FACULTAD DE CIENCIAS EMPRESARIALES

## ESCUELA PROFESIONAL DE ADMINISTRACIÓN

# Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:**

**Licenciada en Administración**


**AUTORA:**

Tello Neira, Mary Nardhy (orcid.org/0000-0002-3991-1894)

**ASESOR:**

Dr. Cárdenas Saavedra, Abraham (orcid.org/0000-0002-9808-7719)


**LÍNEA DE INVESTIGACIÓN:**

Gestión de Organizaciones

**LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:**

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2023

## DEDICATORIA

A mi docente el Dr. Cárdenas Saavedra Abraham por brindarme sus conocimientos y apoyo incondicional para el desarrollo de mi investigación.

## AGRADECIMIENTO

Un agradecimiento especial a Dios, por guiarme en mi proceso profesional, a mis padres, hermanos y a mi esposo por ser mi motivación, por confiar y creer en mí, agradecer a la universidad César Vallejo por darme la oportunidad de cumplir mis metas.

## Declaratoria de autenticidad del asesor

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE CIENCIAS EMPRESARIALES
ESCUELA PROFESIONAL DE ADMINISTRACIÓN

### Declaratoria de Autenticidad del Asesor

Yo, CARDENAS SAAVEDRA ABRAHAM, docente de la FACULTAD DE CIENCIAS EMPRESARIALES de la escuela profesional de ADMINISTRACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023", cuyo autor es TELLO NEIRA MARY NARDHY, constato que la investigación tiene un índice de similitud de 16.00%, 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, 22 de Noviembre del 2023

| Apellidos y Nombres del Asesor: | Firma |
|---|---|
| CARDENAS SAAVEDRA ABRAHAM<br>**DNI:** 07424958<br>**ORCID:** 0000-0002-9808-7719 | Firmado electrónicamente por: ACARDENASS el 25-11-2023 17:36:18 |

Código documento Trilce: TRI - 0660304

INVESTIGA UCV

## Declaratoria de originalidad del autor/autores

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE CIENCIAS EMPRESARIALES
ESCUELA PROFESIONAL DE ADMINISTRACIÓN

### Declaratoria de Originalidad del Autor

Yo, TELLO NEIRA MARY NARDHY estudiante de la FACULTAD DE CIENCIAS EMPRESARIALES de la escuela profesional de ADMINISTRACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

| Nombres y Apellidos | Firma |
|---|---|
| MARY NARDHY TELLO NEIRA<br>**DNI:** 72909685<br>**ORCID:** 0000000239911894 | Firmado electrónicamente por: MTELLONE1992 el 22-11-2023 20:12:51 |

Código documento Trilce: TRI - 0660307

INVESTIGA UCV

# ÍNDICE DE CONTENIDOS

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# RESUMEN

Esta indagación tuvo por objetivo determinar la relación entre la seguridad informática y riesgo operacional en una entidad financiera, Los Olivos, 2023. Por lo que se hizo de una metodología que es de tipo aplicada, bajo un enfoque cuantitativo, asimismo es de diseño no experimental transversal descriptivo y de carácter correlacional, tomando como muestra a 50 empleados de la entidad financiera que fue objeto de este estudio. Asimismo, se aplicó como técnica la encuesta y como instrumento de recolección de datos el cuestionario en el cual se establecen 10 preguntas para la variable Seguridad informática y 10 preguntas para la variable Riesgo operacional, trabajándose mediante la escala Likert para la medición del instrumento utilizado. El procesamiento de datos se llevó a cabo mediante el programa estadístico SPSS 26, en el que se obtuvo como resultado de correlación en las variables, bajo el coeficiente de Rho de Spearman, un total de 0,907, estableciendo así una correlación positiva muy alta entre seguridad informática y riesgo operacional, además se obtuvo como resultado de significancia bilateral un valor de 0,000, por lo tanto, se acepta la hipótesis alterna y se rechaza la hipótesis nula. Se concluye que, la seguridad informática debe ser optimizada y mejor monitoreada para prevenir los riesgos operacionales a los que está expuesta la entidad financiera y sus clientes, debido a que la relación entre las variables es muy estrecha, por lo que se deben hacer implementar los procedimientos necesarios y ofrecer una mejor seguridad en las diferentes operaciones ya que, ambas funcionan en conjunto.



**Palabras clave:** Seguridad informática, riesgo operacional, protección de la información

# ABSTRACT

The objective of this research was to determine the relationship between computer security and operational risk in a financial entity, Los Olivos, 2023. Therefore, a methodology that is applied, under a quantitative approach, is also non-design descriptive cross-sectional experimental and correlational in nature, taking as a sample 50 employees of the financial institution that was the object of this study. Likewise, the survey was applied as a technique and the questionnaire as a data collection instrument in which 10 questions are established for the Computer Security variable and 10 questions for the Operational Risk variable, working using the Likert scale for measuring the instrument used. Data processing was carried out using the SPSS 26 statistical program, in which a total of 0.907 was obtained as a result of correlation in the variables, under Spearman's Rho coefficient, thus establishing a very high positive correlation between security IT and operational risk, a value of 0.000 was also obtained as a result of bilateral significance, therefore, the alternative hypothesis is accepted and the null hypothesis is rejected. It is concluded that computer security must be optimized and better monitored to prevent the operational risks to which the financial institution and its clients are exposed, because the relationship between the variables is very close, so the necessary measures must be implemented. necessary procedures and offer better security in the different operations since both works together.



**Keywords:** Computer security, operational risk, information protection

# I. INTRODUCCIÓN

Desde hace unos años, la tecnología al servicio de las organizaciones empresariales ha tenido un crecimiento sin precedentes, esto ha logrado que los pasos dentro de una cadena productiva ganen eficiencia y por lo tanto se generen mayores grados de rentabilidad. Todo esto fue propiciado por la última pandemia que se dio en el 2020, acelerando dichos avances, debido a que no se podían efectuar las operaciones y transacciones comerciales de la manera que hasta entonces se venía haciendo, así como se presentaron estos cambios positivos, también hubo un aumento de delitos informáticos que hasta la fecha ponen en riesgo las operaciones dentro de los comercios, pero, de manera especial la de las entidades financieras (Ponce, 2021).

Estas entidades invierten grandes sumas de dinero en una diversidad de softwares de seguridad informática, con la finalidad de protegerse de ataques masivos en robos de diversos productos financieros que pueden llegar a ofrecer. Ante el riesgo que corren estas operaciones es que se planifica el uso de diversas herramientas para que se cuide el efectivo y sus distintos equivalentes tanto dentro como fuera de las instalaciones financieras, es así que se encuentran en constante exposición a posibles ataques cibernéticos que amenazan la confidencialidad de la información y los activos financieros de sus clientes (Figueroa et al., 2018).

Según el Consejo de la Unión Europea (2022), en sus estados integrantes, se estima que los ciberataques seguirán en aumento porque para el 2025 se prevé que los dispositivos digitales en esa parte del mundo sobrepasen los 41,000 millones. En España, se ha previsto que las entidades financieras serán el blanco preferido de los ciberdelincuentes, por lo que se vienen implementando medidas en seguridad informática, como por ejemplo el Reglamento de Resiliencia Operativa Digital, con el que se busca minimizar el riesgo de las operaciones dentro de las entidades financieras españolas, así como incrementar la seguridad dentro de sus aplicaciones, sobre todo en aquellas de API libre, de esta forma se espera reducir los robos informáticos ante la crecida de usuarios que realizan sus operaciones en línea.

Al entrar en esta era digital, las distintas entidades van implementando más herramientas tecnológicas al servicio de sus clientes, es así que ahora tenemos la banca digital al alcance de nuestro bolsillo con distintas aplicaciones que nos permiten tener nuestra información en cualquier momento, se espera que para el 2027 en Latinoamérica se generen ingresos por 180,000 millones de dólares, lamentablemente esto también es un riesgo ya que un estudio realizado por Akamai (2023) revela que en el riesgo de las operaciones financieras ha aumentado en un 3,5 veces en el 2022 a diferencia del 2021 y esto se da dentro de las plataformas web como en las interfaces de las distintas operaciones, esto ha venido trayendo pérdidas importantes de dinero.

En nuestro país, los esfuerzos por implementar la seguridad informática dentro de las operaciones de las entidades de nuestro sistema financiero son aún deficientes porque, al mes se reportan en promedio 300 denuncias en relación a delitos informáticos, siendo el más común el de fraude informático, esto se debe a que muchas de estas entidades no cumplen con los protocolos de identificación de sus clientes o lo que es peor, no están capacitados para aplicar dichos protocolos. Sumado a ello, se ve que otra de las modalidades más usadas es, la clonación de páginas web, estas son tan idénticas a las verdaderas que inducen al error a los clientes, actualmente eso está poniendo en riesgo las operaciones que se realizan y todo ello ante la falta de filtros de seguridad que serían de gran ayuda si es que fuesen implementados (El Peruano, 2023).

En el distrito de Los Olivos se encuentran alrededor de 14 entidades financieras de banca múltiple, así como una de origen gubernamental, entre las que se realizan las distintas operaciones de los residentes del distrito, la realidad problemática dentro de este distrito se debe a la falta de seguridad informática dentro de las entidades financieras y el riesgo operacional de las transacciones de los clientes crece de manera exponencial, con lo que ven su dinero e inversiones en constante peligro, además dentro de estas entidades la burocracia que se dan en las denuncias hacen que estos delitos tomen demasiado tiempo en solucionarse y en muchos casos se resuelven en contra del cliente.

La entidad financiera que fue objeto del presente estudio, se encuentra en el distrito de Los Olivos y en ella se han detectado algunos casos sobre las inquietudes por parte de los clientes con respecto a sobre si las operaciones que realizan dentro de la entidad son seguras y no tienen ningún riesgo para ellos ya que, actualmente se ven muchos casos sobre robos cibernéticos, fraude interno, fraude externo, suplantaciones es así que, para evaluar la seguridad informática y el riesgo operacional al momento de que los clientes realizan sus operaciones como las transferencias bancarias, compras vía online, prestamos por banca móvil, entre otras, se evidenció las falencias que la entidad tiene, en el cual se vulneró la seguridad de todos los medios de control.

En referencia a lo antes expuesto, se propuso como problema general de esta tesis ¿De qué manera se relaciona la seguridad informática y el riesgo operacional en una institución financiera, Los Olivos, 2023? y los problemas específicos 1. ¿Cómo se relaciona la protección de información con identificación del riesgo en una institución financiera, Los Olivos, 2023? 2., ¿Cómo se relaciona activo financiero con evaluación y priorización en una institución financiera, Los Olivos, 2023? 3. ¿Cómo se relaciona la confidencialidad con la implementación de controles en una institución financiera, Los Olivos, 2023?

La justificación teórica se sustentó porque se usaron diversas investigaciones de donde se obtuvieron datos importantes para así tener más conocimientos sobre las variables seguridad informática y riesgo operacional, con el uso de estas fuentes confiables se reforzará los conocimientos sobre el tema sobre el cual se está investigando, los resultados que se obtuvieron fueron de ayuda para la entidad financiera, con lo que pudo tener conocimiento del problema y así mitigarlo.

Para Bedoya (2020), la justificación teórica son las razones que fundamentan el porqué de un cuestionamiento o la hipótesis de la investigación ya que, su objetivo es invitar a la crítica y debatir partiendo desde los resultados que se encontraron.

Se justificó de manera práctica ya que, los resultados que con los resultados que se obtuvieron se tuvo un mejor panorama sobre la situación de la entidad financiera, asimismo servirá de referencia para otras entidades financieras con problemas similares.

Según Álvarez (2020), es la que se encarga de mostrar la importancia y el valor que tiene una investigación, sobre todo como esta puede ayudar a realizar un cambio dentro del campo que se está estudiando.

En cuanto a la justificación social, se espera que este proceso ayude a que la entidad financiera pueda brindar una mejor atención a sus clientes y así pueda lograr los objetivos que se propone en cuanto a su crecimiento y aportes a la sociedad.

La justificación social, según Arias & Covinos (2021), es la que se encarga de obtener resultados para así ayudar a un conjunto de personas, considerando que los resultados que se encontraron pueden llegar a tener una incidencia positiva para todos aquellos que se encuentran al interior de un grupo de personas

La justificación metodológica de esta investigación, se espera que sirva de antecedente para otras investigaciones que puedan llegar a presentar la misma problemática en referencia a las dos variables que se están estudiando.

Con la justificación metodológica, Reynosa (2018) asegura que, busca asegurar que todos los procedimientos que se han empleado en una investigación resulten bajo una veracidad comprobada y con lo que se puede obtener contestaciones a los cuestionamientos que se plantearon en esta investigación.

En referencia al objetivo general se propuso Determinar la relación entre la seguridad informática y el riesgo operacional en una institución financiera, Los Olivos, 2023.; y los objetivos específicos:1. Determinar que existe relación entre la protección de información e identificación del riesgo en una institución financiera, Los Olivos, 2023. 2., Determinar que existe relación entre el activo financiero y evaluación y priorización en una institución financiera, Los Olivos, 2023.

3.Determinar que existe relación entre la confidencialidad y la implementación de controles en una institución financiera, Los Olivos, 2023.

Para la hipótesis general se planteó lo siguiente: Existe relación entre la seguridad informática y el riesgo operacional en una institución financiera, Los Olivos, 2023 y entre las hipótesis específicas: 1. Existe relación entre la protección de información e identificación del riesgo en una institución financiera, Los Olivos, 2023. 2., Existe relación entre el activo financiero y evaluación y priorización en una institución financiera, Los Olivos, 2023. 3.Existe relación entre la confidencialidad y la implementación de controles en una institución financiera, Los Olivos, 2023.

## II. MARCO TEÓRICO

A fin de contextualizar y fundamentar esta investigación, se realizó en un marco teórico que sintetice los antecedentes locales e internacionales, así como las teorías y definiciones relevantes.

***A continuación, se dio conocimiento a los antecedentes nacionales que tengan coincidencia las variables de esta tesis.***

Ochoa (2019), en su investigación tuvo a bien presentar un diseño de seguridad para la plataforma Web de una empresa que ofrecía servicios a través de medios telefónicos, que venía sufriendo constantes problemas en su seguridad informática y así optimizar sus sistemas de atención. La metodología implementada fue a través de la norma ISO 27033 que es la que busca hacer recomendaciones a implementar ante escenarios de riesgo y que estas puedan ser usadas en el entorno de aquellas empresas que sufran de estas deficiencias. Los resultados determinaron que la propuesta de modelo se podía aplicar a cualquier empresa, siempre y cuando se hicieran los ajustes necesarios para adaptarlo a las necesidades únicas que puede tener cada ente. Se concluyó que, dentro de la empresa este diseño tenía una efectividad de 95.46% en la precisión, asimismo se presentaron los costos en los que la empresa debe incurrir para implementarlo.

Merino (2021), su tesis fue desarrollada con el propósito de gestionar un anteproyecto de seguridad informática usando la ISO/IEC 27001 dentro de una empresa comercial en Piura y así presentar mejoras para la seguridad digital de los datos de sus clientes. La metodología fue cuantitativa, descriptiva y el diseño no experimental y de corte transversal. Se obtuvieron como resultados que, el nivel de satisfacción del sistema resultó con el 60.00% insatisfacción por parte de los colaboradores de la empresa que fueron entrevistados, mientras que el restante se mostraba lo contrario; asimismo el 80.00% de estos trabajadores expresaron la necesidad de contar con un nuevo sistema y el restante dijo que no era necesario. En conclusión, el autor recomendó que la empresa debe buscar

alternativas a fin de realizar mejoras en su seguridad informática y mantener en reserva los datos de sus usuarios.

Zanabria & Cayo (2018), tuvieron por objetivo conocer las deficiencias dentro en los smartphones con sistema nativo Android para así cuidar la información que estos usuarios tienen dentro de estos dispositivos. La metodología que usaron fue realizar una prueba pentesting que sirve para simular posibles peligros y así detectar la respuesta que se tiene ante estos escenarios simulados y ver qué tan perjudicial puede llegar a ser para el usuario. Los resultados que se materializaron permitieron conocer las vulnerabilidades en seguridad que tienen los dispositivos con este sistema operativo en donde se pudo conocer la vulnerabilidad de los datos confidenciales del dueño del dispositivo, exponiéndolo a muchos peligros. Se concluye que, este sistema operativo debe ofrecer mejores filtros de seguridad y cuidar a sus usuarios, además de que se deben implementar evaluaciones para aquellos desarrolladores de nuevas aplicaciones que se registran de la tienda oficial de estos dispositivos, así mismo se recomienda a los usuarios a no guardar datos confidenciales dentro de sus dispositivos, ante el peligro que esto puede generarles.

Córdova & Ruiz (2021), tuvieron por objetivo buscar cómo se relacionaban los riesgos de operación y la cadena de logística de una exportadora de uvas frescas en los años 2016-2020. La metodología fue mixta, correlacional y cuantitativa, además se llevaron a cabo entrevistas a diferentes entidades del rubro exportador. Los resultados estimaron que las dimensiones que conforman la primera variable se encontraban relacionadas con la cadena logística de las empresas exportadoras que estuvieron sujetas a esta investigación. Se concluyó que, los riesgos operacionales deben ser minimizados para que el impacto dentro de la cadena logística sea el mismo.

