variable Gestión del Riesgo

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Medio	16	35,6	35,6
	Alto	29	64,4	100,0
	Total	45	100,0	

Fuente: Cuestionario Gestión del Riesgo

Figura 6

Dimensión 1 Proceso de Gobernanza de Riesgos de la variable Gestión del Riesgo

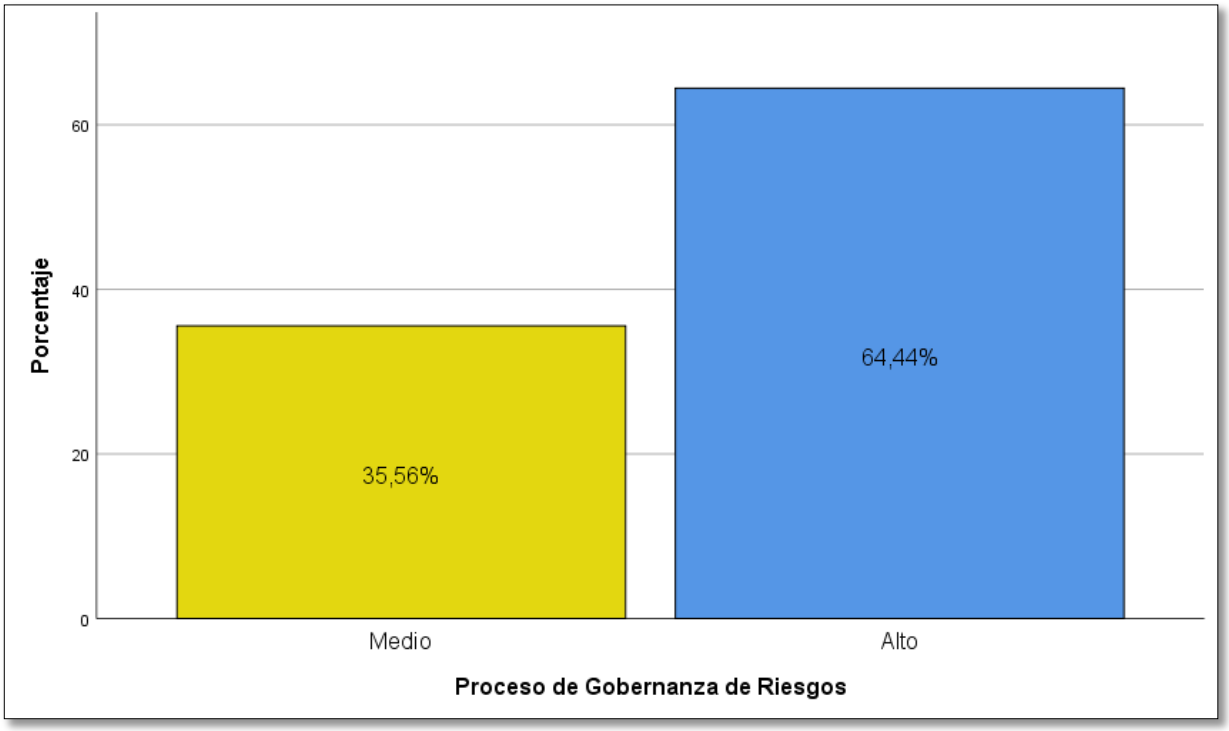


Figura 6 Proceso de Gobernanza de Riesgos

Se determina de la Tabla 6 y Figura 6, que los colaboradores encuestados de una entidad del sistema electoral consideran que la dimensión Proceso de Gobernanza de Riesgos de la variable Gestión del Riesgo es Alto con un 64.44% y Medio con 35.56%.

Tabla 7

Dimensión 2 Cultura consciente del Riesgo de la variable Gestión del Riesgo

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Medio	9	20,0	20,0
	Alto	36	80,0	100,0
	Total	45	100,0	

Fuente: Cuestionario Gestión del Riesgo

Figura 7

Dimensión 2 Cultura consciente del Riesgo de la variable Gestión del Riesgo

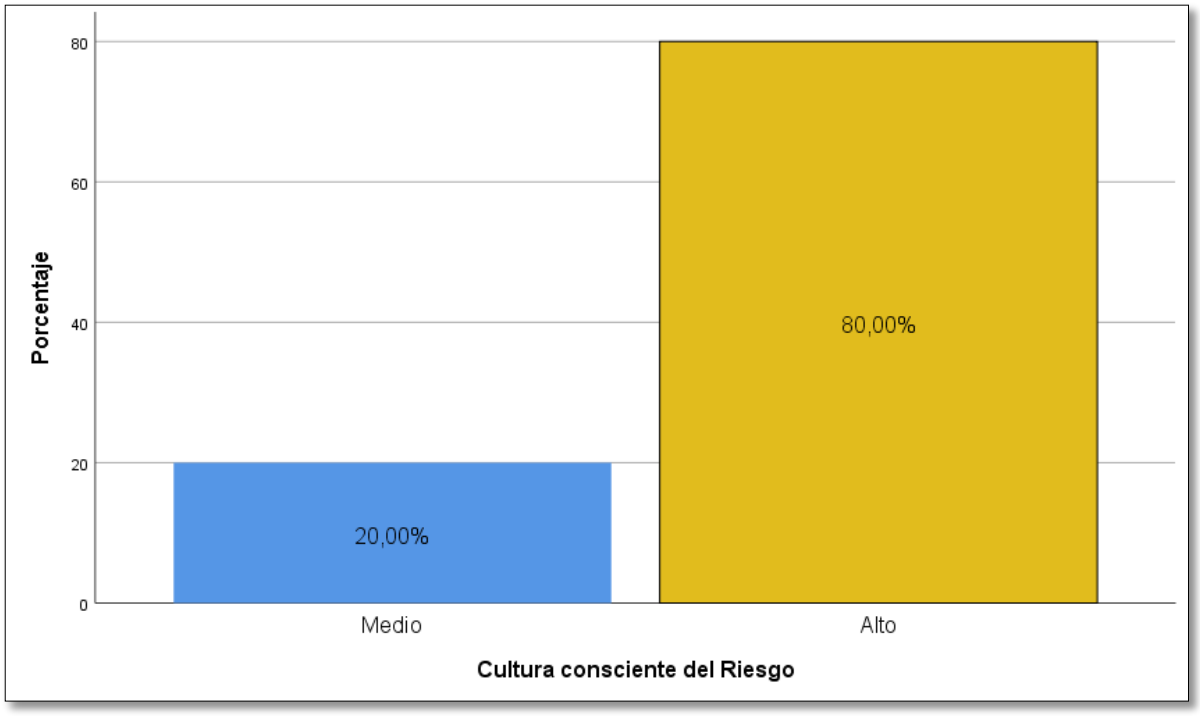


Figura 7 Cultura consciente del Riesgo

Se determina de la Tabla 7 y Figura 7, que los colaboradores encuestados de una entidad del sistema electoral consideran que la dimensión Cultura Consciente del Riesgo de la variable Gestión del Riesgo es Alto con un 80% y Medio con 20%.

Tabla 8

Dimensión 3 Base de Tecnología de la Información Eficaz de la variable Gestión del Riesgo

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Medio	12	26,7	26,7
	Alto	33	73,3	100,0
	Total	45	100,0	

Fuente: Cuestionario Gestión del Riesgo

Figura 8

Dimensión 3 Base de Tecnología de la Información Eficaz de la variable Gestión del Riesgo

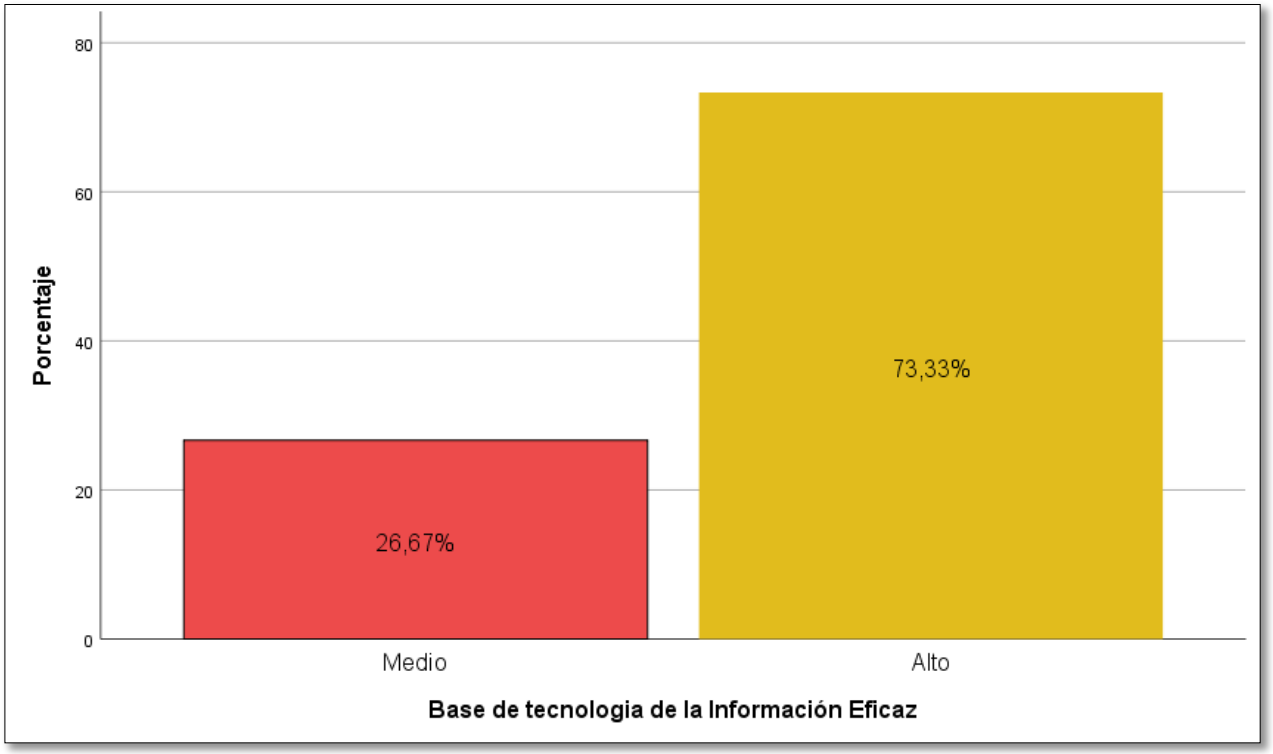


Figura 8 Base de Tecnología de Información Eficaz

Se determina de la Tabla 8 y Figura 8, que los colaboradores encuestados de una entidad del sistema electoral consideran que la dimensión Base de Tecnología de la Información Eficaz de la variable Gestión del Riesgo es Alto con un 73.33% y Medio con 26.67%.

Análisis Bivariado

Tabla 9

*Tabla Cruzada Variable 1 Seguridad de la Información * Variable 2 Gestión del Riesgo*

			Variable 2 Gestión del Riesgo		Total
			Medio	Alto	
Variable 1 Seguridad de la Información	Medio	Recuento	6	1	7
		% del total	13,3%	2,2%	15,6%
	Alto	Recuento	3	35	38
		% del total	6,7%	77,8%	84,4%
Total		Recuento	9	36	45
		% del total	20,0%	80,0%	100,0%

Fuente: Cuestionario de Seguridad de la Información y Gestión del Riesgo

Del análisis cruzado de las variable 1 Seguridad de la Información y de la Variable 2 Gestión del Riesgo los colaboradores de una entidad del sistema electoral manifestaron que existe una relación Media de 13,3 % y Alto de 77.8% sin embargo también podemos evidenciar que cuando la Seguridad de la Información está en un nivel Medio y la Gestión del Riesgo es alto el valor es de 2.2% y cuando la Seguridad de la Información está en nivel Alto y la Gestión del Riesgo está en un nivel Medio el valor es de 6.7%.

Tabla 10

*Tabla cruzada Dimensión 1 Confidencialidad * Variable 2 Gestión del Riesgo*

			Variable 2 Gestión del Riesgo		*Total*
			Medio	Alto	
Dimensión 1 Confidencialidad	Medio	Recuento	5	13	18
		% del total	11,1%	28,9%	40,0%
	Alto	Recuento	4	23	27
		% del total	8,9%	51,1%	60,0%
Total		Recuento	9	36	45
		% del total	20,0%	80,0%	100,0%

Fuente: Cuestionario de Seguridad de la Información y Gestión del Riesgo

Del análisis cruzado de las Dimensión 1 Confidencialidad de la Variable 1 Seguridad de la Información con de la Variable 2 Gestión del Riesgo los colaboradores de una entidad del sistema electoral manifestaron que existe una relación Media de 11,1 % y Alto de 51.1% sin embargo también podemos evidenciar que cuando la Confidencialidad está en un nivel Medio y la Gestión del Riesgo es alto el valor es de 28.9% y cuando la Confidencialidad está en nivel Alto y la Gestión del Riesgo está en un nivel Medio el valor es de 8.9%.

