UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Ciberseguridad para el Proceso de Gestión de Riesgos de TI en una Empresa Transnacional, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de Información

AUTOR:

Flores Cortez, Robinson Anderson (orcid.org/0000-0003-3299-1577)

ASESOR:

Dr. Acuña Benites, Marlon Frank (orcid.org/0000-0001-5207-9353)

CO-ASESOR:

Dr. Pereyra Acosta, Manuel Antonio (orcid.org/0000-0002-2593-5772)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

Dedicatoria

A Dios, a mi Madre quién día a día estuvo allí en apoyo para seguir adelante; asimismo, a mi Padre, quién en vida siempre fue motivación e incentivo mi desarrollo personal profesional y ahora desde el cielo sigue siendo una gran motivación para seguir creciendo.

A mis hijos quienes con una sola sonrisa fueron un gran impulso para no descansar en lograr mis metas, pasos que ellos seguirán. También a mis seres queridos por darme siempre el apoyo moral y emocional.

Agradecimiento

A mi asesor y a los docentes que ayudaron a realizar la presente investigación. Finalmente, a las personas que quiero y que vivieron mi día a día dándome todo su apoyo y motivación, lo que quedara grabado para siempre en mi corazón.

Índice de Contenidos

Pg.

Carátula
Dedicatoria ii
Agradecimiento iii
Índice de Contenidos iv
Índice de Tablas v
Índice de gráficos y figuras vi
Resumen vii
Abstract viii
I. INTRODUCCIÓN 1
II. MARCO TEÓRICO 5
III. METODOLOGÍA 14
3.1. Tipo y diseño de investigación 14
3.2. Variables y operacionalización 15
3.3. Población, muestra y muestreo 16
3.4. Técnicas e instrumentos de recolección de datos 17
3.5. Procedimientos 17
3.6. Método de análisis de datos 18
3.7. Aspectos éticos 19
IV. RESULTADOS 20
V. DISCUSIÓN 37
VI. CONCLUSIONES 43
VII. RECOMENDACIONES 45
REFERENCIAS 48
ANEXOS

Índice de Tablas

Tabla 1 Tabla de frecuencia y percepción de la variable independiente 20
Tabla 2 Tabla de frecuencia y percepción de la variable dependiente 21
Tabla 3 Tabla de frecuencias por cada dimensión Disponibilidad 22
Tabla 4 Tabla de frecuencias por cada dimensión Confidencialidad 23
Tabla 5 Tabla de frecuencias por cada dimensión Integridad 24
Tabla 6 Tabla de frecuencias por cada dimensión Proceso de gobernanza del riesgo 25
Tabla 7 Tabla de frecuencias por cada dimensión Cultura consciente del riesgo 26
Tabla 8. Recursos Humanos 86
Tabla 9. Recursos de Hardware 86
Tabla 10. Resumen de presupuesto 87

Índice de gráficos y figuras

Figura 1. Que es la seguridad de la información 12
Figura 2. Preguntas seguridad de la información 12
Figura 3. Arbol de gestión de riesgos 13
Figura 4. Esquema 14
Figura 5. Pilares de gestión de seguridad de la información. 16

Resumen

El objetivo de la presente investigación “Ciberseguridad para el Proceso de Gestión de Riesgos de TI en una Empresa Transnacional, Lima 2023” es la de determinar la relación existente entre la Ciberseguridad y la Gestión de Riesgos de TI. Para tal fin y metodológicamente hablando se utilizó el enfoque cuantitativo, con un tipo de investigación aplicada, con diseño preexperimental, donde la población fue de 30 trabajadores del departamento de TI de la organización. La técnica que se utilizó fue la de recolección de datos, utilizando la encuesta como instrumento de recolección de datos. El método de análisis de datos fue descriptivo, para la prueba de hipótesis se utilizó la prueba de coeficiente de Spearman y para el manejo de los datos se utilizó la herramienta estadística SPSS.

Como resultado se obtuvo que confiabilidad de las variables es excelente y los datos no tienen distribución normal, después de las pruebas realizadas se obtuvo como resultado un valor de significancia de 0 además de un Rho de Spearman de 0.833, dando como conclusión que Existe una relación directa entre la Ciberseguridad y la Gestión de Riesgos de TI, lo que demuestra la dependencia entre ambas variables.

Palabras Claves: ciberseguridad, gestión de riesgos, disponibilidad, confidencialidad, integridad.

Abstract

The objective of this research "Cybersecurity for the IT Risk Management Process in a Transnational Company, Lima 2023" is to determine the relationship between Cybersecurity and IT Risk Management. For this purpose and methodologically speaking, the qualitative approach was shown, with a type of applied research, with a pre-experimental design, where the population was 30 workers from the organization's IT department. The technique that was captured was that of data collection, using the survey as a data collection instrument. The data analysis method was descriptive, for the hypothesis test the Spearman coefficient test was obtained and for data management the statistical tool SPSS was obtained.

As a result, it was obtained that the reliability of the variables is excellent and the data does not have a normal distribution, after the tests carried out, a significance value of 0 was obtained as a result, in addition to a Spearman's Rho of 0.833, concluding that there is a direct relationship between Cybersecurity and IT Risk Management, which demonstrates the dependence between both variables.

Keywords: cybersecurity, risk management, availability, confidentiality, integrity.

I. INTRODUCCIÓN

Actualmente vivimos en un entorno global tecnológico muy cambiante, debido a que las distintas Tecnologías de Información (TI) evolucionan constantemente y se vuelven cada vez más indispensables en distintos ámbitos, tanto para las grandes y pequeñas empresas, para el uso comercial y personal; es así como esta conlleva a nuevos retos y riesgos asociados, como lo son los ciberataques de distintas formas, phishing, scamming, ingeniería social, ingeniería inversa, secuestro de datos (Ransomware) entre otros. En una investigación realizada por Deloitte (2021) menciona que una gran cantidad de empresas implementaron distintas formas de trabajo remoto, adoptando soluciones en la nube con gastos estimados en $360 billones para el 2022, sirviendo esto para que las empresas brinden mejores soluciones y más dinamismo pero a su vez esto conlleva a mayores incidentes y ataques, que ponen a los servicios en riesgo, siendo esta una gran oportunidad para los ciberdelincuentes que tienen como fin explotar las distintas debilidades tecnológicas que pudieran existir, lo que podría afectar el desarrollo normal de un negocio y paralización de servicios y/o procesos.

Es así como todas estas amenazas hacen que cada vez se pongan mayores esfuerzos para mitigar o que el impacto sea mínimo cuando se está ante cibercriminales, estos además cada día mejoran sus ataques, haciendo que las defensas deban estar encendidas y alertas en todo momento; la “Agencia de la Unión Europea para la Ciberseguridad” ENISA (2019) menciona que en dicho año hubo un incremento de un 80% de incidencias provocadas por cibercriminales en comparación con el año anterior. Aun con estos números, una gran cantidad de organizaciones no hacen lo necesario por invertir en una adecuada gestión de riesgos y ciberseguridad, ocasionando que exista perdidas del activo más valioso que tienen, la información y afectando considerablemente la continuidad de sus negocios.

En América latina somos testigos de cómo el ciberespacio va evolucionando con la masificación del internet de las cosas, tal es así que Valenzuela (2017) indica que estamos viviendo nuevos escenarios que nos obliga a tomar otras medidas

tanto personales y organizacionales, tanto en el diseño, como ejecución de políticas que ayudan a los actores involucrados a minimizar los riesgos que esto conlleva. En la región, diversos países están tomando interés en políticas y estrategias de ciberseguridad para que sean orientados desde el estado. También se menciona que Chile se ostenta altas tasas de penetración, debido a que más del 70% de población está conectada a internet.

Cada vez es más común el uso de plataformas en línea con ayuda de las TIC lo que ha permitido que el comercio electrónico fluya más aun en pandemia, pero esto trae consigo las amenazas de seguridad, tal es que Becerril (2019) menciona que los países cada vez dependen más de los sistemas informáticos en línea, pero que no existe ningún medio que se debe considerar seguro en el mundo del internet, que los gobiernos e instituciones hacen denodados esfuerzo por mitigarlos, y que el costo de inacción de una adecuada gestión de ciberseguridad puede ser mucho mayor. Es por ello que conforme pasa el tiempo es más común escuchar sobre hacking o ciberataques en línea y a los sistemas propios de las instituciones, haciendo que el tema de la ciberseguridad y la protección de información sea cada vez más relevante, ya que las organizaciones están tomando conciencia que el bien más preciado es su propia información.

Para ESAN (2019) según recientes estudios la principal preocupación de las empresas en la region, son los riesgos de la ciberdelincuencia que han crecido de manera exponencial en estos últimos años. En este mismo estudio se detalla que los riesgos de la ciberdelincuencia ha pasado del robo de datos a esquemas mas complejos, que afectan tanto a grandes industrias y a pequeños negocios, en toda la cadena de suministro, ademas mencionan que el 73% de las empresas encuestadas asegura que los riesgos ciberneticos son su principal preocupación.

En Perú cada vez se hace más frecuente saber que una organización o entidad ha sufrido un ataque por cibercriminales que dio como resultado la afectación de los servicios y el daño a la información, que en muchos casos ha sido irrecuperable, Diario Gestion (2019) precisa que ante el inicio de la cuarentena y el

auge del uso de dispositivo móviles para todas las transacciones, conllevó a que los ataques cibernéticos a estos dispositivos se duplicaran, además que los correos con información falsa (pishing) aumentó en un 25% al iniciar el mismo año, haciendo hincapié en que los cibercriminales no dan tregua y que los expertos en cyberdefensa en las organizaciones deben redoblar esfuerzos a fin de dar batalla a la ciberdelincuencia, previniendo, mitigando y reaccionando adecuadamente ante un desastre a puertas.

Es el caso de una reconocida empresa multinacional motivo de la presente investigación, sufrió un ataque de denegación de servicios en el año 2020, que dejó sin acceso a toda la región al sistema ERP propio utilizado, tal es que tampoco fue posible realizar ninguna venta, ni el manejo del inventario, en dicho momento se activó el manejo de la venta por contingencia, realizándose de manera manual por el lapso de 48 horas, esto demostró e hizo ver que se estaba protegiendo de manera inadecuada los servicios lo que llevo a representar pérdidas cuantiosas en los países de la región, estos daños pudieron haberse evitado con una forma adecuada de implementar y/o usar la gestión de las TI, habiendo realizado testing previos de penetración y encubrimiento adecuado de los servicios públicos.

Esta investigación tiene justificación teórica ya que se relata en el marco teórico y conceptual, Según Baena (2017) esto va ligado con el fin del investigador sobre profundizar distintos enfoques de conocimientos en una misma línea de investigación, también se detalla en las dimensiones, siempre tomando en cuenta el amplio uso de revistas científicas, libros indexados y artículos del rubro de ciberseguridad de procedencia científica mundial, los cuales nos permiten contrastar y tener un mejor criterio, así como un mejor enfoque y el aporte de conocimientos adquiridos sobre la ciberseguridad y la correcta administración de TI. Además, se tiene la justificación práctica, que nos permite resolver una interrogante en la organización respecto a la seguridad y poder conocer las debilidades que actualmente tiene toda la infraestructura de TI. Para la justificación metodológica, ya que todas las actividades que se realizan se basan en las buenas prácticas de seguridad que sumadas a la metodología Ethical Hacking nos dan un resultado bastante claro de la situación de vulnerabilidad actual, además considerar

que la metodología antes mencionada cubre el amplio espectro de la seguridad tanto en hardware y software, lo que la hace más completa, siempre en el ámbito académico y científico con fines de prevención y dejando los resultados para conocimiento de la organización.

Según lo mencionado y con el fin de ayudar a resolver un problema en la organización que se menciona, se establece como OG “Determinar la relación existente entre Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023”. Así también se formula los siguientes OE los cuales son, OE1 “Determinar la relación existente entre la dimensión Disponibilidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023”. OE2 “Determinar la relación existente entre la dimensión Confidencialidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023”. OE3 “Determinar la relación existente entre la dimensión Integridad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023”.

En tanto como HG se plantea lo siguiente, “Existe una relación directa entre la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023”. Como HE1 “Existe una relación directa entre la dimensión Disponibilidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023”. Como HE2 “Existe una relación directa entre la dimensión Confidencialidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima 2023”. Y finalmente como HE3 “Existe una relación directa entre la dimensión Integridad de datos de la Ciberseguridad y la Gestión de Riesgos de TI en una empresa Transnacional en Lima 2023.”

II. MARCO TEÓRICO

A nivel internacional, en un estudio sobre SI “Seguridad de la información”, desarrollado en una corporación de productos para el consumo humano o alimentos a nivel de industria, Arévalo (2017) realizó un estudio transversal básico no experimental que incluye pruebas previas y posteriores. Era el proceso de producción de la misma empresa. Dicha investigación posibilita la definición de variables de gestión de riesgos y fortalece la presentación de propuestas para implementación de SGSI, además de haber referenciado a una de las conclusiones del proyecto referente a la relación entre los SGSI basados en riesgos y gestión de estos.

De otro lado Crespo (2016) en el proyecto de investigación sobre Metodologías de GSI “Gobierno de Seguridad de la Información” para analizar y mejorar el manejo y gestión del risk o riesgo aplicable, la que se aplica a las PYMES, fue realizado por un estudio tipo básico de diseño no experimental usando un corte trasversal par el pre y post test, donde eligió población y muestra a 50 pequeñas y medianas empresas. Tal como el estudio lo indica se evaluó en qué estado se encontraba respecto al aseguramiento de la información, es así que obtuvo como conclusión que y la cual se usó para el presente proyecto de investigación donde se menciona que es de vital importancia una adecuada gestión de riesgos de los activos de información estos cruzándose con las dimensiones de evaluación, así como el de tratamiento de riesgos obtenidos para poder mitigarlos de mejor manera.

En una investigación realizada sobre políticas de SI “Seguridad de la información” y la gestión en riesgos por Muñoz (2016), menciona que su investigación fue del tipo básica, con un diseño no experimental con un corte transversal de un antes y después de la prueba lo que se resumen en 2 tiempos. Su población y muestra del presente estudio aplico los fundamentos básicos de 11 de los dominios de seguridad de TI de la Norma ISO27002. Donde además las conclusiones hacen referencias a las dimensione del presente proyecto, sobre disponibilidad, confidencialidad y la integridad de los activos de información en las

organizaciones, ya que estos son piezas claves y vitales para el desarrollo de una empresa y por consiguiente mejora el compliance de las políticas, para mejorar las mitigaciones de riesgos o que estén en un nivel permitido o lo que se llama riesgo asumido.

Por otro lado, Molina (2015) en una investigación sobre SGSI “Gestión de Riesgos de TI” aplicado para una institución Militar Técnico Superior, hizo un estudio básico, de diseño no-experimental con un corte transversal o pre y post test. Donde uso como población y muestra a todo el personal de la base de la escuela politécnica del litoral de dicho país. Con esta investigación se pudo obtener indicaciones, dimensiones sobre gestión de riesgo de TI así como normas internacionales, para que de esta manera se pueda obtener un mejor framework de referencia sobre seguridad de la información y metodología, como lo es MAGERIT, que relaciona la gestión de riesgos y su otro pilar seguridad de la información o ciberseguridad.

Un estudio sobre la gestión SGSI de Castro (2014). La ciudad de Quito está realizando dicha investigación básica con diseño transversal no experimental. A partir de esto fue posible obtener la variable de seguridad de la información (SI) que revelan los atributos que contiene. Una conclusión establece que la SI se basa en la disponibilidad de información de seguridad principalmente, dentro de una organización para reducir el riesgo.

Maggiore (2014) hizo un estudio de tipo básico con un diseño transversal no experimental en un estudio sobre la evaluación de la madurez en la gestión de la seguridad de la información. En 2009 se realizó un corte para analizar y recopilar información sobre el modelo de madurez sobre gestión de seguridad de TI, donde una de sus conclusiones, da como resultado y proporciona un marco integrado para la gestión de riesgos en el que se basa la propuesta final. La aplicación del sistema de seguridad de la información adecuado basado en controles para gestión de riesgos es claramente el modelo que las empresas deben seguir para proteger la información confidencial que se procesa.

Como antecedente nacional se tiene a Otoya (2018) en su trabajo de investigación sobre gestión de los riesgos de las TI y seguridad de la información, SGSI quien realizó una investigación básica con un diseño no-experimental transversal. Se utilizó la causalidad estadística donde su población estuvo formada por 174 colaboradores y/o trabajadores y se encontró que la gestión de riesgos TI tiene un impacto significativo en la seguridad de la información. La mencionada contribuyó a la aplicación de su estado de arte en la teoría de la majerita y sus recursos de información.

Tacza (2018) realizó un estudio prototipo con un diseño transversal no experimental en un estudio de planificación de la seguridad de la información relacionado con la norma ISO 27000. Se utilizó un método de correlación estadística. Se requirió del personal administrativo para la población (100 personas) obteniendo una muestra de 80 empleados. Se concluyo de manera significativa la relación de las dimensiones de la variable dependiente “disponibilidad, integridad y confidencialidad”, corroborando que existe un vínculo directo con la norma “ISO/IEC 27001:2005”. Desde una perspectiva de gestión de riesgos, esto demuestra que está directamente relacionado con la difusión de información.

Pinto (2017) en su estudio de tipo básico con un diseño no experimental y transversal en un estudio sobre gestión y riesgos de seguridad de la información en la academia militar de suboficiales Puente Piedra en el año 2016. Se utilizó un método de correlación estadística. Este tuvo como población a los 117 docentes de la academia de suboficiales de la P.N.P. – Puente Piedra, se muestreó a toda la población. Una conclusión se refiere a la dimensione de gestión de riesgos y seguridad de la información SGSI donde se tiene como conclusión que se reafirma la existencia de relación directa entre ambas variables.

Por otro lado, en el siguiente estudio Mercado (2016), en su proyecto de estudio sobre modelos de GSI para e-government, este llevo a cabo una investigación de tipo básica con un diseño no experimental transversal. Donde se utilizó a 69 entidad del sector público como población con el mismo tamaño en la muestra. Realizando una revisión de los modelos de ciberseguridad de la

información basados en estándares SGSI que definen las organizaciones y funciones de seguridad de la información. Una conclusión se relaciona con la relación entre las dimensiones de disponibilidad y los controles de seguridad para la gestión de riesgos.

Seclen (2016) realizo y llevo a cabo un estudio “Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001” realizo un estudio no experimental de diseño transversal de tipo básico en un estudio de factores que inciden en la implementación de SGSI en instituciones públicas peruanas. Esto es útil ya que proporciono los factores relacionados con la Seguridad de TI respecto a las normas de seguridad.

Tarrilo (2015), en su estudio sobre el impacto de la gestión de riesgos de TI, realizó un tipo de estudio básico utilizando un diseño experimental y transversal. Se utilizó un método de correlación estadística. Donde tuvo como población una muestra aleatoria de 150 trabajadores y 50 trabajadores de la Sede Zona III de Inscripción de Moyobamba. Como resultado, este trabajo proporciona un vínculo directo entre los activos de información relacionados con la SGSI. Por lo tanto, apoyamos esta actividad de investigación.

El trabajo nacional anterior contribuyó al trabajo de investigación actual para identificar calificaciones otorgadas por agencias para variables de investigación, seguridad de la información y gestión de riesgos. Diseñado para utilizar herramientas aplicables a la empresa lo mismo que aplico Llontop. (2018) en su estudio teniendo las mismas variables y también ambos usaron las políticas que se aplicaran al final de la presente investigación.

En cuanto al enfoque teórico, existen variables de ciberseguridad, y está la detección definida por Shin y Lowry (2020), donde la fase de detección detalla las amenazas involucradas, sus orígenes y las estrategias mediante las cuales se pueden tomar contramedidas. Está de acuerdo con los planes y métodos del atacante. Desde otra perspectiva, AlShboul et al. (2018) dijo que la identificación

de los mismos se enfoca en comprender y administrar prácticas que los usuarios pueden adoptar, así como herramientas y tecnologías de protección que crean bloqueos más fuertes para posibles ataques cibernéticos de seguridad.