Merma (2019), se propuso como principal objeto de su indagación, hacer una evaluación para comprobar si existe relación entre riesgo operacional y rentabilidad en una entidad del sistema financiero. La metodología fue realizar una búsqueda de informes en la SBS, siendo esta indagación de carácter básica, no

experimental y longitudinal respectivo. En los resultados se determinó la comprobación de la hipótesis que se planteó, en donde se afirma la relación de las variables, siendo esta significativa.

Sánchez (2020) su propósito fue analizar la seguridad informática en base al ISO 27001 con la finalidad de realizar un trabajo óptimo en la administración de los activos. La metodología fue no experimental, descriptiva, explicativa. En los resultados se encontraron que el total de los encuestados entendían a cabalidad los lineamientos a seguir ante escenarios de riesgo cibernéticos, asimismo manifestaron que el análisis de la seguridad informática es muy necesario ya que, los activos deben estar protegidos. En conclusión, se comprueba que los empleados ven necesario un análisis de los sistemas encargados de salvaguardar los activos.

Nina (2022) su propósito fue proponer mejoras en la gestión de seguridad informática de los GPS aplicando el ISO/IEC 27005:2018. La metodología fue aplicada, no experimental. Los resultados determinaron mejoras considerables en varios de los indicadores al hacer uso de la norma referida. Se concluye que, aplicar el ISO 27005 proporciona un incremento sustancial para gestionar los riesgos que se corren en seguridad informática.

Armas (2020) su propósito fue hacer una evaluación sobre el procedimiento auditor de las actividades que buscan bajar los niveles de riesgo operacional en una entidad financiera. La metodología fue realizar una entrevista, analizar documentación relevante y encuestas. Los resultados hallaron los principales motivos que causan la informalidad de labores. En conclusión, el proceso auditor debe manifestar el manejo de diferentes factores que tienen incidencia en los riesgos operacionales.

Pérez (2018) tuvo como objeto de su indagación, establecer si incidía la administración de TI en los procesos de seguridad informática en un banco del estado. La metodología fue básica, no experimental, transversal, correlacional causal y cuantitativo. Como resultados se encontraron que la administración de TI si tenía repercusión en los procesos de seguridad que implementaba la entidad

financiera. En conclusión, se demostró que la incidencia de la primera variable era de 83.00% dentro de la seguridad informática.

Ancajima (2019) tuvo el propósito de analizar los riesgos que se corrían dentro de una institución educativa con respecto a la seguridad informática. La metodología implementada en el proceso fue cuantitativa, descriptiva, no experimental y de corte transversal. Los resultados expresaron que el 75.00% de los entrevistados expresaron su satisfacción con las TIC dentro del proceso educativo, de la misma forma el 73.00% indicaron su satisfacción sobre la formación y capacitación, siendo el mismo resultado de satisfacción para la seguridad informática. El autor concluyó que, la implementación de políticas dentro de la gestión de la institución será de ayuda para la seguridad informática, estableciendo altos grados de satisfacción dentro de los integrantes que interactúan dentro de la institución educativa, permitiéndoles un fácil manejo de estas TIC.

***A continuación, se dieron a conocer los antecedentes de autores internacionales que tengan a bien coincidir con las variables de esta tesis***

En Ecuador, Bravo & Barrera (2020), orientaron su estudio a analizar la auditoría de la seguridad informática ya que, tenían conocimiento de los inconvenientes de los sistemas de información de algunas entidades. El resultado determinó que los servicios APACHE estaban desactualizados, permitiendo que usuarios ajenos a estas organizaciones tuvieran acceso a la información desde cualquier punto. Ante eso se hizo la propuesta tecnológica con la finalidad de definir los recursos técnicos, operacionales, económicos y legales. Los autores concluyen que, a través de una matriz de aceptación se obtuvo un conocimiento general del problema, así como de las recomendaciones para mejorar la seguridad.

En Panamá, Tejedor et al. (2023) tuvieron como objetivo analizar los diferentes escenarios a los que se entraba la seguridad informática dentro de las casas de enseñanza superior. El método usado se destaca porque fue descriptivo

y documental. Después de realizar una extensa búsqueda de documentos en distintos repositorios se encontraron resultados que determinaron que, los retos se orientan a la manera en que se gestiona esta información, así como la implementación de políticas que sean seguras al momento de usar los medios digitales, asimismo se orientó a que la universidad aplique sistemas de seguridad que satisfagan sus necesidades para lo cual se instó a establecer un gobierno interno que se encargue estas medidas. Se concluyó que, es necesario que se realicen auditorias extensas en los sistemas informáticos dentro de la casa de estudios superior.

En Ecuador, Estrada et al. (2018), buscaron identificar como se mitigan los riesgos en las gestiones de las entidades del sistema financiero. El autor describe su idea e indica que se debía estructurar un mapa de procesos que unifique las operaciones en Cooperativas Segmento 4, para identificar las actividades que se encuentran en riesgo y que subactividades estaban más vulnerables dentro de estas entidades, evaluando distintos factores y eventos dando a conocer cómo impactaban y que tan probable era que ocurriesen. Los resultados determinaron que se debía llevar a cabo la ejecución de medidas que sean fundamentales y tengan como resultado un mejor desempeño dentro del trabajo en grupo. Se llegó a la conclusión que, se debería realizar un monitoreo pertinente con respecto a la administración de los riesgos operacionales para que se pueda conocer lo importante que son y consecuentemente se puedan ejecutar ideas para tenerlas bajo control y en el mejor de los casos desaparecerlas.

En Bolivia, López et al. (2021) tuvieron por propósito conocer cuál era el grado de gestión en los factores de riesgo operacional en las instituciones financieras en Bolivia. Su metodología fue mixta, no experimental, descriptiva y documentaria. Los resultados obtenidos resaltaron que, las COACs si llevaban una gestión adecuada sobre los riesgos en sus operaciones que estaba fundamentada en una resolución gubernamental, ya que se encuentran cimentadas bajo cuatro factores fundamentales. Se determinó como conclusión

que, la administración de riesgos toma como base el documento antes mencionado que fue emitido por las entidades gubernamentales correspondientes.

Enríquez et al. (2022), tuvieron como objetivo primordial, hacer un diagnóstico de los servidores web SQL, XXS Cross Site Script y dar a conocer a que vulnerabilidad estaban expuestas. La metodología fue cualitativa, basándose en una búsqueda documentaria y de campo ya que, se realizó una entrevista a un especialista en estas plataformas web. Los resultados encontrados a través de diferentes pruebas en donde se buscó conocer qué problemas se daban en la seguridad y así se llegó a identificar los riesgos que corrían estas plataformas, asimismo al hacerse una comparación entre las plataformas se alcanzó un 80% para Apache y 30% para Microsoft. Se concluyó que, la técnica que se usó para encontrar tuvo resultados efectivos para organizar y orientar la información sobre el problema de indagación.

Chilan (2021), tuvo como objetivo de estudio hacer una propuesta en medidas de seguridad para así realizar la implementación de un repositorio eficiente de almacenamiento de documentación dentro de una universidad. La metodología fue aplicada y mixta. Se obtuvieron como resultados que los profesores hacían copias de seguridad en CDs, documentos en PC, discos extraíbles y escaneando documentos en un 34%. El autor recomienda en sus conclusiones implementar el sistema que propone para que se lleve una correcta gestión de los documentos en formato electrónico ya que, durante el proceso de investigación se conoció que es necesario realizar esta implementación.

En Colombia, Castilla (2021), tuvo por propósito conocer la influencia del riesgo operacional en las PIFv de las IPS en el servicio farmacéutico de alta complejidad en una ciudad colombiana. La metodología fue observacional, transversal y cuantitativa. Los resultados consolidaron como principales descubrimientos que dentro de las instituciones se llevaban a cabo procedimientos que tenían diferentes impactos ya que, dependía si eran del sector gubernamental o privado. Se determinó como conclusión que, los recursos humanos con los que cuentan los nosocomios eran los principales actores del PIFv, observando que

existía una sobrecarga de labores que pueden ser determinantes dentro del riesgo de las operaciones de estas entidades.

En Colombia, Rodríguez & Rodríguez (2021) en su objetivo buscaron conocer sobre los cambios constantes que tienen incidencia en el riesgo operacional dentro del sector financiero y el periodo en que las cabezas que las dirigen llevaban al mando. Los resultados se destacan las deficiencias en los planes que se ejecutaban dentro del sector, además de verificarse falencias dentro del proceso contable, el lavado de activos, irregularidades en el proceso de reclutamiento de nuevos colaboradores, pero los de mayor impacto fueron los riesgos por fallas dentro de los sistemas informáticos encargados de la seguridad. En conclusión, se determinó que los encargados de dirigir las diferentes empresas del sector tenían una percepción diferente sobre los riesgos encontrados.

En España, Martínez (2019) tuvo como propósito brindar un panorama general claro sobre las deficiencias cibernéticas dentro de las entidades financieras al momento de padecer ataques externos, así como estas entidades las enfrentan. La metodología consistió en realizar el análisis de distintos informes de la entidad a fin de recolectar los datos necesarios. En los resultados se encontraron las distintas formas en que estas empresas han logrado entender los ataques digitales y sobre todo protegerse de estos, para lo cual siguen los lineamientos planificados, que se encuentran sustentados en documentos, sobre cómo actuar en ese tipo de situaciones. Se concluye que, a pesar del conocimiento del riesgo de estos ataques, aún se deben seguir implementando sistemas de seguridad que vayan evolucionando a la par que la tecnología que se encuentra al servicio de las amenazas del exterior.

En Colombia, Diaz et al. (2022) en su objetivo buscaron conocer sobre la situación de la seguridad informática dentro del sector productivo y el conocimiento que se tenía sobre esto dentro de las empresas. En la metodología planteada se ejecutaron acciones pertinentes para el conocimiento integral de la empresa. En los resultados se encontraron distintas amenazas en contra de la seguridad informática del sector estudiado. Concluyeron con realizar

recomendaciones que ayuden a mitigar estas deficiencias sin tener un impacto económico considerable y que con esto puedan mejorar la naturaleza de sus acciones.

***Seguidamente se presentarán las teorías que servirán de sustento para esta tesis y los enfoques conceptuales relevantes.***

Para sustentar esta tesis, se tomó en cuenta el Modelo Biba, que según Saltos Ramírez (2018), es el primer modelo de seguridad dentro del campo de la integridad, este modelo basa su seguridad de acceso en celosías, con la que trata de forma sensible la información en sus distintos niveles. Este modelo resalta en la protección de todo el sistema de información ya que, su idea es ejecutar una estrategia para el flujo de información para lo cual hace uso obligatorio del control de acceso y así reforzarlo de manera discrecional.

Ortiz et al. (2023), se refieren al Modelo Clark Wilson, un modelo que centra su investigación y protección, dentro de los sistemas de informática. En este modelo, el usuario no puede tener acceso y control de los objetos de manera directa; la principal idea de este modelo es, hacer uso de un mecanismo que se encarga de procesar las transacciones que se hacen de manera benigna y ser además un mecanismo que desglose las tareas con lo que se puede garantizar la congruencia de los datos y la veracidad de una transacción. Con este mecanismo de procesamiento de transacciones benignas tiene como significado que, el procesamiento de la información debe ser restringido a solo ciertos privilegios y rangos. Con esto, los usuarios no lograran procesar datos de manera arbitraria.

Para Peña (2022), el Modelo Brewer Nash o también conocido como Gran Muralla China, es un modelo de seguridad que se encarga de proporcionar los controles de acceso a la información y que puede minimizar los intereses en conflicto dentro de las organizaciones y tiene como base el modelo de flujo de información. Su principal virtud, es la confidencialidad, por lo tanto, la información que se encuentra alojada no puede ser leída por personal que es totalmente ajena a la organización y no tiene ninguna función dentro de ella.

En el caso de seguridad informática, para Postigo (2020) son aquellas medidas que se toman para que la protección de datos de empleados y clientes no sea malversada, impidiendo de esta forma que los usuarios no autorizados ejerzan control sobre los sistemas internos y así evitar daños irreversibles dentro de una entidad. Según Castro et al. (2018) estos sistemas son tratados como activos financieros debido a que se encarga de la protección de todos los activos dentro de una entidad financiera, con lo que se minimiza el riesgo de sufrir cualquier robo, además lo califican como un recurso fundamental para que las operaciones se desarrollen con normalidad. Según Bogantes (2020), estos sistemas de seguridad permiten guardar la confidencialidad de todos los datos almacenados, con lo que se asegura que el tratamiento de estos datos solo se use para fines específicos y sin vulnerar la seguridad de las personas que son parte de dicho recurso informático. Entre las dimensiones de esta variable tenemos:

Protección de información, Almaguer et al. (2018) nos dicen que, son acciones que se encargan de proteger la privacidad de los usuarios usando diversas herramientas informáticas con la intención de proteger una información determinada que por lo general se encuentra almacenada dentro de equipos informáticos. Entre sus indicadores tenemos, privacidad, Meraz (2018) sostiene que, se trata del tratamiento que se le da a determinada información y sobre la cual se toman decisiones de ser compartidas o no con terceros, de esta forma se tiene el control de estos datos para ser usados sin malicia; el siguiente indicador es herramientas informáticas, Pita (2018) argumenta que, son los recursos digitales que se encargar de manejar grandes cantidades de datos y son visualizados a través de diferentes dispositivos; el último indicador es base de datos, Hernández et al. (2019), se refirieron a esta como, el almacenamiento de datos que realiza dentro de una organización en donde obtiene información relevante y son debidamente clasificados según el propósito que se tenga al usarlos.

Activo financiero, en concordancia con Cervantes (2020) es un recurso que permite a una entidad financiera el derecho a recibir ingresos futuros y así generar

rentabilidad. Es decir, es un instrumento que otorga beneficios reales al emisor y así se genere la eficiencia de los recursos utilizados. Entre sus indicadores tenemos, rentabilidad, según Santiesteban et al. (2020), la definieron como la capacidad de generar ganancias a partir de una inversión o un negocio. Se mide como el porcentaje de beneficio obtenido en relación al capital invertido o al valor de los activos. La rentabilidad suele estar relacionada positivamente con el riesgo, es decir, a mayor riesgo, mayor rentabilidad potencial y viceversa; otro de sus indicadores es, beneficios, para Figueroa (2019), se trata del resultado positivo que se da entre lo que ingresa y sale de una actividad económica. Los beneficios pueden ser netos o brutos, según se hayan descontado o no los impuestos y otros gastos financieros, estos son una medida del éxito de una empresa o un proyecto y también una fuente de financiación interna y como último indicador tenemos, eficiencia, Urdaneta et al. (2021), se refirieron a ella como, la virtud para lograr un objetivo con el mínimo uso de recursos. Se mide como el cociente entre lo que obtuvo y lo que se utilizó. La eficiencia implica optimizar el proceso productivo, reducir los costes, mejorar la calidad y aumentar la competitividad.

La última dimensión de esta variable es, confidencialidad, según Hernández (2018) la definió como, un principio que garantiza que la información solo puede ser accedida por las personas que tienen autorización, esto se lleva a cabo bajo las políticas y procedimientos que son establecidos por una empresa, entre los que se encuentran un estricto control de contraseñas, para así garantizar la seguridad de la información más sensible. Entre sus indicadores tenemos, políticas y procedimientos, para Heredia (2020), es la seguridad de la información que se lleva a cabo bajo un conjunto de reglas, pautas y normas que establecen cómo se debe gestionar y proteger la información en una organización, mediante estos se establecen las responsabilidades de los usuarios, así como las medidas preventivas y correctivas ante posibles incidentes o amenazas; otro indicador es, control de contraseñas, para Gutiérrez (2022), son las medidas de seguridad que consiste en definir y aplicar criterios para la creación, el uso y el cambio de las contraseñas que permiten el acceso a los sistemas y recursos informáticos, con esto se busca evitar que las contraseñas sean robadas, adivinadas o

comprometidas por terceros no autorizados y por último, seguridad, en referencia a Escalante (2021), es el estado o condición de estar protegido frente a cualquier daño o pérdida, esto implica no violar la seguridad de los usuarios, asimismo se protege la integridad de su información.

En cuanto a la segunda variable, el enfoque de teorías sobre la cual se sustenta esta tesis, según Guerrero et al. (2022) la teoría de valores extremos es usado para analizar y evaluar la probabilidad de riesgo en las operaciones dentro de las entidades financieras, trabajando en base a una serie de eventos que pueden darse de forma aleatoria que pueden ser consideradas de forma singular o como parte de la acción en conjunto ejecutando un proceso defectuoso. De esta manera, se puede cuantificar cómo se distribuyen las pérdidas dentro de las diferentes áreas de una entidad financiera, para esto existen dos métodos que se disgregan de esta teoría, el modelo de bloques máximos y de exceso de umbral, el primero se usa para observaciones grandes y que son distribuidas por igual, en cambio el segundo que, es más actual y poderoso puede hacer observaciones de todo tamaño, incluso de aquellas de nivel superior.