Tabla 11

*Tabla cruzada Dimensión 2 Integridad * Variable 2 Gestión del Riesgo*

			Variable 2 Gestión del Riesgo		Total
			Medio	Alto	
Dimensión 2 Integridad	Medio	Recuento	8	4	12
		% del total	17,8%	8,9%	26,7%
	Alto	Recuento	1	32	33
		% del total	2,2%	71,1%	73,3%
Total		Recuento	9	36	45
		% del total	20,0%	80,0%	100,0%

Fuente: Cuestionario de Seguridad de la Información y Gestión del Riesgo

Del análisis cruzado de las Dimensión 2 Integridad de la Variable 1 Seguridad de la Información con de la Variable 2 Gestión del Riesgo los colaboradores de una entidad del sistema electoral manifestaron que existe una relación Media de 17,8% y Alto de 71.1% sin embargo también podemos evidenciar que cuando la Integridad está en un nivel Medio y la Gestión del Riesgo es alto el valor es de 8.9% y cuando la Integridad está en nivel Alto y la Gestión del Riesgo está en un nivel Medio el valor es de 2.2%.

Tabla 12

*Tabla cruzada Dimensión 3 Disponibilidad * Variable 2 Gestión del Riesgo*

			Variable 2 Gestión del Riesgo		Total
			Medio	Alto	
Disponibilidad	Medio	Recuento	6	2	8
		% del total	13,3%	4,4%	17,8%
	Alto	Recuento	3	34	37
		% del total	6,7%	75,6%	82,2%
Total		Recuento	9	36	45
		% del total	20,0%	80,0%	100,0%

Fuente: Cuestionario de Seguridad de la Información y Gestión del Riesgo

Del análisis cruzado de las Dimensión 3 Disponibilidad de la Variable 1 Seguridad de la Información con de la Variable 2 Gestión del Riesgo los colaboradores de una entidad del sistema electoral manifestaron que existe una relación Media de 13,3% y Alto de 75.6% sin embargo también podemos evidenciar que cuando la Disponibilidad está en un nivel Medio y la Gestión del Riesgo es alto el valor es de 4.4% y cuando la Disponibilidad está en nivel Alto y la Gestión del Riesgo está en un nivel Medio el valor es de 6.7%.

Contrastación de Hipótesis

Pruebas de normalidad

Para la prueba de normalidad se utilizó el procedimiento estadístico de Shapiro Wilk, este procedimiento es adecuado en relación a la cantidad poblacional que para el presente estudio es de 45 encuestados el cual es inferior al valor 50, donde:

H0. La muestra proviene de una distribución normal.

H1. La muestra no proviene de una distribución normal.

Regla:

Sig. < 0,05 rechazar H0

Sig. > 0,05 aceptar H0

Tabla 1

Prueba de Normalidad Shapiro - Wilk

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Sistema de Seguridad de la Información	,947	45	,039
Gestión del Riesgo	,956	45	,085

Fuente: Elaboración Propia

Según Tabla 13, determina que al obtener los valores p=0,039 <0.05 se procederá a validar el criterio de cumplimiento que es negar al H0 y validar que la muestra no proviene de una distribución normal, muestra no paramétrica, por consiguiente se aplica el índice de Rho Spearman.

Prueba de Hipótesis General

Ho= La seguridad de la Información no se relaciona con la gestión del riesgo en una entidad del sistema electoral, año 2021.

Hg= La seguridad de la Información se relaciona con la gestión del riesgo en una entidad del sistema electoral, año 2021.

Tabla 14

Correlación de la Variable 1 Seguridad de la Información y la variable 2 Gestión del Riesgo

			Seguridad de la Información Var1	Gestión del Riesgo Var2
Rho de Spearman	Seguridad de la Información Var1	Coeficiente de correlación	1,000	,924**
		Sig. (bilateral)	.	,000
		N	45	45
	Gestión del Riesgo Var2	Coeficiente de correlación	,924**	1,000
		Sig. (bilateral)	,000	.
		N	45	45

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

Interpretando la Tabla 14 de correlaciones se determina que el nivel de significancia – sig.=0,000 en consecuencia al ser menor a 0.05, se debe rechazar la hipótesis nula - H0 y aceptar la HG - Hipótesis General la cual es, la seguridad de la Información se relaciona con la gestión del riesgo en una entidad del sistema electoral, año 2021, siendo esta relación de un nivel Alto o correlación positiva perfecta, dado que tiene un valor Rho de Spearman de 0.924.

Prueba de Hipótesis Especifica 1 – Confidencialidad

Ho= La Confidencialidad de la Seguridad de la Información no se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021

He1= La Confidencialidad de la Seguridad de la Información se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021

Tabla 15

Correlación de la dimensión Confidencialidad de la seguridad de información y la gestión del riesgo

			Confidencialidad	Gestión del Riesgo
Rho de Spearman	Confidencialidad	Coeficiente de correlación	1,000	,589**
		Sig. (bilateral)	.	,000
		N	45	45
	Gestión del Riesgo	Coeficiente de correlación	,589**	1,000
		Sig. (bilateral)	,000	.
		N	45	45

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

Interpretando la Tabla 15 de correlaciones se determina que el nivel de significancia – sig.=0,000 en consecuencia al ser menor a 0.05, se debe rechazar la hipótesis nula H0 y aceptar la Hipótesis Especifica 1 la cual es, La Confidencialidad de la Seguridad de la Información se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021, siendo esta relación o correlación positiva considerable dado que tiene un valor Rho de Spearman de 0.589.

Prueba de Hipótesis Específica 2 – Integridad

Ho= La Integridad de Seguridad de la Información no se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021

He2= La Integridad de Seguridad de la Información se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021

Tabla 16

Correlación de la dimensión Integridad de la seguridad de información y la gestión del riesgo

			Integridad	Gestión del Riesgo
Rho de Spearman	Integridad	Coeficiente de correlación	1,000	,886**
		Sig. (bilateral)	.	,000
		N	45	45
	Gestión del Riesgo	Coeficiente de correlación	,886**	1,000
		Sig. (bilateral)	,000	.
		N	45	45

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

Interpretando la Tabla 16 de correlaciones se determina que el nivel de significancia – sig.=0,000 en consecuencia al ser menor a 0.05, se debe rechazar la hipótesis nula H0 y aceptar la Hipótesis Especifica 1 la cual es, La Integridad de Seguridad de la Información se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021, siendo esta relación o correlación positiva muy fuerte, dado que tiene un valor Rho de Spearman de 0.886.

Prueba de Hipótesis Específica 3 - Disponibilidad

Ho= La Disponibilidad Seguridad de la Información no se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021.

He3= La Disponibilidad Seguridad de la Información se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021.

Tabla 17

Correlación de la dimensión disponibilidad de la seguridad de información y la gestión del riesgo

			Disponibilidad	Gestión del Riesgo
Rho de Spearman	Disponibilidad	Coeficiente de correlación	1,000	,824**
		Sig. (bilateral)	.	,000
		N	45	45
	Gestión del Riesgo	Coeficiente de correlación	,824**	1,000
		Sig. (bilateral)	,000	.
		N	45	45

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

Interpretando la Tabla 16 de correlaciones se determina que el nivel de significancia – sig.=0,000 en consecuencia al ser menor a 0.05, se debe rechazar la hipótesis nula H0 y aceptar la Hipótesis Especifica 1 la cual es, La Disponibilidad Seguridad de la Información se relaciona con la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021., siendo esta relación o correlación positiva muy fuerte, dado que tiene un valor Rho de Spearman de 0.824.

V. DISCUSIÓN

El objetivo general de la investigación era Identificar la relación que existe entre la Seguridad de la Información y la Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021, además se ha determinado la relación de las dimensiones de la Seguridad de la Información con la variable Gestión del Riesgo.

Los cuestionarios que se han utilizado para una entidad del Sistema Electoral han sido validados por tres expertos dando una calificación de aplicabilidad de ese mismo modo se realizó la prueba de confidencialidad donde se obtuvo un alfa de Cronbach de 0.965 para el cuestionario de Seguridad de la Información y 0.905 el cuestionario de Gestión del Riesgo.

El análisis descriptivo de los cuestionarios realizados a los colaboradores de una entidad del sistema electoral se obtuvo una calificación a la Seguridad de la Información de un nivel alto de 84.44% el cual indica que una mayor parte de los colaboradores se encuentran concientizados respecto a la primera variable sin embargo hay un sector de los colaboradores que califican a la variable en mención con un nivel medio 15.56 %.

El análisis cruzado de las variables de estudios nos indica que un 77.8% considera como alto la Seguridad de la información y la Gestión del Riesgo además también se identificó que un 13.33% de los colaboradores califican como un nivel medio por consiguiente se determinó que existe una relación directa entre las variables la cual fue comprobada a través de la correlación de Rho de Spearman (Rho=0.924, Sig.(Bilateral)=0.000;($p \leq 0.05$), es decir mientras que la Seguridad de la Información se afianza o se posiciona en una entidad del sistema electoral la Gestión del Riesgo también el mismo efecto y o desplazamiento.

Revisando los resultados de la presente investigación y contrastarlos con los antecedentes como los de Pinto (2017) en su investigación en la Escuela de Sub Oficiales de la Policía Nacional del Perú demostró una relación entre sus variables de estudio con una relación inversa (r=-0.647) y significativa (p=000); Calderón (2019) en su estudio en el Ministerio de Educación concluye en una relación positiva entre las variables (r=0.886) y significativa (p=000) con el riesgo de seguridad; Huayllani (2020) en su investigación en el Ministerio de Salud da

como resultado una relación positiva entre sus variables (r=0.592) y significativa (p=000); Huaman (2019) en su investigación en una empresa del sector de telecomunicaciones también obtiene una relación positiva (r=0.592) y significativa (p=000) y finalmente Tarrillo (2015) en su investigación en una Zona Registral en Moyobamba concluye a través de la aplicación del chi cuadrado de Pearson de 15.712 que existe relación entre sus variables de estudio. Es evidente que todos las correlaciones de los estudios de investigación son menores a las del presente estudio sin embargo coinciden que si existe una relación sea directa, positiva, para el presente estudio la relación es positiva fuerte de r=0.924 y significativa p=000.

Respecto a las dimensiones de la Seguridad de la Información, los encuestados determinaron que la Confidencialidad lo califica como alto con un 60% y medio con 40%, respecto a la Integridad obtuvo una calificación alto de 73.33% y medio de 26.67% y la Disponibilidad, alto con un 82.22% y medio de 17.78%; esto evidencio que la dimensión se encuentra con un mayor posicionamiento dentro de la entidad la cual es importante para la seguridad de la información sin embargo se deberá hacer un seguimiento a las dimensiones con valor menor a fin que todas obtengan un mismo nivel alto lo cual fortalecería la seguridad de la información de la institución.

Las dimensiones de la Seguridad de la Información con la variable Gestión del Riesgo pasaron por la prueba estadística de correlación de Rho de Spearman y se obtuvieron los siguientes resultados para la Confidencialidad (Rho=0.589, Sig. (Bilateral) = 0.002); Integridad (Rho=0.886, Sig. (Bilateral) = 0.000) y la Disponibilidad (Rho=0.824, Sig. (Bilateral) = 0.000). Estos resultados evidencian que existe una correlación entre las dimensiones de Seguridad de la Información y la Gestión del Riesgo siendo la más baja la Confidencialidad y la más alta la Integridad y Disponibilidad.