Según definimos las dimensiones Mozaffari et al. (2019) define la prevención como aquella etapa que su fin principal, es la de ofrecer soluciones basadas en el internet de las cosas (IoT) que mejoran las condiciones fisiológicas, físicas y ambientales para prevenir fallos en los servicios. En una perspectiva diferente, García y Gonzales (2013) señalan que la prevención está relacionada con la preparación de los usuarios humanos y junto con las máquinas que ayudan a proteger frente a algún tipo de ciber amenaza para que la gestión adecuada de la seguridad y la seguridad y Evitar tecnologías que sean fáciles de derivación. En otro punto de vista, Arend et al. (2020) señalan que la prevención es la toma de medidas esperadas que podrían poner en peligro a los usuarios en las empresas, en particular incluye tomar medidas específicas en medidas de seguridad que pueden reducir el riesgo de ciberataques.

Desde otra perspectiva, Arend et al. (2020) la prevención apunta a tomar comportamientos esperados que podrían poner en riesgo a los usuarios de la empresa, especialmente incluyendo comportamientos específicos relacionados con medidas de seguridad que pueden reducir el riesgo de ataques cibernéticos. En cuanto a la segunda dimensión de la variable, titulada ciberseguridad, tenemos la detección definida por Shin y Lowry (2020), en la que la fase de detección proporciona detalles sobre las amenazas relevantes, sus orígenes y las estrategias para abordar las contramedidas. Siga el plan y resista los métodos del atacante.

Desde otra perspectiva, AlShboul et al. (2018) afirmaron que la detección se enfoca en las prácticas que los usuarios pueden usar para comprender y administrar las herramientas y tecnologías de protección, creando un mayor bloqueo contra posibles ataques de ciberseguridad. Para la definición final de la dimensión de detección, utilizamos a Romero et al. (2018) quienes identificaron el descubrimiento como la etapa más compleja, requiriendo un nivel adecuado de

conocimientos técnicos para garantizar una gestión eficiente de la información, los elementos y las actividades de seguridad.

Desde otro punto de vista Romero y Col. (2018) Quienes afirman que el descubrimiento es la fase más compleja y se necesita tener un nivel adecuado de conocimiento técnico que pueda asegurar una gestión eficiente de la información, elementos y actividades de seguridad siendo así que los conocimientos teóricos y técnicos son fundamentales para una adecuada gestión de TI y más aún cuando se busca ser eficientes. De otro lado Halvorson, N. (2008). Menciona que los riesgos y el diagnostico y el tratamiento del riesgo, debe estar alineado a los objetivos organizaciones, priorizándolos según los servicios en riesgos.

Se cita a Bashoudhary y Searle (2019) para definir las dimensiones. Muestran que las respuestas se dan cuando ya se ha detectado una amenaza o ataque en el sistema, por lo que utilizan métodos de verificación para prevenir anomalías, bloqueando las acciones del usuario donde persisten las anomalías, indica que es necesario. Ademas Dutton, J. (2016) menciona que el conocimiento técnico de los líderes en ciberseguridad es fundamental para evitar la propagación de amenazas y otros riesgos derivados en infraestructuras poco endurecidas.

En otro sentido, Meszaros y Buchalcevova (2017) señalaron que las opciones apropiadas de tratamiento del riesgo se determinan durante la fase de respuesta e integraron esa acción con: Identificación de tareas apropiadas Definición de prioridades. Realice tareas y vea los resultados y beneficios de tareas específicas. Desde otro punto de vista. Mansfiel (2017) refiere que la fase de respuesta o respuesta es uno de los puntos en los que las organizaciones como las empresas necesitan evolucionar y madurar, y a través de esta combinación seguridad efectiva contra accidentes informáticos asegurados, nos enfocamos en las personas y la tecnología para hacerlo posible.

Como última definición de la categoría de reacción, finalmente nombramos a Romero et al. (2018), quienes señalan que en esta etapa los protocolos a seguir son muy diferentes a los de prevención, ya que en esta etapa se deben tomar las

acciones correctivas para mitigar, corregir o bloquear cualquier anomalía que ocurriera cuando un hecho se ha producido. ya ocurrió, más aún cuando se salió de control, podría traducirse en costos muy altos para la empresa.

En cuanto a la teoría de la Gestión de Riesgos o Risk de TI y seguridad de los datos y la información, IBM (2020) afirma que la gestión de TI se enfoca en monitorear y administrar los elementos involucrados en las TI en una organización; En otras palabras, tienen una relación directa con hardware, software y redes; En este sentido, la gestión de TI se resume en cómo hacer que los sistemas de información y todos sus elementos funcionen de manera eficiente y, además de esto, ayudar a las personas a realizar sus actividades laborales de la mejor manera posible. (Whitman & Mattord, 2013)

Westerman (2006) afirma que la gestión de risk o riesgos tiene un contexto en las Tecnologías de Información de hoy porque no solo se evalúan los risk o riesgos técnicos. Sin embargo, se extiende a todos los niveles de riesgo y puede resultar en pérdidas severas para las empresas y entidades que no monitorean los niveles de riesgo crecientes. Ademas Alvizuri (2014) cree que una visión presupuestaria para la compra de equipos es necesario para minimizar el riesgo en caso de un incidente que afecte la información bajo control. de la empresa. En retrospectiva Rodríguez (2016) indica que los lineamientos establecidos por las normas de seguridad, vienen a seguir guias que se adaptan a toda orgnizacion, independientemente de su tamaño o sector, por lo que los riesgos son transversales en ese sentido.

Figura 1. “Que es la seguridad de la información”

Figura 2. “Preguntas seguridad de la información”

Figura 3. “Arbol de gestión de riesgos”

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

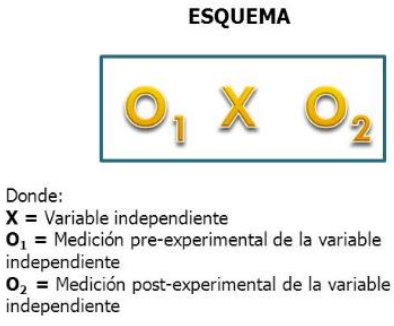
En base al estudio realizado por el autor Fernández y Baptista (2010), el presente estudio se realizó con un enfoque cuantitativo. Esto porque se debe a que la recopilación de datos se realizó esencialmente para probar hipótesis basadas en mediciones numéricas y los análisis estadísticos correspondientes. De esta manera se hace posible determinar la relación o influencias entre variables y además debido a que existen varias etapas que no se pueden eludir y proceder secuencialmente, el enfoque cuantitativo es continuo y determinista.

Esta investigación es del tipo aplicada tecnológica, porque tenemos más de una característica sobre innovación tecnológica, dado que se menciona métodos y normas de tecnologías y activos digitales, por ende, se puede usar como una herramienta para impulsar el rubro de innovación. (Sampieri, 2019)

Diseño de investigación: Experimental tipo preexperimental.

El procedimiento es el de pre- y post-test por un solo grupo: Este grupo se utilizará para la pre-evaluación, los trabajos serán procesados como paso siguiente, y para este fin se realizará la evaluación post-ensayo. Este diseño tiene la intención de confirmar que la categoría de apoyo como origen estaba en la agrupación de la variable dependiente antes del ensayo, y así expresarlo como un estudio completo, esto contrasta con el precedente (Salas, 2013)

Figura 4. Esquema



3.2. **Variables y operacionalización**

Crear originalidad en el estudio es de suma importancia. Ayuda a simbolizar cosas que son alcanzables y, si es poco probable, difíciles de cambiar. En este estudio, aplicamos la variable fuente como 'independiente' y la variable resultada como 'dependiente'. (Losh, 2017)

V1-Ciberseguridad

La ciberseguridad se caracteriza, si no el resultado, por la combinación aleatoria de comportamiento en el ciberespacio y expresión en políticas y leyes específicas. El mismo representante también agregó que la diversidad de la ciberseguridad se refleja en los dispositivos que utilizamos ya que cada vez es mas común el uso de medios tecnologicos. Se asigna la variable dependiente del punto más sensible (Bejarano, Rodriguez, & Merseguer, 2021).

V2-Proceso de Gestión de Riesgos de TI

El grave sometimiento de la sociedad a los sistemas informáticos y electrónicos hace que la sociedad sea más vulnerable a posibles ataques desde el ciberespacio. Asimismo, el ciberespacio es una herramienta de vía simple, donde los humanos logran realizar un ataque complejo para enlazar, por lo que Internet se convierte en un gran lugar para los delincuentes y los terroristas traducen sus objetivos en operaciones y acciones. Por lo tanto, los ciberdelincuentes deben ser la amenaza más básica que perciben al espiar a la comunidad. (López, 2018). Para obtener dicho conocimiento, después de este estudio, se revelan las estadísticas de cada componente que ayuda a prevenir los delitos en línea y sus respectivas consecuencias en Internet. Además, se han desarrollado medidas preventivas para evitar el aumento de los delitos informáticos o de la ciberseguridad es el sujeto humano. (Friedman, 2015)

Figura 5. Pilares de gestión de seguridad de la información.

3.3. **Población, muestra y muestreo**

Pará Sánchez y Reyes (2002, p.111) la población está comprendida por todos los miembros o cual clase que este definida o segmentada bajo un criterio establecido.

En la investigación se utilizará como población a 35 trabajadores del departamento de TI de la organización Forever Living, los cuales apoyaran con el llenado de las encuestas para el presente proyecto.

Según Hernández (2010), en un muestreo probabilístico todos los elementos de la población tienen la misma probabilidad de selección, determinada por las

características o tipo de la población asi como el tamaño de una muestra, y por elegir la unidad de análisis de forma aleatoria o mecánica.

Para (Sánchez Carlessi, Reyes Romero y Mejía Sánchez 2018, p, 93) el muestro aleatorio simple es una muestra estadística que garantiza una probabilidad igual de selección para cada caso o individuo de dicha población.

3.4. **Técnicas e instrumentos de recolección de datos**

Técnicas de recolección: En la presente investigación se usó la técnica de recolección de datos por encuesta. Ya que de acuerdo con Fabbri (2020), es un proceso por el cual se basa en almacenar datos sobre el objeto que se tiene en consideración, la técnica de recolección, datos almacenados para que el observador elabore la información que puede separar de acuerdo a los datos establecidos por algún tipo de categoría y tener un panorama mayor de la problemática en particular.

Instrumentos de recolección: Como instrumento utilizado en el presente estudio es un cuestionario utilizando una escala de Likert modificada. Según Hernández (2020), el cual es un método de medición muy utilizado por los investigadores con el único objetivo de poder medir la opinión y la actitud de las personas en diversos problemas para investigar de acuerdo con criterios estipulados.

3.5. **Procedimientos**

Para realizar esta investigación se inició por revisar las incidencias respecto a la gestión de riesgos y seguridad de la información que la empresa tenía, luego de esto se realizó una reunión con el country mánager de la oficina local, para que pueda indicar sus puntos de vista, así como explicarle la relevancia que implica el tener una adecuada gestión de riesgos de TI en la organización. Se estableció que,

de acuerdo con los resultados y propuestas de la presente investigación, todas las áreas se verían involucradas con las recomendaciones a seguir. (ISOTools, 2019)

También se necesitó de realizar capaciones al personal, mostrándoles lo relevante que es el factor humano para la gestión de riesgos, ya que como se sabe en la cadena de la ciberseguridad es eslabón más débil, es el usuario final.

Sobre el factor humano se realizó pruebas con herramientas de la plataforma knowbe4 para conocer que tanto conocimiento sobre seguridad tiene cada uno de ellos. Estas pruebas se realizaron de manera furtiva en el tramo de análisis de los riesgos y tener mejor información para poder realizar los análisis siguientes. (Calder, 2009)

Luego de realizado todos estos, se procedió al llenado de los cuestionarios para realizar el pre-test de la investigación, la cual sería la primera muestra. Luego de esta se cruzó la información con los lineamientos de ciberseguridad y seguridad de la información, “integridad, confidencialidad y disponibilidad”, tal como lo menciona (INCIBE-CERT, 2017)

Luego de las recomendaciones se reforzo los puntos débiles, mediante políticas de seguridad de TI, y finalizando estas, se tomó el segundo test, (Post test), para el contraste respectivo.

3.6. **Método de análisis de datos**

Hernández et al., (2006). Es claro que para realizar un estudio sobre datos cuantitativos se deben considerar una serie de lineamientos para los resultados de un proyecto de investigación.

El objetivo de este proyecto de tesis es cuantitativo, ya que los dos indicadores de este estudio se pueden expresar en datos. Para ello se utilizarán

métodos estadísticos para realizar el análisis de los datos y poder procesar las hipótesis planteadas.

Análisis descriptivo, consiste en narrar o detallar las tendencias puntuales en la data existente para que nos lleven a conocer nuevos hechos, por lo que este método está basado en una o varias preguntas en la investigación y no cuenta con una hipótesis Mood (2014).

Kolmogorov Smirnov, es un contraste no paramétrico cuyo objetivo principal es determinar si la frecuencia de dos datos distintos sigue una misma distribución alrededor de su media. Hernández (2021). Asimismo, Shapiro Wilk, se usa para resaltar si un dato o conjunto de estos siguen a una distribución normal o no, este método es usada cuando se analizan muestras compuestas por menos de 50 elementos

Para el análisis y la revisión de datos como la información se usará un software reporteador de datos e información estadística de nombre SPSS y para probar las hipótesis se usará una prueba para medir el del coeficiente de correlación de Spearman, con lo que se compararán las hipótesis y se sacarán conclusiones.

3.7. **Aspectos éticos**

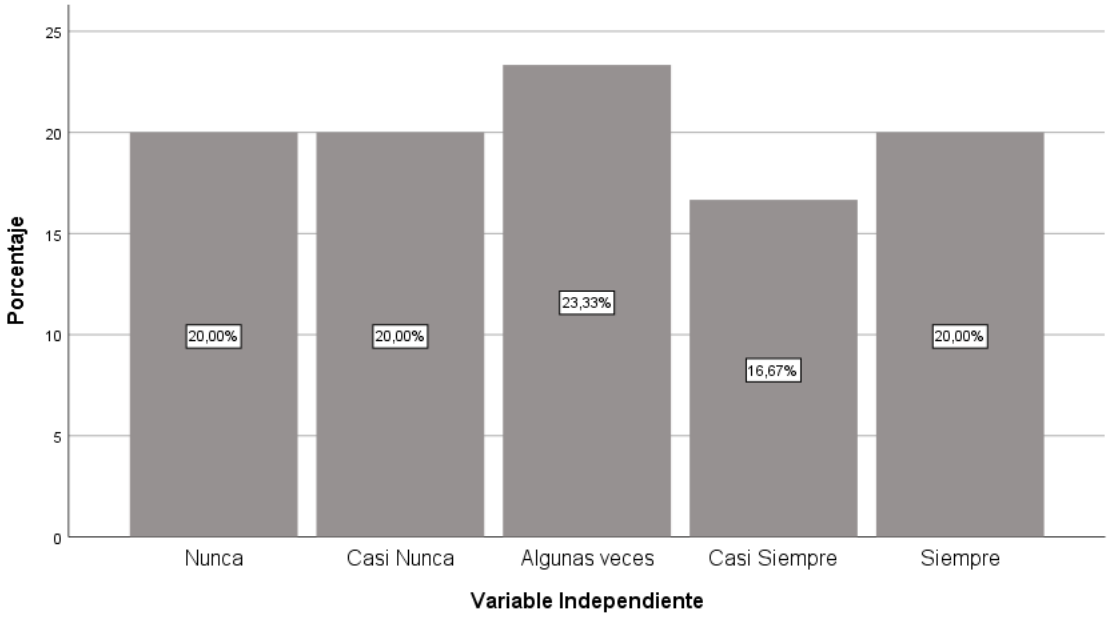
En esta presente investigación se respetó el derecho y propiedad intelectual, así como toda fuente de información, así también toda información obtenida del departamento de TI de la organización es confidencial y solo se usó lo necesario sin recabar mayor información que la necesaria para el desarrollo del presente proyecto, además de ser de autoría propia y mediante el uso del programa Turnitin para asegurar la originalidad de este, así como respetando los lineamientos según “Resolución de Vicerrectorado N°110-2022-VI-UCV”. El cuál es el vigente y se siguieron todos los parámetros, así como las citas de las cuentas en formato APA en su séptima edición.

IV. RESULTADOS

Tabla 1 Tabla de frecuencia y percepción de la variable independiente

V1- Ciberseguridad

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	6	20,0	20,0	20,0
	Casi Nunca	6	20,0	20,0	40,0
	Algunas veces	7	23,3	23,3	63,3
	Casi Siempre	5	16,7	16,7	80,0
	Siempre	6	20,0	20,0	100,0
	Total	30	100,0	100,0	



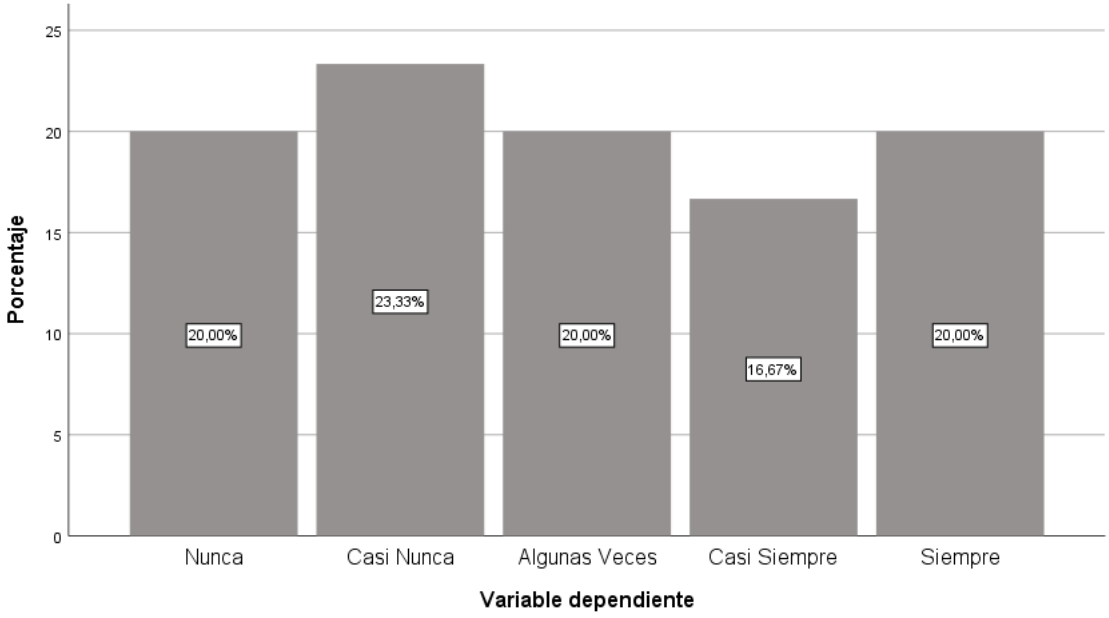
Interpretación:

Se visualiza la tabla de frecuencias de la variable independiente, así como el valor en porcentajes según la percepción del usuario, respecto al cuestionario proporcionado.