La teoría del riesgo, para Morales (2019), Sharpe estableció un modelo para la valoración de activos financieros (CAPM) que, es una herramienta fundamental dentro del campo de las teorías aplicadas a las entidades financieras, mediante la cual se puede proyectar cuál será la rentabilidad de un activo financiero en consecuencia del riesgo con el que cuenta. A pesar de ser una herramienta que cuenta con limitaciones en su aplicación, sigue siendo tomada en cuenta en la actualidad para conocer cuáles serán los flujos de dinero, tomando en cuenta el riesgo de dicha inversión, por lo tanto, es ideal usarla para la evaluación de activos y tomar decisiones. Esta teoría se basa en otra que fue propuesta por Harry Markowitz que trata la diversificación y la modernización de la teoría de portafolio financiero.

Según Llerena (2022) el Enfoque de Comité de Basilea se encarga de regular las operaciones de las entidades financieras, con el propósito de que estas cuenten con los fondos necesarios para que tengan una respuesta óptima ante

escenarios adversos que lo pueden poner en serios riesgos económicos y financieros y puedan tener una mejor estabilidad ante las amenazas externas que se dan a nivel mundial, esto lo hace a través de diferentes metodologías que buscan medir el riesgo operacional dentro del sector de las finanzas. Se conoce que la implementación de este enfoque se encuentra en crecimiento en todas las entidades del mundo desde 1988, pasando hasta el momento por tres acuerdos, Basilea I, II y III; estos van adecuándose a la realidad del entorno y sus amenazas para que las entidades financieras puedan asegurar la estabilidad de sus operaciones ante las adversidades que puedan enfrentar.

El riesgo operacional, según Gómez et al. (2020) se refirieron a ella como, la que se evidencia de los conflictos de interés entre los empleados y los jefes de cada una de las áreas en una empresa. Los primeros pueden actuar de forma oportunista o negligente, causando pérdidas o daños a la empresa, para reducir este riesgo, se requiere un adecuado sistema de incentivos, supervisión y control. Para Sahun (2019), es riesgo que se tiene como resultado de la interacción dinámica y no lineal de los diversos elementos que conforman una empresa, estos elementos pueden generar comportamientos emergentes e impredecibles, que pueden afectar negativamente el desempeño de la empresa, para gestionar el riesgo operacional, se necesita una visión sistémica y adaptativa. Como dicen Estrada et al. (2018), Se origina por la incapacidad de una organización para aprender de sus errores y mejorar sus prácticas, estos errores pueden ser causados por factores internos (falta de conocimiento, habilidades, motivación, etc.) o externos (cambios en el entorno, competencia, regulación, etc.), si es que se quiere minimizar el riesgo operacional, se requiere una cultura de aprendizaje continuo y una gestión del conocimiento efectiva.

Entre sus dimensiones tenemos, identificación del riesgo, según De Berrio (2019), es un escenario adverso que afecta el funcionamiento normal de una organización, como puede ser un ciberataque, originando que lo controles de seguridad sean perjudicas y se tengan pérdidas económicas, ante eso es importante capacitar al personal para que tenga conocimiento de cómo actuar en

esos casos. Entre sus indicadores tenemos, ciberataque, para Cano (2020), son los actos que fueron planificados para así evitar grandes daños dentro de los sistemas de informática o perder de manera accidental información sensible, estos son motivados por diferentes factores, como el crimen, la protesta, el espionaje, el ciberterrorismo o la ciberguerra; el siguiente indicador es, controles, como menciona Urdanegui (2018), son las medidas que se implementan para prevenir, detectar o mitigar los riesgos en las operaciones y los ciberataques, tienden a ser de tipo técnico, administrativo o físico; por último tenemos, capacitación del personal, en conocimiento de Navarrete (2018), es el proceso de enseñar y entrenar a los empleados y colaboradores de una organización para que adquieran las herramientas que los ayudarán a desempeñar sus funciones de manera eficiente y segura, este factor es fundamental para reducir el riesgo en las operaciones y los ciberataques, ya que permite mejorar el rendimiento, la calidad, la innovación y la cultura de seguridad.

La segunda dimensión es, evaluación y priorización, según Mendoza & Vega (2019), se trata del proceso de identificar, analizar y clasificar los riesgos según su importancia y urgencia, para estimar la probabilidad de ocurrencias de un fraude y el impacto de los riesgos, mientras que la priorización implica asignar recursos y acciones para mitigarlos, el desarrollo de esta actividad es un factor clave para la gestión de proyectos, la auditoría interna y la prevención de fraudes. Entre sus indicadores tenemos, probabilidad de ocurrencia de un fraude, Escorcia et al. (2021) la definieron como, la medida de la posibilidad de que se produzca un hecho delincuencia que se caracteriza principalmente por el exceso de confianza; el siguiente indicador es, fraude, De La Torre & Quiroz (2020) propusieron que, la consecuencia del mal actuar de ciertos individuos es busca de obtener un beneficio a costa de dañar a otra persona; por último se tiene a uso inteligente de buscadores de internet, para Toudert (2019), es el uso de los recursos disponibles en la web para encontrar, evaluar y usar información relevante, confiable y actualizada, esto implica conocer las características y funciones de los diferentes buscadores, aplicar técnicas y estrategias de búsqueda efectivas, seleccionar las fuentes más apropiadas según el propósito y el contexto.

Por último, tenemos a la dimensión, implementación de controles, para Serrano (2018) es el proceso de detección y mitigación de los problemas que en ocasiones afectan el funcionamiento y los objetivos de una organización con el uso de sistemas confiables, con esto se garantiza tener un registro de acceso de todos los usuarios con la finalidad de monitorearlos continuamente. Entre sus indicadores tenemos, sistema confiable, en definición de Poma & Vargas (2019), es el que cumple con características la autenticidad de los datos y los recursos que gestiona, por lo tanto, es capaz de resistir y recuperarse de posibles amenazas, como errores, logrando minimizar el impacto negativo en sus usuarios y en la organización; el siguiente indicador es, registro de acceso, para El Maadioui El Issaties (2023), es el conjunto de datos que almacena y documenta las actividades de entrada y salida de los usuarios a un sistema o a un lugar, lo que permite llevar un control y una trazabilidad de quién, cuándo, cómo y desde dónde accede a la información o a los recursos y finalmente tenemos, monitoreo continuo, en concordancia de Álvarez et al. (2020), es el proceso de observar y evaluar periódicamente el desempeño y el estado de un sistema o de una actividad y permite identificar oportunamente las desviaciones, los problemas o las mejoras posibles, así como tomar las acciones correctivas o preventivas necesarias.

# III. METODOLOGÍA

## 3.1 Tipo y diseño de investigación

### Tipo de Investigación

Fue de tipo aplicada, descriptiva, bajo un enfoque cuantitativo porque se fundamentó en una escala numerada con la finalidad de encontrar las referencias necesarias en base los fenómenos que se estaban estudiando (Hernández y Mendoza, 2018)

### Diseño de investigación

Fue no experimental de corte transversal y correlacional, en donde se buscaba una correlación entre seguridad informática y riesgo operacional. Para Ríos (2017) la finalidad de este diseño de indagación es establecer una correlación entre ambas variables y ver si llega a ser significativa.

## 3.2. Variable y operacionalización

### Variable 1: Seguridad informática

### Definición conceptual:

Para Postigo (2020) son aquellas medidas que se toman para que la protección de datos de empleados y clientes no sea malversada, impidiendo de esta forma que los usuarios no autorizados ejerzan control sobre los sistemas internos y así evitar daños irreversibles dentro de una entidad. Según Castro et al. (2018) estos sistemas son tratados como activos financieros debido a que se encarga de la protección de todos los activos dentro de una entidad financiera, con lo que se minimiza el riesgo de sufrir cualquier robo, además lo califican como un recurso fundamental para que las operaciones se desarrollen con normalidad. Según Bogantes (2020), estos sistemas de seguridad permiten guardar la confidencialidad de todos los datos almacenados, con lo que se asegura que el tratamiento de estos datos solo se use para fines específicos y sin vulnerar la seguridad de las personas que son parte de dicho recurso informático.

**Definición operacional:**

Se midió la variable “Seguridad informática” con el instrumento del cuestionario, contando con las dimensiones protección de información, activo financiero, confidencialidad.

**Variable 2: Riesgo operacional**

**Definición conceptual:**

Gómez et al. (2020) se refirieron a ella como, la que se evidencia de los conflictos de interés entre los empleados y los jefes de cada una de las áreas en una empresa. Los primeros pueden actuar de forma oportunista o negligente, causando pérdidas o daños a la empresa, para reducir este riesgo, se requiere un adecuado sistema de incentivos, supervisión y control. Para Sahun (2019), es riesgo que se tiene como resultado de la interacción dinámica y no lineal de los diversos elementos que conforman una empresa, estos elementos pueden generar comportamientos emergentes e impredecibles, que pueden afectar negativamente el desempeño de la empresa, para gestionar el riesgo operacional, se necesita una visión sistémica y adaptativa. Como dicen Estrada et al. (2018), se origina por la incapacidad de una organización para aprender de sus errores y mejorar sus prácticas, estos errores pueden ser causados por factores internos (falta de conocimiento, habilidades, motivación, etc.) o externos (cambios en el entorno, competencia, regulación, etc.), si es que se quiere minimizar el riesgo operacional, se requiere una cultura de aprendizaje continuo y una gestión del conocimiento efectiva.

**Definición operacional:**

Se midió la variable “Riesgo operacional” con el instrumento del cuestionario, contando con las dimensiones Identificación del riesgo, evaluación y priorización e implementación de controles.

### 3.3. Población

**Población:**

Fue censal y fueron 50 sujetos, para Ventura (2018) se encuentra delimitada a una cierta cantidad de componentes en el cual se busca estudiar alguna característica en particular. La investigación estuvo integrada por los usuarios de una entidad financiera, para lo cual se tomó en cuenta a aquellos que con más frecuencia visitaban la financiera.

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

Fue la encuesta, con la que se buscó realizar la recopilación de información de las variables según la información que nos proporcionaron las personas que fueron objeto de este estudio. Según Arias (2020), se usa para de manera amplia en el campo de la investigación científica a fin de recolectar información sobre un evento o hecho de vital importancia, además de que los sujetos en estudio sienten comodidad al realizarlas y ante ese hecho se recomienda su uso en investigaciones cuantitativas o cualitativas.

**Instrumento:**

Fue el cuestionario, con el que se buscó medir la seguridad informática y riesgo operacional, esta fue aplicada a 50 colaboradores de una entidad financiera en Los Olivos. El instrumento estuvo conformado por 20 ítems, que se encuentran distribuidos en 6 dimensiones. Para Martínez (2022), este instrumento se encuentra preparado para realizar la medición de las variables que son objeto dentro de una investigación con el cual se busca dar respuesta a los objetivos y problemas esenciales que se están investigando.

### 3.5. Procedimiento

Autorización:

En la ejecución de este procedimiento de investigación, contamos con las autorizaciones de los subordinados de la entidad financiera, además se les hizo de pleno conocimiento cuál fue la motivación para llevar a cabo este estudio y darles

a entender la forma en que se ejecutaría cada paso en dónde tuviesen intervención directa.

**Aplicación del instrumento de recolección de datos:**

A cada uno de los entrevistados, se dio las aclaraciones necesarias en base a los fundamentos de nuestro proceder científico, así como también sobre el campo donde se usarán todos los datos que se obtengan, de igual forma se le dio la tranquilidad de que sus datos personales no serían expuesto ya que, es un estudio que los mantendrá en el anonimato. El tiempo promedio, para que cada colaborador brinde sus respuestas fue de 5 a 6 minutos y al concluir con sus respuestas se les agradeció por su colaboración.

### 3.6. Métodos de análisis de datos

Una vez terminada la toma de datos, se ingresaron estos a una hoja de Excel con el cuidado de no modificar ninguna de las respuestas, después se materializó la información al interior del paquete de estadística SPSS V.26. Con el propósito de tener conocimiento de la confiabilidad del instrumento, se procedió a utilizar el Alfa de Cronbach en las variables estudiadas, seguidamente se ejecutó la estadística descriptiva para lo cual se usaron tablas de frecuencia y gráficos de barra para tener un conocimiento porcentual de los resultados, finalmente para obtener los datos en la estadística inferencial, se usó el coeficiente Rho de Spearman para la contrastación de las hipótesis.

### 3.7. Aspectos éticos

En concordancia de Gagñay et al. (2020) hacen referencia que, mediante la ética dentro de una investigación, se busca garantizar la integridad, confianza y responsabilidad de los resultados que se obtienen dentro del proceso, con lo que buscan cumplir con los estándares necesarios en favor de la protección de los participantes.

Los aspectos éticos de este procedimiento sólo pretenden que los datos proporcionados por los encuestados solo sirvan para debatir académicamente, además de asegurar la identidad de los colaboradores al asegurar que este

estudio es anónimo, por lo tanto, sus datos se encuentran bajo estricta confidencialidad. Además, se buscó dar cumplimiento a los requisitos de la universidad, que se están reflejados en la RVI N.º 062-2023-VI-UCV.

# IV. RESULTADOS

## Estadística Descriptiva

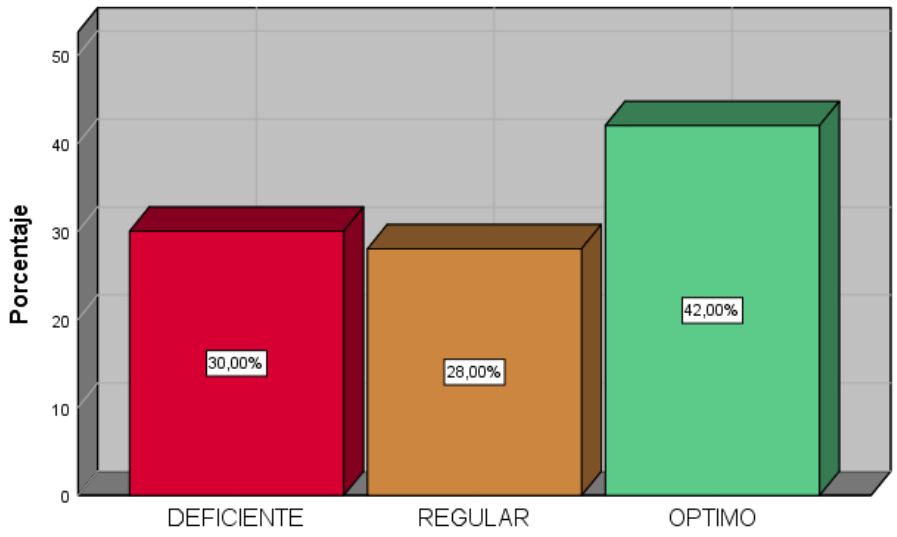
**Tabla 1**

*Niveles de Seguridad informática*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | DEFICIENTE | 15 | 30,0 | 30,0 | 30,0 |
| | REGULAR | 14 | 28,0 | 28,0 | 58,0 |
| | OPTIMO | 21 | 42,0 | 42,0 | 100,0 |
| | Total | 50 | 100,0 | 100,0 | |

**Figura 1**

*Porcentaje de Seguridad informática*




En la Tabla 1 y figura 1, de un total del 100% de encuestados, el 42% señalaron que el nivel de seguridad informática es óptimo, el 30% indicó que el nivel es deficiente y el 28% sostuvieron que el nivel es regular.

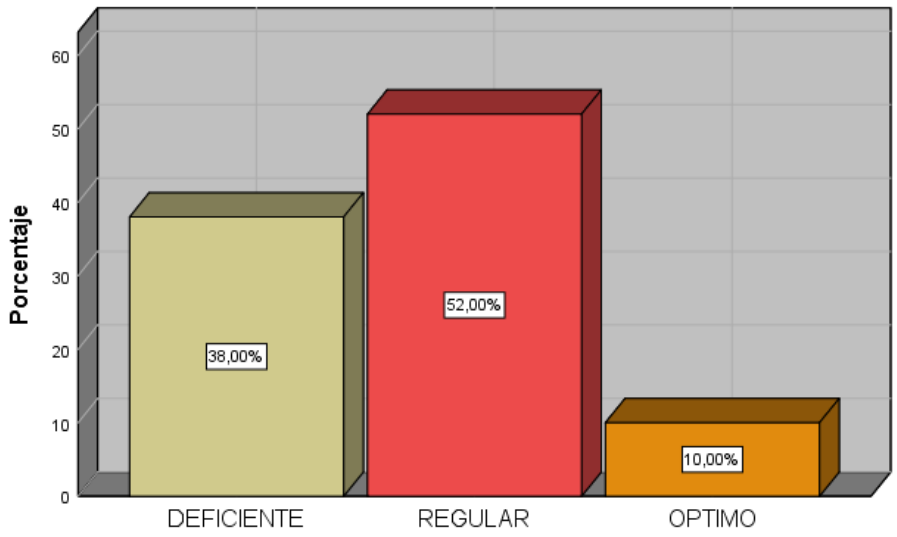
**Tabla 2**

*Niveles de protección de información*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | DEFICIENTE | 19 | 38,0 | 38,0 | 38,0 |
| | REGULAR | 26 | 52,0 | 52,0 | 90,0 |
| | OPTIMO | 5 | 10,0 | 10,0 | 100,0 |
| | Total | 50 | 100,0 | 100,0 | |

**Figura 2**

*Porcentaje de protección de información*




Según a la Tabla 2 y figura 2, de un total del 100% de personas encuestadas, el 52% mencionaron que el nivel de Protección de información es regular, el 38% revelaron que es deficiente y solo el 10% refirió que es óptimo.