Comparando los resultados de la investigación con los antecedentes nacionales Pinto (2017) sus dimensiones obtuvieron un valor negativo de correlación de Rho de Spearman (Rho=-0.608, Sig. (Bilateral) = 0.002) para información interna; (Rho=-0.639, Sig. (Bilateral) = 0.002) para Liderazgo y (Rho=-0.608, Sig. (Bilateral) = 0.002) para información corporativa (Rho=-0.692, Sig. (Bilateral) =

0.002) esto significa que tienen un desplazamiento de la variable inverso, cuando las dimensiones tienen una calificación alta o eficiente los Riesgos de seguridad tiene una percepción baja. Para las dimensiones del estudio de Calderón (2019) obtuvieron un valor negativo de correlación de Rho de Spearman (Rho=0.886, Sig. (Bilateral) = 0.000) para sus tres dimensiones evidenciando una relación altamente significativa y una relación directa entre la Disponibilidad, Confidencialidad e Integridad de los Datos. En su investigación de Huayllani (2020) la dimensión Orientación al Sistema de Gestión de Riesgo con el Sistema de Gestión de Seguridad de la Información es de correlación positiva y significativa (Rho=0.747, Sig. (Bilateral) = 0.000), también se observa que la dimensión Supervisión del Sistema de Gestión del Riesgo es de correlación positiva con el Sistema de Gestión de Seguridad de la Información (Rho=0.553, Sig. (Bilateral) = 0.000)

Revisando los resultados de la presente investigación y contrastarlos con los antecedentes internacionales, como los de Aguilar (2020) en su investigación en una institución superior demostró que a través de un análisis descriptivo que el 34% de las instituciones tiene un sistema de gestión de seguridad de la información implementado apropiado y en relación a la gestión de riesgos obtuvo que el 67% de las universidades tienen implementadas medidas de tratamiento de riesgos eficientes y esto aunado al juicio de experto recomiendan su implementación de un SGSI y Nieves (2017) en su investigación la cual tiene como finalidad implementar un SGSI bajo la norma ISO 27001:2013, realizó un análisis descriptivo de los 14 controles de la norma en mención, seis (43) de ellos tienen una valoración baja de 40 %, los seis (57%) restantes tienen una valoración media y alta de 40%, por ello comparándolo con el análisis bivariado de la presente investigación donde la variable seguridad de la información y gestión del riesgo tiene un nivel alto de percepción por los colaboradores de 77.8%, se deduce que existe una convergencia con seguridad de la información y la gestión del riesgo dado tienen un impacto positivo en su implementación y apreciación.

Cruzando los resultados de Bermúdez y Bailón (2015) en su investigación a través del análisis descriptivo obtuvo los siguientes porcentajes de 100% por no

tener un repositorio de incidentes, no existe una política de bloque de equipos y además el 91.30% de colaboradores no recibe capacitación, el autor concluye que hay una afectación a la seguridad de la información y la gestión del riesgo el cual converge con los resultados del presente estudio que determinó que existe una relación directa entre las variables la cual fue comprobada a través de la correlación de Rho de Spearman (Rho=0.924, Sig.(Bilateral)=0.000;($p \leq 0.05$), es decir mientras que la Seguridad de la Información se afianza o se posiciona en una entidad del sistema electoral la Gestión del Riesgo también el mismo efecto y o desplazamiento.

Revisando los resultados de Guaman (2015) a través de la recolección de datos en una institución militar, obtiene un diagnostico cuantitativo del nivel de cumplimiento de cada control o dimensión, respecto a la política de seguridad de la información obtuvo que un 35.29% no existe la prioridad de implementar un documento o manual respecto a ello, referente a la seguridad física y ambiental un 49.02% y 41.18 , Siempre y Algunas veces respectivamente, consideran que si existe este tipo de control, respecto a control de accesos existe un cumplimiento del 43% evidenciando una política de control , contrastándolo con los resultados descriptivos de la presente investigación respecto al punto cumplimiento a los procedimientos de la seguridad de la información 4.4% algunas veces lo cumple, en relación a los ambientes seguros , existe la percepción que un 53% y 44% casi siempre se protege la información, y sobre los controles un 53.3% y 24% casi siempre y siempre respectivamente lo cumple, para el autor de la investigación internacional concluye que sus resultados demuestran que se debe implementar un SGIS que proteja la información y gestione el riesgo lo cual converge con los resultados de la presente investigación donde la relación de las variables de estudio tienen una relación alta de 77.8% y una correlación de Rho de Spearman (Rho=0.924, Sig.(Bilateral)=0.000;($p \leq 0.05$).

Contrastando los resultados de Castro (2014) según su análisis descriptivos de su variable seguridad de la información determina que la falta de un SGSI tiene un riesgo de injerencia negativa de pérdida económica de un 30% y 60% lo cual evidencia una relación directa entre la seguridad de la información y el riesgo, lo cual converge con los resultados de la presente investigación donde la relación de

las variables de estudio tienen una relación o percepción alta de 77.8% y una correlación de Rho de Spearman (Rho=0.924, Sig.(Bilateral)=0.000;($p \leq 0.05$).

Se concluye que a través de los antecedentes, teorías de esta investigación y la aplicación de la estadística descriptiva e inferencial determinar que existe una correlación entre las variables Seguridad de la Información y la Gestión del Riesgo, por lo tanto mientras la entidad del Sistema Electoral fortalezca la seguridad de la información a través de los controles implementados, la concientización la Gestión del Riesgo se fortalecerá.

VI. CONCLUSIONES

Terminado de aplicar los instrumentos de recolección de datos y los procedimientos estadísticos en una entidad del sistema electoral, se concluye lo siguiente:

PRIMERA: Que existe una correlación positiva perfecta entre la variable seguridad de la información y gestión del riesgo, con valor de significancia es 0.00 y con Rho de Spearman de 0,924**. Teniendo como base que la seguridad de la información y Gestión del Riesgo tiene un nivel alto de percepción por los colaboradores de 84.44% y 80% respectivamente, como análisis univariado, no obstante, en un análisis Bivariado ambas variables convergen en un nivel alto con un 77.8%, esto significa que mientras se fortalece la seguridad de la información la gestión del riesgo ira en el mismo sentido ascendente, o, si deja de hacer seguimiento, invertir en la seguridad de la información la gestión del riesgo descenderá y la organización será vulnerable ante la sociedad.

SEGUNDA: Se identificó que existe una correlación positiva considerable entre la dimensión confidencialidad y la variable gestión del riesgo, con valor de significancia es 0.00 y con Rho de Spearman de 0,589**, teniendo como base en su análisis bivariado ambos convergen en un nivel alto de percepción por los colaboradores con 51.1%, la diferencia se distribuye entre el valor medio, no obstante es importante considerar también que en el análisis de la frecuencias de los items se evidencia que los colaboradores no utilizan todas las herramientas que garanticen la confidencialidad por ejemplo el uso de la criptografía 37.8% casi nadie lo usa, el acceso a los ambientes se encuentran protegidos el 31.1% de los colaboradores indican que algunas veces.

TERCERA: También se identificó una correlación positiva muy fuerte entre la dimensión integridad y la variable gestión del riesgo, con valor de significancia es 0.00 y con Rho de Spearman de 0,886**, en su análisis bivariado ambos convergen en un nivel alto de percepción por lo colaboradores en un 71.1%, la diferencia se distribuye entre el valor medio, esto manifiesta que existe una predisposición por el personal un garantizar y salvaguardar la información y evitar sus modificaciones o cambios por acciones involuntarias o de terceros.

CUARTO: Finalmente se identificó una correlación positiva muy fuerte entre la dimensión disponibilidad y la variable gestión del riesgo, con valor de significancia es 0.00 y con Rho de Spearman de 0,824**, en su análisis bivariado ambos convergen en un nivel alto de percepción por lo colaboradores en un 75.6%, la diferencia se distribuye entre el valor medio, significando que existe una preocupación e interés por la organización en garantizar que los colaboradores tengan los recursos disponibles.

VII. RECOMENDACIONES

La variable seguridad de la información tiene una correlación positiva perfecta con la gestión del riesgo, en ese sentido se recomienda hacer seguimiento a lo implementado en lo concerniente a los controles de la seguridad de la información asimismo cumplir con el plan de gestión integral de riesgos normado por la Contraloría General de República del Perú esto con la finalidad de seguir manteniendo estos niveles positivos además la entidad debe establecer actividades de control en el Plan Operativo Institucional, seguir con la capacitaciones y sensibilizaciones al personal en materia de seguridad de la información y gestión de riesgos teniendo como base metodológica, la andragogía, deberá también invertir en tecnología dado que los ciberataques son los riesgos más latentes en la actualidad.

Respecto a la dimensión confidencialidad cuya correlación es positiva considerable con la gestión del riesgo, en ese sentido a fin de desplazar esta correlación a una muy fuerte es importante que la entidad implemente el uso de la firma digital criptográfica en los documentos generados por el proceso, fortalecer los accesos a los ambientes físicos, esto porque en el análisis descriptivo de las frecuencias tomadas de los cuestionarios, han dado resultados que nunca o casi nunca son usados o implementados, por ello el proceso debe mapear sus actividades a un enfoque sistematizado donde uso de la firma digital debe primar para todo el personal esto generaría un ahorro en el consumo de papelería, tiempo, mano de obra directa, contrataciones de terceros, presupuesto que puede ser destinado a la adquisición de tecnología de vigilancia en los ambientes de la sede.

En relación a la dimensión integridad cuya correlación es positiva muy fuerte con la gestión del riesgo y si el objetivo es mantener ese nivel o desplazarlo una correlación positiva perfecta la entidad debe seguir con el seguimiento a las actividades implementes o programadas según su certificación de la Norma ISO 27001 Seguridad de la Información, se debería realizar pasantías en entidades que tengan la certificación ISO a fin compartir experiencias y fortalecer la seguridad y la gestión del riesgo, involucrar al personal en las auditorías internas y/o externas dado que según el análisis descriptivo existe un grupo que participa

algunas veces, las copias de seguridad deber ser una actividad permanente y obligatoria al termino del día, debe renovar los equipos informáticos dado que su funcionamiento adecuado es casi siempre el cual debería ser siempre.

En cuanto a la dimensión disponibilidad cuya correlación positiva muy fuerte con la variable gestión del riesgo, en ese sentido es importante hacer el seguimiento a las actividades programadas y planificadas según su Certificación ISO 27001, no obstante el proceso debe intensificar el uso de la tecnología dado que disponibilidad de la información ya no puede ser física a raíz del Covid -19, la disponibilidad de la información para atención de servicios primarios deben ser virtuales a fin de evitar o cortar la continuidad del negocio, para ello se debe priorizar la sistematización de sus actividades lo cual generaría un ahorro en papelería , una potenciación y especialización del personal.

REFERENCIAS

Aenor (2015) Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.

Aguilar, N. (2020). *Modelo de Seguridad de la Información para Instituciones de Educación Superior* (Tesis de Maestría, Universidad Francisco de Paula Santander Ocaña). Archivo Digital. http://repositorio.ufpso.edu.co/bitstream/123456789/419/1/32686.pdf

Alexander, A. (2007) *Diseño de un Sistema de Gestión de Seguridad de Información. Óptica ISO 27001:2005.*

Alvarado, C. (2021, 26 de Marzo) Sistema de gestión de seguridad de la información: qué es y sus etapas. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

Arias (2006) Proyecto de Investigación. Introducción a la Metodología Científica.

Bermúdez, K. y Bailón, E. (2015). *Análisis en Seguridad Informática y Seguridad de información basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información Dirigido a una Empresa de Servicios Financiero.* (Título Pregrado, Universidad Politécnica Salesiana Sede Guayaquil). Archivo Digital. https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

Bernal, C. (2010). Metodología de la Investigación.

Calderón, J. (2019). *Seguridad de la información y la gestión de riesgos en los trabajadores de la Digere del Ministerio de Educación, 2018.*

Cardona, O. (2008). Medición de la Gestión del riesgo en América Latina. Revista internacional de Sostenibilidad y Humanismo. 2008(3). https://upcommons.upc.edu/bitstream/handle/2099/7056/cardona.pdf

Carlino, P. (2021). Antecedentes y marco teórico en los proyectos de investigación: aportes para construir este apartado. https://www.aacademica.org/paula.carlino/274.pdf

Castro, C. (2014). 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. (Tesis de Maestría). Archivo Digital. http://dspace.udla.edu.ec/handle/33000/3376

Celina, H. y Campo Arias, A. (2005). Aproximación al uso del coeficiente alfa de Cronbach. Metodología de la Investigación y lectura crítica de estudios, 14(4), 575-576. https://www.redalyc.org/pdf/806/80634409.pdf.