Tabla 2 Tabla de frecuencia y percepción de la variable dependiente

V2 – Proceso de Gestión de Riesgos de TI

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	6	20,0	20,0	20,0
	Casi Nunca	7	23,3	23,3	43,3
	Algunas Veces	6	20,0	20,0	63,3
	Casi Siempre	5	16,7	16,7	80,0
	Siempre	6	20,0	20,0	100,0
	Total	30	100,0	100,0	



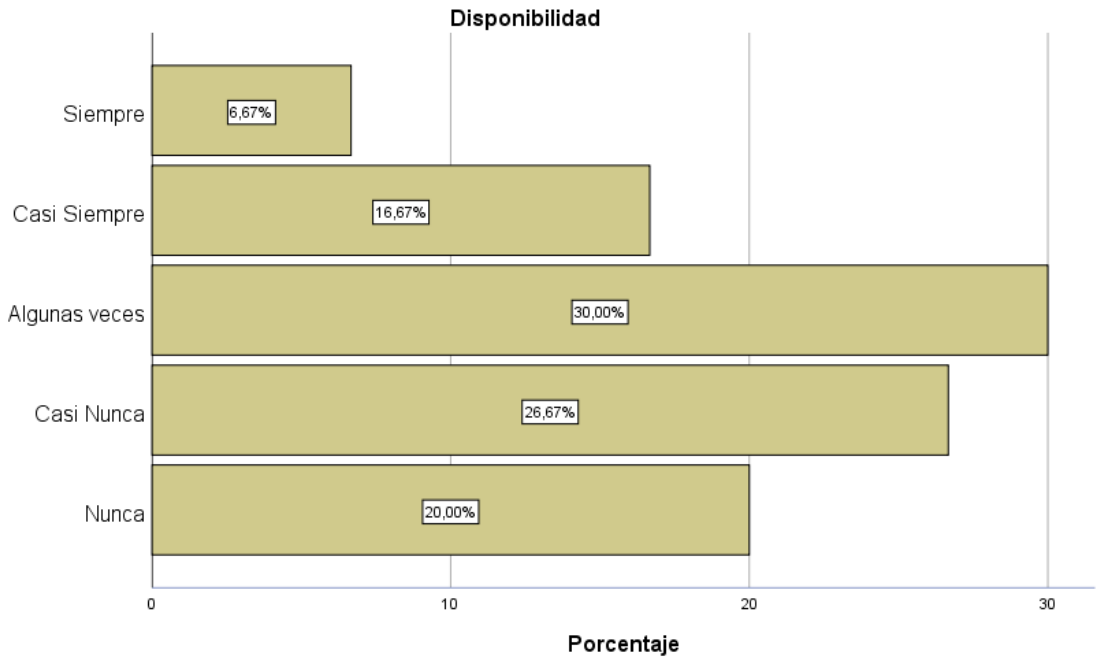
Interpretación:

Se puede ver la tabla de frecuencias de la variable dependiente, así como el valor en porcentajes según la percepción del usuario, respecto al cuestionario proporcionado

Tabla 3 Tabla de frecuencias por cada dimensión Disponibilidad

Disponibilidad

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	6	20,0	20,0	20,0
	Casi Nunca	8	26,7	26,7	46,7
	Algunas veces	9	30,0	30,0	76,7
	Casi Siempre	5	16,7	16,7	93,3
	Siempre	2	6,7	6,7	100,0
	Total	30	100,0	100,0	



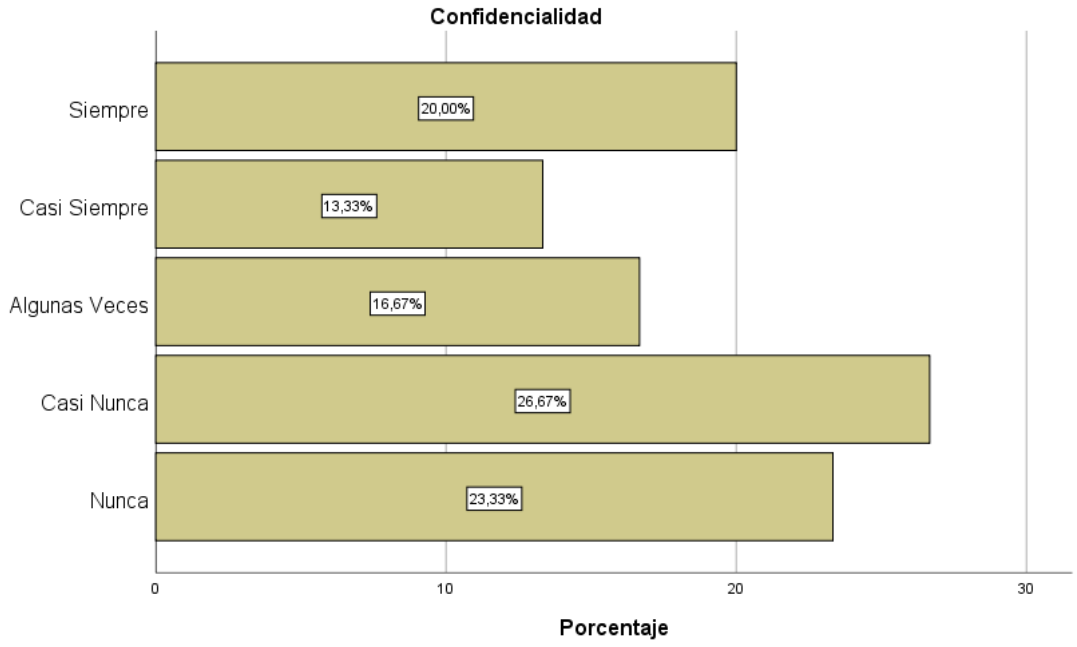
Interpretación:

Tenemos que la dimensión Disponibilidad muestra un valor bajo de cumplimiento de 6.67%, indicando que este sería un punto débil que pueda ser mejorado en las recomendaciones indicadas.

Tabla 4 Tabla de frecuencias por cada dimensión Confidencialidad

Confidencialidad

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	7	23,3	23,3	23,3
	Casi Nunca	8	26,7	26,7	50,0
	Algunas Veces	5	16,7	16,7	66,7
	Casi Siempre	4	13,3	13,3	80,0
	Siempre	6	20,0	20,0	100,0
	Total	30	100,0	100,0	



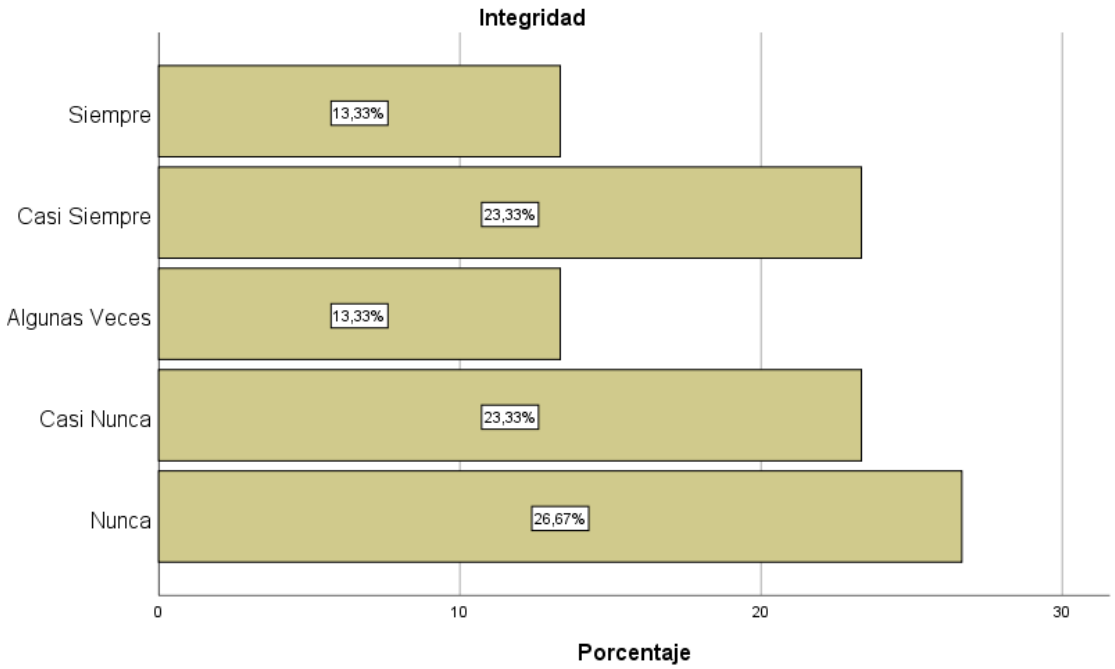
Interpretación:

Tenemos que la dimensión Confidencialidad muestra un valor alto de cumplimiento de 20%, indicando que esta implementado, pero puede mejorarse con las recomendaciones de esta investigación.

Tabla 5 Tabla de frecuencias por cada dimensión Integridad

Integridad

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	8	26,7	26,7	26,7
	Casi Nunca	7	23,3	23,3	50,0
	Algunas Veces	4	13,3	13,3	63,3
	Casi Siempre	7	23,3	23,3	86,7
	Siempre	4	13,3	13,3	100,0
	Total	30	100,0	100,0	



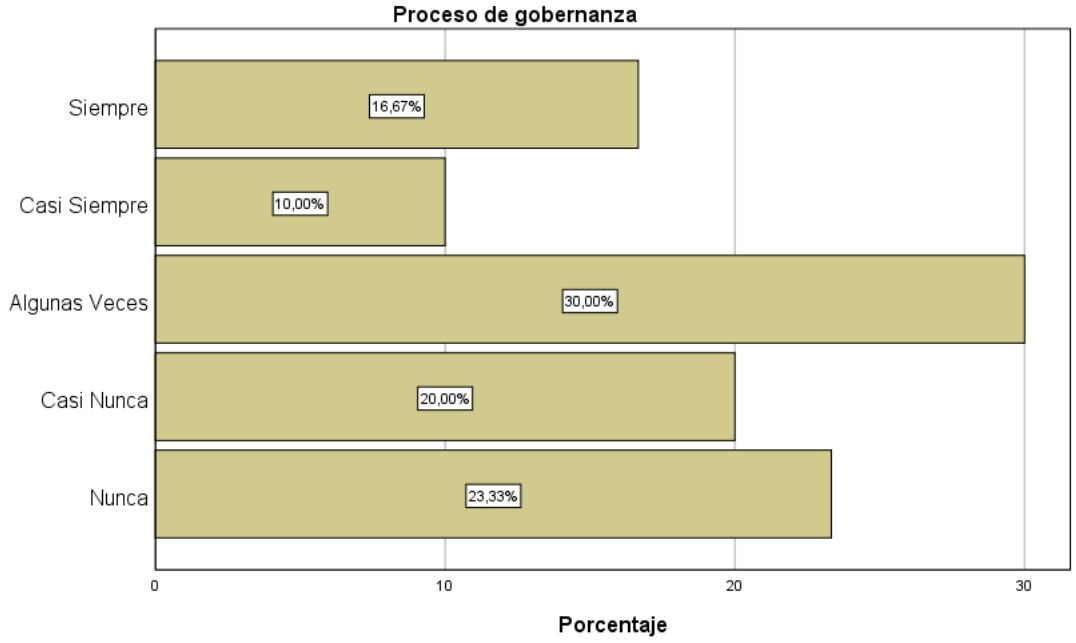
Interpretación:

Tenemos que la dimensión Integridad muestra un valor alto de cumplimiento de 13.3%, indicando que esta implementado, pero puede mejorarse con las recomendaciones de esta investigación.

Tabla 6 Tabla de frecuencias por cada dimensión Proceso de gobernanza del riesgo

Proceso de gobernanza del riesgo

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	7	23,3	23,3	23,3
	Casi Nunca	6	20,0	20,0	43,3
	Algunas Veces	9	30,0	30,0	73,3
	Casi Siempre	3	10,0	10,0	83,3
	Siempre	5	16,7	16,7	100,0
	Total	30	100,0	100,0	



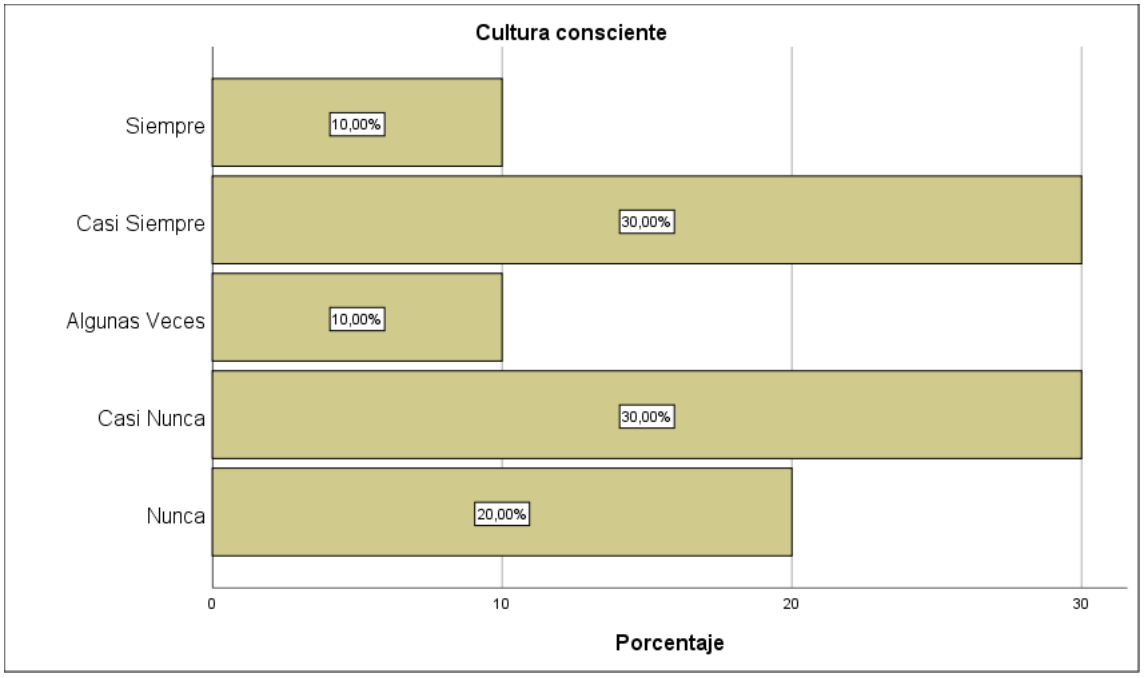
Interpretación:

Tenemos que la dimensión Proceso de gobernanza del riesgo muestra un valor alto de cumplimiento de 16.67%, indicando que esta implementado pero puede mejorarse con las recomendaciones de esta investigación.

Tabla 7 Tabla de frecuencias por cada dimensión Cultura consciente del riesgo

Cultura consciente del riesgo

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	6	20,0	20,0	20,0
	Casi Nunca	9	30,0	30,0	50,0
	Algunas Veces	3	10,0	10,0	60,0
	Casi Siempre	9	30,0	30,0	90,0
	Siempre	3	10,0	10,0	100,0
	Total	30	100,0	100,0	



Interpretación:

Tenemos que la dimensión Cultura consciente del riesgo muestra un valor dentro del rango de cumplimiento de 10.00%, indicando que esta implementado, pero puede mejorarse con las recomendaciones de esta investigación.

Estadísticos descriptivos

Estadísticas del valor total de elementos

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
p1	117,27	395,582	,318	,951
p2	117,33	389,402	,638	,949
p3	117,60	390,317	,525	,949
p4	117,50	383,845	,443	,950
p5	117,13	391,913	,455	,950
p6	117,07	405,030	,040	,952
p7	117,00	392,690	,477	,949
p8	117,37	385,689	,591	,949
p9	117,53	377,430	,752	,947
p10	117,10	381,403	,714	,948
p11	117,10	384,852	,540	,949
p12	117,07	393,995	,328	,951
p13	117,23	387,289	,456	,950
p14	117,80	378,648	,529	,949
p15	117,37	382,585	,526	,949
p16	117,23	384,599	,644	,948
p17	117,33	374,161	,646	,948
p18	117,90	368,231	,710	,947
p19	117,60	375,559	,685	,948
p20	117,87	368,464	,721	,947
p21	117,73	371,099	,623	,949
p22	117,50	369,224	,776	,947
p23	117,37	383,275	,735	,948
p24	117,03	386,309	,624	,948
p25	117,47	373,775	,819	,946
p26	117,60	365,628	,874	,946
p27	117,60	376,455	,729	,947
p28	117,60	367,628	,788	,946
p29	117,70	377,941	,692	,948
p30	117,53	366,671	,845	,946

Interpretación:

Podemos visualizar los estadísticos descriptivos, como el alfa de Cronbach, la correlación, la varianza y la media de la escala.

Análisis de Confiabilidad

Para el siguiente análisis, se utilizó el siguiente cuadro para poder interpretar los resultados

"Intervalo coeficiente Alfa de Cronbach"	"Fiabilidad y valoración de ítems revisados"
[0 : 0.5]	Inaceptable
[0,5 : 0.6]	Pobre
[0,6 : 0.7]	Débil
[0,7 : 0.8]	Aceptable
[0,8 : 0.9]	Bueno
[0,9 : 1]	Excelente

Estadísticas de fiabilidad de la variable independiente

Alfa de Cronbach	N de items
,950	18

Fuente: SPSS

Interpretación:

Realizando el análisis correspondiente se tomaron los resultados del SPSS, donde se obtuvo un Alfa de Cronbach de 0.950, lo que indica que los datos tienen una confiabilidad Excelente.

Estadísticas de fiabilidad de la variable dependiente

Alfa de Cronbach	N de items
,950	12

Fuente: SPSS

Interpretación:

Realizando el análisis correspondiente se tomaron los resultados del SPSS, donde se obtuvo un Alfa de Cronbach de 0.950, lo que indica que los datos tienen una confiabilidad Excelente

Pruebas de Normalidad

Variable Ciberseguridad

Ho: “Los datos tiene una distribución normal”

Pruebas de normalidad			
	Shapiro-Wilk		
CIBERSEGURIDAD	,868	30	,00

Fuente: SPSS

Interpretación:

Podemos interpretar que, dado que nuestra población es igual o menor a 30, se utilizara la prueba normalidad de Shapiro-Wilk. Además, el valor (sig.) es menor que 0.05 por tanto se puede decir que se rechaza la hipótesis nula, concluyendo que la distribución de los datos no es normal, por ello se utilizó la correlación Spearman para probar la hipótesis no paramétrica.

Dimensión Disponibilidad

Ho: “Los datos tiene una distribución normal”

Pruebas de normalidad			
	Shapiro-Wilk		
DISPONIBILIDAD	,864	30	,00

Fuente: SPSS

Interpretación:

Podemos interpretar que, dado que nuestra población es igual o menor a 30, se utilizara la prueba normalidad de Shapiro-Wilk. Además, el valor (sig.) es menor que 0.05 por tanto se puede decir que se rechaza la hipótesis nula, concluyendo que la distribución de los datos no es normal, por ello se utilizó la correlación Spearman para probar la hipótesis no paramétrica.

Dimensión Confiabilidad

Ho: "Los datos tiene una distribución normal"

Pruebas de normalidad

	Shapiro-Wilk		
CONFIABILIDAD	,905	30	,01

Fuente: SPSS

Interpretación:

Podemos interpretar que, dado que nuestra población es igual o menor a 30, se utilizara la prueba normalidad de Shapiro-Wilk. Además, el valor (sig.) es menor que 0.05 por tanto se puede decir que se rechaza la hipótesis nula, concluyendo que la distribución de los datos no es normal, por ello se utilizó la correlación Spearman para probar la hipótesis no paramétrica.

Dimensión Integridad

Ho: “Los datos tiene una distribución normal”

Pruebas de normalidad			
	Shapiro-Wilk		
INTEGRIDAD	,919	30	,02

Fuente: SPSS

Interpretación:

Podemos interpretar que, dado que nuestra población es igual o menor a 30, se utilizara la prueba normalidad de Shapiro-Wilk. Además, el valor (sig.) es menor que 0.05 por tanto se puede decir que se rechaza la hipótesis nula, concluyendo que la distribución de los datos no es normal, por ello se utilizó la correlación Spearman para probar la hipótesis no paramétrica.

Variable Proceso de Gestión de Riesgos de TI

Ho: “Los datos tiene una distribución normal”

Pruebas de normalidad			
	Shapiro-Wilk		
PROCESO DE GESTION DE RIESGOS DE TI	,883	30	,00

Fuente: SPSS

Interpretación:

Podemos interpretar que, dado que nuestra población es igual o menor a 30, se utilizara la prueba normalidad de Shapiro-Wilk. Además, el valor (sig.) es menor que 0.05 por tanto se puede decir que se rechaza la hipótesis nula, concluyendo que la distribución de los datos no es normal, por ello se utilizó la correlación Spearman para probar la hipótesis no paramétrica.

Prueba de Hipótesis General

“Existe una relación directa entre la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.”

HO: “No existe una relación directa entre la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.”

Correlaciones

			CIBERSEGURIDAD	PROCESO DE GESTION
Rho de Spearman	CIBERSEGURIDAD	Coeficiente de correlación	1,000	,833
		Sig. (unilateral)	.	,000
		N	30	30
	PROCESO DE GESTION	Coeficiente de correlación	,833	1,000
		Sig. (unilateral)	,000	.
		N	30	30

Fuente: SPSS

Interpretación:

Como el P valor es menor que 0.05 entonces se rechaza la hipótesis nula por lo tanto “Existe una relación directa entre la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.”

Prueba de Hipótesis Especifica 1 de la investigación

“Existe una relación directa entre la dimensión Disponibilidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.”

HO: “No existe una relación directa entre la dimensión Disponibilidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.”