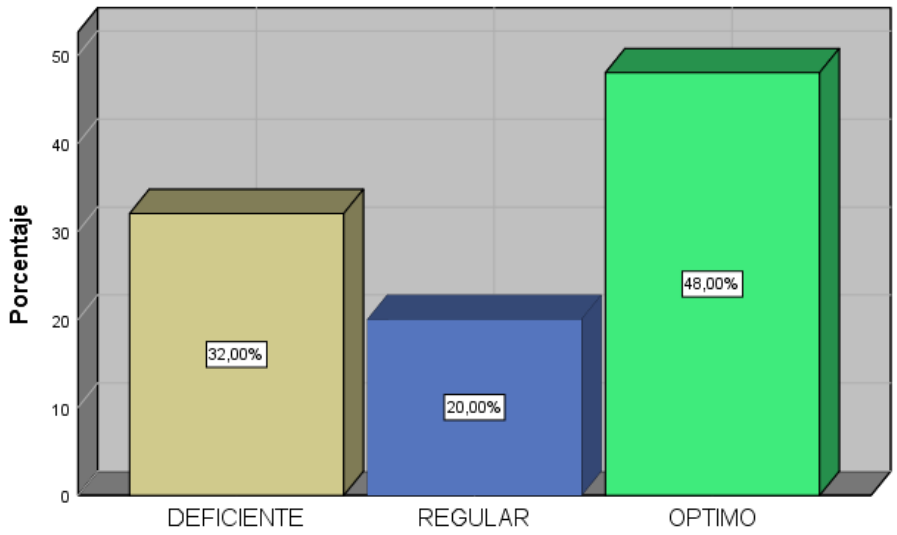
**Tabla 3**

*Niveles de activo financiero*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | DEFICIENTE | 16 | 32,0 | 32,0 | 32,0 |
| | REGULAR | 10 | 20,0 | 20,0 | 52,0 |
| | OPTIMO | 24 | 48,0 | 48,0 | 100,0 |
| | Total | 50 | 100,0 | 100,0 | |

**Figura 3**

*Niveles de activo financiero*




En vista de la Tabla 3 y figura 3, de un total del 100% de personas encuestadas, el 48% mencionaron que el nivel de Activo financiero es óptimo, el 32% sostuvo que es deficiente y el 20% refirió que el nivel es regular.

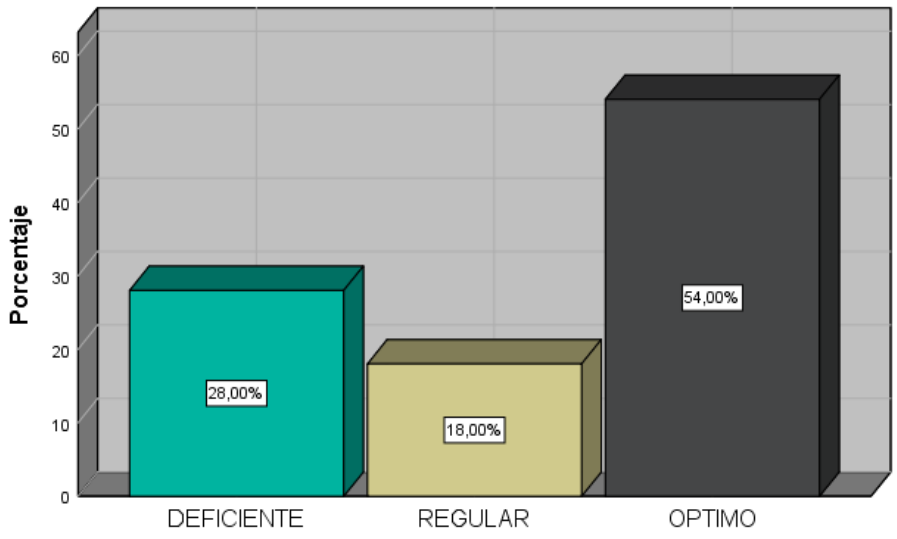
**Tabla 4**

*Niveles de confidencialidad*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | DEFICIENTE | 14 | 28,0 | 28,0 | 28,0 |
| | REGULAR | 9 | 18,0 | 18,0 | 46,0 |
| | OPTIMO | 27 | 54,0 | 54,0 | 100,0 |
| | Total | 50 | 100,0 | 100,0 | |

**Figura 4**

*Porcentaje de confidencialidad*




Respecto a la Tabla 4 y figura 4, de un total del 100% de personas encuestadas, el 54% mencionaron que el nivel de Confidencialidad es óptimo, el 28% refirió que es deficiente y el 18% manifestaron que el nivel es regular.

**Tabla de frecuencia agrupada de la variable Riesgo operacional**

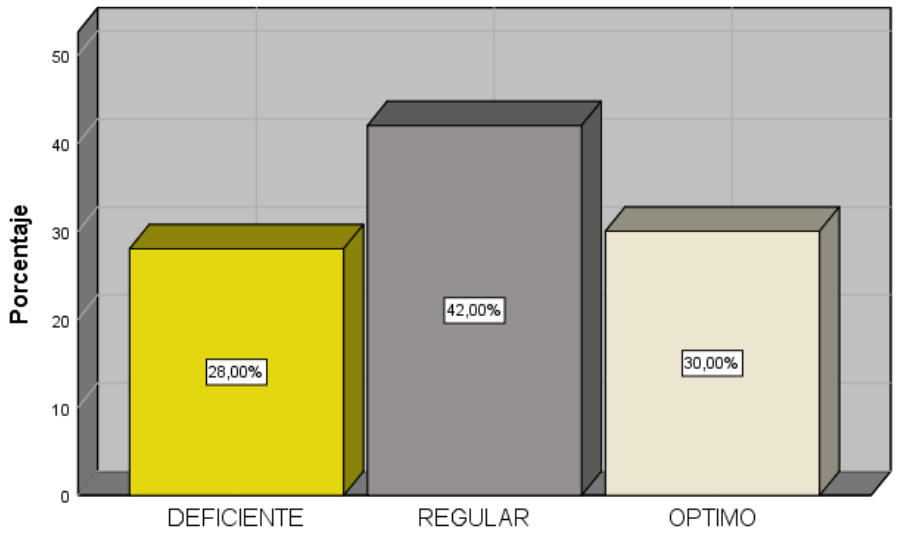
**Tabla 5**

*Niveles de Riesgo operacional*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | DEFICIENTE | 14 | 28,0 | 28,0 | 28,0 |
| | REGULAR | 21 | 42,0 | 42,0 | 70,0 |
| | OPTIMO | 15 | 30,0 | 30,0 | 100,0 |
| | Total | 50 | 100,0 | 100,0 | |

**Figura 5**

*Porcentaje de Riesgo operacional*




Se observa en la Tabla 5 y figura 5, de un total del 100% de personas encuestadas, el 42% mencionaron que el nivel de Riesgo operacional es regular, el 30% señalaron que es óptimo y el 28% sostuvo que es deficiente.

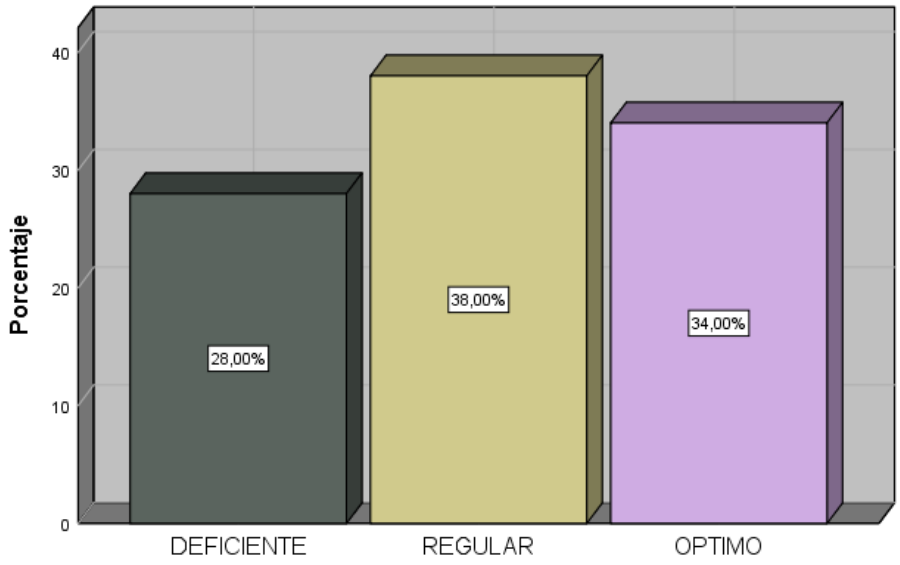
**Tabla 6**

*Niveles de Identificación del riesgo*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | DEFICIENTE | 14 | 28,0 | 28,0 | 28,0 |
| | REGULAR | 19 | 38,0 | 38,0 | 66,0 |
| | OPTIMO | 17 | 34,0 | 34,0 | 100,0 |
| | Total | 50 | 100,0 | 100,0 | |

**Figura 6**

*Porcentaje de Identificación del riesgo*




En referencia a la Tabla 6 y figura 6, de un total del 100% de personas encuestadas, el 38% mencionaron que el nivel de Identificación de riesgo es regular, el 34% que es óptimo y el 28% sostuvo que es deficiente.

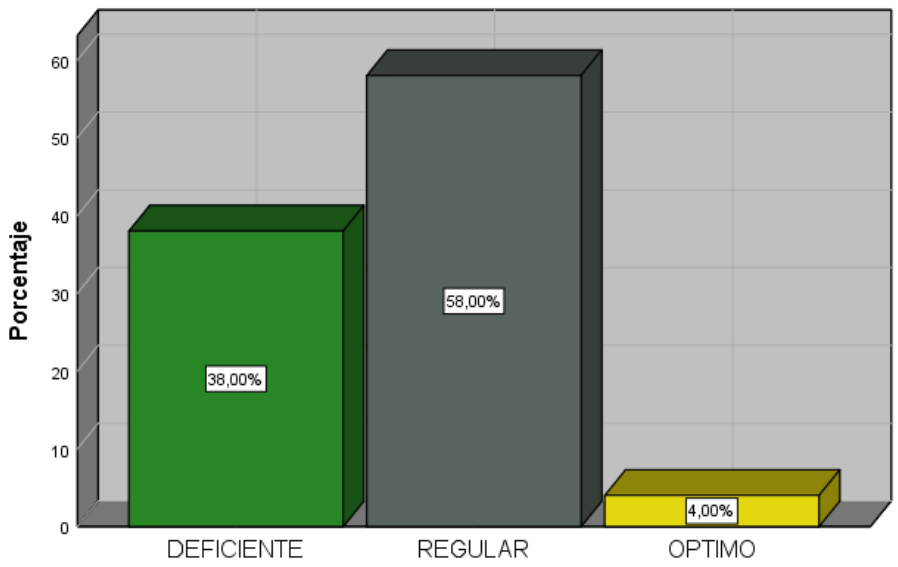
**Tabla 7**

*Niveles de evaluación y priorización*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | DEFICIENTE | 19 | 38,0 | 38,0 | 38,0 |
| | REGULAR | 29 | 58,0 | 58,0 | 96,0 |
| | OPTIMO | 2 | 4,0 | 4,0 | 100,0 |
| | Total | 50 | 100,0 | 100,0 | |

**Figura 7**

*Porcentaje de evaluación y priorización*




En observancia de la Tabla 7 y figura 7, de un total del 100% de personas encuestadas, el 58% mencionó que el nivel de Evaluación y priorización es regular, el 38% sostuvo que es deficiente y solo el 4% mencionaron que es óptimo.

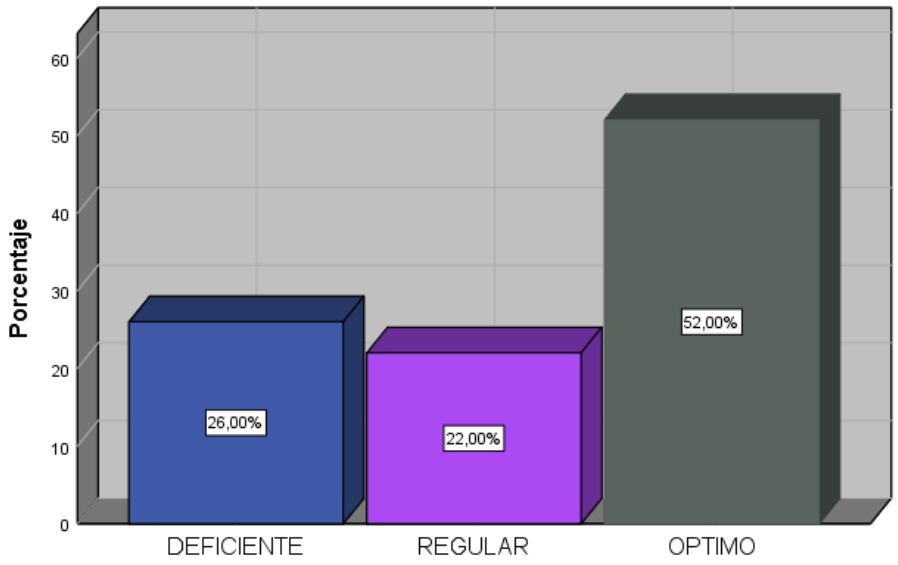
**Tabla 8**

*Niveles de implementación de controles*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | DEFICIENTE | 13 | 26,0 | 26,0 | 26,0 |
| | REGULAR | 11 | 22,0 | 22,0 | 48,0 |
| | OPTIMO | 26 | 52,0 | 52,0 | 100,0 |
| | Total | 50 | 100,0 | 100,0 | |

**Figura 8**

*Porcentaje de la dimensión implementación de controles*




En consecuencia de la Tabla 8 y figura 8, de un total del 100% de personas encuestadas, el 52% mencionaron que el nivel de Implementación de controles es óptimo, el 26% indicaron que es deficiente y el 22% refirió que es regular.

## 4.2 Estadística Inferencial

### 4.2.1 Prueba de normalidad de la muestra

| Shapiro - Wilk | Kolmorov - Smirnov |
|---|---|
| **n<=50** | **n>50** |

**Planteamiento de hipótesis**

Ho: La distribución de la muestra es normal

Ha: La distribución de la muestra no es normal

**Nivel de confianza**

Confianza: 95%

Significancia (alfa(α): 5%,

**Criterio de decisión**

Si p < 0,05 rechazamos Ho y acepto la Ha

Si p >= 0,05 aceptamos la Ho y rechazamos la Ha

**Tabla 9**

*Prueba de normalidad de la muestra*

| Pruebas de normalidad | | | |
|---|---|---|---|
| | Shapiro-Wilk | | |
| | Estadístico | gl | Sig. |
| SEGURIDAD INFORMATICA | ,863 | 50 | ,000 |
| RIESGO OPERACIONAL | ,912 | 50 | ,001 |