Concytec (2018) Reglamento de calificación, clasificación y registro de los investigadores del sistema nacional de ciencia, tecnología e innovación tecnológica. Diario Oficial El Peruano Nº 400-2018. https://portal.concytec.gob.pe/images/renacyt/reglamento_renacyt_version_final.pdf

Decreto Supremo N° 081-2013-PCM. (2013, 09 de Julio). Presidencia de Consejo de Ministros. Diario Oficial El Peruano 498979. https://cdn.www.gob.pe/uploads/document/file/357106/DS_N%C2%BA_081-2013-PCM.pdf

Decreto de Urgencia N° 0007-2020 aprueba el Marco de Confianza Digital Dispone medidas para su fortalecimiento. (2020, 8 de Enero). Presidencia de Consejo de Ministros. Diario Oficial El Peruano N° 1844001-1. https://busquedas.elperuano.pe/download/url/decreto-de-urgencia-que-aprueba-el-marco-de-confianza-digita-decreto-de-urgencia-n-007-2020-1844001-2

Delgado, G. (2019, 27 Octubre). Ciberseguridad en minería: ¿A qué tipo de riesgos están expuestos las empresas de minería?. Gestión https://gestion.pe/economia/empresas/ciberseguridad-en-mineria-a-que-tipo-de-riesgos-estan-expuestas-las-empresas-noticia/?ref=gesr

Directiva N° 0006-2019-CG/INTEG- Implementación del Sistema de Control Internos en las Entidades del Estado (2019, 15 de Mayo). Contraloría General de la Republica. https://cdn.www.gob.pe/uploads/document/file/1938561/directiva%20006-2019.pdf.pdf

Echaiz, C.(2018). Taller de Tesis. Instituto para la calidad de la educación. https://www.usmp.edu.pe/iced/instituto/organizacion/contenido-web/de5-taller%20-tesis-I.pdf

EY Ernst & Young Global Limited – EY Perú (EY, 2020, 11 de Junio). Encuesta sobre seguridad de la información por EY Ernst & Young Global Limited – EY Perú. https://www.ey.com/es_pe/news/2020/06/ciberseguridad-lineas-negocio-neutral

EY Ernst & Young Global Limited – EY PERU (2021, 21 de Octubre). Resultados de la Encuesta Global de Seguridad de la Información 2021 de EY – Ernst & Young Global Limited

https://www.ey.com/es_pe/news/2021/10/empresas-peruanas-preocupacion-ataques-ciberseguridad

Figueroa, J., Rodríguez, R., Bone, C., Saltos, J. (2017). Information security and information security 2(12), 147-149. https://DOI: 10.23857/pc.v2i12.420

Flores, C. y Flores, K. (2021). Tests to Verify the Normality of data in production processes: anderson-darling, ryan-joiner, shapiro-wilk and kolmogorovsmirnov. 23(02), 90-91. https://revistas.up.ac.pa/index.php/societas.

Gallardo, E. (2017). Metodología de la Investigación. Universidad Continental. Manual Autoformativo Interactivo. https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

Gerber, M. y Von-Solms, R. (2005) “Management of risk in the information age”. Computers & security, v. 24, n. 1, pp. 16-30. https://www.researchgate.net/publication/222827356_Management_of_risk_in_the_information_age https://doi.org/10.1016/j.cose.2004.11.002

Guaman, J. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para instituciones Militares.* (Tesis de Maestría, Escuela Politécnica Nacional). Archivo Digital. https://1library.co/document/zx5okenq-diseno-sistema-gestion-seguridad-informacion-instituciones-militares.html

Hernández, R, Fernández, C y Baptista L. (2014). Metodología de la Investigación.

Huaura, M. (2019). *Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones.*

Huayllani, O. (2020). *Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud, 2019.*

Incibe. (2015). La seguridad vista desde sus inicios. https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

ISO 27000:2021.(2021). Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2018)

ISO 27001:2017.(2017). Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

ISO 27002:2017. (2017). Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

ISO 27004:2010.(2010). Information technology - Security techniques - Informa tion security management - Measurement.

ISO 27005:2018.(2018). Information technology — Security techniques — Information security risk management

ISO 27006:2015.(2015). Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

ISO 27032. (2012) Information technology - Security techniques - Gui delines for cybersecurity

ISO 17799 (2007) EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. http://spij.minjus.gob.pe/Graficos/Peru/2007/agosto/25/RM-246-2007-PCM_25-08-07.pdf

ISO 31000:2018.(2018). Risk Management — Guidelines

ISOTools Excellence (2017). ¿Seguridad informática o seguridad de la información? https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Latina (2021, 17 Octubre). Migraciones: información personal de personajes públicos era enviada por chats de Whatsapp https://www.latina.pe/noticias/punto-final/migraciones-informacion-personal-de-personajes-publicos-era-enviada-por-chats-de-whatsapp

Lavado. (2020). Epistemología e Investigación. (Fondo Editorial) http://www.une.edu.pe/uneweb/wp-content/uploads/2021/04/Libro-Epistemolog%C3%ADa-e-investigaci%C3%B3n.pdf

Ley N°29733 Ley de Protección de Datos Personales. (2011,21 de Junio). Congreso de la Republica. Diario Oficial el Peruano N° 445746. https://leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Ley N° 27658 – Ley Marco de Modernización de la Gestión del Estado. (2002, 29 de Enero). Congreso de la Republica. Diario Oficial el Peruano N° 216537. https://www.mincetur.gob.pe/wp-content/uploads/documentos/institucional/gestion_descentralizada/transferencia_sectorial/normas_proceso_transferencia/3_LEY_Nro_27658.pdf

Martin, S.(2013). Aplicación de los principios éticos a la metodología de la investigación. *Enfermería Cardiología, 58(59),* 27-30. https://www.enfermeriaencardiologia.com/wp-content/uploads/58_59_02.pdf

Millan, A. (2017). Beneficiencia y No Maleficiencia. Ética en la investigación con seres humanos. http://repositorio.pucp.edu.pe/index/handle/123456789/71381

Mondragón, M. (2014). *Uso de la Correlación de Spearman en un estudio de intervención en fisioterapia.* Mov.cient.Vol.8 (1): 98-104.

Nieves, A. (2017). *Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) Basados en la Norma ISO/IEC 27001:2013* (Tesis de Pregrado, Institución Universitaria Politécnico Grancolombiano). Archivo Digital. https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y

Peltier, T. (2014) Information Security Fundamentals. 2da. Edición. Florida: CRC Press, 2014. 375 pp. ISBN 9781439810620.

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

PNP: delincuentes obtienen huellas digitales para suplantar identidad. (2021, 25 Noviembre). La Republica. https://larepublica.pe/sociedad/2021/11/25/delincuentes-obtienen-huellas-digitales-para-suplantar-identidad/

PriceWaterhouseCoopers (2018). Encuesta The Global State Of Information Security Survey. https://www.pwc.com/sg/en/publications/assets/gsiss-2018.pdf

Reglamento de Organización de Funciones (2021,15 de Mayo). Registro Nacional de Identificación y Estado Civil.

Resolución Ministerial N° 129-2012-PCM. (2012, 23 de Mayo). Presidencia de Consejo de Ministros. https://cdn.www.gob.pe/uploads/document/file/303765/RM_129_2012PCM.pdf

Resolución Ministerial N° 0004-2016- PCM. (2016, 8 de Enero). Presidencia de Consejo de Ministros. https://cdn.www.gob.pe/uploads/document/file/357224/Resoluci%C3%B3n_Ministerial_N__004-2016-PCM20190902-25578-19siyuu.pdf

Rojas, M. (2019) *Seguridad en los datos e implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC*. (Tesis de Pregrado) Archivo Digital. https://repositorio.ucv.edu.pe/handle/20.500.12692/43660

Rosales, J. (2021). Evolución histórica de la concepción de la gestión de riesgos de desastres: algunas consideraciones. Revista Kawsaypacha n.7 , 67-81 https://doi.org/10.18800/kawsaypacha.202101.004

Sánchez, H, Reyes C. y Mejía K. (2018). Manual de Términos de Investigación científica, tecnológica y humanística . 2018,(1),1-146. http://repositorio.urp.edu.pe/handle/URP/1480?show=full

Soriano, M. (2014) *Seguridad en redes y seguridad de la información.* (Innovative Methodology for Promising VET Areas) http://improvet.cvut.z/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf.

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides, M. del C. (2015). Methodology of analysis and risk assessment applied to computer security and information under the ISO / IEC 27001. Revista Tecnológica - ESPOL, 28(5),487. http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Sullivan, P. (2016). Gestión de riesgos de seguridad de la información: Comprensión de los componentes. https://www.computerweekly.com/es/consejo/Gestion-de-riesgos-de-seguri dad-de-la-informacion-Comprension-de-los-componentes

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

Westerman, George F.(2006) It Risk Management: From IT Necessity to Strategic Business Value. MIT Sloan Research Paper No. 4658-07. SSRN: https://ssrn.com/abstract=1010226 or http://dx.doi.org/10.2139/ssrn.1010226

ANEXO 1: MATRIZ DE OPERACIONALIZACIÓN

Matriz de operacionalización

Variable: Seguridad de la Información

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Ítems	Escala de Medición
Seguridad de la Información	El concepto de seguridad de la información significa proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados. Soriano (2014)	La Seguridad de la Información tiene que ver con la confidencialidad, integridad, disponibilidad de los datos, independientemente de su formato. Durante más de veinte años, los pilares básicos de la seguridad de la información han sido la confidencialidad, integridad y disponibilidad, de acuerdo a los siguientes niveles y rangos: Bajo: Hasta 41 puntos Medio De 42 hasta 65 puntos Alto De 66 a más	Confidencialidad Integridad Disponibilidad	Protección de la Información Accesos Redes Técnicas Criptográficas Información Critica Claves y/o Contraseñas .Protección de Datos Fiabilidad de Recursos Ataque Almacenamiento Sistemas de Información Técnicas Criptográficas Acceso a la Información Sistemas de Información Aspectos Técnicos Fenómenos Naturales Causas Humanas Voluntad	1-2-3-4-5-6 7-8-9-10-11-12 13-14-15-16-17-18	Ordinal El inventario está compuesto por 18 reactivos de opción múltiple: Nunca = 1 Casi nunca = 2 A veces = 3 Casi siempre = 4 Siempre = 5

Fuente: adaptado de Calderón (2019)

Matriz de Operacionalización

Variable: Gestión del Riesgo

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Ítems	Escala de Medición
Gestión del Riesgo	La gestión de riesgos de TI está ganando visibilidad en las empresas del mundo, dado que no solo es los riesgos técnicos, sino también cómo los riesgos de Tecnología de la Información influyen en los riesgos a nivel empresarial. La visión del ejecutivo sobre el riesgo de TI va más allá de la disponibilidad y la administración de acceso para examinar la precisión de la información y la agilidad estratégica. La capacidad eficaz de gestión de riesgos tiene una serie de recompensas como un mejor manejo de cómo están abordando los riesgos de alta prioridad y, lo que es más importante, qué riesgos están eligiendo. Están seguros de que están centrando el dinero y el esfuerzo en los riesgos que realmente importan y pueden buscar oportunidades que otras empresas encontrarían demasiado riesgosas para emprender. Westerman (2006)	Una gestión eficaz del riesgo es una combinación cohesiva de tres disciplinas básicas: Proceso de Gobernanza de Riesgos, Cultura Consciente del Riesgo y Base de la Tecnología de la Información Eficaz. Westerman (2006) Bajo: Hasta 41 puntos Medio De 42 hasta 65 puntos Alto De 66 a más	Proceso de Gobernanza de Riesgos Cultura Consciente del Riesgo Base de la Tecnología de la Información Eficaz	Política de Riesgo Eficacia Proceso Identificar Riesgos Evaluar Riesgos Prioriza Riesgos Monitorea Riesgos Capacitación Conocimiento Identificar Amenazas Evaluar Amenazas Implementación Eficaz Infraestructura Aplicaciones Riesgo Diseño Administrar	1-2 3-4-5-6-7-8 9-10-11-12-13 14-15-16-17-18	Ordinal El inventario está compuesto por 18 reactivos de opción múltiple: Nunca = 1 Casi nunca = 2 A veces = 3 Casi siempre = 4 Siempre = 5

Fuente: adaptado de Calderón (2019)

ANEXO 2: INSTRUMENTO DE MEDICIÓN

CUESTIONARIO DE SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DEL RIESGO

Instrucciones : El siguiente cuestionario tiene 36 preguntas referente a la Seguridad de la Información y la Gestión del Riesgo en una entidad del Sistema Electoral, en ese sentido se le solicita marcar la opción que considere correcto

RUBRO: SEGURIDAD DE LA INFORMACIÓN *

	Nunca	Casi nunca	A veces	Casi siempre	Siempre
1. Cumple activamente con los procedimientos de Protección de la información.	◯	◯	◯	◯	◯
2. Los accesos a los ambientes de trabajo siempre se encuentran protegidos.	◯	◯	◯	◯	◯
3. Gestiona la aplicación de los procedimientos de protección y mantenimiento de redes informáticas.	◯	◯	◯	◯	◯
4. Siempre se usa la tecnica criptografica como la firma digital para validar la documentación.	◯	◯	◯	◯	◯
5. La información critica del proceso se encuentra en ambientes seguros y resguardada bajo llaves.	◯	◯	◯	◯	◯
6. Cambia periodicamente las contraseñas de acceso a sus aplicativos.	◯	◯	◯	◯	◯