Correlaciones

			DISPONIBILIDAD	PROCESO DE GESTION
Rho de Spearman	DISPONIBILIDAD	Coeficiente de correlación	1,000	,352
		Sig. (unilateral)	.	,028
		N	30	30
	PROCESO DE GESTION	Coeficiente de correlación	,352	1,000
		Sig. (unilateral)	,028	.
		N	30	30

Fuente: SPSS

Interpretación:

Como el P valor es menor que 0.05 entonces se rechaza la hipótesis nula por lo tanto “Existe una relación directa entre la dimensión Disponibilidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.”

Prueba de Hipótesis Especifica 2 de la investigación

“Existe una relación directa entre la dimensión Confidencialidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima 2023.”

HO: “No existe una relación directa entre la dimensión Confidencialidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima 2023.”

Correlaciones

			CONFIABILIDAD	PROCESO DE GESTION
Rho de Spearman	CONFIABILIDAD	Coeficiente de correlación	1,000	,702
		Sig. (unilateral)	.	,000
		N	30	30
	PROCESO DE GESTION	Coeficiente de correlación	,702	1,000
		Sig. (unilateral)	,000	.
		N	30	30

Fuente: SPSS

Interpretación:

Vemos que el P valor es menor a 0.05 por lo que se rechaza la hipótesis nula por lo tanto “Existe una relación directa entre la dimensión Confidencialidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima 2023.”

Prueba de Hipótesis Especifica 3 de la investigación

“Existe una relación directa entre la dimensión Integridad de datos de la Ciberseguridad y la Gestión de Riesgos de TI en una empresa Transnacional en Lima 2023.”

HO: “No Existe una relación directa entre la dimensión Integridad de datos de la Ciberseguridad y la Gestión de Riesgos de TI en una empresa Transnacional en Lima 2023.”

Correlaciones

			INTEGRIDAD	PROCESO DE GESTION
Rho de Spearman	INTEGRIDAD	Coeficiente de correlación	1,000	,795
		Sig. (unilateral)	.	,000
		N	30	30
	PROCESO DE GESTION	Coeficiente de correlación	,795	1,000
		Sig. (unilateral)	,000	.
		N	30	30

Fuente: SPSS

Interpretación:

Como el P valor es menor que 0.05 entonces se rechaza la hipótesis nula por lo tanto “Existe una relación directa entre la dimensión Integridad de datos de la Ciberseguridad y la Gestión de Riesgos de TI en una empresa Transnacional en Lima 2023.”

Frecuencia de las Variables

Estadísticos de las variables

		V1	V2
N	Válido	30	30
	Perdidos	0	0
Media		2,97	2,93
Mediana		3,00	3,00
Desv. Desviación		1,426	1,437
Varianza		2,033	2,064
Rango		4	4
Mínimo		1	1
Máximo		5	5

Fuente: SPSS

Interpretación:

Podemos visualizar la frecuencia de ambas variables, como los valores de desviación, la varianza y los casos válidos.

V. DISCUSIÓN

Después del análisis realizado de cada uno de los datos, variables y luego de obtener el resultado de estos, se compararon con los antecedentes referenciados en el presente trabajo de investigación, con los que se confirmaron cada una de las hipótesis planteadas, siendo así se pudo determinar que la HG - Hipótesis General que tiene como planteamiento que “Existe una relación directa entre la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023”, donde según el análisis de confiabilidad de Alfa de Cronbach el valor de 0.950, indicando que tiene un confiabilidad excelente, además según las pruebas estadísticas, realizadas y utilizadas dan como resultado que la correlación es No Paramétrica de Rho de Spearman de 0.833, siendo este resultado una asociación alta entre ambas variables y teniendo como un valor $p = 0.000$ ($p < 0.01$) es decir se confirma la influencia existente entre ambas, mostrando un alto grado de influencia.

Respecto al análisis inferencial respecto con el proceso de evaluación de encuestas, se utilizó Shapiro Wilk para poder definir la normalidad debido a que la muestra era de <=30, donde se obtuvo un valor de Sig. 0.002 en la Variable 1 y 0.003 en la Variable 2, siendo estos menores a 0.05 por lo que se realizo la prueba no parametrica de Spearman para poder contrastar las hipótesis. Cabe precisar que como resultado del Alfa de Cronbach se obtuvo el valor de 0.950, demostrando que los datos tienen una confiabilidad Excelente.

Respecto a los estadísticos descriptivos y la percepción se pudo visualizar en la variable dependiente tuvo resultado del 20% en Siempre, el 16.67% en Casi Siempre, 23.33% en Algunas Veces, 20% en Casi nunca y 20% en Nunca. En la variable dependiente tenemos que la percepción fue 20% en Siempre, 16.67 en Casi siempre, 20% en Algunas veces, 23.33 en Casi Nunca y 20% en Nunca.

Del mismo modo las dimensiones indicadas en la presentación investigación toma como alta la relación existente entre ambas variables, confirmando que existe

influencia entre la Ciberseguridad y la Gestión de Riesgos de TI por lo que el fortalecimiento de cualquier de estas tendrá un resultado positivo respecto a salvaguardar los datos y activos digitales de la organización. Lo cual tiene similitud con Seclén (2016) ya que menciona que un hecho importante para la protección de datos y activos siempre es importante cubrir la necesidad al más alto nivel de establecer un Gobierno de TI en Seguridad, que debe ser integrada por especialistas en Ciberseguridad, seguridad de la información y Hacking ético, que operen como uno solo, en donde su principal función es la de analizar y monitorear el desarrollo del gobierno de seguridad, monitoreando la ejecución de las etapas para la implementación de un SGSI en toda la region, con el apoyo de la Gerencia de T.I Latam.

En contraste, Otoya (2018), es concluyente que cada vez más profesionales tienen como prioridad y preocupación la seguridad, así como el de transmitir a sus clientes una seguridad aparente, que estos mismos no siempre conocen los procesos que la acrecientan tangiblemente, por lo que muchas veces no es posible poner en practica en sus propios proyectos tecnológicos. Siendo esto así en Peru se establecido que la ONGEI “Oficina Nacional de Gobierno Electrónico e Informático”, también llamada Secretaria de Gobierno Digital, es claro en disponer de uso obligatorio según norma “NTP ISO 17999:2014” para la adecuada Gestión de la Seguridad de la Información, así tambien tenemos a la norma “ISO/IEC 27001” como un estándar para la Seguridad de la Información y protección de amenazas, con el fin de tener un framework sobre buenas prácticas en seguridad que en la actualidad todas las empresas u organizaciones deberían aplicarla independiente de su sector o el tamaño de la misma.

Se tiene los resultados similares de Muños (2016), porque concluye que las dimensiones confidencialidad, disponibilidad e integridad son de mucha importancia para el compliance de políticas de seguridad, ayudando a disminuir el risk o riesgo, frente a este estudio podemos comparar que en los resultados que se obtuvieron en 3 pruebas de hipótesis realizadas nos arrojo en la dimensión Disponibilidad un P valor de 0.028 y un Rho de Spearman de 0.352 por lo confirma la relacion e influencia en la Gestión de Riesgos de TI.

Con respecto a la dimensión “Confidencialidad” se tiene un Valor P de 0.000 y una correlación de Rho Spearman de 0.702, por lo que también corrobora la importancia respecto al trabajo previo discutido y por último la dimensión de Integridad tiene un P valor de 0.000 y una correlación de Rho de Spearman de 0.795 corroborando rotundamente la relación e influencia de las 3 dimensiones respecto a la Gestión de Riesgos de TI. Esto no solo demuestra que ambos estudios obtuvieron resultados positivos las dimensiones mencionadas, sino que la Ciberseguridad es un factor clave en toda organización moderna o que quiera permanecer en el mercado, no solo por la seguridad sino por la seguridad que transmite tanto a los clientes internos como al cliente externo, haciendo que no solo se proyecte fiabilidad, sino que también se proyecte fortaleza frente a los competidos en el ámbito en que se desarrolla.

Se tiene el trabajo de investigación de Maggiore (2014) el cual se asemeja a la presente investigación porque una de sus conclusiones es que se tomara como marco integrado o framework la Gestión de Riesgos de TI, donde el correcto uso de la Ciberseguridad da como influencia en el primero, siendo esto proporcional al resultado obtenido donde las dimensiones de la ciberseguridad influyen en la Gestion de Riesgos de TI, siendo así también se evidencia que ambas se correlacionan para obtener las mejores prácticas de Seguridad para las distintas organizaciones.

Sin embargo Otoya (2018) en su investigación concluyó que existe influencia muy importante y significativa sobre la Gestion de Riesgos de TI en la Seguridad y Ciberseguridad de tal manera comparando con este trabajo de investigación se obtuvo como resultado de Rho de Spearman al correlacionar ambas variables el valor de 0.833 lo que indica que tal como detalla el autor, la relación es alta. Lo que ayudo también a corroborar que el uso de la herramienta de Magerit así como su aplicación en los activos de TI e información tiene una estrecha relación de éxito.

El resultado de una de las conclusiones de Tacza (2018) en su investigación menciona las dimensiones tal como integridad, disponibilidad y confidencialidad,

donde el autor afirma que existe una relación directa respecto a la normal ISO 27001:2005 (Norma sobre Seguridad de la información), la presente se usó en las discusiones anteriores de la presente investigación, donde fue concluyente que dicha normal tiene estrecha relación con las dimensiones que en la presente investigación dieron resultados confiables y altos de influencia sobre la seguridad y ciberseguridad. Es así que tendríamos otro autor confirmando las dimensiones de la presente investigación, cabe decir además que la norma ISO ayudo a tener un marco de mejores prácticas que se establecerán en toda organización independiente del sector o tamaño, lo que la hace una guía multisectorial con el fin de obtener mejores resultados frente a los ciberataques que día a día mejoran sus herramientas y estrategias, siendo el factor humano el punto débil en la cadena de la Ciberseguridad.

Asimismo, Pinto (2017) en su investigación tuvo como resultado que la dimensión de Gestión de Riesgos de TI y la Ciberseguridad tienen relación dado que su hipótesis alterna fue aceptada, en esta investigación si bien es cierto tuvieron como muestra un valor mayor comparado con la presente investigación, pero en ambos se obtuvo el mismo resultado.

Con similitud en los resultados de Calderon (2019), este relaciono la seguridad y la gestión de riesgos de TI, donde obtuvo que su muestra era no paramétrica de Spearman con un valor de 0.886** valor muy parecido al obtenido al relacionar las variables de esta investigación, en ambos casos se obtuvo un valor P=0.000 ($p<0.01$) obteniendo bastante similitud en los resultados relacionados. Respecto a las dimensiones se obtuvo que estas influyen al cruzarlas con el valor de la variable, esto llevo a que en las 3 dimensiones se acepten las Hipótesis Alternas, guardando relación a los resultados encontrados. En su prueba de Hipótesis Especifica tiene como resultado que existe relación debido a que el resultado del valor P es <= 0.05, este resultado es similar en la prueba de hipótesis de la dimensión 2, donde los valores son menores a 0.05. Las dimensiones usadas son las mismas ocupadas con esta investigación que si bien es cierto los valores no son los mismos en ambas investigaciones se aceptan las hipótesis alternas por el valor obtenido. Como punto resaltante ambas tienes las mismas conclusiones

respecto a que siempre el eslabón más débil viene siendo el factor humano y este es punto clave para asegurar el mejorar la Seguridad de Infraestructura frente a la seguridad, considerando que, a pesar de una buena política, correcto cumplimiento e infraestructura adecuada, por lo que en ambas se habla de la capacitación y concientización de este último es clave para todo proyecto de Seguridad.

Los procedimientos metodológicos usados en el presente estudio ayudo a fortalecer cada uno de los puntos evaluados, así como el procedimiento estadístico nos mostro la validez de los datos obtenidos. Además, al medir la interacción de ambas variables se pudo conocer que tan efectiva es la relación de ambas, o si no existía relación alguna, ya que partiendo desde un punto de vista de auditoria era necesario conocer la percepción de la población muestra respecto a puntos y dimensiones establecidas en esta investigación.

Siempre es relevante mencionar que la encuesta en línea como instrumento para la recolección de información y datos lo que permitió un adecuado seguimiento y registro de las respuestas. En cuanto al software y herramientas estadísticas utilizadas es el SPSS en su Versión 24, para elaborar los modelos mostrados en los resultados, los que fueron relevantes para ayudar a entender de manera grafica e intuitiva la distribución de los datos y la confiabilidad de estos.

En el mismo contexto, los indicadores utilizados contribuyen al soporte de las variables estudiados, ya que permitieron cuantificar y tener información para poder ser explotados por la institución.

Los resultados de esta investigación aquí discutidos van de la mano con la tendencia mencionada por Gartner (2021) que para el 2024 las empresas que adopten estos pilares de Ciberseguridad indicados en la presente investigación reducirán el efecto financiero frente a incidentes individuales de Seguridad en un 90% (de media). Esto se da debido a que cada vez las instituciones necesitan soluciones que sean flexibles y adaptables, de tal manera que las dimensiones sirvan como una malla de ciberseguridad para no solo proteger los activos de TI, sino que la identidad fuera la organización, teniendo así una visión holística de toda

la organización. Lo que también contribuye a mejorar la seguridad en todo el ámbito. Todo lo aquí analizado servirá para la adopción en los próximos años de mejorar los procesos de Gestión de Riesgos de TI y en la Ciberseguridad con una visión de 360 grados.

Respecto a la importancia social, la presente investigación aporta datos y conocimientos respaldados en otros autores, todo esto ayudara a su aplicación o interpretación en distintas organizaciones de todos los sectores, como una solución en sus procesos.

VI. CONCLUSIONES

Primera

Se determinó que “existe correlación entre la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima”, ya que se obtuvo el valor de significancia de 0 y además de un Rho de Spearman de 0.833. Además, que el resultado un valor sigma unilateral, nos manifiesta que se han realizado las pruebas de hipótesis dando como lectura que “Existe relación directa entre la Ciberseguridad y la Gestión de Riesgos de TI”.

Segunda

Se determinó que en la Hipótesis Especifica 1 se utilizó la correlación de Rho de Spearman y que dio como resultado un valor de coeficiente de correlación de 0.352 y un valor sig. de 0.028, esto quiere decir que la hipótesis de estudio del investigador se ha probado la cual llegaría a concluir que “Existe una relación significativa y positiva entre la dimensión Disponibilidad de la variable Ciberseguridad y la Gestión de Riesgos de TI”. Es importante recalcar que los resultados obtenidos del software estadístico “SPSS” han considerado el nivel sig. unilateral.

Tercera

Se determinó queen la Hipótesis Especifica 2 se utilizó la correlación de Rho de Spearman y que dio como resultado un valor de coeficiente de correlación de 0.702 y un valor sig. de 0.000, esto quiere decir que la hipótesis de estudio del investigador ha sido comprobada la cual llegaría a concluir que “Existe una relación directa entre la dimensión Confidencialidad de la variable Ciberseguridad y la Gestión de Riesgos de TI”. Es importante recalcar que los resultados obtenidos del software estadístico SPSS han considerado el nivel sig. unilateral.

Cuarta

Se determinó que en la Hipótesis Especifica 3 se utilizó la correlación de Rho de Spearman y que dio como resultado un valor de coeficiente de correlación de 0.795 y un valor sig. de 0.000, esto quiere decir que la hipótesis de estudio del investigador ha sido comprobada la cual llegaría a concluir que “Existe una relación directa entre la dimensión integridad de datos de la variable Ciberseguridad y la gestión de riesgos”. Esto viene a ser importante recalcando que los resultados obtenidos del software estadístico SPSS han considerado el nivel sig. unilateral.

Quinta

Se determinó que, “Si existe una relación directa entre la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023”, ya que según los datos y resultados analizados en el capítulo de resultados, las variables de Ciberseguridad y la variable Gestión de Riesgos de TI, se contrastaron entre si obteniendo un valor de significancia de 0, lo que confirma la relación y dependencia de ambas

VII. RECOMENDACIONES

Primera

Se recomienda al gerente de TI de Latinoamérica que debe alinear los objetivos estratégicos de Seguridad con la Gerencia de Operaciones para que puedan asignar una mayor partida para fortalecer la infraestructura física y virtual tecnológica; lo que servirá para un correcto compliance de las políticas de Seguridad establecidas, bajo la nueva realidad.

Segunda

La “Disponibilidad” tiene influencia respecto a la Gestión de Riesgos de TI, por lo que se recomienda al jefe del departamento de TI debería establecer un DRP “Plan de recuperación de desastres”, así como un BCP “Plan de continuidad del negocio” a fin de tener asegurar y tener mapeado los servicios de mayor impacto, es así que ningún servicio indispensable debe quedar fuera de este plan.

Tercera

La “Confidencialidad” tiene influencia respecto con la Gestión de Riesgos de TI, por lo que se recomienda al jefe del departamento de TI, en conjunto con la alta dirección programen capacitaciones de concientización sobre el manejo e importancia del manejo de información confidencial. Del uso correcto del material físico y digital, así como el correcto almacenamiento bajo llave el material físico o su destrucción cuando ya no sea de utilidad, respecto a la información digital, el correcto uso de los medios tecnológicos, el fortalecimiento de conocimientos para poder asegurarla con el apoyo del departamento de TI, mediante encriptación, carpetas y accesos con doble factor de autenticación o Multi Factor Authentication (MFA) para un correcto manejo de la información.

Cuarta

La “Integridad de datos tiene influencia directa con relación a la Gestión de Riesgos de TI”, por lo que se recomienda al departamento de TI deba revisar las políticas de acceso a la información, además se recomienda un mejor manejo de respaldos locales y en la nube con historial de cambios. En el mismo sentido se debe realizar pruebas de pentesting para detectar vulnerabilidades que puedas perjudicar la integridad de los datos.

Quinta

Luego de que se estableciera que existe una relación entre las variables de la presente investigación, se recomienda al jefe de TI tener una adecuada implementación de SGSI en la organización, para que se tenga un mejor mapeo de los activos en riesgo y se pueda establecer prioridades para mitigar los mismos, así también en la misma línea se debe realizar pruebas de pentesting tanto de caja negra y de caja blanca para corregir de manera temprana las vulnerabilidades encontradas, además de capacitar al personal en las distintas formas de vulnerabilidad existentes, mediante campañas con el uso de de herramientas como knowb4 que permiten simular correos verídicos con la frecuencia que se establezca por dicho departamento y asi poder saber que usuario o departamentos es el más vulnerables por error humano, ya que este ultimo también fue concluyente en dicho capitulo. Todo lo antes mencionado y en su conjuntos permitirá el endurecimiento de la seguridad de la organización.

REFERENCIAS

Agencia de la Unión Europea para la Ciberseguridad ENISA. (2019). Tendencias emergentes. *Panorama de Amenazas de la ENISA*, 20. Recuperado el 10 de 2022, de https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-emerging-trends-ebook-en-es.pdf

Aguilar, L. J. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). Cuadernos de estrategia, (185), 19-64.

Alba. (2021). Planeación de la seguridad de la información corporativa sensible contra amenazas internas (Tesis de Maestría). *Instituto Politécnico Nacional*. Obtenido de http://www.repositoriodigital.ipn.mx/bitstream/123456789/12642/1/Trabajo%20de%20Investigaci%C3%B3n%20-%20Jorge%20Alba%20Cruz.pdf

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

Arevalo. (2017). Elaboración y plan de implementación de política de seguridad de la información aplicada a una empresa nacional de alimentos. (Tesis de Maestría). *Universidad de Cuenta Ecuador*.

Arévalo, E. K. (2016). La gestión de riesgo TI y la efectividad de los sistemas de seguridad de información: caso de procesos críticos en las pequeñas entidades financieras de Lambayeque. Obtenido de http://journal.upao.edu.pe/PuebloContinente/article/download/395/360

Barbosa Fernandez, M. A. (2020). Modelo De Ciberseguridad Dirigido A Entidades Financieras, Alineado A Marcos De Referencia De Gestión Y Gobierno De Ti (Doctoral Dissertation).