**Gráfico 9**

*Histograma Seguridad informática*

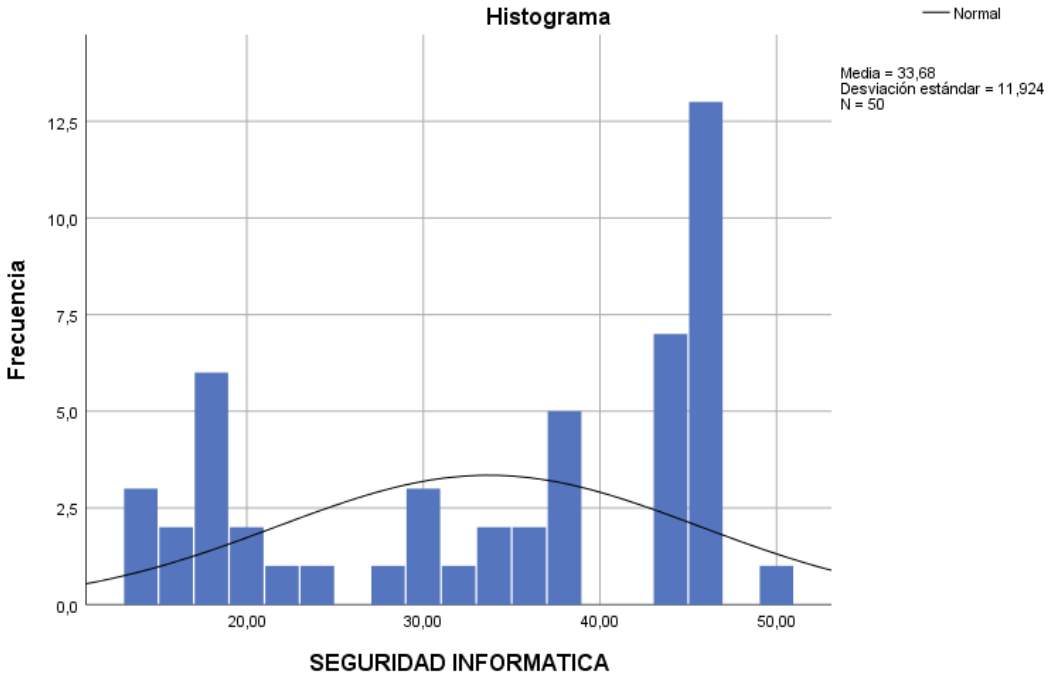
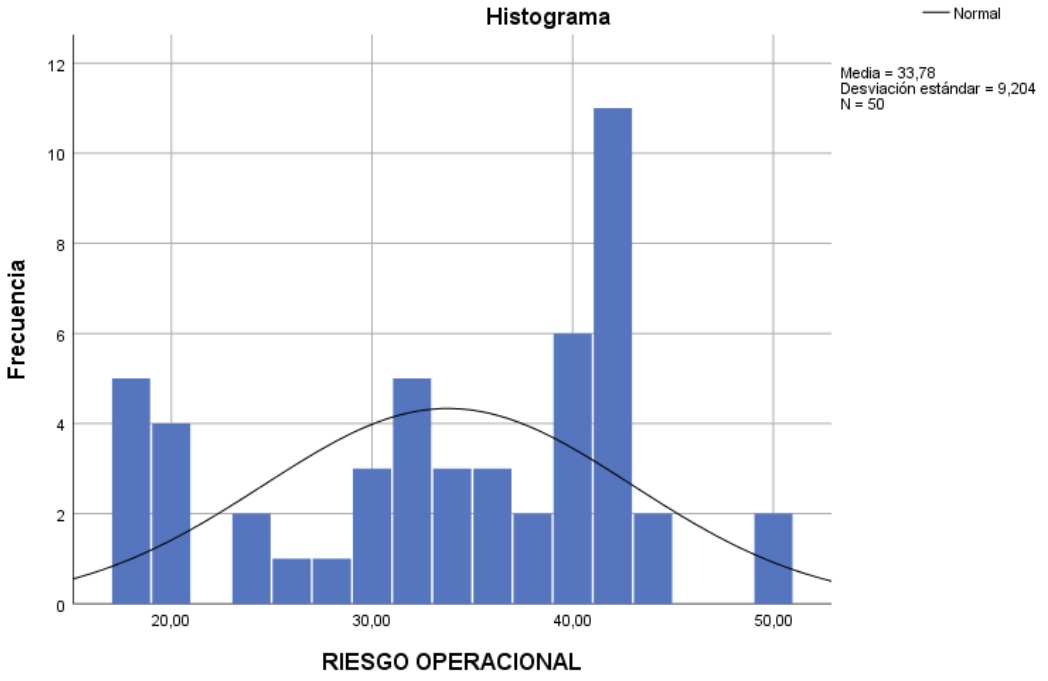



**Gráfico 10**

*Histograma Riesgo operacional*



Según los datos de Shapiro – Wilk se obtuvo un p=0.000 < 0.05; para la variable seguridad informática y p= 0.001 < 0.005 para la variable riesgo operacional. Por lo tanto, se rechaza la Ha y se acepta la Ho, la información referente a la muestra de esta investigación evidencia una distribución normal. En conclusión, para la validar las diferentes hipótesis se utilizó el estadístico no paramétrico. (Rho de Spearman)

### 4.2.2 Regla de decisión para la validación de hipótesis

**Regla de decisión**

Si el valor de sig (Bilateral) es < 0,05, la correlación es significativa

Si el valor de sig (Bilateral) es > 0,05, la correlación no es significativa

**Nivel de confianza**

Confianza: 95%

Significancia (alfa(α): 5%,

**Criterio de decisión**

Si p < (menor) 0,05 rechazamos Ho y acepto la Ha

Si p >= (mayor o igual) 0,05 aceptamos la Ho y rechazamos la Ha

### 4.2.3 Prueba de Hipótesis

**Hipótesis General**

**H0:** Seguridad informática y riesgo operacional no se relacionan significativamente en una entidad financiera en Los Olivos, 2023.

**Ha:** Seguridad informática y riesgo operacional se relacionan significativamente en una entidad financiera en Los Olivos, 2023.

**Tabla 11**

*Correlación de Seguridad informática y riesgo operacional*

| | | | SEGURIDAD INFORMÁTICA | RIESGO OPERACIONAL |
|---|---|---|---|---|
| Rho de Spearman | SEGURIDAD INFORMÁTICA | Coeficiente de correlación | 1,000 | ,907** |
| | | Sig. (bilateral) | . | ,000 |
| | | N | 50 | 50 |
| | RIESGO OPERACIONAL | Coeficiente de correlación | ,907** | 1,000 |
| | | Sig. (bilateral) | ,000 | . |
| | | N | 50 | 50 |

Según los datos de la tabla 11, la correlación hallada fue de (0.907), correlación positiva, además es significativa (Sig. = 0.000 < alfa = 0.05). Por consiguiente, se acepta Ha y se rechaza la Ho. En definitiva, existe una correlación significativa entre las variables seguridad informática y riesgo operacional.

**Hipótesis específica 1:**

**H0:** La relación de protección de información con identificación de riesgo no es significativamente positiva.

**Ha:** La relación de protección de información con identificación de riesgo es significativamente positiva.

**Tabla 12**

*Correlación protección de información con Identificación de riesgo*

| | | | PROTECCION DE INFORMACION | IDENTIFICACIÓN DE RIESGO |
|---|---|---|---|---|
| Rho de Spearman | PROTECCION DE INFORMACION | Coeficiente de correlación | 1,000 | ,830** |
| | | Sig. (bilateral) | . | ,000 |
| | | N | 50 | 50 |
| | IDENTIFICACIÓN DE RIESGO | Coeficiente de correlación | ,830** | 1,000 |
| | | Sig. (bilateral) | ,000 | . |
| | | N | 50 | 50 |

En la tabla 12, el coeficiente de correlación de las dimensiones estudiadas es de (0.830), correlación positiva alta entre ellas, además es significativa (Sig. = 0.000 < alfa = 0.05). Por lo tanto, se acepta la Ha y se rechaza la Ho. Se llegó a la conclusión que, existe correlación significativa entre las dimensiones activo financiero y evaluación y priorización.

**Hipótesis específica 2:**

**H0:** La relación de activo financiero y evaluación y priorización no es significativamente positiva.

**Ha:** La relación de activo financiero y evaluación y priorización es significativamente positiva.

**Tabla 13**

*Correlación de activo financiero con evaluación y priorización*

| | | | ACTIVO FINANCIERO | EVALUACIÓN Y PRIORIZACION |
|---|---|---|---|---|
| Rho de Spearman | ACTIVO FINANCIERO | Coeficiente de correlación | 1,000 | ,615** |
| | | Sig. (bilateral) | . | ,000 |
| | | N | 50 | 50 |
| | EVALUACIÓN Y PRIORIZACION | Coeficiente de correlación | ,615** | 1,000 |
| | | Sig. (bilateral) | ,000 | . |
| | | N | 50 | 50 |

En la tabla 13, el coeficiente de correlación de las dimensiones estudiadas es de (0.615), correlación positiva moderada entre ellas, además es significativa (Sig. = 0.000 < alfa = 0.05). Por lo tanto, se acepta la Ha y se rechaza la Ho. Se llegó a la conclusión que, existe correlación significativa entre las dimensiones activo financiero y evaluación y priorización.

**Hipótesis específica 3:**

**H0:** La relación de confidencialidad e implementación de controles no es significativamente positiva.

**Ha:** La relación de confidencialidad e implementación de controles es significativamente positiva.

**Tabla 14**

*Correlación de confidencialidad con implementación de controles*

| | | | CONFIDENCIALIDAD | IMPLEMENTACION DE CONTROLES |
|---|---|---|---|---|
| Rho de Spearman | CONFIDENCIALIDAD | Coeficiente de correlación | 1,000 | ,912** |
| | | Sig. (bilateral) | . | ,000 |
| | | N | 50 | 50 |
| | IMPLEMENTACION DE CONTROLES | Coeficiente de correlación | ,912** | 1,000 |
| | | Sig. (bilateral) | ,000 | . |
| | | N | 50 | 50 |

En la tabla 14, el coeficiente de correlación de las dimensiones estudiadas es de (0.912), correlación positiva muy alta entre ellas, además es significativa (Sig. = 0.000 < alfa = 0.05). Por lo tanto, se acepta la Ha y se rechaza la Ho. Se llegó a la conclusión que, existe correlación significativa entre las dimensiones activo financiero y evaluación y priorización.

.

## V. DISCUSIÓN

En vista del primer objetivo específico, en el cual se usó el coeficiente Rho de Spearman, el cual estableció una correlación positiva alta entre las dimensiones protección de información e identificación de riesgos con un r = 0,830, por lo tanto, se evidencia una relación entre ambas actividades dentro de una institución financiera. Estos resultados fueron comparados con la investigación de Ochoa (2019) el cual tuvo a bien realizar la implementación de una red de seguridad informativa que permita identificar los riesgos dentro de un Call Center ya que, se evidenciaron problemas informáticos que tenían impacto directo dentro de los sistemas de información, haciendo que la protección de información se vea perjudicada ante una nula identificación de riesgos dentro de la empresa, por lo que al implementar dicho plan se evidenciaron mejorar en el control de riesgo ya que, se mejoró la protección informática con lo que se pudieron tener más conocimientos de los riesgos a los que se estaban expuestos, asimismo el autor concluyó que, mejorar el primero minimizaba los riesgos del segundo. En concordancia de Merino (2021) este determinó que la protección de la información dentro de una empresa comercial ayudaba a que se tenga un plan de prevención y de control de riesgos, haciendo que la empresa no caiga en fraudes o robos informáticos, así como cuidar los datos personales de sus clientes y que estos no se vean vulnerados por hackers.

Con respecto al segundo objetivo específico, en el cual se usó el coeficiente Rho de Spearman, el cual estableció una correlación positiva moderada entre las dimensiones activo financiero y evaluación y priorización con un r = 0,615, por consiguiente, se evidencia una relación entre ambas actividades dentro de una institución financiera, por lo que se tomar en cuenta que la institución financiera considera como un activo importante la seguridad ya que, le permite evaluar y priorizar los riesgos a los que se enfrenta. Los resultados a los que se llegó en este objetivo fueron comparados con Merma (2019) que evaluó los riesgos a los que se enfrentaba una entidad financiera y cómo estos impactaban en la rentabilidad de los resultados económicos, la autora resalta dentro de los resultados de su investigación que, la evaluación de los riesgos a los que se

enfrentaba la institución tenían un impacto moderado con respecto a los activos financieros de la entidad ya que, además de realizar una evaluación de las operaciones, también se evidenciaban otros factores a tomar en cuenta y que tenían un impacto más grande dentro de los activos. Concluye con que, dentro de la entidad financiera existe una relación significativa entre los ingresos que generan sus activos y evaluación de los riesgos.

Para el tercer objetivo específico, en el cual se usó el coeficiente Rho de Spearman, el cual estableció una correlación positiva muy alta entre las dimensiones confidencialidad e implementación de controles con un r = 0,912, por consiguiente, se evidencia una relación entre ambas actividades dentro de una institución financiera, por lo que se debe tomar en cuenta dentro de la institución financiera para el cuidado y protección de la información personal de sus clientes y establecer canales de control eficientes. Con el propósito de contrastar el resultado encontrado se tomó en cuenta la investigación que realizó Ancajima (2019) en el cual buscó estudiar los riesgos de una institución educativa con la finalidad de proponer un mejor trato en la confidencialidad de los datos al implementar un sistema de control que brinde seguridad, para esto propuso hacer uso de las tecnologías de la información ya que, se evidenciaba dentro del personal un manejo de herramientas informáticas en un 75% y que la institución brindaba capacitación sobre temas de seguridad de datos personales en un 73%, el autor concluye que, implementar políticas para mejorar la implementación de controles de seguridad permitió que la institución resguarde los datos personales.

Finalmente, con respecto al objetivo general, para lo cual se utilizó el coeficiente Rho de Spearman, el cual permitió establecer una correlación positiva muy alta entre las variables seguridad informática y riesgo operacional con un r = 0,907, por consiguiente, se evidencia una relación entre ambas variables dentro de una institución financiera, por lo tanto, se puede visualizar que dentro de la entidad financiera los riesgos operacionales tienen una relación directa con la seguridad informática que se implementa ya que, en la actualidad estos riesgos han evolucionado y son más sofisticados en vulnerar las bases de datos de las

diferentes entidades, por lo tanto la entidad financiera debe establecer mejores controles que evidencien la seguridad de sus operaciones, así como las de sus clientes. Los resultados encontrados en el objetivo general fueron comparados con los de Bravo & Barrera (2020) que buscar realizar una auditoría sobre todos los procesos UTM PFESENSE y correlacionador de eventos SIEM que seguía la seguridad informática dentro de las operaciones que realizaban las empresas, en el cual encontró que los procedimientos de estas entidades se encontraban en constante vulneración por no implementar actualizaciones dentro de sus sistemas informáticos, que se veían en constante riesgo porque se establecían con facilidad conexiones de manera remota. Ante eso los autores, recomendaron un plan tecnológico con el propósito de mejorar los recursos técnicos y así tener mejor control dentro de las operaciones, concluyen con que, debía elaborar una matriz describiendo los objetivos de esta implementación y así ver si se ajustaban a los requerimientos de las empresas.

## VI. CONCLUSIONES

1. En consecuencia, en base al primer objetivo específico se determinó a una relación entre las dimensiones protección de información e identificación de riesgo, los que alcanzaron un nivel de correlación de 0,830 y un grado de significancia de 0,000 por lo que se rechazó la hipótesis nula y se acepta la hipótesis alterna; confirmando de esta manera la existencia de una correlación positiva alta entre ambas dimensiones estudiadas, asimismo se consideró que, la protección de la información dentro de la entidad financiera tiene un papel importante en la identificación del riesgo en las operaciones que los clientes y empleados realizan de manera cotidiana, por lo cual se debe elaborar un plan que permita que ambas dimensiones se encuentren protegidas ante los riesgos físicos y virtuales a los que se enfrentan.

2. En conclusión, en el segundo objetivo específico se determinó una relación entre las dimensiones activo financiero y evaluación y priorización, los que alcanzaron un nivel de correlación de 0,615 y un grado de significancia de 0,000 por lo que se rechazó la hipótesis nula y se acepta la hipótesis alterna; estableciendo de esta manera la existencia de una correlación positiva moderada entre ambas dimensiones estudiadas, asimismo se consideró que, la institución financiera toma como un activo financiero la seguridad informática pero, que para llegar a establecer esto se deben tomar en cuenta otros factores además de la evaluación y priorización, factores que tienen un impacto más directo dentro de los riesgos que se afrontan dentro de las inversiones que buscan generar rentabilidad.

3. Además, en el tercer objetivo específico se determinó una relación entre las dimensiones confidencialidad e implementación de controles, los que alcanzaron un nivel de correlación de 0,912 y un grado de significancia de 0,000 por lo que se rechazó la hipótesis nula y se acepta la hipótesis alterna; estableciendo de esta manera la existencia de una correlación

positiva muy alta entre ambas dimensiones estudiadas, por lo que se consideró que la entidad financiera deben implementar y tener mejores sistemas de seguridad dentro de sus operaciones, con la finalidad de salvaguardar la confidencialidad de los datos personales de sus clientes y sus empleados para lo cual se deben establecer planes para un mejor control ya que, ambas dimensiones se encuentran muy relacionadas.

4. Para finalizar, con respecto al objetivo general se determinó una relación entre las variables Seguridad informática y riesgo operaciones ya que, se obtuvo un nivel de correlación de 0,907 y un nivel de significancia de 0,000, en donde se llegó a admitir la hipótesis alterna y rechazar la hipótesis nula; por lo tanto se llega a la conclusión de que existe un nivel correlación positiva muy alta entre las variables, determinando de esta manera que la seguridad informática tienen incidencia dentro de los riesgo operacionales de la entidad ya que, un sistema vulnerable puede poner en riesgo toda las operaciones de la entidad y perjudicarlo económicamente, además de ver afectada su reputación frente a sus clientes.

## VII. RECOMENDACIONES

1. En primer lugar, se recomienda al gerente de la institución financiera, se planteen estrategias que permitan resguardar los datos de todos sus usuarios mediante una oportuna identificación de los riesgos dentro de sus operaciones diarias, con la finalidad de tener un mejor control y minimizar el impacto negativo que puede tener cualquier vulneración de la información, para lo que se debe hacer uso de planes de prevención dentro de todas las operaciones que se realizan.
2. En segundo lugar, se recomienda que, el gerente de la institución defina su posición frente al trato que debe tener la seguridad informática dentro de la institución, si es que debe o no ser considerado como un activo financiero, en vista de lo que se encontró como resultado, este importante factor debe ser tomado en cuenta como un activo ya que, permite, además de brindar seguridad, generar rentabilidad dentro de la institución porque, minimiza los riesgos dentro de las operaciones haciendo que la institución pueda atraer más clientes y así propiciar mejores ingresos.
3. En tercer lugar, se sugiere a la entidad financiera tener un sistema de seguridad que permita mostrar evidencia sobre los usuarios que hacen uso de la información sensible de la entidad, de esta manera se tendrá una mejor confidencialidad sobre estos datos tan importantes, es así que la implementación de controles es una necesidad en vista de que se debe proporcionar toda la protección a los clientes y evitar filtraciones de datos desde la interna para evitar cualquier robo o fraude informático.
4. Por último, se recomienda tanto a jefes como subordinados de la institución financiera a hacer caso de todos los protocolos de seguridad informática con los que se cuentan, porque se tiene evidencia de que muchos de los empleados omiten ciertos procedimientos por encontrarlos en muchos casos tediosos e innecesarios, produciéndose filtración de datos importantes de los clientes que se ven perjudicados por robos informáticos o asaltos físicos cerca de la entidad financiera, asimismo se deben hacer una evaluación sobre el sistema actual a fin de mejorarlo o hacer cambios

sustanciales que sean efectivos y minimicen los riesgos operacionales, tanto de los clientes como de los empleados ya que, ambos comparten las mismas probabilidades de sufrir contratiempos que perjudiquen sus ingresos económicos.