7. Establece controles de protección de datos frente a modificaciones , eliminaciones por entes no autorizados	◯	◯	◯	◯	◯
8. Garantiza la fiabilidad de los equipos informáticos, funcionan adecuadamente.	◯	◯	◯	◯	◯
9. Establece medidas de prevención contra ataques de virus informaticos.	◯	◯	◯	◯	◯
10. Gestiona el Backup de almacenamiento y/o copias de respaldo.	◯	◯	◯	◯	◯
11. Participa activamente en las auditorias periodicas de sistemas de información	◯	◯	◯	◯	◯
12. Gestiona el desarrollo de software bajo tecnicas criptograficas para la protección de la información	◯	◯	◯	◯	◯
13. El acceso a la información se encuentre disponible para realizar las labores.	◯	◯	◯	◯	◯

14. Se garantiza la rapidez de respuesta de los sistemas de información.	◯	◯	◯	◯	◯
15. Cuenta con un plan de mantenimiento de equipos informaticos para la prevención de fallas tecnicas	◯	◯	◯	◯	◯
16. Cuenta con un plan de contingencia para recuperación de la información en caso de desastres.	◯	◯	◯	◯	◯
17. Establece controles preventivos frente a errores humanos en el tratamiento de la información.	◯	◯	◯	◯	◯
18.Tiene la voluntad de aplicar controles de seguridad de la información en sus labores diarias de trabajo	◯	◯	◯	◯	◯

RUBRO GESTIÓN DEL RIESGO *

	NUNCA	CASI NUNCA	A VECES	CASI SIEMPRE	SIEMPRE
1. Cumple con la Política de Gestión de Riesgos de la Institución	◯	◯	◯	◯	◯
2. Implementa políticas con la finalidad de mitigar los riesgos de seguridad de la información	◯	◯	◯	◯	◯
3. Los controles implementados en la gestión del riesgo son eficaces	◯	◯	◯	◯	◯
4. Participa en la implementación de oportunidades y /o procesos de mejora continua	◯	◯	◯	◯	◯
5. Participa activamente en la identificación de riesgos	◯	◯	◯	◯	◯
6. Evalúa riesgos que pueden afectar el desarrollo de las actividades diarias	◯	◯	◯	◯	◯
7. Prioriza los riesgos que tienen sus actividades laborales	◯	◯	◯	◯	◯

8. Realiza el seguimiento y monitoreo de los controles implementados para los riesgos identificados	◯	◯	◯	◯	◯
9. Recibe capacitación constante sobre seguridad de la información y gestión de riesgos	◯	◯	◯	◯	◯
10. El conocimiento adquirido en las capacitaciones lo aplica en sus actividades diarias	◯	◯	◯	◯	◯
11. Identifica amenazas que pueden afectar el desarrollo de las actividades diarias	◯	◯	◯	◯	◯
12. Evalúa amenazas que pueden afectar el desarrollo de las actividades diarias	◯	◯	◯	◯	◯
13. Implementa las acciones eficaces necesarias para afrontar los riesgos	◯	◯	◯	◯	◯
14. Cuenta con la infraestructura tecnológica adecuada , para la realización de sus labores	◯	◯	◯	◯	◯

14. Cuenta con la infraestructura tecnológica adecuada , para la realización de sus labores	◯	◯	◯	◯	◯
15. Cambia usted sin autorización las aplicaciones o software que se encuentran en su computador poniendo en riesgo la seguridad de la información	◯	◯	◯	◯	◯
16. Reporta y/o Comunica incidentes que pongan en riesgo la seguridad de la información.	◯	◯	◯	◯	◯
17. El diseño y desarrollo de software se realizan en entornos seguros	◯	◯	◯	◯	◯
La administración renueva la tecnología en pro de la seguridad de la información	◯	◯	◯	◯	◯

Enviar

Borrar formulario

ANEXO 3 : CONFIABILIDAD

Item	SEGURIDAD DE LA INFORMACIÓN																	
	CONFIDENCIALIDAD						INTEGRIDAD						DISPONIBILIDAD					
	DSV1.1	DSV1.2	DSV1.3	DSV1.4	DSV1.5	DSV1.6	DSV1.7	DSV1.8	DSV1.9	DSV1.10	DSV1.11	DSV1.12	DSV1.13	DSV1.14	DSV1.15	DSV1.16	DSV1.17	DSV1.18
1	4	3	4	1	4	3	4	3	4	4	3	4	4	5	3	2	5	4
2	5	4	3	1	3	3	3	3	3	3	3	4	3	2	4	5	3	4
3	4	5	4	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3
4	5	3	4	4	4	3	3	4	3	3	3	3	3	3	3	3	2	3
5	4	4	3	5	4	3	2	4	1	3	3	4	2	1	3	5	4	4
6	5	3	4	1	3	3	5	4	1	3	3	2	3	3	3	3	5	5
7	4	4	4	1	5	3	5	3	5	3	3	3	5	3	3	3	5	5
8	5	3	2	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4
9	4	4	2	4	3	4	4	4	4	2	3	4	4	4	4	4	4	4
10	5	3	2	4	3	4	4	4	4	4	4	3	4	4	4	4	5	5
11	4	2	3	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4
12	5	4	3	1	5	4	4	4	4	2	3	4	2	4	4	4	4	4
13	5	3	4	1	5	4	3	4	4	4	4	4	4	4	3	4	4	4
14	3	4	4	3	4	4	4	4	3	4	3	4	4	3	4	4	4	4
15	5	4	3	1	4	4	4	4	4	4	4	4	3	4	4	3	5	4
16	4	5	4	1	2	4	4	4	4	4	4	4	4	4	4	4	4	4
17	5	3	3	1	4	4	4	4	4	4	4	3	4	4	3	4	4	4
18	4	4	4	4	3	4	4	4	4	4	4	4	2	4	4	3	5	4
19	5	5	5	5	4	4	4	4	4	4	4	4	4	4	3	4	4	4
20	4	3	5	4	4	4	4	4	4	4	4	3	3	4	4	3	4	3
21	5	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	5	4
22	3	3	5	4	4	4	5	5	1	4	4	3	5	4	3	4	4	4
23	4	3	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
24	5	3	5	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4
25	5	2	3	1	4	4	4	4	4	4	4	4	5	4	4	4	5	5

26	4	1	2	1	5	5	2	4	4	5	5	5	4	5	5	5	5	5	4
27	5	4	4	5	5	5	1	5	5	5	5	5	1	5	5	5	5	5	5
28	5	5	2	2	4	5	4	4	5	5	5	5	4	5	5	5	4	4	
29	4	3	3	5	5	4	2	5	5	5	5	5	2	5	5	5	5	5	
30	5	3	4	5	4	5	4	3	5	5	5	4	4	5	4	5	4	5	
31	4	4	3	5	5	4	5	4	3	5	4	4	5	5	5	4	5	5	
32	5	4	4	5	4	5	3	4	5	5	5	5	4	5	5	5	4	5	
33	4	4	4	4	5	4	5	5	5	5	5	5	5	5	4	4	3	2	
34	5	4	5	1	4	5	4	3	4	5	4	5	5	5	5	5	5	4	
35	4	5	4	1	4	4	4	3	5	5	5	5	5	5	5	4	4	5	
36	5	5	4	1	5	5	5	5	5	5	5	3	3	5	5	5	5	5	
37	4	4	3	1	4	4	4	4	4	4	4	4	5	5	5	5	4	5	
38	5	4	4	1	5	5	2	5	5	5	5	5	5	5	5	5	5	5	
39	4	4	5	3	4	5	4	4	4	5	5	5	4	5	5	5	4	4	
40	5	5	4	4	5	4	4	4	5	4	4	4	5	5	5	4	4	5	
41	4	4	4	4	4	5	5	5	4	5	5	5	5	5	4	5	5	4	
42	5	4	4	4	5	5	5	5	4	4	3	4	5	5	5	4	5	5	
43	4	3	4	5	4	4	5	5	5	5	5	5	5	5	4	5	5	4	
44	5	4	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	
45	4	5	5	5	5	4	5	5	5	5	5	4	5	5	4	5	5	5	

Fiabilidad

Escala: SEGURIDAD DE LA INFORMACIÓN

Resumen de procesamiento de casos

		N	%
Casos	Válido	20	100,0
	Excluido[a]	0	,0
	Total	20	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,965	,965	24

Item	GESTIÓN DEL RIESGO																	
	PROCESO DE GOBERNANZA DE RIESGOS								CULTURA CONSCIENTE DEL RIESGO					BASE DE LA TECNOLOGIA DE LA INFORMACIÓN EFICAZ				
	DGV1.1	DGV1.2	DGV1.3	DGV1.4	DGV1.5	DGV1.6	DGV1.7	DGV1.8	DGV1.9	DGV1.10	DGV1.11	DGV1.12	DGV1.13	DGV1.14	DGV1.15	DGV1.16	DGV1.17	DGV1.18
1	3	2	3	4	3	3	4	4	4	4	3	4	4	5	4	2	5	4
2	4	3	4	3	4	4	4	5	3	3	4	3	4	2	3	5	4	4
3	3	4	3	3	3	3	3	4	3	3	3	3	3	3	4	3	4	4
4	4	3	4	2	2	4	4	3	4	3	4	3	4	3	4	3	2	5
5	3	3	5	4	3	3	2	4	1	3	4	3	2	2	3	5	4	5
6	2	2	4	3	1	4	1	5	1	4	3	2	5	4	4	4	5	5
7	3	3	4	4	3	3	5	4	5	3	3	3	5	3	3	3	5	2
8	4	2	1	4	4	4	4	5	4	4	4	3	4	5	4	3	4	5
9	4	4	2	3	3	4	4	4	4	2	3	4	5	4	2	4	4	4
10	3	3	2	4	4	4	4	5	4	4	4	3	4	4	4	4	5	5
11	3	4	3	4	1	5	4	4	4	4	4	3	5	4	4	3	4	4
12	4	3	3	3	4	4	4	5	4	2	3	4	2	4	4	4	4	4
13	4	4	4	4	4	4	3	4	4	4	4	4	4	4	3	3	4	4
14	3	3	4	3	5	5	4	5	3	4	3	3	4	3	4	4	4	3
15	4	4	3	4	4	4	4	4	4	5	4	4	3	4	3	3	4	4
16	3	3	4	4	4	1	5	4	5	4	4	4	5	4	4	4	4	5
17	4	4	4	5	1	5	4	3	4	4	4	3	4	5	3	4	4	3
18	3	4	4	4	4	4	5	3	5	5	4	4	2	4	4	3	5	4
19	2	1	4	4	4	4	4	4	4	5	4	4	4	5	3	4	4	5
20	4	4	5	2	1	1	5	5	5	5	4	3	3	4	4	3	4	3
21	4	4	4	4	2	4	4	4	4	4	4	4	4	5	4	4	5	4
22	1	4	5	4	4	4	5	5	1	4	3	3	5	4	3	3	4	4
23	4	2	5	4	4	1	4	4	4	4	4	4	4	5	4	4	4	4
24	4	4	5	5	4	4	1	3	4	4	3	4	4	4	4	1	4	4
25	4	5	3	4	4	2	4	4	4	4	4	4	5	5	4	4	5	5

26	5	5	2	1	2	5	2	3	4	5	5	5	4	5	5	5	5	4
27	4	5	4	5	2	5	1	5	5	4	5	1	5	4	4	5	5	5
28	5	4	2	2	4	2	4	4	5	3	4	5	4	5	5	5	4	4
29	5	5	3	5	3	4	2	5	5	4	5	5	2	4	3	5	5	5
30	5	4	4	5	4	5	4	3	5	4	4	4	4	5	4	5	4	3
31	5	5	3	2	2	4	5	4	3	3	4	4	5	4	5	4	5	5
32	5	5	4	5	4	5	3	4	5	4	5	5	4	5	5	5	4	3
33	5	4	4	5	5	4	5	5	5	3	5	5	5	4	4	4	3	2
34	4	5	5	5	4	5	4	4	4	4	4	5	5	5	5	5	5	4
35	4	5	4	2	4	4	4	4	5	3	5	5	5	4	3	4	4	5
36	5	5	4	5	5	5	5	5	5	4	5	3	3	5	4	5	5	5
37	5	4	3	5	4	4	4	4	4	4	4	4	5	4	3	5	4	5
38	4	5	4	4	5	5	2	5	5	5	5	5	5	5	4	5	5	5
39	5	5	5	5	4	5	4	4	4	5	5	5	4	4	5	5	4	4
40	4	3	4	4	5	4	4	4	5	4	4	4	5	5	5	4	4	5
41	5	5	4	5	4	5	5	5	4	5	5	5	5	4	4	5	5	4
42	5	4	4	4	5	5	5	5	4	4	3	4	5	5	5	4	5	5
43	4	5	4	5	4	4	5	5	5	5	5	5	5	4	4	5	5	4
44	5	4	5	4	5	5	5	5	4	4	4	5	5	5	5	5	5	5
45	5	5	5	5	5	4	5	5	4	5	4	4	5	4	4	5	4	4