Becerril, A. (2019). La ciberseguridad en los Tratados de Libre Comercio. *REVISTA CHILENA DE DERECHO Y TECNOLOGÍA*, 111-137. https://doi.org/10.5354/0719-2584.2019.53447

Bejarano, Rodriguez, & Merseguer. (2021). A Vision For Improving Business Continuity Through Cyber-Resilience Mechanisms And Frameworks. Iberian Conference On Information Systems And Technologies, Cisti,. *Cisti*. https://doi.org/https://doi.org/10.23919/Cisti52073.2021.9476324

Boehmer. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. *Securware*, 224-231. https://doi.org/10.1109/SECURWARE.2008.7

Borek, A., Parlikad, A., Webb, J., & Woodall, P. (2013). Total information risk management: maximizing the value of data and information assets. *Elsevier*. https://doi.org/ISBN: 978-0-12-405547-6

Breier, J., & Schindler, F. (2014). Assets Dependencies Model in Information Security Risk Management. In: Linawati, Mahendra M.S., Neuhold E.J., Tjoa A.M., You I (eds) Information and Communication Technology. ICT-EurAsia. *Lecture Notes in Computer Science*. https://doi.org/ISBN : 978-3-642-55031-7

Brenner, J. (2007). ISO 27001: Risk management and compliance. *Risk Management Magazine Vol54*. Obtenido de https://link.gale.com/apps/doc/A157587924/AONE?u=univcv&sid=googleScholar&xid=43e6d8c5

Calder, A. (2009). Information Security Based on ISO 27001/ISO 27002. *A Management Guide. Van Haren Publishing*.

Castro Quinde, C. O. (2014). Elaboración de un sistema de gestión de la seguridad de la información (SGSI) para la empresa radical CIA LTDA en la ciudad de quito para el año 2014. *Tesis de Maestria - Universidad de las Américas Ecuador*. Obtenido de http://dspace.udla.edu.ec/handle/33000/3376

Contreras, A., & Medina, G. (2019). Gestión de riesgo en seguridad digital en el sector privado y mixto-contexto general. La seguridad en el ciberespacio: un desafío para Colombia, 169-199.

Deloitte. (2021). Tendencias de Ciberseguridad 2021. Recuperado el 10 de 2022, de https://www2.deloitte.com/cl/es/pages/risk/articles/tendencias-de-ciberseguridad-2021.html

Diario Gestion. (2019). Menos de 150 empresas peruanas cuentan con certificación en seguridad de la información. *Seccion Tecnologia*. Recuperado el 10 de 2022, de https://gestion.pe/tecnologia/150-empresas-peruanas-cuentan-certificacion-cibercrimen-262366-noticia/

Dutton, J. (2016). Identifying assets for conducting an asset-based information security risk assessment. *Portal Vigilant Software*.

ESAN. (2019). La necesidad de leyes para la ciberseguridad en América Latina. *Conexión ESAN*. Recuperado el 10 de 2022, de https://www.esan.edu.pe/conexion-esan/la-necesidad-de-leyes-para-la-ciberseguridad-en-america-latina

Ganesan, e. a. (2016). Dynamic Scheduling Of Cybersecurity Analysts For Minimizing Risk Using Reinforcement Learning.Acm Transactions On Intelligent Systems And Technology. https://doi.org/https://doi.org/10.1145/2882969

Ghazouani, M., Faris, S., Medromi, H., & Sayouti, H. (2014). Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk. *International Journal of Computer Applications*.

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

Guzmán Pacheco, G. F. (2015). Metodología para la seguridad de tecnologías de información y comunicaciones en la Clínica Ortega. *Repositorio UNCP*. Obtenido de http://hdl.handle.net/20.500.12894/1478

Halvorson, N. (2008). Information Risk Management: A Process Approach to Risk Diagnosis and Treatment. *Auerbach Publications.*

Hernández, R., Fernández, C., & Baptista, M. (2014). Metodología de la investigación. *Interamericana Editores, S.A. de C.V*. Obtenido de https://eticainvestigativa.wordpress.com/2016/03/29/aspectos-eticos-en-la-investigacion-cientifica/

INCIBE-CERT. (2017). Análisis de riesgos en 6 pasos. Obtenido de https://www.incibe.es/en/node/2789

ISO 27001. (2015). El método MAGERIT. Obtenido de https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

ISOTools. (2019). Gestión de riesgos de seguridad de la información. Obtenido de https://www.isotools.org/2019/08/20/gestion-de-riesgos-de-seguridad-de-la-informacion-un-aspecto-clave-en-las-organizaciones-actuales/

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

Kouns, B., & Minoli, M. (2010). Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams. https://doi.org/ISBN:9780471762546

Lee, S. (2018). Resiliency Of Mobile Os Security For Secure Personal Ubiquitous Computing. Personal And Ubiquitous Computing, Vol 22 . https://doi.org/https://doi.org/10.1007/S00779-017-1098-X

Llontop. (2018). Gestión de riesgos de Tecnologías de Información de las Empresas de Nephila Networks. *Universidad Cesar Vallejo*. Obtenido de https://hdl.handle.net/20.500.12692/17596

Magerit. (2012). Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro I Método - versión 3.0. *Ministerio de Hacienda y Administraciones Públicas.* Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Maggiore, M. (2014). Modelo de Evaluación de Madurez para la Gestión . *Tesis Maestria .Universidad de Buenos Aires*. Obtenido de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0550_MaggioreML.pdf

Medina, C. A. C. (2019). Ciberseguridad: Por dónde Empezar…. Revista de Tecnología, 18(1), 89-100.

Mercado. (2016). Modelo de gestión de seguridad de la información para el E-Gobierno. *Universidad Nacional Mayor de San Marcos*. Obtenido de https://hdl.handle.net/20.500.12672/6414

Merino, F., & Cañizares, D. (2011). Implantación de un Sistema de Gestión de Seguridad de la Información según la ISO 27001. (1a ed.). Bogotá. *Ediciones de la U*.

Muñoz Ñauta, J. D. (2016). Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (dtic) de la Universidad de Cuenca. *(Tesis de Maestría).* Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/25646

Niño, N. (2018). Modelo de un sistema de gestión de seguridad de Información, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto nacional de estadística e informática Filial lambayeque. *Universidad Nacional Pedro Ruiz Gallo*.

Olaf, P., & Publishing, V. (2010). Enterprise Risk Management.

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

Rodríguez, Y. (2016). Diseño y formulación de un sistema de gestión de riesgos basados en los lineamientos establecidos por la norma NTC- ISO 31000.

Seclén, J. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. *Universidad Nacional Mayor de San Marcos*.

Valderrama, S. (2013). Pasos para elaborar proyectos y tesis de investigación. *San Marcos*.

Valenzuela, D. (2017). Editorial: Los desafíos de la ciberseguridad en Chile. *Revista Chilena de Derecho y Tecnología, 6*(2), 1-2. https://doi.org/10.5354/0719-2584.2017.48027

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

Whitman, M., & Mattord, H. (2013). Management of information security. *Cengage Learning.*

ANEXOS

ANEXO 1: Matriz de Operacionalización

Ciberseguridad para el Proceso de Gestión de Riesgos de TI en una Empresa Transnacional, Lima 2023.

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Items	Tecnica	Instrumento	Escala de Medicion	Escala de valores
Ciberseguridad	Para Basuchoudhary y Searle (2019) la ciberseguridad es cuando se intenta proteger mediante la deteccion de una amenaza o ataque los sistemas, por lo que deben mitigar a travez de acciones del usuario en las que la anomalía ha sido detectada y que puedan proceder con realizar los métodos de revisión para evitar la propagación de la amenaza, aquí es fundamental el conocimiento técnico de los responsables de Ciberseguridad.	Según Gallardo (2020) menciona que es importante mantener el ritmo de innovación en la ciberseguridad para poder adaptarse a las nuevas tendencias tecnologías y que se mantenga un nivel de riesgo aceptable.	Disponibilidad	Tiempo que tarda en obtener la informacion que se requiere	1 al 6	Encuesta	Cuestionario	Likert	1-Nunca 2-Casi Nunca 3-Algunas Veces 4-Casi Siempre 5-Siempre
			Confidencialidad	Politicas de seguridad de información	7 al 12				
			Integridad	Encriptacion y aseguramiento de la información	13 al 18				
Variable	**Definición Conceptual**	**Definición Operacional**	**Dimensiones**	**Indicadores**	**Items**	**Tecnica**	**Instrumento**		**Escala de valores**
Proceso de Gestión de Riesgos de TI	Vega y Ramos (2017) mencionan que el escenario ideal es el de minimizar los ataques e infiltraciones no deseados, para esto es necesario tomar medidas de proteccion y seguridad de toda la infraestructura de TI, esto junto a politicas en la Gestion de riesgos de TI, se puede tener un red mas segura, lo que se logra en conjunto con las herramientas tecnologicas y aplicaciones para mitigarlos.	Según Fitni (2020)defienden la idea de contar con buenas políticas seguridad con una buena capacitación al personal son el arma ideal para minimizar el riesgo en la gestion de TI en una organización	Proceso de Gobernanza del Riesgo	Efectividad en la definicion de los Riesgos de TI Según las categorias	19 al 24	Encuesta	Cuestionario	Likert	1-Nunca 2-Casi Nunca 3-Algunas Veces 4-Casi Siempre 5-Siempre
			Cultura consiente sobre Riesgos	Grado de consientizacion	25 al 30				

Fuente: Elaboración propia

ANEXO 2: Matriz de consistencia

Ciberseguridad para el Proceso de Gestión de Riesgos de TI en una Empresa Transnacional, Lima 2023.

Problema General	Objetivo General	Hipotesis General	Variables	Dimensiones	Indicadores	Metodologia
¿Que relacion existe entre Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023?	Determinar la relación existente entre Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.	Existe una relación directa entre la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.	Ciberseguridad	Disponibilidad	Tiempo que tarda en obtener la informacion que se requiere	Enfoque: Cuantitativo Tipo: Aplicada Diseño: Preexperimental Tecnica: Recoleccion de datos Instrumento: Encuesta
				Confidencialidad	Politicas de seguridad de información	
				Integridad	Encriptacion y aseguramiento de la información	
Problemas Especificos	**Objetivos Especificos**	**Hipotesis Especificas**	**Variables**	**Dimensiones**	**Indicadores**	
¿Que relacion existe entre la dimensión Disponibilidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023?	Determinar la relación existente entre la dimensión Disponibilidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.	Existe una relación directa entre la dimensión Disponibilidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.	Proceso de Gestión de Riesgos de TI	Proceso de Gobernanza del Riesgo	Efectividad en la definicion de los Riesgos de TI Según las categorias	
¿Que relacion existe entre la dimensión Confidencialidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023?	Determinar la relación existente entre la dimensión Confidencialidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.	Existe una relación directa entre la dimensión Confidencialidad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima 2023.		Cultura consiente sobre Riesgos	Grado de consientizacion	
¿Que relacion existe entre la dimensión Integridad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023?	Determinar la relación existente entre la dimensión Integridad de la Ciberseguridad y la Gestión de Riesgos de TI en una Empresa Transnacional en Lima, 2023.	Existe una relación directa entre la dimensión Integridad de datos de la Ciberseguridad y la Gestión de Riesgos de TI en una empresa Transnacional en Lima 2023.				

Fuente: Elaboración propia

ANEXO 3: Instrumento de recolección de datos

ENCUESTA

Para medir la relación entre la Ciberseguridad y el Proceso de Gestión de Riesgos de TI en una Transnacional, Lima 2023.

Se ha diseñado el presente cuestionario con el objeto de tener un buen procedimiento de medición sobre la seguridad y disponibilidad de la información, por lo que necesitamos de su colaboración. Marque de acuerdo con la valoración que usted le asigne.

Autor (Calderon 2019)

	V1 - CIBERSEGURIDAD	ESCALA				
		1	2	3	4	5
Ítem	**V1 D1 | Disponibilidad**					
1	¿Se encuentra disponible la información que requiere?					
2	¿Los sistemas con que cuenta la institución son rápidos?					
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?					
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?					
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores?					
6	¿Los sitios web de la empresa se encuentran activos en todo momento?					
	V1 D2 | CONFIDENCIALIDAD					
7	¿La empresa cuenta con políticas de seguridad de la información?					
8	¿La Entidad distribuye y capacita a los trabajadores sobre la política de información con que cuenta?					
9	¿La empresa capacita a los trabajadores acerca de la clasificación de los activos de información y su importancia?					
10	¿Usted resguarda la información de la entidad en medios seguros?					

11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?					
12	¿Existen accesos restringidos al área de redes y comunicaciones?					
	V1 D3 | INTEGRIDAD DE DATOS					
13	¿Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de su ubicación?					
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?					
15	¿La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave?					
16	¿Los antivirus instalados en su equipo son actualizados continuamente?					
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?					
18	¿La institucion realiza capacitaciones acerca de ataques virus en sus diversas modalidades?					

	V2 - GESTION DE RIESGOS DE TI	**ESCALA**				
		1	**2**	**3**	**4**	**5**
Ítem	**V2 D1 | CULTURA CONSCIENTE SOBRE RIESGOS DE TECNOLOGIAS DE INFORMACION**					
19	¿Ha recibido capacitación referente a seguridad de la información?					
20	¿La Entidad implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?					
21	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?					
22	¿La empresa recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?					
23	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información que maneja?					
24	¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza?					

	V2 D2 | PROCESO DE GOBERNANZA DEL RIESGO					
25	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?					
26	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?					
27	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?					
28	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?					
29	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?					
30	Finalmente ¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?					

ANEXO 4: Matriz de datos

Variable: Ciberseguridad

	V1 - Ciberseguridad																	
	Disponibilidad						Confidencialidad						Integridad					
N°	P01	P02	P03	P04	P05	P06	P07	P08	P09	P10	P11	P12	P13	P14	P15	P16	P17	P18
1	4	5	4	5	5	5	5	5	5	5	3	5	5	5	5	4	2	1
2	5	4	4	4	4	4	5	5	4	4	4	5	5	2	3	3	4	4
3	4	4	3	1	4	4	4	2	2	4	5	5	4	1	3	3	5	1
4	5	4	4	4	5	4	4	4	3	4	3	5	5	4	4	4	3	3
5	4	4	4	5	5	5	5	5	4	5	5	5	3	3	3	5	5	5
6	2	2	1	2	2	4	5	5	4	3	1	1	2	5	1	5	4	1
7	4	4	4	4	4	5	5	5	5	5	5	5	5	3	5	5	5	5
8	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
9	5	5	4	5	4	4	4	3	4	5	5	5	5	3	4	5	4	4
10	5	4	5	5	5	5	5	4	2	3	5	3	3	3	5	3	5	2
11	4	4	4	5	5	5	5	4	3	3	4	3	5	2	4	4	5	5
12	4	4	4	2	4	4	5	4	4	5	5	5	5	3	5	5	5	3
13	5	4	4	5	5	4	3	3	5	5	5	5	5	5	5	5	5	5
14	5	4	4	5	5	5	5	4	3	5	5	5	2	3	5	5	5	4
15	2	4	4	4	5	5	5	5	4	4	5	5	5	2	5	4	5	4
16	4	5	4	5	5	5	4	5	5	4	5	4	4	5	5	4	5	4
17	4	4	4	4	3	4	3	3	4	4	4	4	3	4	5	3	3	3
18	5	4	4	5	5	5	5	4	4	5	5	5	5	3	3	3	3	3
19	4	4	3	4	4	4	5	4	3	5	4	4	5	4	4	5	4	3
20	5	5	4	5	5	4	5	4	4	5	4	5	5	5	4	5	5	4
21	5	4	4	1	3	5	4	4	3	5	5	5	4	5	5	4	1	3
22	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
23	5	5	5	4	5	1	5	5	5	5	5	5	5	5	5	5	5	5

24	4	4	3	4	4	4	4	4	4	5	5	4	4	4	4	4	4	4
25	4	5	4	2	4	5	5	5	4	3	4	4	4	5	4	5	5	5
26	3	3	3	3	4	4	3	2	2	2	2	4	3	1	1	2	1	1
27	3	3	3	3	3	4	3	3	3	3	4	4	2	2	4	4	2	2
28	5	4	4	4	5	4	5	4	5	5	5	5	5	4	5	4	4	5
29	4	5	5	4	4	5	4	4	5	5	5	4	5	5	4	5	5	4
30	5	4	4	5	4	5	4	4	5	5	4	3	4	4	3	4	5	4

Matriz de datos

Variable: Gestión de Riesgos de TI

	V2 - Gestión de Riesgos de TI											
	Proceso de Gobernanza del Riesgo						Cultura consiente sobre Riesgos					
N°	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30
1	3	3	2	4	5	5	4	3	4	5	4	4
2	4	4	5	4	4	4	4	4	4	2	3	3
3	2	2	2	3	3	4	4	3	4	2	3	4
4	3	3	3	3	3	5	3	2	2	2	2	2
5	5	5	5	5	4	5	5	5	5	5	3	5
6	5	5	5	5	4	4	2	2	4	5	5	3
7	5	5	5	5	5	5	5	5	4	5	5	5
8	4	5	5	5	5	5	5	5	5	5	5	5
9	4	4	4	4	4	5	4	5	5	4	4	4
10	3	1	5	5	3	4	3	4	3	3	3	3
11	1	1	1	1	4	2	4	2	2	3	3	3
12	4	4	3	5	4	5	5	4	4	5	4	5
13	3	3	2	5	5	5	5	5	5	4	4	4
14	5	4	3	4	4	5	5	5	4	5	3	5
15	4	4	5	4	5	5	4	4	4	3	3	4
16	5	5	4	4	5	4	4	5	4	4	5	4
17	3	4	4	4	3	5	4	4	3	4	4	5
18	3	3	3	3	4	4	4	4	4	4	4	4
19	4	4	4	4	4	4	4	4	4	4	4	4
20	5	4	5	5	4	5	4	4	5	5	4	5
21	4	1	1	3	3	5	2	2	2	3	3	2
22	5	5	5	5	5	5	5	5	5	5	5	5
23	5	5	5	5	5	5	5	5	3	5	5	5
24	4	4	4	4	4	4	4	4	4	4	4	4

25	5	5	5	5	4	4	4	5	5	5	4	5
26	2	1	1	1	2	2	1	1	2	1	2	1
27	2	2	2	1	4	4	3	2	2	1	1	1
28	5	4	5	5	4	4	4	4	5	4	5	4
29	4	4	5	4	5	5	5	4	5	5	4	5
30	5	4	4	4	5	5	5	5	4	4	5	5

ANEXO 5: Validación de Instrumentos

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "CIBERSEGURIDAD"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DISPONIBILIDAD	Si	No	Si	No	Si	No	
1	¿Se encuentra disponible la información que requiere?	X		X		X		
2	¿Los sistemas con que cuenta la institución son rápidos?	X		X		X		
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?	X		X		X		
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?	X		X		X		
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores?	X		X		X		
6	¿Los sitios web de la empresa se encuentran activos en todo momento?	X		X		X		
	CONFIDENCIALIDAD	Si	No	Si	No	Si	No	
7	¿La empresa cuenta con políticas de seguridad de la información?	X		X		X		
8	¿La Entidad distribuye y capacita a los trabajadores sobre la política de información con que cuenta?	X		X		X		
9	¿La empresa capacita a los trabajadores acerca de la clasificación de los activos de información y su importancia?	X		X		X		
10	¿Usted resguarda la información de la entidad en medios seguros?	X		X		X		
11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?	X		X		X		
12	¿Existen accesos restringidos al área de redes y comunicaciones?	X		X		X		
	INTEGRIDAD DE DATOS	Si	No	Si	No	Si	No	
13	¿Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de su ubicación?	X		X		X		
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?	X		X		X		
15	¿La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave?	X		X		X		
16	¿Los antivirus instalados en su equipo son actualizados continuamente?	X		X		X		
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?	X		X		X		
18	¿La institución realiza capacitaciones acerca de ataques virus en sus diversas modalidades?	X		X		X		

Observaciones (precisar si hay suficiencia):_El instrumento cuenta con lo necesario y la pertinencia para su aplicación.

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

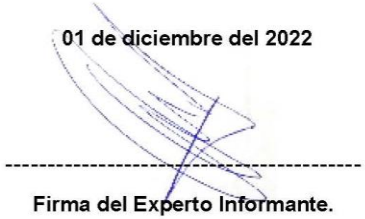
Apellidos y nombres del juez validador. Dr/ Mg: **Henry Paúl Bermejo Terrones. DNI: 18214307**

Especialidad del validador: Maestro en Ingeniería de Sistemas con mención en Tecnologías de Información

[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

01 de diciembre del 2022



Firma del Experto Informante.