## REFERENCIAS


Akamai (2023). *Superando las brechas de seguridad*: el auge de los ataques de aplicaciones y API's contra organizaciones. https://www.akamai.com/es/blog/security/the-rise-of-application-and-api-attacks

Almaguer, O. A., Osmán, E. D. J. P. A., & Cuesta, R. R. (2018). *La protección de la información*. Una visión desde las entidades educativas cubanas. Ciencias de la Información, 41-47. https://cinfo.idict.cu/index.php/cinfo/article/download/129/129

Álvarez-Risco, A. (2020). *Justificación de la Investigación*. https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/10821/Nota%20Acad%C3%A9mica%205%20%2818.04.2021%29%20-%20Justificaci%C3%B3n%20de%20la%20Investigaci%C3%B3n.pdf?sequence=4&isAllowed=y

Ancajima Mendoza, M. A. (2019). *Propuesta de implementación de seguridad informática en las tic de la IE San Miguel Arcángel, Catacaos-Piura; 2016.* https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/9386/CONTROL_SEGURIDAD_ANCAJIMA_MENDOZA_MARIA_ALEJANDRA.pdf?sequence=1

Arias Gonzáles, J. L., & Covinos Gallardo, M. (2021). *Diseño y metodología de la investigación.* https://repositorio.concytec.gob.pe/bitstream/20.500.12390/2260/1/Arias-Covinos-Dise%C3%B1o_y_metodologia_de_la_investigacion.pdf

Armas Jara, Z. D. (2020). *Auditoria de las operaciones de ahorro para minimizar el riesgo operacional caja Piura Cajabamba-2018.* https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/7365/Armas%20Jara%20Zoila%20Diana.pdf?sequence=1&isAllowed=y

Bedoya, V. H. F. (2020). *Tipos de justificación en la investigación científica*. Espíritu emprendedor TES, 4(3), 65-76.

http://espirituemprendedortes.com/index.php/revista/article/download/207/275

Bogantes, A. (2020). *El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados.* Revista Sistemas, Cibernética e Informática, 17(1), 24-29. https://www.iiisci.org/journal/PDV/risci/pdfs/CB294NT20.pdf

Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., ... & Merino, M. A. C. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* (Vol. 46). 3Ciencias. https://books.google.es/books?hl=es&lr=&id=5Z9yDwAAQBAJ&oi=fnd&pg=PA29&dq=seguridad+inform%C3%A1tica+&ots=ymzTyZb7Pq&sig=1DTDq7eowC6f96zJzSxLFnR31gI

Cervantes, P. A. M. (2020). *Hacia un modelo estocástico eficiente para la valoración de activos financieros basado en el volumen de negociación*: fundamentos teóricos e implementación práctica (Vol. 370). Universidad Almería. https://dialnet.unirioja.es/servlet/tesis?codigo=178326

CHILÁN GONZÁLEZ, G. G. (2021). *MEDIDAS DE SEGURIDAD INFORMÁTICA PARA LA IMPLEMENTACIÓN DE REPOSITORIO DE ALMACENAMIENTO DE DOCUMENTOS EN LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN, UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ* (Bachelor's thesis, Jipijapa. UNESUM). http://repositorio.unesum.edu.ec/bitstream/53000/2874/1/TESIS%20-%20CHIL%C3%81N%20GONZALEZ%20GUIDO%20GABRIEL.pdf

Consejo de la Unión Europea (2022). *Finanzas digitales*: el Consejo adopta el Reglamento sobre la resiliencia operativa digital. https://www.consilium.europa.eu/es/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/

Cordova Garay, C. M., & Ruiz Romero, F. F. (2019). *Los riesgos operacionales y su relación en la cadena logística de las exportaciones peruanas de uva*

*fresca a Estados Unidos durante el período 2016-2020.* https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/657775/Cordova_GC.pdf?sequence=3

Diaz Soto, D. J., Peña Bohórquez, F. M., & Silva Ucar, H. J. (2022). *Análisis del estado actual de la seguridad informática de una PYME del sector de construcción de obras civiles*. https://repositorio.unbosque.edu.co/bitstream/handle/20.500.12495/6582/Diaz%20_Soto_Dimas_Jahir_2022.pdf?sequence=8

De Berrio, G. M. (2019). *Tipología del riesgo financiero y normativa bancaria panameña.* Revista saberes APUDEP, 2(2), 21-28. http://uptv.up.ac.pa/index.php/saberes_apudep/article/download/827/707

El Maadioui El Issati, S. (2023). *Registro y acceso a una página web mediante tecnologías de reconocimiento facial* (Bachelor's thesis, Universitat Politècnica de Catalunya). https://upcommons.upc.edu/bitstream/handle/2117/390802/tfg-soufian-elmaadioui-elissati.pdf?sequence=2

El Peruano (2023). *Delitos informáticos en el Perú*. https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru

Escalante Quimis, O. A. (2021). *Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica* (Bachelor's thesis). https://dspace.ups.edu.ec/bitstream/123456789/20576/1/UPS-GT003301.pdf

Estrada, I., Andrade Martínez, A. C., & Espín Oleas, M. E. (2018). *Riesgo operacional:* control y mitigación en pérdidas financieras de Cooperativas Segmento 4. Observatorio de la Economía Latinoamericana, (marzo). https://www.eumed.net/rev/oel/2018/03/cooperativas-segmento4.html

Figueroa Guzmán, L. (2019). *Beneficios económicos del uso de semilla certificada en la producción de arroz* (Oryza sativa) en el Perú. https://repositorio.lamolina.edu.pe/bitstream/handle/20.500.12996/4161/figueroa-guzman-livia.pdf?sequence=1&isAllowed=y

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). *La seguridad informática y la seguridad de la información.* Polo del conocimiento, 2(12), 145-155. https://polodelconocimiento.com/ojs/index.php/es/article/download/420/791

Gagñay, L. K. I., Chicaiza, S. L. T., & Aguirre, J. L. (2020*). Ética en la investigación científica.* Revista Imaginario Social, 3(1). https://www.revista-imaginariosocial.com/index.php/es/article/download/10/19

Guerrero, M. S. P., Aguirre, A. A. A., Medina, R. A. R., & Duque, P. L. (2022). *Valor en Riesgo y simulación*: una revisión sistemática. Económicas CUC, 43(1), 57-82. https://dialnet.unirioja.es/descarga/articulo/8439220.pdf

Gutiérrez Nagua, J. J. (2022). *Aplicación para gestionar las contraseñas en una corporación o empresa* (Bachelor's thesis). https://dspace.utpl.edu.ec/handle/20.500.11962/29854

Heredia, A. (2020*). Políticas de fomento para la incorporación de las tecnologías digitales en las micro, pequeñas y medianas empresas de América Latina*: revisión de experiencias y oportunidades. https://repositorio.cepal.org/bitstream/handle/11362/45096/1/S1900987_es.pdf

Hernández, H. M., Cantero, L. G. Z., Vidal, D. M. R., & Villadiego, L. R. (2019). *Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia*. Revista venezolana de gerencia, 2, 528-541. https://www.redalyc.org/journal/290/29063446029/29063446029.pdf

Hernández Rodríguez, S. (2018). *El reto de la era digital*: privacidad y confidencialidad de la información de pacientes. Gen, 72(1), 00-01.

http://ve.scielo.org/scielo.php?pid=S0016-35032018000100001&script=sci_arttext

Llerena, V. R. S. (2022). *Los estándares internacionales del Comité de Supervisión Bancaria de Basilea (BCBS) para una adecuada regulación bancaria.* Dataismo, 2(7), 1-18. http://dataismo.org.pe/index.php/data/article/view/102

Martínez Landrove, N. (2019). *Ciberseguridad y riesgo operacional en las organizaciones.* https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/42317/TFM001173.pdf?sequence=1

Mendoza Silva, L. F., & Vega Gallegos, G. R. (2019*). Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa Sisc.* https://repositorio.up.edu.pe/bitstream/handle/11354/2250/Luis_Tesis_Maestria_2019.pdf?sequence=1

Meraz Espinoza, A. I. (2018). *Empresa y privacidad*: el cuidado de la información y los datos personales en medios digitales. Revista IUS, 12(41), 293-310. https://www.scielo.org.mx/scielo.php?pid=S1870-21472018000100293&script=sci_arttext

Merma Arohuanca, J. I. (2019). *El Riesgo Operacional y su Incidencia en la Rentabilidad del Banco Financiero Periodo 2015-2017.* https://repositorio.upt.edu.pe/bitstream/handle/20.500.12969/772/Merma-Arohuanca-Jorge.pdf?sequence=1&isAllowed=y

Merino Rosas, C. A. (2021*). Implementación de un plan de seguridad informática con la norma* ISO/IEC 27001 en la empresa RANSA Comercial SA-Piura; 2021. http://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/24698/SEGURIDAD_INFORMATICA_MERINO_ROSAS_CESAR.pdf?sequence=1

Morales, V. M. (2019). Revisió n de la Literatura sóbre el *Módeló Financieró CAPM. Journal of finance, 19(3), 425-442.* https://www.researchgate.net/profile/Victor-Morales-18/publication/337464209_Revision_de_la_Literatura_sobre_el_Modelo_Financiero_CAPM/links/5dd8bb6c458515dc2f459f21/Revision-de-la-Literatura-sobre-el-Modelo-Financiero-CAPM.pdf

Navarrete Villota, M. J. (2018). *La capacitación del personal y el desempeño laboral* (Master's thesis, Universidad Técnica de Ambato. Facultad de Ciencias Administrativas. Maestría en Gestión del Talento Humano.). http://repositorio.uta.edu.ec/bitstream/123456789/28329/1/49%20GTH.pdf

Nina Yana, A. (2022). Aplicación de la Norma Internacional ISO/IEC 27005: 2018 para la *Gestión de Riesgos de Seguridad de la Información en Dispositivos GPS, 2022.* https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/111984/Nina_YA-SD.pdf?sequence=1

Ochoa Palomino, A. (2019). *Diseño de una Red de Seguridad Informática para la Protección del Sistema Web de un Call Center ante Ataques Informáticos Aplicando la Norma ISO 27033.* https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625726/ochoa_pa.pdf?sequence=1

Ortiz-Garcés, I., Briones, L., Singo, M., & Echeverría, A. (2023). *Implementación de un Modelo de Ciberseguridad de una Arquitectura de Sensores de Monitoreo IoT en la Niebla.* Revista Ibérica de Sistemas e Tecnologias de Informação, (E56), 371-382. https://www.researchgate.net/profile/Aaron-Echeverria/publication/371868308_Implementacion_de_un_Modelo_de_Ciberseguridad_de_una_Arquitectura_de_Sensores_de_Monitoreo_IoT_en_la_Niebla/links/649a00ac8de7ed28ba5a7cc7/Implementacion-de-un-Modelo-de-Ciberseguridad-de-una-Arquitectura-de-Sensores-de-Monitoreo-IoT-en-la-

Niebla.pdf?origin=journalDetail&_tp=eyJwYWdlIjoiam91cm5hbERldGFpbCJ9

Pérez Castillo, M. R. (2018). *Administración de tecnologías de información en los procedimientos de seguridad informática del Banco de la Nación, 2016.* https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/12698/P%C3%A9rez_CMR.pdf?sequence=1

Pita, G. E. C. (2018). *Las TICs en las empresas*: evolución de la tecnología y cambio estructural en las organizaciones. Dominio de las Ciencias, 4(1), 499-510. https://dialnet.unirioja.es/descarga/articulo/6313252.pdf

Ponce Larreategui, J. G. (2021). *Indicadores de compromiso (IOC) para detección de amenazas en la seguridad informática con enfoque en el código malicioso (Bachelor's thesis).* https://sistemas.acis.org.co/index.php/sistemas/article/download/11/8

Reynosa Navarro, E. (2018). *Trabajo de investigación.* Teoría, metodología y práctica. https://www.aacademica.org/ern/12.pdf

Rodríguez, C. E. L., & Rodríguez, M. A. E. (2021). *Riesgo operacional: comportamiento de sus factores en el sector bancario de Bogotá Colombia.* Revista Venezolana de Gerencia: RVG, 26(6), 439-456. https://dialnet.unirioja.es/descarga/articulo/8890596.pdf

Sahún Pacheco, R. (2019). *Riesgo operacional y servicio público*. DERECHO PÚBLICO. https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-PB-2019-156

Saltos Ramirez, E. M. (2018). ARTÍCULO CIENTÍFICO*:" Factores que inciden en la seguridad informática y aplicabilidad en el Cloud Computing de las empresas del sector industrial en la ciudad de Manta, Provincia de Manabí".*

Sánchez Palacios, E. S. (2020). Análisis para la seguridad informática basado en la norma ISO/IEC 27001 en el área de cómputo de la dirección regional de educación–Tumbes; 2020.

http://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/19763/INFORMACION_ISO2700_SANCHEZ_PALACIOS_EDINSON_SAMIR.pdf?sequence=3

Santiesteban-Zaldívar, E., Frías, V. G. F., & Cardeñosa, E. L. (2020). *Análisis de la Rentabilidad Económica.* Tecnología propuesta para incrementar la eficiencia empresarial. Editorial Universitaria (Cuba). https://books.google.com.pe/books?hl=es&lr=&id=33n1DwAAQBAJ&oi=fnd&pg=PP2&dq=rentabilidad+beneficios+eficiencia&ots=kKywgWRba6&sig=Zj2uR9NLUnC_3y509JgLHFQ1q4M

Tejedor, B. G. S., Castrellón, H. V., De León, E. T., & de Ayala, D. V. (2023). *Seguridad de los Sistemas Informáticos Universitarios:* Retos Pendientes. REICIT, 2(2), 113-142. http://uptv.up.ac.pa/index.php/REICIT/article/download/3585/3104

Toudert, D. (2019). *Brecha digital, uso frecuente y aprovechamiento de Internet en México.* Convergencia, 26(79). https://www.scielo.org.mx/scielo.php?pid=S1405-14352019000100003&script=sci_arttextUrdaneta-Montiel, A. J., Borgucci-García, E. V., & Jaramillo-Escobar, B. (2021). Crecimiento económico y la teoría de la eficiencia dinámica. RETOS. Revista de Ciencias de la Administración y Economía, 11(21), 93-116. http://scielo.senescyt.gob.ec/pdf/retos/v11n21/1390-6291-Retos-11-21-00093.pdf

Zanabria Ticona, E. D., & Cayo Mamani, E. (2018). *Seguridad informática en dispositivos móviles con Sistemas Operativos Android mediante Pentesting*. http://repositorio.unap.edu.pe/handle/UNAP/7047

# ANEXOS

## ANEXO 1. MATRIZ DE OPERACIONALIZACION DE LA VARIABLE

### SEGURIDAD INFORMÁTICA Y RIESGO OPERACIONAL EN UNA ENTIDAD FINANCIERA, LOS OLIVOS 2023

| VARIABLE | DEFINICIÓN CONCEPTUAL | DEFINICIÓN OPERACIONAL | DIMENSIONES | INDICADORES | ESCALA DE MEDICIÓN |
|---|---|---|---|---|---|
| SEGURIDAD INFORMATICA | Para Postigo (2020) son aquellas medidas que se toman para que la protección de datos de empleados y clientes no sea malversada, impidiendo de esta forma que los usuarios no autorizados ejerzan control sobre los sistemas internos y así evitar daños irreversibles dentro de una entidad. Según Castro et al. (2018) estos sistemas son tratados como activos financieros debido a que se encarga de la protección de todos los activos dentro de una entidad financiera, con lo que se minimiza el riesgo de sufrir cualquier robo, además lo califican como un recurso fundamental para las operaciones se desarrollen con normalidad en función de los objetivos que se proponen. Según Bogantes (2020), estos sistemas de seguridad permiten guardar la confidencialidad de todos los datos almacenados, con lo que se asegura que el tratamiento de estos datos solo se use para fines específicos y sin vulnerar la seguridad de las personas que son parte de dicho recurso informático. | Se medirá la variable "Seguridad informática" con el instrumento del cuestionario, contando con las dimensiones protección de información, activo financiero y confidencialidad. | Protección de información | Privacidad | **Likert Ordinal:**<br><br>5: Siempre<br>4: Casi Siempre<br>3: A veces<br>2: Casi nunca<br>1: Nunca |
| | | | | Herramientas informaticas | |
| | | | | Base de datos | |
| | | | Activo financiero | Rentabilidad | |
| | | | | Beneficios | |
| | | | | Eficiencia | |
| | | | Confidencialidad | Políticas y procedimientos | |
| | | | | Control de contraseñas | |
| | | | | Seguridad | |

| | | | | | |
|---|---|---|---|---|---|
| **RIESGO OPERACIONAL** | | Se medirá la variable "Riesgo operacional" con el instrumento del cuestionario, contando con las dimensiones identificación de riesgo, evaluación y priorización e implementación de controles. | Identificación del riesgo | Riesgo en las operaciones | **Ordinal**<br><br>5: Siempre<br>4: Casi Siempre<br>3: A veces<br>2: Casi nunca<br>1: Nunca |
| | | | | Ciberataque | |
| | | | | Controles | |
| | | | | Capacitación del personal | |
| | | | Evaluación y priorización | Probabilidad de ocurrencia de un fraude | |
| | | | | Fraude | |
| | | | | Uso inteligente de los buscadores de internet | |
| | | | Implementación de controles | Sistema confiable | |
| | | | | Registro de acceso | |
| | | | | Monitoreo continuo | |

**Anexo 2. Instrumento de Recolección de datos**

**UNIVERSIDAD CESAR VALLEJO**

**ESCUELA PROFESIONAL DE ADMINISTRACION**

**FICHA DE ENCUESTA**

Estimado cliente/colaborador, sus respuestas en el siguiente cuestionario son de mucha importancia ya que contribuirán a una investigación de tipo académica, que busca establecer la relación entre las variables; incidentes de seguridad – riesgo, evaluación y gestión de riesgos. Toda la información será confidencial. Toda la información será confidencial.