Fiabilidad

Escala: GESTION DEL RIESGO

Resumen de procesamiento de casos

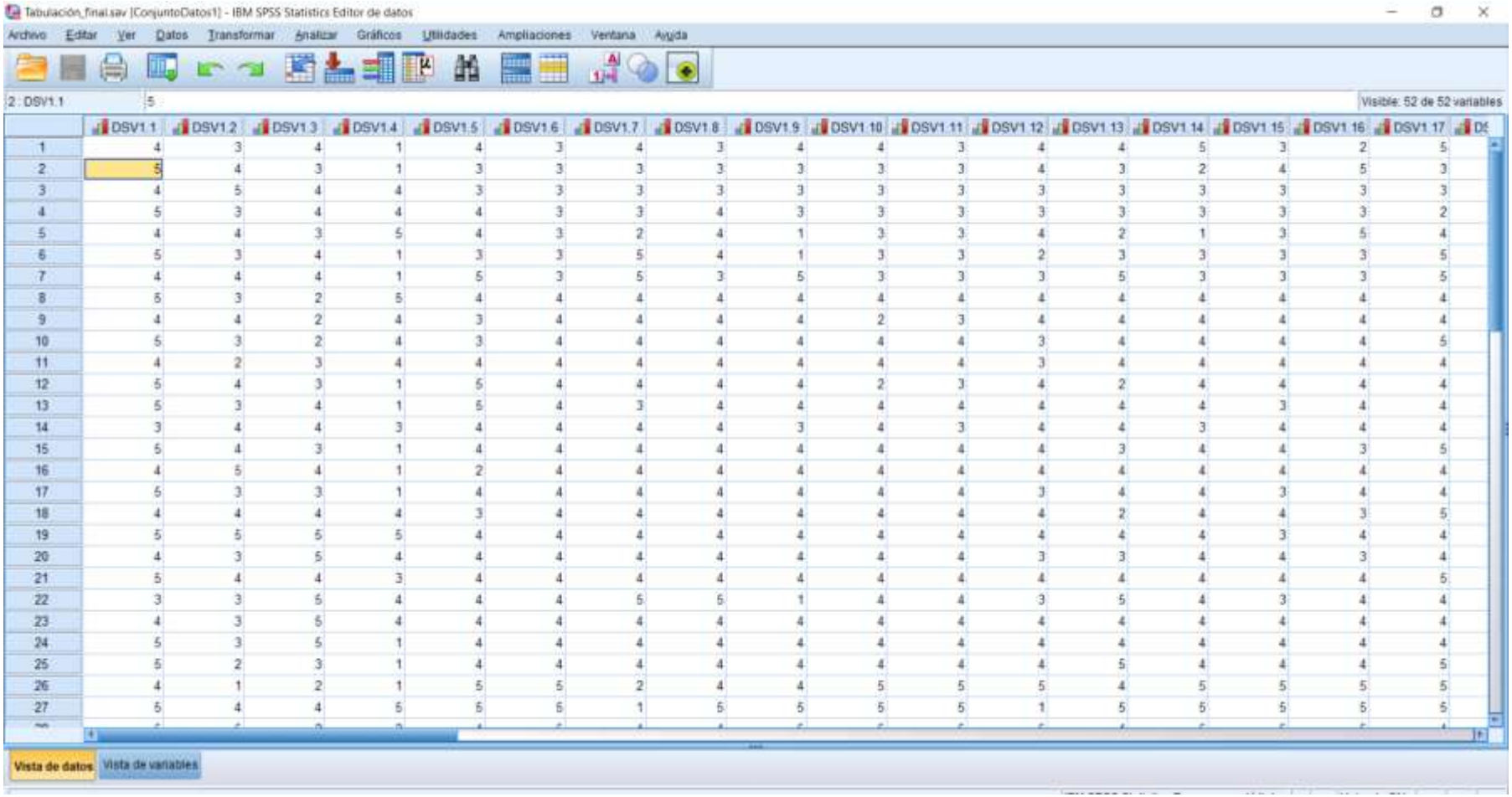
		N	%
Casos	Válido	20	100,0
	Excluido[a]	0	,0
	Total	20	100,0

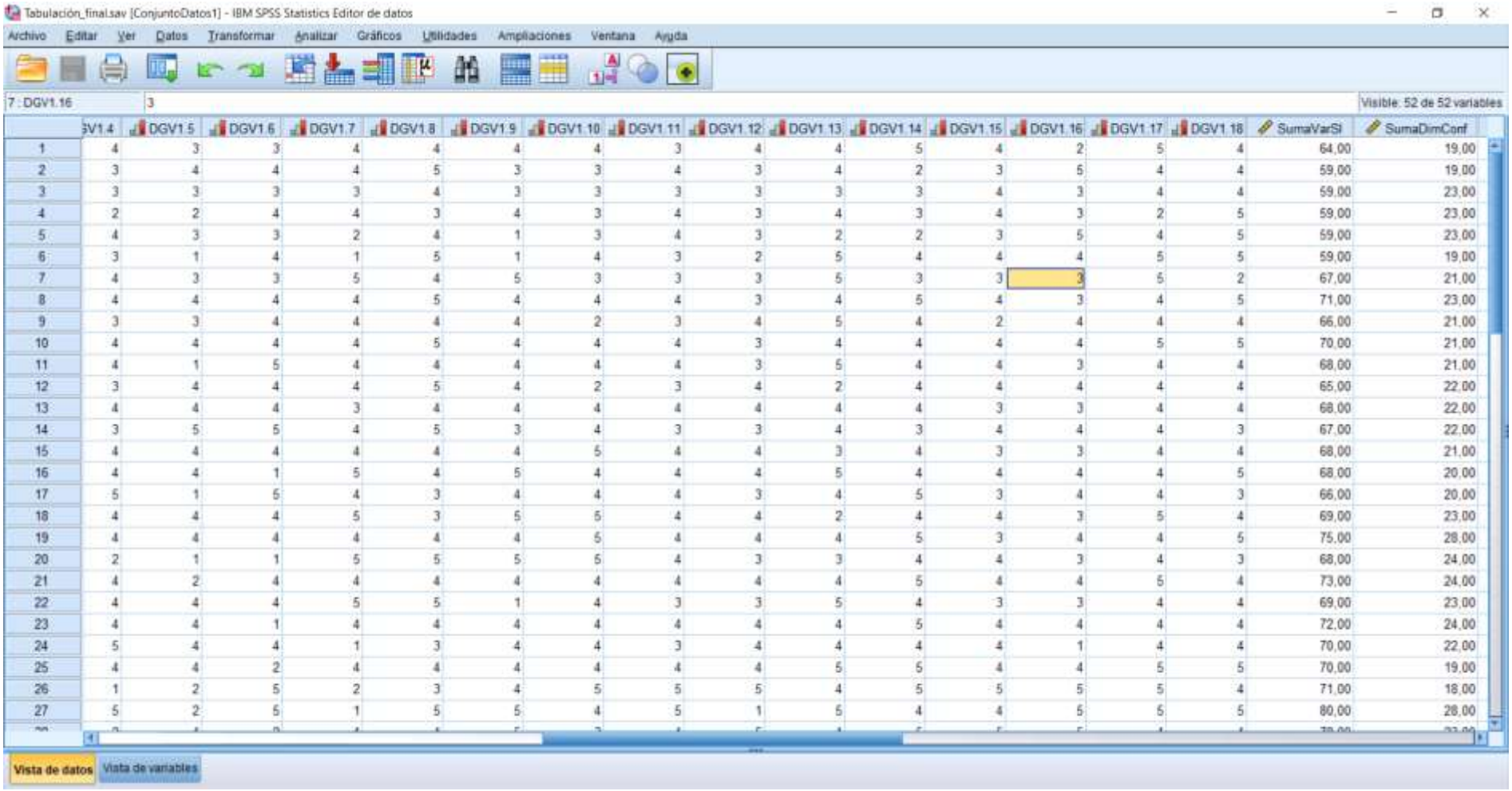
a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,905	20

ANEXO 4: BASE DE DATOS SPSS





	GV1.4	DGV1.5	DGV1.6	DGV1.7	DGV1.8	DGV1.9	DGV1.10	DGV1.11	DGV1.12	DGV1.13	DGV1.14	DGV1.15	DGV1.16	DGV1.17	DGV1.18	SumaVarSI	SumaDimConf
1	4	3	3	4	4	4	4	3	4	4	5	4	2	5	4	64,00	19,00
2	3	4	4	4	5	3	3	4	3	4	2	3	5	4	4	59,00	19,00
3	3	3	3	3	4	3	3	3	3	3	3	4	3	4	4	59,00	23,00
4	2	2	4	4	3	4	3	4	3	4	3	4	3	2	5	59,00	23,00
5	4	3	3	2	4	1	3	4	3	2	2	3	5	4	5	59,00	23,00
6	3	1	4	1	5	1	4	3	2	5	4	4	4	5	5	59,00	19,00
7	4	3	3	5	4	5	3	3	3	5	3	3	3	5	2	67,00	21,00
8	4	4	4	4	5	4	4	4	3	4	5	4	3	4	5	71,00	23,00
9	3	3	4	4	4	4	2	3	4	5	4	2	4	4	4	66,00	21,00
10	4	4	4	4	5	4	4	4	3	4	4	4	4	5	5	70,00	21,00
11	4	1	5	4	4	4	4	4	3	5	4	4	3	4	4	68,00	21,00
12	3	4	4	4	5	4	2	3	4	2	4	4	4	4	4	65,00	22,00
13	4	4	4	3	4	4	4	4	4	4	4	3	3	4	4	68,00	22,00
14	3	5	5	4	5	3	4	3	3	4	3	4	4	4	3	67,00	22,00
15	4	4	4	4	4	4	5	4	4	3	4	3	3	4	4	68,00	21,00
16	4	4	1	5	4	5	4	4	4	5	4	4	4	4	5	68,00	20,00
17	5	1	5	4	3	4	4	4	3	4	5	3	4	4	3	66,00	20,00
18	4	4	4	5	3	5	5	4	4	2	4	4	3	5	4	69,00	23,00
19	4	4	4	4	4	4	5	4	4	4	5	3	4	4	5	75,00	28,00
20	2	1	1	5	5	5	5	4	3	3	4	4	3	4	3	68,00	24,00
21	4	2	4	4	4	4	4	4	4	4	5	4	4	5	4	73,00	24,00
22	4	4	4	5	5	1	4	3	3	5	4	3	3	4	4	69,00	23,00
23	4	4	1	4	4	4	4	4	4	4	5	4	4	4	4	72,00	24,00
24	5	4	4	1	3	4	4	3	4	4	4	4	1	4	4	70,00	22,00
25	4	4	2	4	4	4	4	4	4	5	5	4	4	5	5	70,00	19,00
26	1	2	5	2	3	4	5	5	5	4	5	5	5	5	4	71,00	18,00
27	5	2	5	1	5	5	4	5	1	5	4	4	5	5	5	80,00	28,00

ANEXO 5 : CERTIFICADO DE VALIDEZ DE EXPERTO

Certificado de Validez de contenido del Instrumento que mide Seguridad de la Información

Inventario Seguridad de la Información

Nº	DIMENSIONES / ítems	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
		MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
	DIMENSIÓN 1: CONFIDENCIALIDAD													
1	Cumple activamente con los procedimientos de Protección de la información.				X				X				X	
2	Los accesos a los ambientes de trabajo siempre se encuentran protegidos.				X				X				X	
3	Gestiona la aplicación de los procedimientos de protección y mantenimiento de redes informáticas.				X				X				X	
4	Siempre se usa la técnica criptográfica como la firma digital para validar la documentación.				X				X				X	
5	La información crítica del proceso se encuentra en ambientes seguros y resguardados bajo llaves.				X				X				X	
6	Cambia periódicamente las contraseñas de acceso a sus aplicativos.				X				X				X	
	DIMENSIÓN 2: INTEGRIDAD													
7	Establece controles de protección de datos frente a modificaciones , eliminaciones por entes no autorizados				X				X				X	
8	Garantiza la fiabilidad de los equipos informáticos, funcionan adecuadamente.				X				X				X	
9	Establece medidas de prevención contra ataques de virus informáticos.				X				X				X	
10	Gestiona el Backup de almacenamiento y/o copias de respaldo.				X				X				X	
11	Participa activamente en las auditorias periódicas de sistemas de información				X				X				X	
12	Gestiona el desarrollo de software bajo técnicas criptográficas para la protección de la información				X				X				X	
Nº	DIMENSIONES / ítems													Sugerencias
	DIMENSIÓN 3: DISPONIBILIDAD													
13	El acceso a la información se encuentre disponible para realizar las labores.				X				X				X	
14	Se garantiza la rapidez de respuesta de los sistemas de información				X				X				X	
15	Cuenta con un plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas				X				X				X	
16	Cuenta con un plan de contingencia para recuperación de la información en caso de desastres				X				X				X	
17	Establece controles preventivos frente a errores humanos en el tratamiento de la información.				X				X				X	
18	Tiene la voluntad de aplicar controles de seguridad de la información en sus labores diarias de trabajo				X				X				X	