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "GESTION DE RIESGOS DE T.I"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CULTURA CONSCIENTE SOBRE RIESGOS DE TECNOLOGIAS DE INFORMACION	Si	No	Si	No	Si	No	
1	¿Ha recibido capacitación referente a seguridad de la información?	X		X		X		
2	¿La Entidad implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?	X		X		X		
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?	X		X		X		
4	¿La empresa recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?	X		X		X		
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información que maneja?	X		X		X		
6	¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza?	X		X		X		
	PROCESO DE GOBERNANZA DEL RIESGO	Si	No	Si	No	Si	No	
7	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?	X		X		X		
8	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?	X		X		X		
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?	X		X		X		
10	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?	X		X		X		
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?	X		X		X		
12	Finalmente ¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?	X		X		X		

Observaciones (precisar si hay suficiencia):_____

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

Apellidos y nombres del juez validador. Dr/ Mg: **Henry Paúl Bermejo Terrones** **DNI: 18214307**

Especialidad del validador: Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información

01 de diciembre del 2022

Firma del Experto Informante.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** 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

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "CIBERSEGURIDAD"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DISPONIBILIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Se encuentra disponible la información que requiere?	X		X		X		
2	¿Los sistemas con que cuenta la institución son rápidos?	X		X		X		
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?	X		X		X		
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?	X		X		X		
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores?	X		X		X		
6	¿Los sitios web de la empresa se encuentran activos en todo momento?	X		X		X		
	CONFIDENCIALIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿La empresa cuenta con políticas de seguridad de la información?	X		X		X		
8	¿La Entidad distribuye y capacita a los trabajadores sobre la política de información con que cuenta?	X		X		X		
9	¿La empresa capacita a los trabajadores acerca de la clasificación de los activos de información y su importancia?	X		X		X		
10	¿Usted resguarda la información de la entidad en medios seguros?	X		X		X		
11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?	X		X		X		
12	¿Existen accesos restringidos al área de redes y comunicaciones?	X		X		X		
	INTEGRIDAD DE DATOS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de su ubicación?	X		X		X		
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?	X		X		X		
15	¿La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave?	X		X		X		
16	¿Los antivirus instalados en su equipo son actualizados continuamente?	X		X		X		
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?	X		X		X		
18	¿La institución realiza capacitaciones acerca de ataques virus en sus diversas modalidades?	X		X		X		

Observaciones (precisar si hay suficiencia):_____

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

Apellidos y nombres del juez validador. Dr/ Mg: **ACUÑA BENTIES MARLON FRANK** **DNI: 42097456**
Especialidad del validador: METODOLÓGICO

01 de diciembre del 2022

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del Experto Informante.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** 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

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "GESTION DE RIESGOS DE T.I"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CULTURA CONSCIENTE SOBRE RIESGOS DE TECNOLOGIAS DE INFORMACION	Si	No	Si	No	Si	No	
1	¿Ha recibido capacitación referente a seguridad de la información?	X		X		X		
2	¿La Entidad implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?	X		X		X		
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?	X		X		X		
4	¿La empresa recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?	X		X		X		
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información que maneja?	X		X		X		
6	¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza?	X		X		X		
	PROCESO DE GOBERNANZA DEL RIESGO	Si	No	Si	No	Si	No	
7	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?	X		X		X		
8	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?	X		X		X		
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?	X		X		X		
10	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?	X		X		X		
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?	X		X		X		
12	Finalmente ¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?	X		X		X		

Observaciones (precisar si hay suficiencia):_____

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

Apellidos y nombres del juez validador. Dr/ Mg: **ACUÑA BENTIES MARLON FRANK** **DNI: 42097456**
Especialidad del validador: METODOLÓGICO

01 de diciembre del 2022

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del Experto Informante.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** 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

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "CIBERSEGURIDAD"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DISPONIBILIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Se encuentra disponible la información que requiere?	x		x		x		
2	¿Los sistemas con que cuenta la institución son rápidos?	x		x		x		
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?	x		x		x		
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?	x		x		x		
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores?	x		x		x		
6	¿Los sitios web de la empresa se encuentran activos en todo momento?	x		x		x		
	CONFIDENCIALIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿La empresa cuenta con políticas de seguridad de la información?	x		x		x		
8	¿La Entidad distribuye y capacita a los trabajadores sobre la política de información con que cuenta?	x		x		x		
9	¿La empresa capacita a los trabajadores acerca de la clasificación de los activos de información y su importancia?	x		x		x		
10	¿Usted resguarda la información de la entidad en medios seguros?	x		x		x		
11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?	x		x		x		
12	¿Existen accesos restringidos al área de redes y comunicaciones?	x		x		x		
	INTEGRIDAD DE DATOS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de su ubicación?	x		x		x		
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?	x		x		x		
15	¿La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave?	x		x		x		
16	¿Los antivirus instalados en su equipo son actualizados continuamente?	x		x		x		
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?	x		x		x		
18	¿La institución realiza capacitaciones acerca de ataques virus en sus diversas modalidades?	x		x		x		

Observaciones (precisar si hay suficiencia):_____

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

Apellidos y nombres del juez validador. Mg: **TEJADA RUIZ ROBERTO JUAN** **DNI: 17930425**

Especialidad del validador:..... ingeniero industrial / sistema de gestión de calidad

01 de diciembre del 2022

[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

Ing. Roberto Juan Tejada Ruiz
INGENIERO INDUSTRIAL - C.I.P. 242352

Firma del Experto Informante.

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "GESTION DE RIESGOS DE T.I"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CULTURA CONSCIENTE SOBRE RIESGOS DE TECNOLOGIAS DE INFORMACION	Si	No	Si	No	Si	No	
1	¿Ha recibido capacitación referente a seguridad de la información?	x		x		x		
2	¿La Entidad implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?	x		x		x		
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?	x		x		x		
4	¿La empresa recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?	x		x		x		
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información que maneja?	x		x		x		
6	¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza?	x		x		x		
	PROCESO DE GOBERNANZA DEL RIESGO	Si	No	Si	No	Si	No	
7	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?			x		x		
8	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?	x		x		x		
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?	x		x		x		
10	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?	x		x		x		
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?	x		x		x		
12	Finalmente ¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?	x		x		x		

Observaciones (precisar si hay suficiencia):_____

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

Apellidos y nombres del juez validador. Mg: **TEJADA RUIZ ROBERTO JUAN** **DNI: 17930425**

Especialidad del validador:..... ingeniero industrial / sistema de gestión de calidad

01 de diciembre del 2022

[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

Ing. Roberto Juan Tejada Ruiz
INGENIERO INDUSTRIAL - C.I.P. 242352
Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "CIBERSEGURIDAD"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DISPONIBILIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Se encuentra disponible la información que requiere?	Si		Si		Si		
2	¿Los sistemas con que cuenta la institución son rápidos?	Si		Si		Si		
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?	Si		Si		Si		
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?	Si		Si		Si		
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores?	Si		Si		Si		
6	¿Los sitios web de la empresa se encuentran activos en todo momento?	Si		Si		Si		
	CONFIDENCIALIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿La empresa cuenta con políticas de seguridad de la información?	Si		Si		Si		
8	¿La Entidad distribuye y capacita a los trabajadores sobre la política de información con que cuenta?	Si		Si		Si		
9	¿La empresa capacita a los trabajadores acerca de la clasificación de los activos de información y su importancia?	Si		Si		Si		
10	¿Usted resguarda la información de la entidad en medios seguros?	Si		Si		Si		
11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?	Si		Si		Si		
12	¿Existen accesos restringidos al área de redes y comunicaciones?	Si		Si		Si		
	INTEGRIDAD DE DATOS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de su ubicación?	Si		Si		Si		
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?	Si		Si		Si		
15	¿La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave?	Si		Si		Si		
16	¿Los antivirus instalados en su equipo son actualizados continuamente?	Si		Si		Si		
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?	Si		Si		Si		
18	¿La institución realiza capacitaciones acerca de ataques virus en sus diversas modalidades?	Si		Si		Si		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

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

Apellidos y nombres del juez validador. POLETTI GAITAN, EDUARDO HUMBERTO **DNI:** 18073124

Especialidad del validador: MAESTRO

30 de diciembre del 2022

Firma del Experto Informante.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** 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

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "GESTION DE RIESGOS DE T.I"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CULTURA CONSCIENTE SOBRE RIESGOS DE TECNOLOGIAS DE INFORMACION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Ha recibido capacitación referente a seguridad de la información?	Si		Si		Si		
2	¿La Entidad implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?	Si		Si		Si		
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?	Si		Si		Si		
4	¿La empresa recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?	Si		Si		Si		
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información que maneja?	Si		Si		Si		
6	¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza?	Si		Si		Si		
	PROCESO DE GOBERNANZA DEL RIESGO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?	Si		Si		Si		
8	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?	Si		Si		Si		
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?	Si		Si		Si		
10	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?	Si		Si		Si		
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?	Si		Si		Si		
12	Finalmente ¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?	Si		Si		Si		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

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

Apellidos y nombres del juez validador. POLETTI GAITAN, EDUARDO HUMBERTO **DNI:** 18073124

Especialidad del validador: MAESTRO

[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

30 de diciembre del 2022

Firma del Experto Informante.

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "CIBERSEGURIDAD"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DISPONIBILIDAD	Si	No	Si	No	Si	No	
1	¿Se encuentra disponible la información que requiere?	✓		✓		✓		
2	¿Los sistemas con que cuenta la institución son rápidos?	✓		✓		✓		
3	¿El tiempo de recuperación de un sistema ante una incidencia es rápido?	✓		✓		✓		
4	¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?	✓		✓		✓		
5	¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores?	✓		✓		✓		
6	¿Los sitios web de la empresa se encuentran activos en todo momento?	✓		✓		✓		
	CONFIDENCIALIDAD	Si	No	Si	No	Si	No	
7	¿La empresa cuenta con políticas de seguridad de la información?	✓		✓		✓		
8	¿La Entidad distribuye y capacita a los trabajadores sobre la política de información con que cuenta?	✓		✓		✓		
9	¿La empresa capacita a los trabajadores acerca de la clasificación de los activos de información y su importancia?	✓		✓		✓		
10	¿Usted resguarda la información de la entidad en medios seguros?	✓		✓		✓		
11	¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?	✓		✓		✓		
12	¿Existen accesos restringidos al área de redes y comunicaciones?	✓		✓		✓		
	INTEGRIDAD DE DATOS	Si	No	Si	No	Si	No	
13	¿Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de su ubicación?	✓		✓		✓		
14	¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?	✓		✓		✓		
15	¿La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave?	✓		✓		✓		
16	¿Los antivirus instalados en su equipo son actualizados continuamente?	✓		✓		✓		
17	¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?	✓		✓		✓		
18	¿La institución realiza capacitaciones acerca de ataques virus en sus diversas modalidades?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Ninguno

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

Apellidos y nombres del juez validador. Dr/ Mg: Huanca Zarate Jonathan Alexis **DNI:** 44268195

Especialidad del validador: Ing. Sistemas CIP

01 de diciembre del 2022

CIP: 173970

Firma del Experto Informante.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** 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

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE DE "GESTION DE RIESGOS DE T.I"

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	CULTURA CONSCIENTE SOBRE RIESGOS DE TECNOLOGIAS DE INFORMACION	Si	No	Si	No	Si	No	
1	¿Ha recibido capacitación referente a seguridad de la información?	✓		✓		✓		
2	¿La Entidad implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?	✓		✓		✓		
3	¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?	✓		✓		✓		
4	¿La empresa recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?	✓		✓		✓		
5	¿El personal esta concientizado sobre los riesgos a los que está expuesta la información que maneja?	✓		✓		✓		
6	¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza?	✓		✓		✓		
	PROCESO DE GOBERNANZA DEL RIESGO	Si	No	Si	No	Si	No	
7	¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?	✓		✓		✓		
8	¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?	✓		✓		✓		
9	¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?	✓		✓		✓		
10	¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?	✓		✓		✓		
11	¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?	✓		✓		✓		
12	Finalmente ¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Ninguno

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

Apellidos y nombres del juez validador. Dr/ Mg: Puente Tavara Jonathan Alexis **DNI:** 44268198

Especialidad del validador: Ing. Sistemas

01 de diciembre del 2022

CIP: 173971

Firma del Experto Informante.

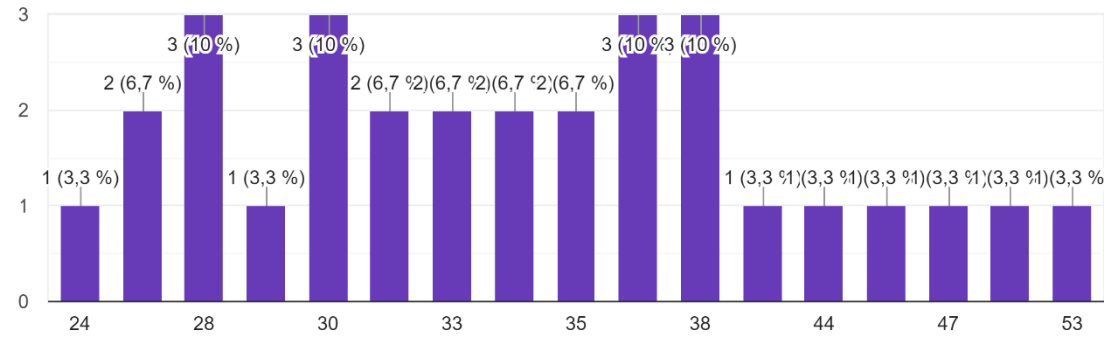
[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

ANEXO 6: Resumen de Encuestas Realizadas

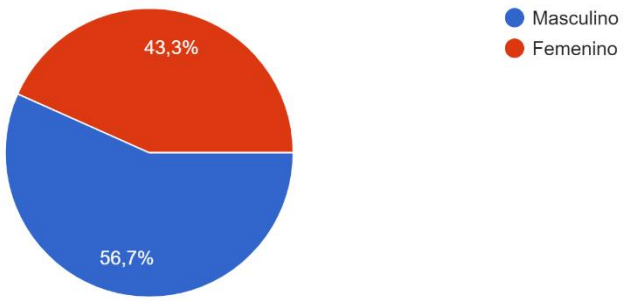
Edad

30 respuestas



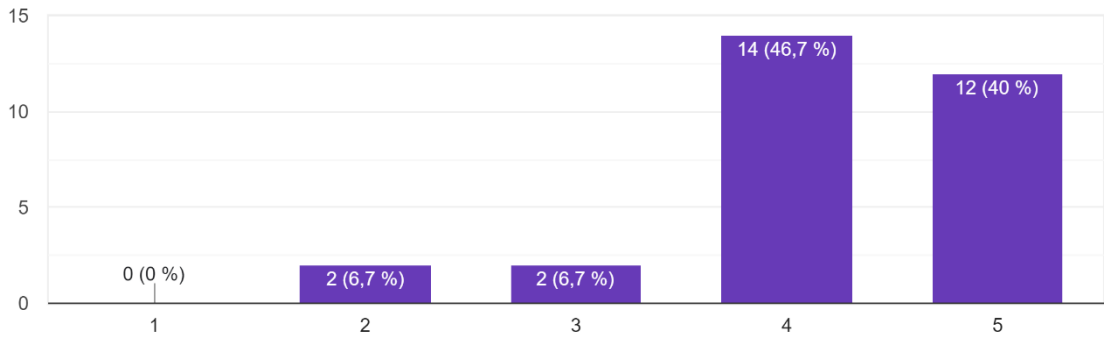
Sexo

30 respuestas



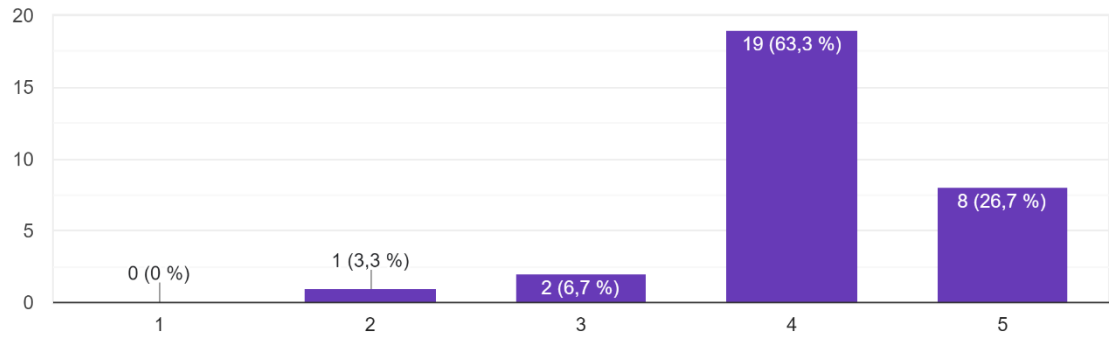
1.- ¿Se encuentra disponible la información que requiere?

30 respuestas



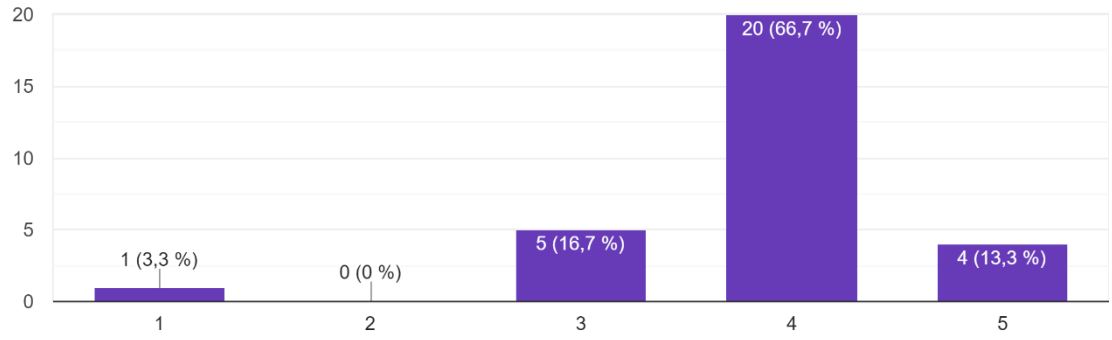
2.- ¿Los sistemas con que cuenta la empresa son rápidos?

30 respuestas



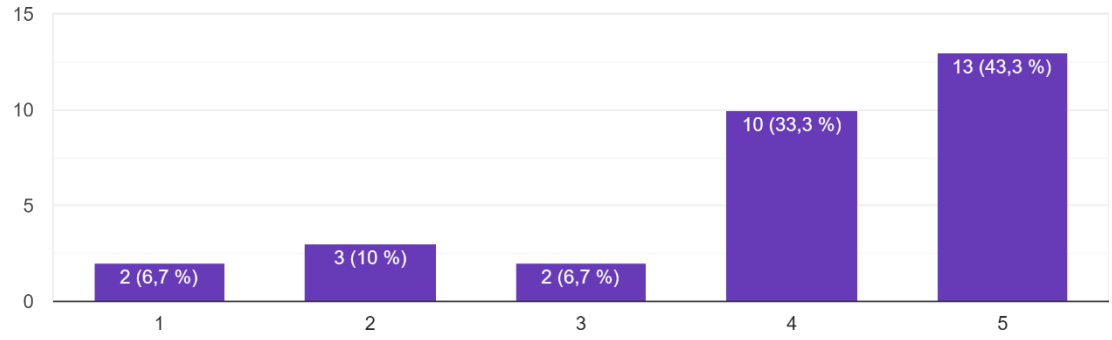
3.- ¿El tiempo de recuperación de un sistema ante una incidencia es rápido?

30 respuestas



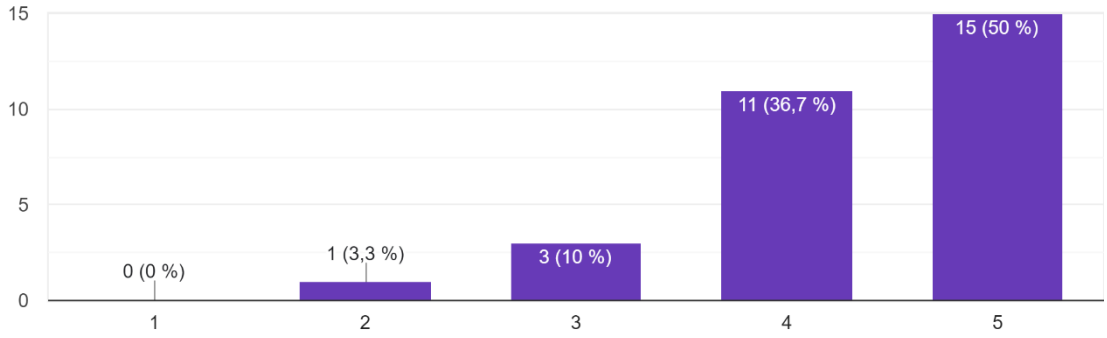
4.- ¿Cuándo ha necesitado que se recupere información borrada por error desde una carpeta compartida, el área de TI le proporciono una copia de respaldo?