De la misma manera se requiere su **consentimiento informado** para poder aplicarle el instrumento de investigación. En ese sentido agradeceré marcar el siguiente recuadro en señal de conformidad:

Declaro estar informado de la aplicación de la siguiente encuesta y en señal de conformidad marco con una x el casillero:

Estoy de acuerdo ☐

No estoy de acuerdo ☐

**TIEMPO DE DURACIÓN: 15 MINUTOS**

**INSTRUCCIONES**

Marcar con una (X) el número según la importancia que usted considere

| ESCALA DE VALORACIÓN | NUNCA | CASI NUNCA | A VECES | CASI SIEMPRE | SIEMPRE |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |

| V1. SEGURIDAD INFORMATICA | | | | OPCIÓN DE RESPUESTA | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 |
| Dimensión | Indicador | N° | Ítems | NUNCA | CASI NUNCA | A VECES | CASI SIEMPRE | SIEMPRE |
| Protección de información | Privacidad | 1 | Se cuidad la privacidad de los datos personales de los cienes. | | | | | |
| | | 2 | Ha sido testigo de algun caso de vulneración de los datos de los clientes. | | | | | |
| | Herramientas informáticas | 3 | Se hace uso de un software de gestión de datos eficiente y seguro. | | | | | |
| | Base de datos | 4 | Los datos de los clientes se encuentran respaldadas en una base de datos segura. | | | | | |
| Activo financiero | Rentabilidad | 5 | El sistema de seguridad informática que se usa genera rentabilidad a la financiera. | | | | | |
| | Beneficios | 6 | El sistema de seguridad actual le genera beneficios a la entidad financiera. | | | | | |
| | Eficiencia | 7 | La eficiencia de los empleados se debe al uso del sistema de seguridad. | | | | | |
| Confidencialidad | Políticas y procedimientos | 8 | En las políticas de la entidad financiera se siguen los procedimientos necesarios para proteger la confidencialidad de los datos de los clientes. | | | | | |
| | Control de contraseñas | 9 | Se realiza un control constante en las contraseñas al cambiarlas regularmente | | | | | |
| | Seguridad | 10 | Se evalúa constantemente la seguridad de los softwares usados en la entidad financiera. | | | | | |

| V2. RIESGO OPERACIONAL | | | | OPCIÓN DE RESPUESTA | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 |
| Dimensión | Indicador | N° | Ítems | NUNCA | CASI NUNCA | A VECES | CASI SIEMPRE | SIEMPRE |
| Identificación de riesgo | Riesgo operacional | 11 | La entidad financiera implementa los controles necesarios para minimizar el riesgo en las operaciones. | | | | | |
| | Ciberataque | 12 | Ha ocurrido un ciberataque a los sistemas de seguridad de la entidad financiera. | | | | | |
| | Controles | 13 | Se lleva un control sobre las operaciones que tienen mayor riesgo de un ataque cibernético. | | | | | |
| | Capacitación del personal | 14 | Se capacita al personal sobre cómo actuar en una situación de riesgo en las operaciones financieras. | | | | | |
| Evaluación y priorización | Probabilidad de ocurrencia de un fraude | 15 | Existe un plan de acción ante la posibilidad de un fraude dentro de la entidad financiera. | | | | | |
| | Fraude | 16 | Ha sido testigo de algún fraude por parte de los colaboradores de la entidad financiera. | | | | | |
| | Uso inteligente de los buscadores de internet | 17 | Se tiene algún filtro de seguridad para no acceder a páginas webs sospechosas. | | | | | |
| Implementación de controles | Sistema confiable | 18 | El sistema de seguridad que se usa actualmente es confiable. | | | | | |
| | Registro de acceso | 19 | Se lleva un control sobre los empleados que tienen acceso a los sistemas informáticos de la entidad financiera. | | | | | |
| | Monitoreo continuo | 20 | Se realiza la supervisión y monitoreo de actividades de todos los empleados que hacen uso de los softwares de la entidad financiera. | | | | | |

**Muchas gracias**

## Anexo 3. Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento **"Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023"**. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

### 1. Datos generales del juez

| | | |
|---|---|---|
| **Nombres y Apellidos del juez:** | Julio Cesar Manrique Cespedes | |
| **Grado profesional:** | Maestría ( ) | Doctor (X ) |
| **Área de formación académica:** | Clínica ( ) | Social ( ) |
| | Educativa ( ) | Organizacional ( **X** ) |
| **Áreas de experiencia profesional:** | Docente de la Escuela Profesional de Administración | |
| **Institución donde labora:** | Universidad César Vallejo | |
| **Tiempo de experiencia profesional el área:** | 2 a 4 años ( )<br>Más de 5 años ( **X** ) | |

### 2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

### 3. Datos de la escala:

| | |
|---|---|
| Nombre de la Prueba: | Cuestionario en escala ordinal |
| Autora: | Tello Neira, Mary Nardhy |
| Procedencia: | De la autora |
| Administración: | Virtual |
| Tiempo de aplicación: | 15 minutos |
| Ámbito de aplicación: | Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023 |

| | |
|---|---|
| Significación: | Está compuesta por dos variables:<br>- La primera variable contiene 03 dimensiones, de 10 indicadores y 10 Ítems en total. El objetivo es medir la relación de variables.<br>- La segunda variable contiene 03 dimensiones, de 10 indicadores y 10 ítems en total. El objetivo es medir la relación de variables. |

## 4. Soporte teórico

- **Variable 1: Seguridad informática**

Postigo (2020) son aquellas medidas que se toman para que la protección de datos de empleados y clientes no sea malversada, impidiendo de esta forma que los usuarios no autorizados ejerzan control sobre los sistemas internos y así evitar daños irreversibles dentro de una entidad.

- **Variable 2: Riesgo operacional**

Gómez et al. (2020) se refirieron a ella como, la que se evidencia de los conflictos de interés entre los empleados y los jefes de cada una de las áreas en una empresa. Los primero pueden actuar de forma oportunista o negligente, causando pérdidas o daños a la empresa, para reducir este riesgo, se requiere un adecuado sistema de incentivos, supervisión y control.

| Variable | Dimensiones | Definición |
|---|---|---|
| **Seguridad informatica** | Protección de información | Almaguer et al. (2018) nos dicen que, son acciones que se encargan de proteger la privacidad de los usuarios usando diversas herramientas informáticas con el propósito de proteger una determinada base de datos que por lo general se encuentran almacenadas dentro de equipos informáticos. |
| | Activo financiero | Cervantes (2020) es un recurso que, permite a una entidad financiera el derecho a recibir ingresos futuros y así generar rentabilidad. Es decir, es un instrumento que otorga beneficios reales al emisor y así se genere la eficiencia de los recursos utilizados |

| | | |
|---|---|---|
| | Confidencialidad | Hernández (2018) la definió como, un principio que garantiza que la información solo puede ser accedida por las personas que tienen autorización, esto se lleva a cabo bajo las políticas y procedimientos que son establecidos por una empresa, entre los que se encuentran un estricto control de contraseñas, para así garantizar la |
| | Identificación de riesgos | De Berrio (2019), es la probabilidad de que ocurra un evento adverso que afecte el funcionamiento normal de una organización, como puede ser un ciberataque, originando que lo controles de seguridad sean perjudicas y se tengan pérdidas económicas, ante eso es importante capacitar al personal para que tenga conocimiento de cómo actuar en esos casos. |
| **Riesgo operacional** | Evaluación y priorización | Mendoza & Vega (2019), se trata del proceso de identificar, analizar y clasificar los riesgos según su importancia y urgencia, para estimar la probabilidad de ocurrencias de un fraude y el impacto de los riesgos, mientras que la priorización implica asignar recursos y acciones para mitigarlos, el desarrollo de esta actividad es un factor clave para la gestión de proyectos, la auditoría interna y la prevención de fraudes. Entre sus indicadores tenemos, probabilidad de ocurrencia de un fraude. |
| | Implementación de controles | Serrano (2018) es el proceso de poner en práctica las medidas de prevención, detección y mitigación de los riesgos que pueden afectar el funcionamiento y los objetivos de una organización con el uso de sistemas confiables, con esto se garantiza tener un registro de acceso de todos los usuarios con la finalidad de monitorear continuamente y así garantizar la eficacia y la eficiencia de las actividades. |

**5. Presentación de instrucciones para el juez**:

A continuación, a usted le presento el cuestionario "Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023**"**

elaborado por Tello Neira, Mary Nardhy en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD**<br>El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | El ítem no es claro. |
| | 2. Bajo Nivel | El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos del ítem. |
| | 4. Alto nivel | El ítem es claro, tiene semántica y sintaxis adecuada. |
| **COHERENCIA**<br>El ítem tiene relación lógica con la dimensión o indicador que está midiendo. | 1. Totalmente en desacuerdo (no cumple con el criterio) | El ítem no tiene relación lógica con la dimensión. |
| | 2. Desacuerdo (bajo nivel de acuerdo) | El ítem tiene una relación tangencial /lejana con la dimensión. |
| | 3. Acuerdo (moderado nivel) | El ítem tiene una relación moderada con la dimensión que se está midiendo. |
| | 4. Totalmente de Acuerdo (alto nivel) | El ítem se encuentra está relacionado con la dimensión que está midiendo. |
| **RELEVANCIA**<br>El ítem es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión. |
| | 2. Bajo Nivel | El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide |
| | 3. Moderado nivel | El ítem es relativamente importante. |
| | 4. Alto nivel | El ítem es muy relevante y debe ser |

*Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde*

*sus observaciones que considere pertinente*

| |
|---|
| 1. No cumple con el criterio |
| 2. Bajo Nivel |
| 3. Moderado nivel |
| 4. Alto nivel |

**Variable del instrumento**: **SEGURIDAD INFORMATICA**

Primera dimensión: Protección de información

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Eficacia | 1 | 4 | 4 | 4 | |
| Efectividad | 2 | 4 | 4 | 4 | |
| Recursos | 3 | 4 | 4 | 4 | |

Segunda dimensión: Activo financiero

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Habilidad | 4 | 4 | 4 | 4 | |
| Herramienta | 5 | 4 | 4 | 4 | |
| Detección | 6 | 4 | 4 | 4 | |

- Tercera dimensión: Confidencialidad

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Recuperación | 7 | 4 | 4 | 4 | |
| Implementación | 8 | 4 | 4 | 4 | |
| Medidas | 9 | 4 | 4 | 4 | |

**Variable del instrumento**: **Riesgo operacional**

- Primera dimensión: Identificación de riesgo

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Riesgo operacional | 10 | 4 | 4 | 4 | |
| Ciberataque | 11 | 4 | 4 | 4 | |

| | | | | | |
|---|---|---|---|---|---|
| Controles | 12 | 4 | 4 | 4 | |

- Segunda dimensión: Evaluación y priorización

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Probabilidad de ocurrencia de un fraude | 13 | 4 | 4 | 4 | |
| Fraude | 14 | 4 | 4 | 4 | |
| Uso inteligente de los buscadores de internet | 15 | 4 | 4 | 4 | |

- Tercera dimensión: Implementación de controles

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Sistema confinable | 16 | 4 | 4 | 4 | |
| Politicas | 17 | 4 | 4 | 4 | |
| Procedimientos | 18 | 4 | 4 | 4 | |

Dr.Julio Cesar Manrique Cespedes
DNI: 07424958

Pd.: el presente formato debe tomar en cuenta:

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra

bibliografía.

**Evaluación por juicio de expertos**

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento **"Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023"**. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

## 1. Datos generales del juez

| | | |
|---|---|---|
| **Nombres y Apellidos del juez:** | Victor Dávila Arenaza | |
| **Grado profesional:** | Maestría ( ) | Doctor (X ) |
| **Área de formación académica:** | Clínica ( ) | Social ( ) |
| | Educativa ( ) | Organizacional ( **X** ) |
| **Áreas de experiencia profesional:** | Docente de la Escuela Profesional de Administración | |
| **Institución donde labora:** | Universidad César Vallejo | |
| **Tiempo de experiencia profesional el área:** | 2 a 4 años ( )<br>Más de 5 años ( **X** ) | |

## 2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

## 3. Datos de la escala:

| | |
|---|---|
| Nombre de la Prueba: | Cuestionario en escala ordinal |
| Autora: | Tello Neira, Mary Nardhy |
| Procedencia: | De la autora |
| Administración: | Virtual |
| Tiempo de aplicación: | 15 minutos |
| Ámbito de aplicación: | Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023 |

| | |
|---|---|
| Significación: | Está compuesta por dos variables:<br>- La primera variable contiene 03 dimensiones, de 10 indicadores y 10 Ítems en total. El objetivo es medir la relación de variables.<br>- La segunda variable contiene 03 dimensiones, de 10 indicadores y 10 ítems en total. El objetivo es medir la relación de variables. |

## 4. Soporte teórico

- **Variable 1: Seguridad informática**

Postigo (2020) son aquellas medidas que se toman para que la protección de datos de empleados y clientes no sea malversada, impidiendo de esta forma que los usuarios no autorizados ejerzan control sobre los sistemas internos y así evitar daños irreversibles dentro de una entidad.

- **Variable 2: Riesgo operacional**

Gómez et al. (2020) se refirieron a ella como, la que se evidencia de los conflictos de interés entre los empleados y los jefes de cada una de las áreas en una empresa. Los primero pueden actuar de forma oportunista o negligente, causando pérdidas o daños a la empresa, para reducir este riesgo, se requiere un adecuado sistema de incentivos, supervisión y control.

| Variable | Dimensiones | Definición |
|---|---|---|
| **Seguridad informatica** | Protección de información | Almaguer et al. (2018) nos dicen que, son acciones que se encargan de proteger la privacidad de los usuarios usando diversas herramientas informáticas con el propósito de proteger una determinada base de datos que por lo general se encuentran almacenadas dentro de equipos informáticos. |
| | Activo financiero | Cervantes (2020) es un recurso que, permite a una entidad financiera el derecho a recibir ingresos futuros y así generar rentabilidad. Es decir, es un instrumento que otorga beneficios reales al emisor y así se genere la eficiencia de los recursos utilizados |

| | | |
|---|---|---|
| | Confidencialidad | Hernández (2018) la definió como, un principio que garantiza que la información solo puede ser accedida por las personas que tienen autorización, esto se lleva a cabo bajo las políticas y procedimientos que son establecidos por una empresa, entre los que se encuentran un estricto control de contraseñas, para así garantizar la |
| | Identificación de riesgos | De Berrio (2019), es la probabilidad de que ocurra un evento adverso que afecte el funcionamiento normal de una organización, como puede ser un ciberataque, originando que lo controles de seguridad sean perjudicas y se tengan pérdidas económicas, ante eso es importante capacitar al personal para que tenga conocimiento de cómo actuar en esos casos. |
| **Riesgo operacional** | Evaluación y priorización | Mendoza & Vega (2019), se trata del proceso de identificar, analizar y clasificar los riesgos según su importancia y urgencia, para estimar la probabilidad de ocurrencias de un fraude y el impacto de los riesgos, mientras que la priorización implica asignar recursos y acciones para mitigarlos, el desarrollo de esta actividad es un factor clave para la gestión de proyectos, la auditoría interna y la prevención de fraudes. Entre sus indicadores tenemos, probabilidad de ocurrencia de un fraude. |
| | Implementación de controles | Serrano (2018) es el proceso de poner en práctica las medidas de prevención, detección y mitigación de los riesgos que pueden afectar el funcionamiento y los objetivos de una organización con el uso de sistemas confiables, con esto se garantiza tener un registro de acceso de todos los usuarios con la finalidad de monitorear continuamente y así garantizar la eficacia y la eficiencia de las actividades. |