Observaciones: _____

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

Apellidos y nombres del juez validador Dr. / Mg: **Candia Menor Marco Antonio** **DNI: 10050551**

Especialidad del validador: Temático - Metodológico

04 de diciembre del 2021

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

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

Firma del Experto Informante.
Especialidad

Certificado de Validez de contenido del Instrumento que mide Gestión del Riesgo

Inventario Gestión del Riesgo

Nº	DIMENSIONES / ítems	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
		MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
	DIMENSIÓN 1: PROCESO DE GOBERNANZA DE RIESGOS													
1	Cumple con la Política de Gestión de Riesgos de la Institución				X				X				X	
2	Implementa políticas con la finalidad de mitigar los riesgos de seguridad de la información				X				X				X	
3	Los controles implementados en la gestión del riesgo son eficaces				X				X				X	
4	Participa en la implementación de oportunidades y /o procesos de mejora continua				X				X				X	
5	Participa activamente en la identificación de riesgos				X				X				X	
6	Evalúa riesgos que pueden afectar el desarrollo de las actividades diarias				X				X				X	
7	Prioriza los riesgos que tienen sus actividades laborales				X				X				X	
8	Realiza el seguimiento y monitoreo de los controles implementados para los riesgos identificados				X				X				X	
	DIMENSIÓN 2: CULTURA CONSCIENTE DEL RIESGO													
9	Recibe capacitación constante sobre seguridad de la información y gestión de riesgos				X				X				X	
10	El conocimiento adquirido en las capacitaciones lo aplica en sus actividades diarias				X				X				X	
11	Identifica amenazas que pueden afectar el desarrollo de las actividades diarias				X				X				X	
12	Evalúa amenazas que pueden afectar el desarrollo de las actividades diarias				X				X				X	
13	Implementa las acciones eficaces necesarias para afrontar los riesgos				X				X				X	
Nº	**DIMENSIONES / ítems**													**Sugerencias**
	DIMENSIÓN 3: BASE DE LA TECNOLOGIA DE LA INFORMACIÓN EFICAZ													
14	Se garantiza la rapidez de respuesta de los sistemas de información				X				X				X	
15	Cuenta con un plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas				X				X				X	
16	Cuenta con un plan de contingencia para recuperación de la información en caso de desastres				X				X				X	
17	Establece controles preventivos frente a errores humanos en el tratamiento de la información.				X				X				X	
18	Tiene la voluntad de aplicar controles de seguridad de la información en sus labores diarias de trabajo				X				X				X	

Observaciones: _____

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

Apellidos y nombres del juez validador Dr. / Mg: **Candia Menor Marco Antonio** **DNI: 10050551**

Especialidad del validador: Temático - Metodológico

04 de diciembre del 2021

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

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

Firma del Experto Informante.

Especialidad

Certificado de Validez de contenido del Instrumento que mide Seguridad de la Información

Inventario Seguridad de la Información

N°	DIMENSIONES / ítems	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
	DIMENSIÓN 1: CONFIDENCIALIDAD	MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
1	Cumple activamente con los procedimientos de Protección de la información.				X				X				X	
2	Los accesos a los ambientes de trabajo siempre se encuentran protegidos.				X				X				X	
3	Gestiona la aplicación de los procedimientos de protección y mantenimiento de redes informáticas.				X				X				X	
4	Siempre se usa la técnica criptográfica como la firma digital para validar la documentación.				X				X				X	
5	La información crítica del proceso se encuentra en ambientes seguros y resguardados bajo llaves.				X				X				X	
6	Cambia periódicamente las contraseñas de acceso a sus aplicativos.				X				X				X	
	DIMENSION 2: INTEGRIDAD													
7	Establece controles de protección de datos frente a modificaciones , eliminaciones por entes no autorizados				X				X				X	
8	Garantiza la fiabilidad de los equipos informáticos, funcionan adecuadamente.				X				X				X	
9	Establece medidas de prevención contra ataques de virus informáticos.				X				X				X	
10	Gestiona el Backup de almacenamiento y/o copias de respaldo.				X				X				X	
11	Participa activamente en las auditorias periódicas de sistemas de información				X				X				X	
12	Gestiona el desarrollo de software bajo técnicas criptográficas para la protección de la información				X				X				X	
N°	DIMENSIONES / ítems													Sugerencias
	DIMENSION 3: DISPONIBILIDAD				X				X				X	
13	El acceso a la información se encuentre disponible para realizar las labores.				X				X				X	
14	Se garantiza la rapidez de respuesta de los sistemas de información				X				X				X	
15	Cuenta con un plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas				X				X				X	
16	Cuenta con un plan de contingencia para recuperación de la información en caso de desastres				X				X				X	
17	Establece controles preventivos frente a errores humanos en el tratamiento de la información.				X				X				X	
18	Tiene la voluntad de aplicar controles de seguridad de la información en sus labores diarias de trabajo				X				X				X	

Observaciones: _____

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

Apellidos y Nombres del Juez Validador Dr. Javier Fernando Díaz Molinari **DNI: 29594699**

Especialidad del validador: Doctor en Administración

04 de diciembre del 2021

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

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

Firma del Experto Informante.
Docente de posgrado: Gestión Pública

Certificado de Validez de contenido del Instrumento que mide Gestión del Riesgo

Inventario Gestión del Riesgo

N°	DIMENSIONES / ítems	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
	DIMENSIÓN 1: PROCESO DE GOBERNANZA DE RIESGOS	MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
1	Cumple con la Política de Gestión de Riesgos de la Institución				X				X				X	
2	Implementa políticas con la finalidad de mitigar los riesgos de seguridad de la información				X				X				X	
3	Los controles implementados en la gestión del riesgo son eficaces				X				X				X	
4	Participa en la implementación de oportunidades y /o procesos de mejora continua				X				X				X	
5	Participa activamente en la identificación de riesgos				X				X				X	
6	Evalúa riesgos que pueden afectar el desarrollo de las actividades diarias				X				X				X	
7	Prioriza los riesgos que tienen sus actividades laborales				X				X				X	
8	Realiza el seguimiento y monitoreo de los controles implementados para los riesgos identificados				X				X				X	
	DIMENSIÓN 2: CULTURA CONSCIENTE DEL RIESGO													
9	Recibe capacitación constante sobre seguridad de la información y gestión de riesgos				X				X				X	
10	El conocimiento adquirido en las capacitaciones lo aplica en sus actividades diarias				X				X				X	
11	Identifica amenazas que pueden afectar el desarrollo de las actividades diarias				X				X				X	
12	Evalúa amenazas que pueden afectar el desarrollo de las actividades diarias				X				X				X	
13	Implementa las acciones eficaces necesarias para afrontar los riesgos				X				X				X	
N°	DIMENSIONES / ítems													Sugerencias
	DIMENSION 3: BASE DE LA TECNOLOGIA DE LA INFORMACION EFICAZ				X				X				X	
14	Se garantiza la rapidez de respuesta de los sistemas de información				X				X				X	
15	Cuenta con un plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas				X				X				X	
16	Cuenta con un plan de contingencia para recuperación de la información en caso de desastres				X				X				X	
17	Establece controles preventivos frente a errores humanos en el tratamiento de la información.				X				X				X	
18	Tiene la voluntad de aplicar controles de seguridad de la información en sus labores diarias de trabajo				X				X				X	

Observaciones: _____

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

Apellidos y Nombres del Juez validador Dr. Javier Fernando Díaz Molinari **DNI: 29594699**

Especialidad del validador: Doctor en Administración

04 de diciembre del 2021

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

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

Firma del Experto Informante.
Docente de posgrado: Gestión Pública

Certificado de Validez de contenido del Instrumento que mide Seguridad de la Información

Inventario Seguridad de la Información

Nº	DIMENSIONES / ítems	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
		MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
	DIMENSIÓN 1: CONFIDENCIALIDAD													
1	Cumple activamente con los procedimientos de Protección de la información.				X				X				X	
2	Los accesos a los ambientes de trabajo siempre se encuentran protegidos.				X				X				X	
3	Gestiona la aplicación de los procedimientos de protección y mantenimiento de redes informáticas.				X				X				X	
4	Siempre se usa la técnica criptográfica como la firma digital para validar la documentación.				X				X				X	
5	La información crítica del proceso se encuentra en ambientes seguros y resguardados bajo llaves.				X				X				X	
6	Cambia periódicamente las contraseñas de acceso a sus aplicativos.				X				X				X	
	DIMENSIÓN 2: INTEGRIDAD													
7	Establece controles de protección de datos frente a modificaciones , eliminaciones por entes no autorizados				X				X				X	
8	Garantiza la fiabilidad de los equipos informáticos, funcionan adecuadamente.				X				X				X	
9	Establece medidas de prevención contra ataques de virus informáticos.				X				X				X	
10	Gestiona el Backup de almacenamiento y/o copias de respaldo.				X				X				X	
11	Participa activamente en las auditorias periódicas de sistemas de información				X				X				X	
12	Gestiona el desarrollo de software bajo técnicas criptográficas para la protección de la información				X				X				X	
Nº	DIMENSIONES / ítems													Sugerencias
	DIMENSIÓN 3: DISPONIBILIDAD													
13	El acceso a la información se encuentre disponible para realizar las labores.				X				X				X	
14	Se garantiza la rapidez de respuesta de los sistemas de información				X				X				X	
15	Cuenta con un plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas				X				X				X	
16	Cuenta con un plan de contingencia para recuperación de la información en caso de desastres				X				X				X	
17	Establece controles preventivos frente a errores humanos en el tratamiento de la información.				X				X				X	
18	Tiene la voluntad de aplicar controles de seguridad de la información en sus labores diarias de trabajo				X				X				X	

Observaciones: _____

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

Apellidos y nombres del juez validador Dr. / Mg: Luis Enrique León Alvarado..... **DNI: 09742840**

Especialidad del validador: Gestión Publica .....

04 .de…Diciembre…… del 2021…

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

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

---

Firma del Experto Informante.

Especialidad

Certificado de Validez de contenido del Instrumento que mide Gestión del Riesgo

Inventario Gestión del Riesgo

Nº	DIMENSIONES / ítems	Pertinencia[1]				Relevancia[2]				Claridad[3]				Sugerencias
		MD	D	A	MA	MD	D	A	MA	MD	D	A	MA	
	DIMENSIÓN 1: PROCESO DE GOBERNANZA DE RIESGOS													
1	Cumple con la Política de Gestión de Riesgos de la Institución				X				X				X	
2	Implementa políticas con la finalidad de mitigar los riesgos de seguridad de la información				X				X				X	
3	Los controles implementados en la gestión del riesgo son eficaces				X				X				X	
4	Participa en la implementación de oportunidades y /o procesos de mejora continua				X				X				X	
5	Participa activamente en la identificación de riesgos				X				X				X	
6	Evalúa riesgos que pueden afectar el desarrollo de las actividades diarias				X				X				X	
7	Prioriza los riesgos que tienen sus actividades laborales				X				X				X	
8	Realiza el seguimiento y monitoreo de los controles implementados para los riesgos identificados				X				X				X	
	DIMENSION 2: CULTURA CONSCIENTE DEL RIESGO													
9	Recibe capacitación constante sobre seguridad de la información y gestión de riesgos				X				X				X	
10	El conocimiento adquirido en las capacitaciones lo aplica en sus actividades diarias				X				X				X	
11	Identifica amenazas que pueden afectar el desarrollo de las actividades diarias				X				X				X	
12	Evalúa amenazas que pueden afectar el desarrollo de las actividades diarias				X				X				X	
13	Implementa las acciones eficaces necesarias para afrontar los riesgos				X				X				X	
Nº	DIMENSIONES / ítems													Sugerencias
	DIMENSIÓN 3: BASE DE LA TECNOLOGIA DE LA INFORMACIÓN EFICAZ													
14	Se garantiza la rapidez de respuesta de los sistemas de información				X				X				X	
15	Cuenta con un plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas				X				X				X	
16	Cuenta con un plan de contingencia para recuperación de la información en caso de desastres				X				X				X	
17	Establece controles preventivos frente a errores humanos en el tratamiento de la información.				X				X				X	
18	Tiene la voluntad de aplicar controles de seguridad de la información en sus labores diarias de trabajo				X				X				X	

Observaciones: _____

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

Apellidos y nombres del juez validador Dr. / Mg: ..... Luis Enrique León Alvarado ..... **DNI: 09742840**

Especialidad del validador:.....