30 respuestas



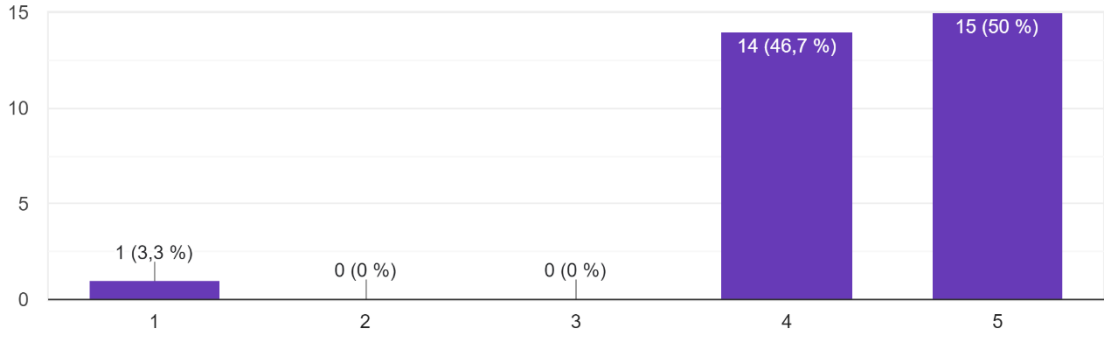
5.- ¿Cuenta en todo momento con acceso a la información que requiere para realizar sus labores?

30 respuestas



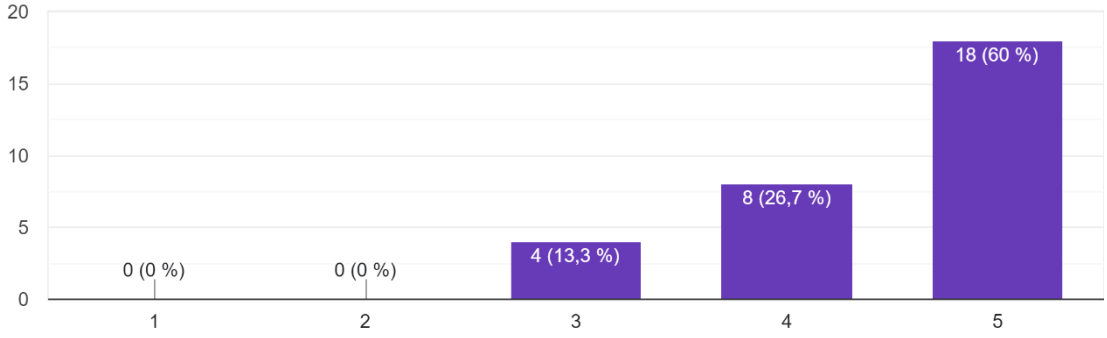
6.- ¿Los sitios web de la empresa se encuentran activos en todo momento?

30 respuestas



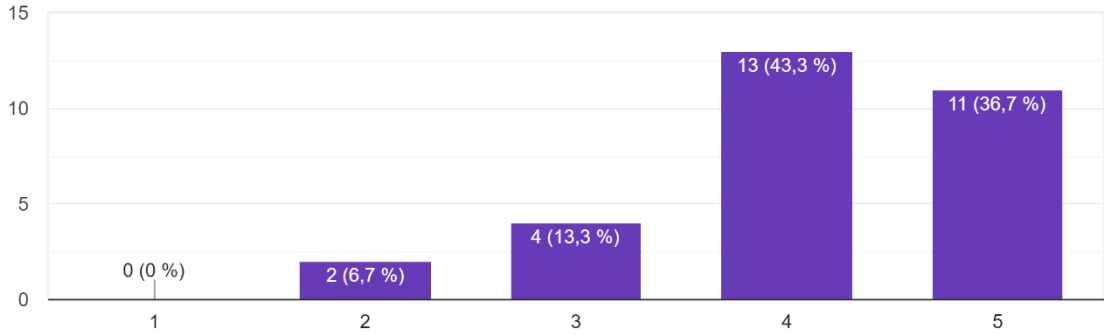
7.- ¿La empresa cuenta con políticas de seguridad de la información?

30 respuestas



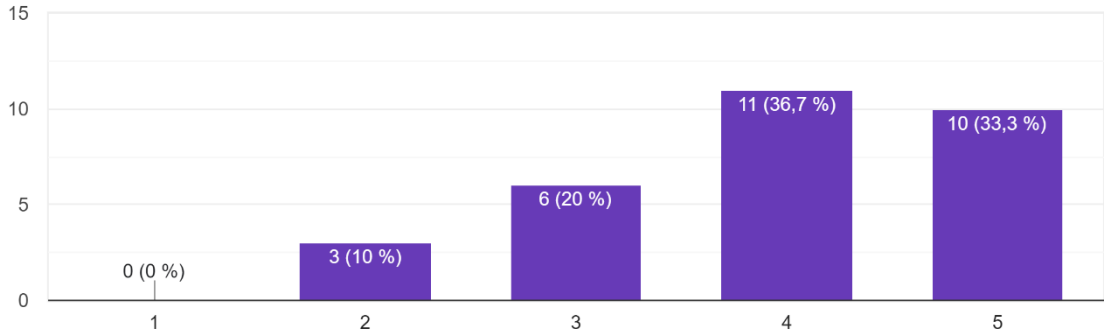
8.- ¿La Entidad distribuye y capacita a los trabajadores sobre la política de información con que cuenta?

30 respuestas



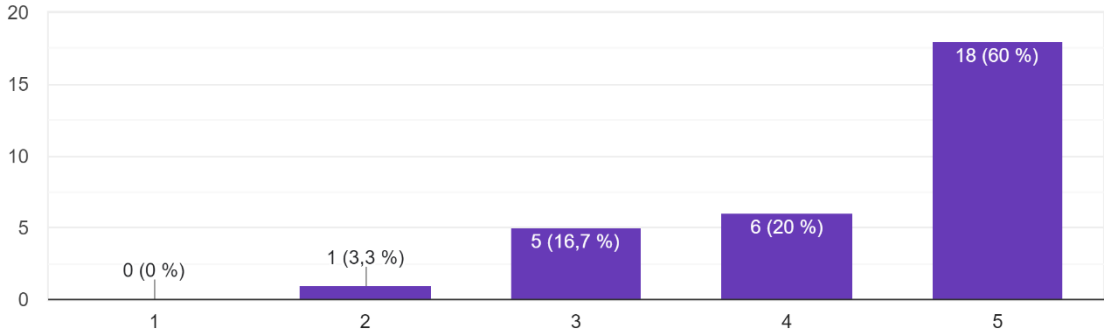
9.- ¿La empresa capacita a los trabajadores acerca de la clasificación de los activos de información y su importancia?

30 respuestas



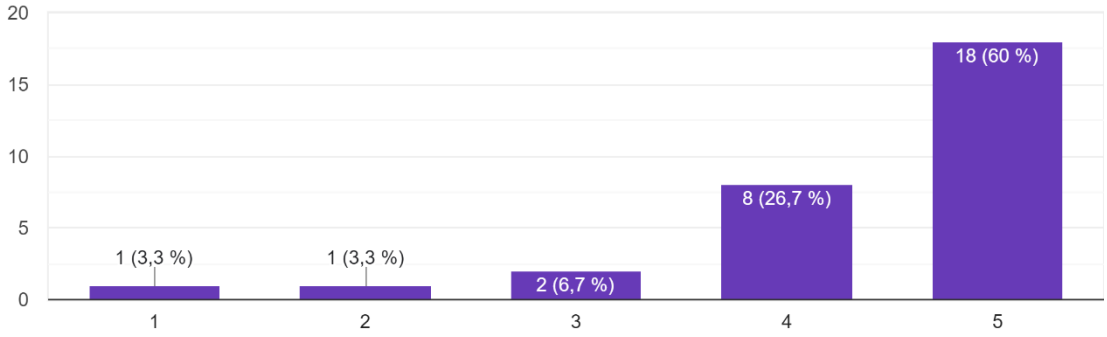
10.- ¿Usted resguarda la información de la entidad en medios seguros?

30 respuestas



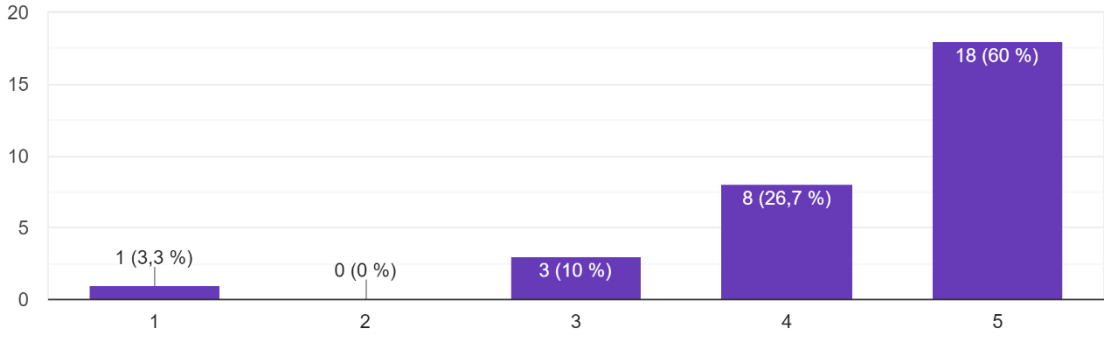
11.- ¿Los archivos que usted comparte en carpetas cuentan con permiso solo para las personas autorizadas?

30 respuestas



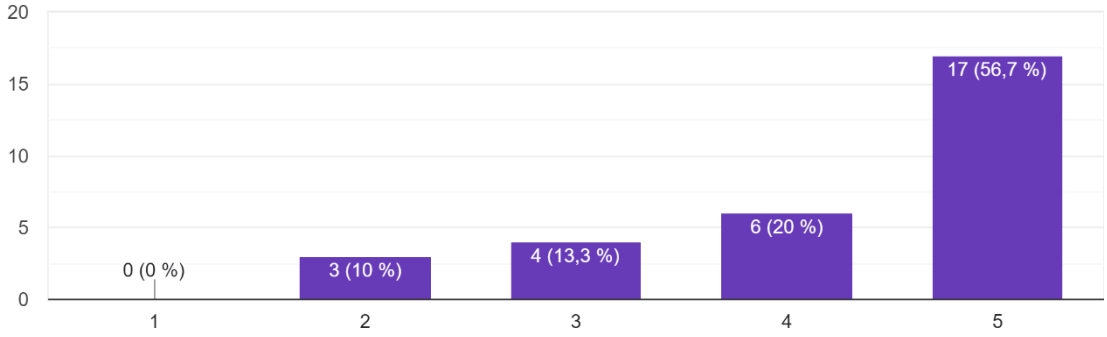
12.- ¿Existen accesos restringidos al área de redes y comunicaciones?

30 respuestas



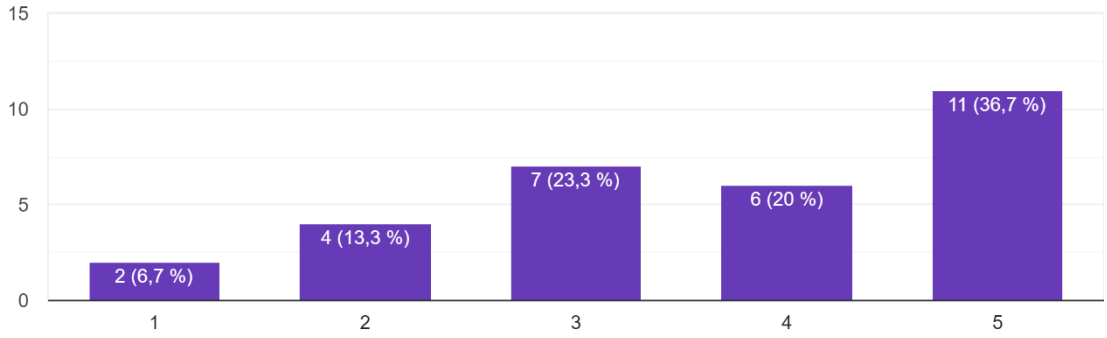
13.- ¿Realiza el bloqueo de su sesión de usuario en su equipo de cómputo al retirarse de su ubicación?

30 respuestas



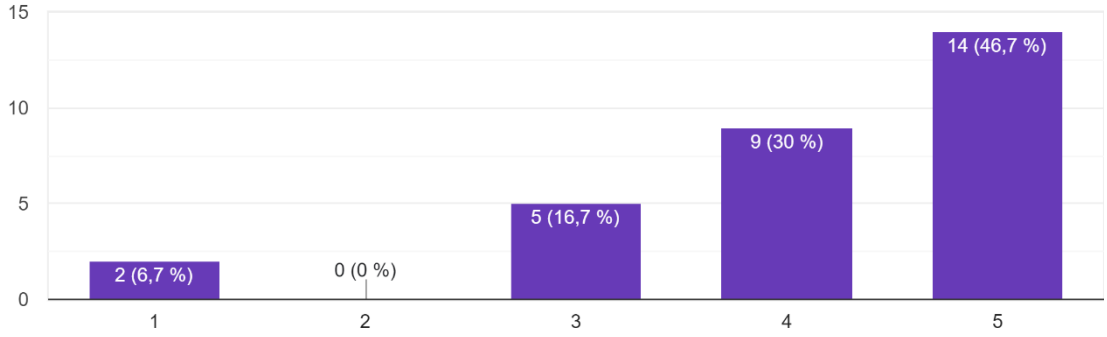
14.- ¿Realiza el cambio continuo de contraseña para ingresar a su equipo de cómputo?

30 respuestas



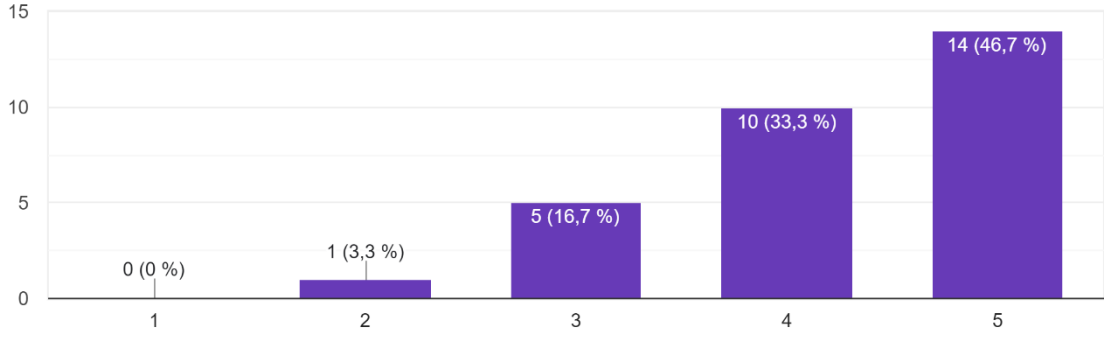
15.- ¿La documentación en físico que usted maneja se encuentra resguardada en un lugar seguro y bajo llave?

30 respuestas



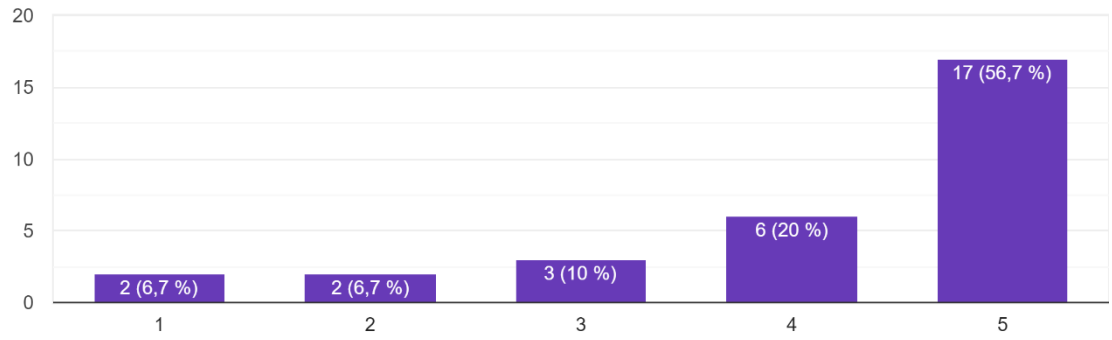
16.- ¿Los antivirus instalados en su equipo son actualizados continuamente?

30 respuestas



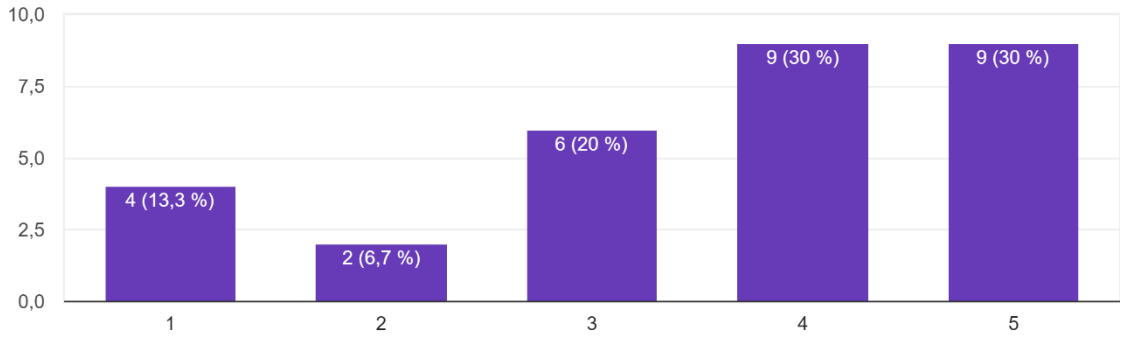
17.- ¿Ante cortes eléctricos imprevistos, cuenta con medidas de contingencia?

30 respuestas



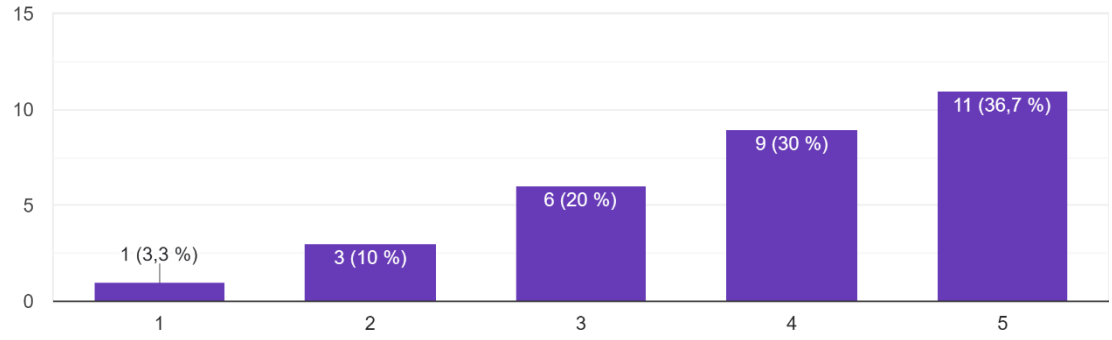
18.- ¿La institucion realiza capacitaciones acerca de ataques virus en sus diversas modalidades?

30 respuestas



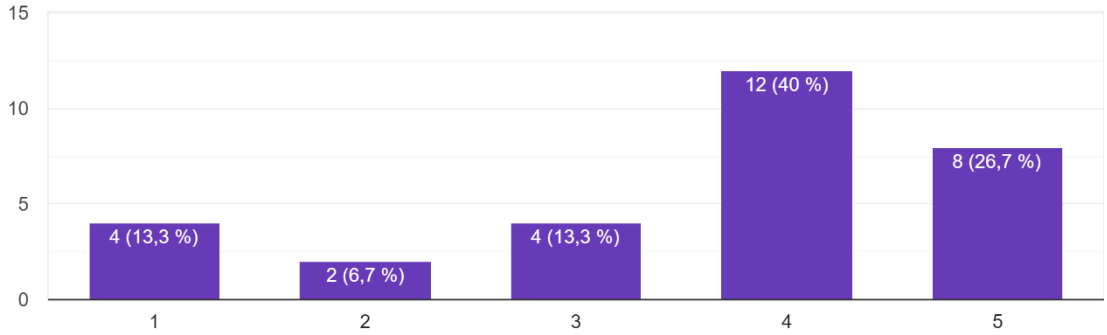
19.- ¿Ha recibido capacitación referente a seguridad de la información?