04 .de...Diciembre..... del 2021...

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

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

---

Firma del Experto Informante.

Especialidad

ANEXO 6: ANALISIS DESCRIPTIVO – TABLAS DE FRECUENCIAS SEGURIDAD DE LA INFORMACIÓN - SPSS

1. Cumple activamente con los procedimientos de Protección de la información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALGUNAS VECES	2	4,4	4,4	4,4
	CASI SIEMPRE	20	44,4	44,4	48,9
	SIEMPRE	23	51,1	51,1	100,0
	Total	45	100,0	100,0	

2. Los accesos a los ambientes de trabajo siempre se encuentran protegidos.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	2	4,4	4,4	6,7
	ALGUNAS VECES	14	31,1	31,1	37,8
	CASI SIEMPRE	20	44,4	44,4	82,2
	SIEMPRE	8	17,8	17,8	100,0
	Total	45	100,0	100,0	

3. Gestiona la aplicación de los procedimientos de protección y mantenimiento de redes informáticas.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	5	11,1	11,1	11,1
	ALGUNAS VECES	10	22,2	22,2	33,3
	CASI SIEMPRE	21	46,7	46,7	80,0
	SIEMPRE	9	20,0	20,0	100,0
	Total	45	100,0	100,0	

4. Siempre se usa la técnica criptográfica como la firma digital para validar la documentación.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	17	37,8	37,8	37,8
	CASI NUNCA	1	2,2	2,2	40,0
	ALGUNAS VECES	3	6,7	6,7	46,7
	CASI SIEMPRE	13	28,9	28,9	75,6
	SIEMPRE	11	24,4	24,4	100,0
	Total	45	100,0	100,0	

5. La información crítica del proceso se encuentra en ambientes seguros y resguardada bajo llaves.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	1	2,2	2,2	2,2
	ALGUNAS VECES	6	13,3	13,3	15,6
	CASI SIEMPRE	24	53,3	53,3	68,9
	SIEMPRE	14	31,1	31,1	100,0
	Total	45	100,0	100,0	

6. Cambio periódicamente las contraseñas de acceso a sus aplicativos.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALGUNAS VECES	7	15,6	15,6	15,6
	CASI SIEMPRE	26	57,8	57,8	73,3
	SIEMPRE	12	26,7	26,7	100,0
	Total	45	100,0	100,0	

7. Establece controles de protección de datos frente a modificaciones , eliminaciones por entes no autorizados

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	4	8,9	8,9	11,1
	ALGUNAS VECES	5	11,1	11,1	22,2
	CASI SIEMPRE	24	53,3	53,3	75,6
	SIEMPRE	11	24,4	24,4	100,0
	Total	45	100,0	100,0	

8. Garantiza la fiabilidad de los equipos informáticos, funcionan adecuadamente.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALGUNAS VECES	7	15,6	15,6	15,6
	CASI SIEMPRE	27	60,0	60,0	75,6
	SIEMPRE	11	24,4	24,4	100,0
	Total	45	100,0	100,0	

9. Establece medidas de prevención contra ataques de virus informáticos.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	3	6,7	6,7	6,7
	ALGUNAS VECES	5	11,1	11,1	17,8
	CASI SIEMPRE	24	53,3	53,3	71,1
	SIEMPRE	13	28,9	28,9	100,0
	Total	45	100,0	100,0	

10. Gestiona el Backup de almacenamiento y/o copias de respaldo.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	2	4,4	4,4	4,4
	ALGUNAS VECES	6	13,3	13,3	17,8
	CASI SIEMPRE	21	46,7	46,7	64,4
	SIEMPRE	16	35,6	35,6	100,0
	Total	45	100,0	100,0	

11. Participa activamente en las auditorias periódicas de sistemas de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALGUNAS VECES	11	24,4	24,4	24,4
	CASI SIEMPRE	20	44,4	44,4	68,9
	SIEMPRE	14	31,1	31,1	100,0
	Total	45	100,0	100,0	

12. Gestiona el desarrollo de software bajo técnicas criptográficas para la protección de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	1	2,2	2,2	4,4
	ALGUNAS VECES	9	20,0	20,0	24,4
	CASI SIEMPRE	22	48,9	48,9	73,3
	SIEMPRE	12	26,7	26,7	100,0
	Total	45	100,0	100,0	

13. El acceso a la información se encuentre disponible para realizar las labores.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	4	8,9	8,9	8,9
	ALGUNAS VECES	7	15,6	15,6	24,4
	CASI SIEMPRE	18	40,0	40,0	64,4
	SIEMPRE	16	35,6	35,6	100,0
	Total	45	100,0	100,0	

14. Se garantiza la rapidez de respuesta de los sistemas de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	1	2,2	2,2	4,4
	ALGUNAS VECES	5	11,1	11,1	15,6
	CASI SIEMPRE	17	37,8	37,8	53,3
	SIEMPRE	21	46,7	46,7	100,0
	Total	45	100,0	100,0	

15. Cuenta con un plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALGUNAS VECES	10	22,2	22,2	22,2
	CASI SIEMPRE	20	44,4	44,4	66,7
	SIEMPRE	15	33,3	33,3	100,0
	Total	45	100,0	100,0	

16. Cuenta con un plan de contingencia para recuperación de la información en caso de desastres

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	1	2,2	2,2	2,2
	ALGUNAS VECES	7	15,6	15,6	17,8
	CASI SIEMPRE	20	44,4	44,4	62,2
	SIEMPRE	17	37,8	37,8	100,0
	Total	45	100,0	100,0	

17. Establece controles preventivos frente a errores humanos en el tratamiento de la información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	1	2,2	2,2	2,2
	ALGUNAS VECES	3	6,7	6,7	8,9
	CASI SIEMPRE	21	46,7	46,7	55,6
	SIEMPRE	20	44,4	44,4	100,0
	Total	45	100,0	100,0	

18.Tiene la voluntad de aplicar controles de seguridad de la información en sus labores diarias de trabajo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	1	2,2	2,2	2,2
	ALGUNAS VECES	3	6,7	6,7	8,9
	CASI SIEMPRE	24	53,3	53,3	62,2
	SIEMPRE	17	37,8	37,8	100,0
	Total	45	100,0	100,0	

ANEXO 7: ANALISIS DESCRIPTIVO – TABLAS DE FRECUENCIAS GESTION DEL RIESGO – SPSS

1. Cumple con la Política de Gestión de Riesgos de la Institución

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	2	4,4	4,4	6,7
	ALGUNAS VECES	9	20,0	20,0	26,7
	CASI SIEMPRE	19	42,2	42,2	68,9
	SIEMPRE	14	31,1	31,1	100,0
	Total	45	100,0	100,0	

2. Implementa políticas con la finalidad de mitigar los riesgos de seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	4	8,9	8,9	11,1
	ALGUNAS VECES	9	20,0	20,0	31,1
	CASI SIEMPRE	17	37,8	37,8	68,9
	SIEMPRE	14	31,1	31,1	100,0
	Total	45	100,0	100,0	

3. Los controles implementados en la gestión del riesgo son eficaces

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	4	8,9	8,9	11,1
	ALGUNAS VECES	9	20,0	20,0	31,1
	CASI SIEMPRE	22	48,9	48,9	80,0
	SIEMPRE	9	20,0	20,0	100,0
	Total	45	100,0	100,0	

4. Participa en la implementación de oportunidades y /o procesos de mejora continua

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	5	11,1	11,1	13,3
	ALGUNAS VECES	6	13,3	13,3	26,7
	CASI SIEMPRE	19	42,2	42,2	68,9
	SIEMPRE	14	31,1	31,1	100,0
	Total	45	100,0	100,0	

5. Participa activamente en la identificación de riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	4	8,9	8,9	8,9
	CASI NUNCA	5	11,1	11,1	20,0
	ALGUNAS VECES	6	13,3	13,3	33,3
	CASI SIEMPRE	22	48,9	48,9	82,2
	SIEMPRE	8	17,8	17,8	100,0
	Total	45	100,0	100,0	

6. Evalúa riesgos que pueden afectar el desarrollo de las actividades diarias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	3	6,7	6,7	6,7
	CASI NUNCA	2	4,4	4,4	11,1
	ALGUNAS VECES	4	8,9	8,9	20,0
	CASI SIEMPRE	22	48,9	48,9	68,9
	SIEMPRE	14	31,1	31,1	100,0
	Total	45	100,0	100,0	

7. Prioriza los riesgos que tienen sus actividades laborales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	3	6,7	6,7	6,7
	CASI NUNCA	4	8,9	8,9	15,6
	ALGUNAS VECES	3	6,7	6,7	22,2
	CASI SIEMPRE	22	48,9	48,9	71,1
	SIEMPRE	13	28,9	28,9	100,0
	Total	45	100,0	100,0	

8. Realiza el seguimiento y monitoreo de los controles implementados para los riesgos identificados

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALGUNAS VECES	6	13,3	13,3	13,3
	CASI SIEMPRE	21	46,7	46,7	60,0
	SIEMPRE	18	40,0	40,0	100,0
	Total	45	100,0	100,0	

9. Recibe capacitación constante sobre seguridad de la información y gestión de riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	3	6,7	6,7	6,7
	ALGUNAS VECES	4	8,9	8,9	15,6
	CASI SIEMPRE	23	51,1	51,1	66,7
	SIEMPRE	15	33,3	33,3	100,0
	Total	45	100,0	100,0	

10. El conocimiento adquirido en las capacitaciones lo aplica en sus actividades diarias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	2	4,4	4,4	4,4
	ALGUNAS VECES	9	20,0	20,0	24,4
	CASI SIEMPRE	24	53,3	53,3	77,8
	SIEMPRE	10	22,2	22,2	100,0
	Total	45	100,0	100,0	

11. Identifica amenazas que pueden afectar el desarrollo de las actividades diarias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	ALGUNAS VECES	10	22,2	22,2	22,2
	CASI SIEMPRE	24	53,3	53,3	75,6
	SIEMPRE	11	24,4	24,4	100,0
	Total	45	100,0	100,0	

12. Evalúa amenazas que pueden afectar el desarrollo de las actividades diarias

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	1	2,2	2,2	4,4
	ALGUNAS VECES	13	28,9	28,9	33,3
	CASI SIEMPRE	18	40,0	40,0	73,3
	SIEMPRE	12	26,7	26,7	100,0
	Total	45	100,0	100,0	

13. Implementa las acciones eficaces necesarias para afrontar los riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	4	8,9	8,9	8,9
	ALGUNAS VECES	4	8,9	8,9	17,8
	CASI SIEMPRE	17	37,8	37,8	55,6
	SIEMPRE	20	44,4	44,4	100,0
	Total	45	100,0	100,0	

14. Cuenta con la infraestructura tecnológica adecuada , para la realización de sus labores

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	2	4,4	4,4	4,4
	ALGUNAS VECES	4	8,9	8,9	13,3
	CASI SIEMPRE	22	48,9	48,9	62,2
	SIEMPRE	17	37,8	37,8	100,0
	Total	45	100,0	100,0	

15. Cambia usted sin autorización las aplicaciones o software que se encuentran en su computador poniendo en riesgo la seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	1	2,2	2,2	2,2
	ALGUNAS VECES	11	24,4	24,4	26,7
	CASI SIEMPRE	24	53,3	53,3	80,0
	SIEMPRE	9	20,0	20,0	100,0
	Total	45	100,0	100,0	

16. Reporta y/o Comunica incidentes que pongan en riesgo la seguridad de la información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NUNCA	1	2,2	2,2	2,2
	CASI NUNCA	1	2,2	2,2	4,4
	ALGUNAS VECES	10	22,2	22,2	26,7
	CASI SIEMPRE	16	35,6	35,6	62,2
	SIEMPRE	17	37,8	37,8	100,0
	Total	45	100,0	100,0	

17. El diseño y desarrollo de software se realizan en entornos seguros

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	1	2,2	2,2	2,2
	ALGUNAS VECES	1	2,2	2,2	4,4
	CASI SIEMPRE	25	55,6	55,6	60,0
	SIEMPRE	18	40,0	40,0	100,0
	Total	45	100,0	100,0	

18. La administración renueva la tecnología en pro de la seguridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	2	4,4	4,4	4,4
	ALGUNAS VECES	5	11,1	11,1	15,6
	CASI SIEMPRE	20	44,4	44,4	60,0
	SIEMPRE	18	40,0	40,0	100,0
	Total	45	100,0	100,0	