30 respuestas



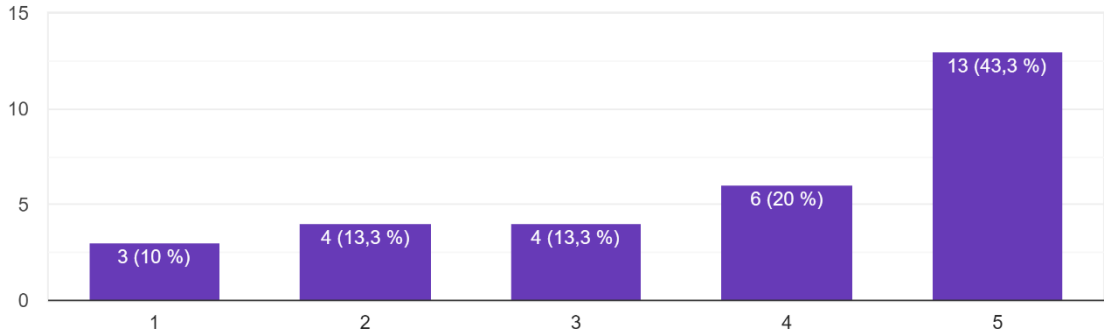
20.- ¿La Entidad implementa capacitaciones referidas a seguridad de la información y/o gestión de riesgos?

30 respuestas



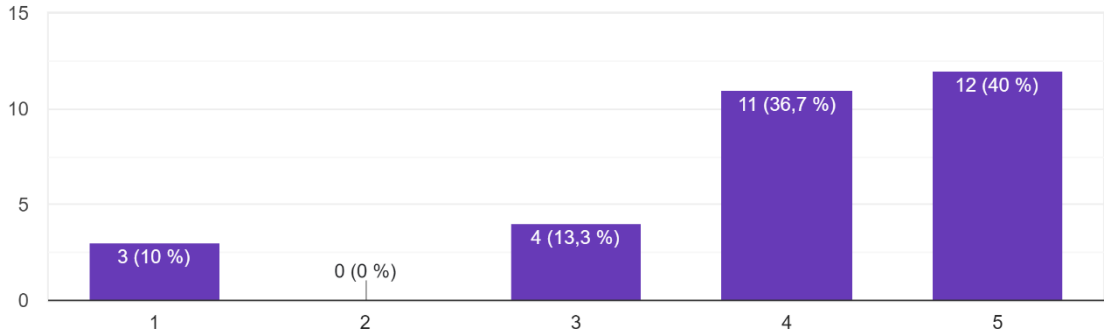
21.- ¿El personal recibe capacitaciones periódicas sobre gestión de riesgo asociados al manejo de la información?

30 respuestas



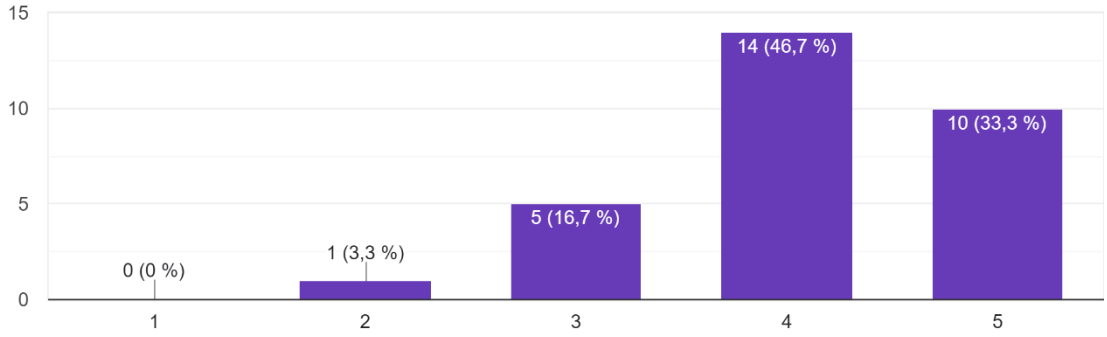
22.- ¿La empresa recomienda conductas de concientización en la gestión de riesgos para la seguridad de la información?

30 respuestas



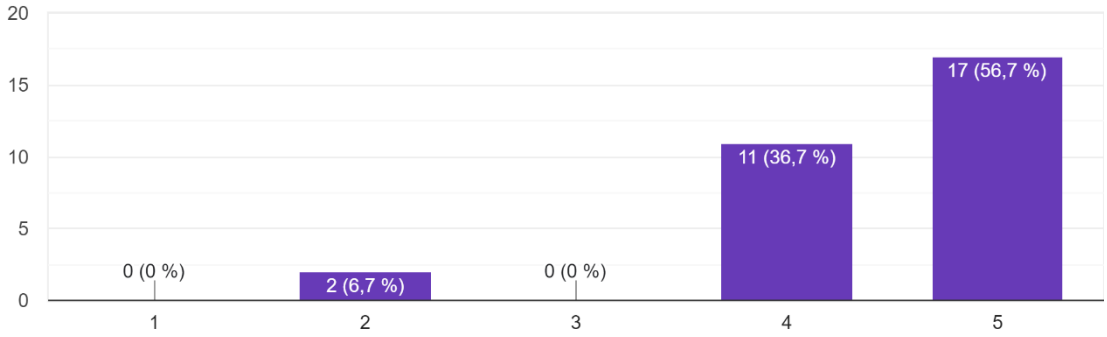
23.- ¿El personal esta concientizado sobre los riesgos a los que está expuesta la información que maneja?

30 respuestas



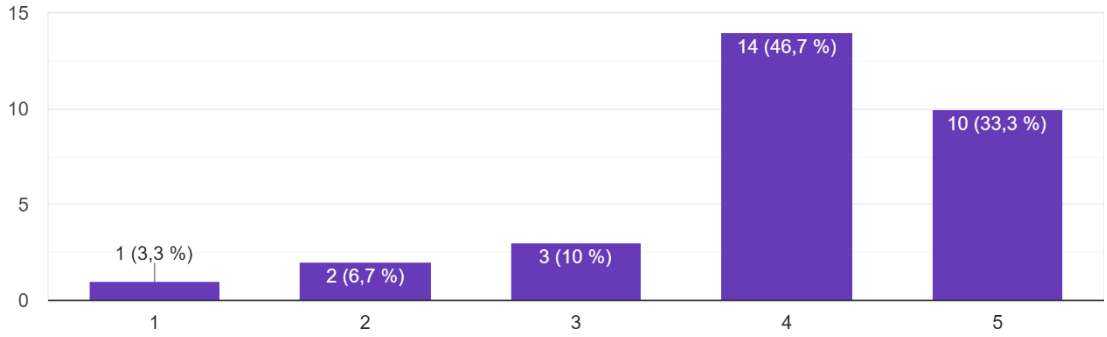
24.- ¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que utiliza?

30 respuestas



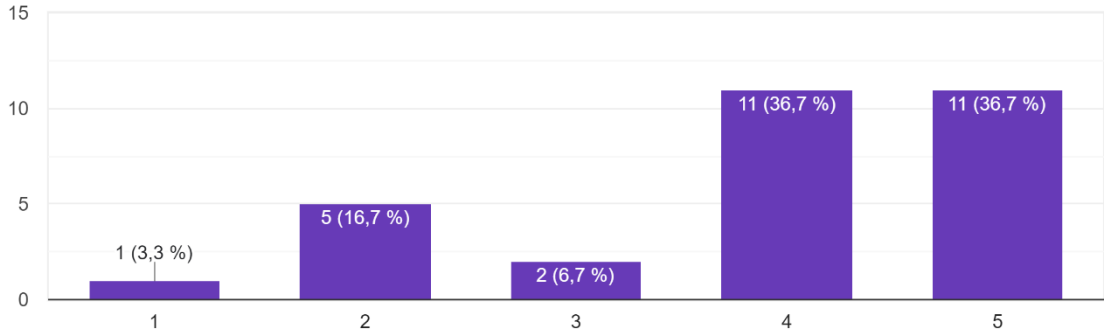
25.- ¿La Entidad ha implementado un plan de tratamiento de riesgos para la seguridad de la información?

30 respuestas



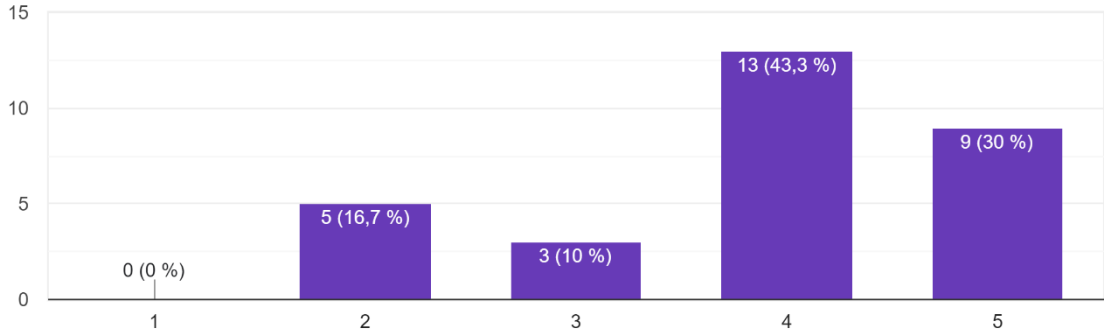
26.- ¿La institución ha puesto en práctica el plan de gestión de riesgos en la seguridad de la información?

30 respuestas



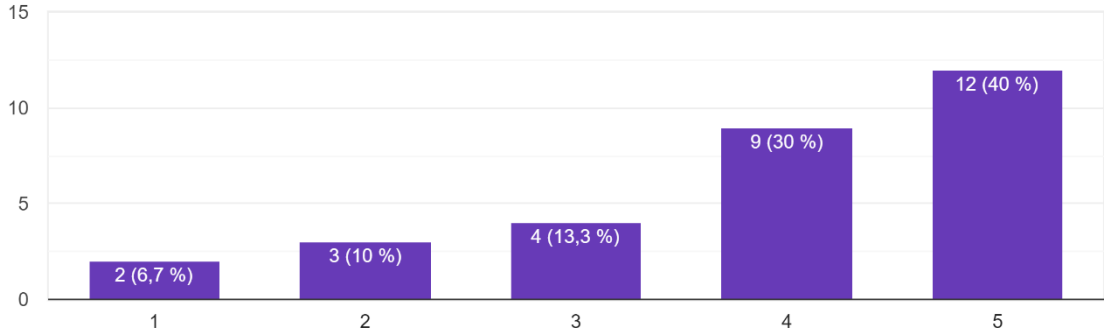
27.- ¿Se han identificado los riesgos que pueden afectar el desarrollo de las actividades diarias?

30 respuestas



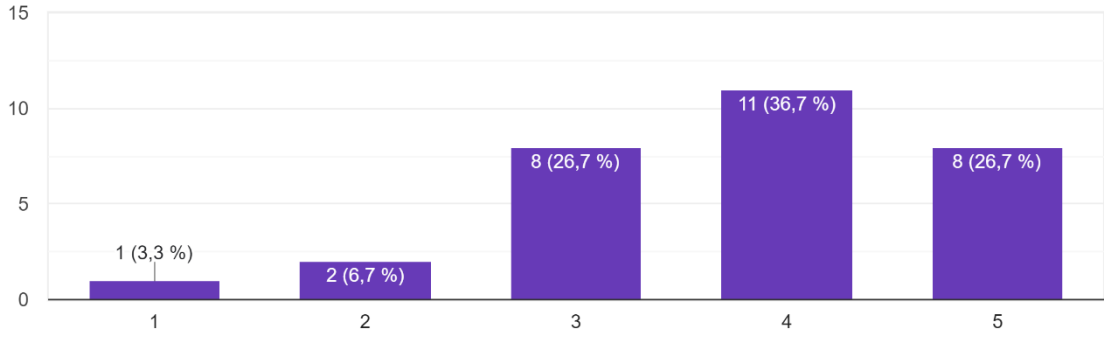
28.- ¿Se ha participado en la identificación de los riesgos a los que está expuesta la información en el área que labora?

30 respuestas



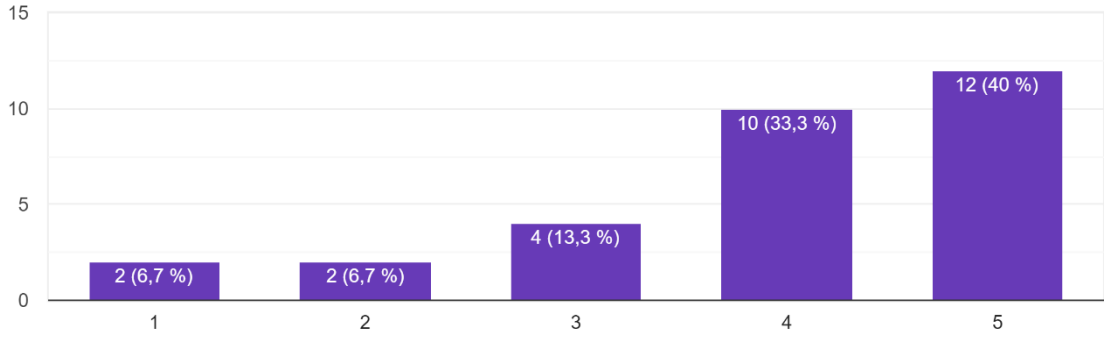
29.- ¿En el desarrollo de sus actividades se ha determinado y cuantificado la posibilidad de que ocurran los riesgos identificados?

30 respuestas



30.- Finalmente ¿Se han establecido las acciones necesarias para afrontar los riesgos evaluados?

30 respuestas



ANEXO 7: Carta de autorización

UNIVERSIDAD CÉSAR VALLEJO

"Año del Fortalecimiento de la Soberanía Nacional"

Lima, 22 de diciembre de 2022
Carta P. 1401-2022-UCV-VA-EPG-F01/J

Lic.
JOSE LUIS ZAVALA CHUMBIAUCA
GERENTE ADMINISTRATIVO
FOREVER LIVING PRODUCTS PERU S.R.L.

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a FLORES CORTEZ, ROBINSON ANDERSON; identificado con DNI N° 43452604 y con código de matrícula N° 6700286571; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

Ciberseguridad para el Proceso de Gestión de Riesgos de TI en una Empresa Transnacional, Lima 2023

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador FLORES CORTEZ, ROBINSON ANDERSON asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dra. Estrella A. Esquiagola Aranda
Jefa
Escuela de Posgrado UCV
Filial Lima Campus Los Olivos

FOREVER LIVING PRODUCTS PERU S.R.L.
JOSE LUIS ZAVALA CH.
REPRESENTANTE LEGAL

ANEXO 8: Constancia de Ingles PG

CENTRO DE IDIOMAS
UNIVERSIDAD CÉSAR VALLEJO

CID- 2021-01-LN-0374

CONSTANCIA

El(la) Coordinador(a) del Centro de Idiomas de la Universidad César Vallejo – Lima Los Olivos

Hace Constar:

Que, el(la) Sr(a). **FLORES CORTEZ, ROBINSON ANDERSON**; estudiante del Programa de **MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN** de la Universidad César Vallejo – Lima Los Olivos; con código N° 6700286571, ha aprobado satisfactoriamente el curso de 192 horas INGLÉS POSTGRADO, obteniendo la nota de 19 (diecinueve)/20, lo que equivale al Nivel A2 del MERC.

Se expide la presente constancia a solicitud de la parte interesada para los fines que estime conveniente.

Lima Los Olivos, 8 de julio de 2021

Atentamente,

CENTRO DE IDIOMAS LIMA NORTE

Dra. Erica De Paz Berrospi
Coordinadora del Centro de Idiomas
Universidad César Vallejo – Lima Los Olivos

ANEXO 9: Aspectos administrativos

Recursos y Presupuesto

Para la siguiente tabla, se detalla el recurso humano ocupado para la realizar el siguiente proyecto de investigación:

Se señala que el recurso humano que se ocupa es el del investigador el cual para fines del proyecto

Tabla 8. Recursos Humanos

Id	Recursos Humanos	Unidades	Tiempo de duración en meses	Coste al Mes	Sub total
2.5.3.1.1.1	Honorario	1	4	3500	14000
				Total	**S/ 14,000.00**

(Fuente: Elaborado por autor)

Recursos tecnológicos, así como materiales que se ocuparan

Para el siguiente cuadro se muestra el recurso tecnológico ocupado para desarrollo y soporte del presente proyecto.:

Tabla 9. Recursos de Hardware

Id	Recursos Tecnologicos	Descripcion	Cantidad	Precio Unit.	Sub total
74.08.0500.0001	Notebook	Intel Core i7 11va Genración Memoria Ram 16GB SSD NVMe 480GB	1	6500	6500
				Total	**S/ 6,500.00**

(Fuente: Elaborado por autor)

Tabla 10. Resumen de presupuesto

Resumen	
Recursos Humanos	14000
Recursos Tecnologicos	6500
Total	**S/ 20,500.00**

(Fuente: Elaborada por autor)

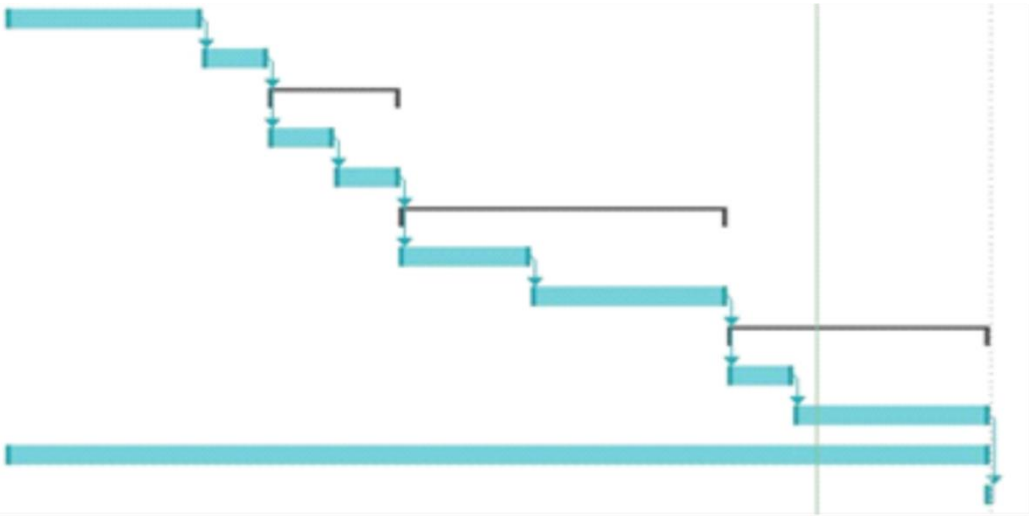
Según resumen del presupuesto tenemos un total de S/20500 Soles (Veinte mil quinientos con 00/100 soles).

Financiamiento

El siguiente proyecto será autofinanciado para fines propios de la investigación, así como el apoyo de parte de la organización en cuanto a facilidades de información y de sus instalaciones para el desarrollo del presente proyecto.

ANEXO 10: Cronograma de ejecución

	Nombre de tarea	Duración
1	Determinación del Problema de Investigación	3 mss
2	Marco Teórico	1 ms
3	Antecedentes	**40 días**
4	Nacionales	1 ms
5	Internacionales	1 ms
6	Aplicación Instrumentos	**100 días**
7	Coordinación	2 mss
8	Recolección de Datos	3 mss
9	Resultados	**80 días**
10	Procesamiento de Datos	1 ms
11	Interpretación de los Datos	3 mss
12	Redaccción del Trabajo de Investigación	15 mss
13	Sustentación de Tesis	1 día



UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, MARLON FRANK ACUÑA BENITES, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Ciberseguridad para el Proceso de Gestión de Riesgos de TI en una Empresa Transnacional, Lima 2023", cuyo autor es FLORES CORTEZ ROBINSON ANDERSON, constato que la investigación tiene un índice de similitud de 18.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 05 de Enero del 2023

Apellidos y Nombres del Asesor:	**Firma**
MARLON FRANK ACUÑA BENITES **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 05-01-2023 14:14:33

Código documento Trilce: TRI - 0510211

INVESTIGA UCV