**5. Presentación de instrucciones para el juez:**

A continuación, a usted le presento el cuestionario "Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023**"** elaborado por Tello Neira, Mary Nardhy en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD** El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | El ítem no es claro. |
| | 2. Bajo Nivel | El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos del ítem |
| | 4. Alto nivel | El ítem es claro, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** El ítem tiene relación lógica con la dimensión o indicador que está midiendo. | 1. Totalmente en desacuerdo (no cumple con el criterio) | El ítem no tiene relación lógica con la dimensión. |
| | 2. Desacuerdo (bajo nivel de acuerdo) | El ítem tiene una relación tangencial /lejana con la dimensión. |
| | 3. Acuerdo (moderado nivel) | El ítem tiene una relación moderada con la dimensión que se está midiendo. |
| | 4. Totalmente de Acuerdo (alto nivel) | El ítem se encuentra está relacionado con la dimensión que está midiendo. |
| **RELEVANCIA** El ítem es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión. |
| | 2. Bajo Nivel | El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide |
| | 3. Moderado nivel | El ítem es relativamente importante. |
| | 4. Alto nivel | El ítem es muy relevante y debe ser |

*Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde*

*sus observaciones que considere pertinente*

| | |
|---|---|
| 5. | No cumple con el criterio |
| 6. | Bajo Nivel |

| |
|---|
| 7. Moderado nivel |
| 8. Alto nivel |

**Variable del instrumento**: **SEGURIDAD INFORMATICA**

Primera dimensión: Protección de información

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Eficacia | 1 | 4 | 4 | 4 | |
| Efectividad | 2 | 4 | 4 | 4 | |
| Recursos | 3 | 4 | 4 | 4 | |

Segunda dimensión: Activo financiero

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Habilidad | 4 | 4 | 4 | 4 | |
| Herramienta | 5 | 4 | 4 | 4 | |
| Detección | 6 | 4 | 4 | 4 | |

- Tercera dimensión: Confidencialidad

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Recuperación | 7 | 4 | 4 | 4 | |
| Implementación | 8 | 4 | 4 | 4 | |
| Medidas | 9 | 4 | 4 | 4 | |

**Variable del instrumento**: **Riesgo operacional**

- Primera dimensión: Identificación de riesgo

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Riesgo operacional | 10 | 4 | 4 | 4 | |
| Ciberataque | 11 | 4 | 4 | 4 | |
| Controles | 12 | 4 | 4 | 4 | |

- Segunda dimensión: Evaluación y priorización

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Probabilidad de ocurrencia de un fraude | 13 | 4 | 4 | 4 | |
| Fraude | 14 | 4 | 4 | 4 | |
| Uso inteligente de los buscadores de internet | 15 | 4 | 4 | 4 | |

- Tercera dimensión: Implementación de controles

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Sistema confinable | 16 | 4 | 4 | 4 | |
| Politicas | 17 | 4 | 4 | 4 | |
| Procedimientos | 18 | 4 | 4 | 4 | |

Dr. Victor Dávila Arenaza

DNI: 08467692

Pd.: el presente formato debe tomar en cuenta:

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra

bibliografía.

**Evaluación por juicio de expertos**

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento **"Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023"**. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

## 1. Datos generales del juez

| | | |
|---|---|---|
| **Nombres y Apellidos del juez:** | Teodoro Carranza Estela | |
| **Grado profesional:** | Maestría (x ) | Doctor (X ) |
| **Área de formación académica:** | Clínica ( ) | Social ( ) |
| | Educativa ( ) | Organizacional ( **X** ) |
| **Áreas de experiencia profesional:** | Docente de la Escuela Profesional de Administración | |
| **Institución donde labora:** | Universidad César Vallejo | |
| **Tiempo de experiencia profesional el área:** | 2 a 4 años ( )<br>Más de 5 años ( **X** ) | |

## 2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

## 3. Datos de la escala:

| | |
|---|---|
| Nombre de la Prueba: | Cuestionario en escala ordinal |
| Autora: | Tello Neira, Mary Nardhy |
| Procedencia: | De la autora |
| Administración: | Virtual |
| Tiempo de aplicación: | 15 minutos |
| Ámbito de aplicación: | Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023 |

| | |
|---|---|
| Significación: | Está compuesta por dos variables:<br>- La primera variable contiene 03 dimensiones, de 10 indicadores y 10 Ítems en total. El objetivo es medir la relación de variables.<br>- La segunda variable contiene 03 dimensiones, de 10 indicadores y 10 ítems en total. El objetivo es medir la relación de variables. |

## 4. Soporte teórico

- **Variable 1: Seguridad informática**

Postigo (2020) son aquellas medidas que se toman para que la protección de datos de empleados y clientes no sea malversada, impidiendo de esta forma que los usuarios no autorizados ejerzan control sobre los sistemas internos y así evitar daños irreversibles dentro de una entidad.

- **Variable 2: Riesgo operacional**

Gómez et al. (2020) se refirieron a ella como, la que se evidencia de los conflictos de interés entre los empleados y los jefes de cada una de las áreas en una empresa. Los primero pueden actuar de forma oportunista o negligente, causando pérdidas o daños a la empresa, para reducir este riesgo, se requiere un adecuado sistema de incentivos, supervisión y control.

| Variable | Dimensiones | Definición |
|---|---|---|
| **Seguridad informatica** | Protección de información | Almaguer et al. (2018) nos dicen que, son acciones que se encargan de proteger la privacidad de los usuarios usando diversas herramientas informáticas con el propósito de proteger una determinada base de datos que por lo general se encuentran almacenadas dentro de equipos informáticos. |
| | Activo financiero | Cervantes (2020) es un recurso que, permite a una entidad financiera el derecho a recibir ingresos futuros y así generar rentabilidad. Es decir, es un instrumento que otorga beneficios reales al emisor y así se genere la eficiencia de los recursos utilizados |

| | | |
|---|---|---|
| | Confidencialidad | Hernández (2018) la definió como, un principio que garantiza que la información solo puede ser accedida por las personas que tienen autorización, esto se lleva a cabo bajo las políticas y procedimientos que son establecidos por una empresa, entre los que se encuentran un estricto control de contraseñas, para así garantizar la |
| | Identificación de riesgos | De Berrio (2019), es la probabilidad de que ocurra un evento adverso que afecte el funcionamiento normal de una organización, como puede ser un ciberataque, originando que lo controles de seguridad sean perjudicas y se tengan pérdidas económicas, ante eso es importante capacitar al personal para que tenga conocimiento de cómo actuar en esos casos. |
| **Riesgo operacional** | Evaluación y priorización | Mendoza & Vega (2019), se trata del proceso de identificar, analizar y clasificar los riesgos según su importancia y urgencia, para estimar la probabilidad de ocurrencias de un fraude y el impacto de los riesgos, mientras que la priorización implica asignar recursos y acciones para mitigarlos, el desarrollo de esta actividad es un factor clave para la gestión de proyectos, la auditoría interna y la prevención de fraudes. Entre sus indicadores tenemos, probabilidad de ocurrencia de un fraude. |
| | Implementación de controles | Serrano (2018) es el proceso de poner en práctica las medidas de prevención, detección y mitigación de los riesgos que pueden afectar el funcionamiento y los objetivos de una organización con el uso de sistemas confiables, con esto se garantiza tener un registro de acceso de todos los usuarios con la finalidad de monitorear continuamente y así garantizar la eficacia y la eficiencia de las actividades. |

**5. Presentación de instrucciones para el juez:**

A continuación, a usted le presento el cuestionario "Seguridad informática y riesgo operacional en una entidad financiera, Los Olivos 2023**"** elaborado por Tello Neira, Mary Nardhy en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

| Categoría | Calificación | Indicador |
|---|---|---|
| **CLARIDAD** El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas. | 1. No cumple con el criterio | El ítem no es claro. |
| | 2. Bajo Nivel | El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas. |
| | 3. Moderado nivel | Se requiere una modificación muy específica de algunos de los términos del ítem |
| | 4. Alto nivel | El ítem es claro, tiene semántica y sintaxis adecuada. |
| **COHERENCIA** El ítem tiene relación lógica con la dimensión o indicador que está midiendo. | 1. Totalmente en desacuerdo (no cumple con el criterio) | El ítem no tiene relación lógica con la dimensión. |
| | 2. Desacuerdo (bajo nivel de acuerdo) | El ítem tiene una relación tangencial /lejana con la dimensión. |
| | 3. Acuerdo (moderado nivel) | El ítem tiene una relación moderada con la dimensión que se está midiendo. |
| | 4. Totalmente de Acuerdo (alto nivel) | El ítem se encuentra está relacionado con la dimensión que está midiendo. |
| **RELEVANCIA** El ítem es esencial o importante, es decir debe ser incluido. | 1. No cumple con el criterio | El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión. |
| | 2. Bajo Nivel | El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide |
| | 3. Moderado nivel | El ítem es relativamente importante. |
| | 4. Alto nivel | El ítem es muy relevante y debe ser |

*Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde*

*sus observaciones que considere pertinente*

| |
|---|
| 9. No cumple con el criterio |
| 10. Bajo Nivel |

| |
|---|
| 11. Moderado nivel |
| 12. Alto nivel |

**Variable del instrumento**: **SEGURIDAD INFORMATICA**

Primera dimensión: Protección de información

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Eficacia | 1 | 4 | 4 | 4 | |
| Efectividad | 2 | 4 | 4 | 4 | |
| Recursos | 3 | 4 | 4 | 4 | |

Segunda dimensión: Activo financiero

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Habilidad | 4 | 4 | 4 | 4 | |
| Herramienta | 5 | 4 | 4 | 4 | |
| Detección | 6 | 4 | 4 | 4 | |

- Tercera dimensión: Confidencialidad

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Recuperación | 7 | 4 | 4 | 4 | |
| Implementación | 8 | 4 | 4 | 4 | |
| Medidas | 9 | 4 | 4 | 4 | |

**Variable del instrumento**: **Riesgo operacional**

- Primera dimensión: Identificación de riesgo

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Riesgo operacional | 10 | 4 | 4 | 4 | |
| Ciberataque | 11 | 4 | 4 | 4 | |
| Controles | 12 | 4 | 4 | 4 | |

- Segunda dimensión: Evaluación y priorización

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Probabilidad de ocurrencia de un fraude | 13 | 4 | 4 | 4 | |
| Fraude | 14 | 4 | 4 | 4 | |
| Uso inteligente de los buscadores de internet | 15 | 4 | 4 | 4 | |

- Tercera dimensión: Implementación de controles

| Indicadores | Ítem | Claridad | Coherencia | Relevancia | Observaciones |
|---|---|---|---|---|---|
| Sistema confinable | 16 | 4 | 4 | 4 | |
| Politicas | 17 | 4 | 4 | 4 | |
| Procedimientos | 18 | 4 | 4 | 4 | |

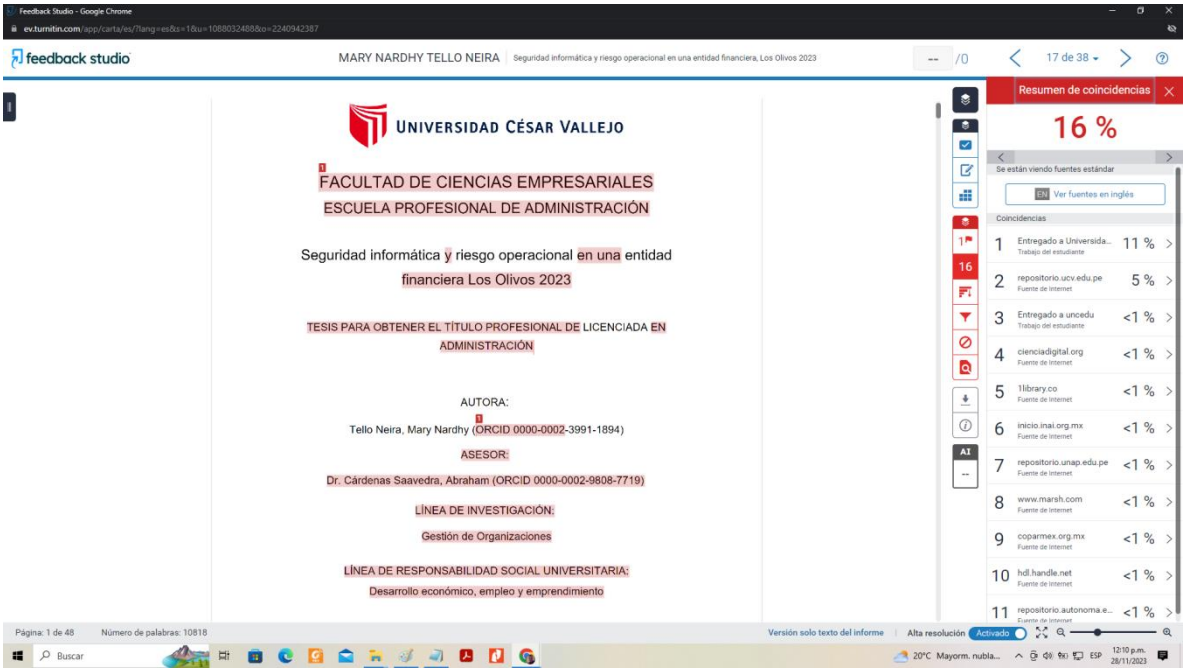

Pd.: el presente formato debe tomar en cuenta:

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra

Bibliografía

# Anexo 4. Resultados de similitud



## Anexo 5. Estadística de fiabilidad

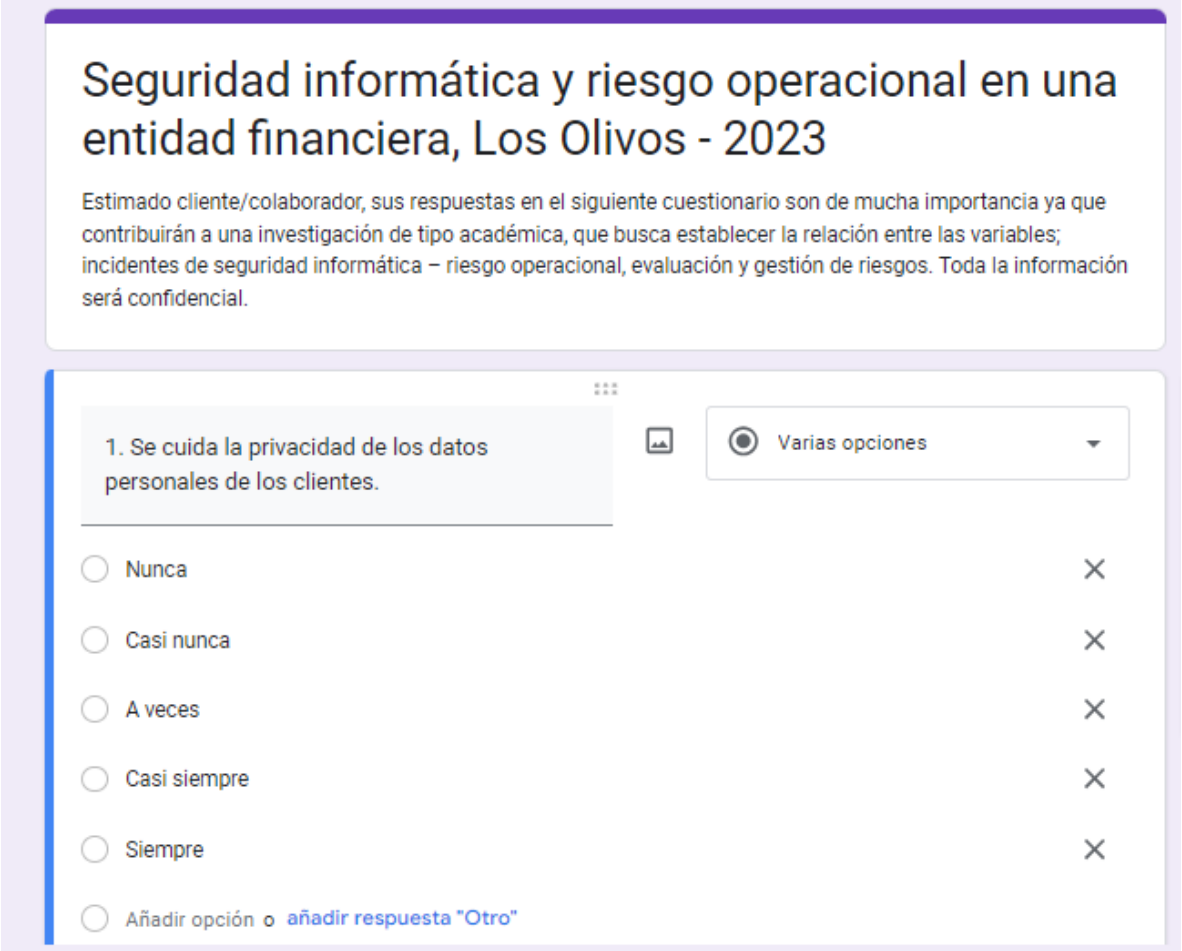
### Fiabilidad de la variable 1: Seguridad informática

| Estadísticas de fiabilidad | |
|---|---|
| Alfa de Cronbach | N de elementos |
| ,834 | 10 |

### Fiabilidad de la variable 2: Riesgo operacional

| Estadísticas de fiabilidad | |
|---|---|
| Alfa de Cronbach | N de elementos |
| ,793 | 10 |

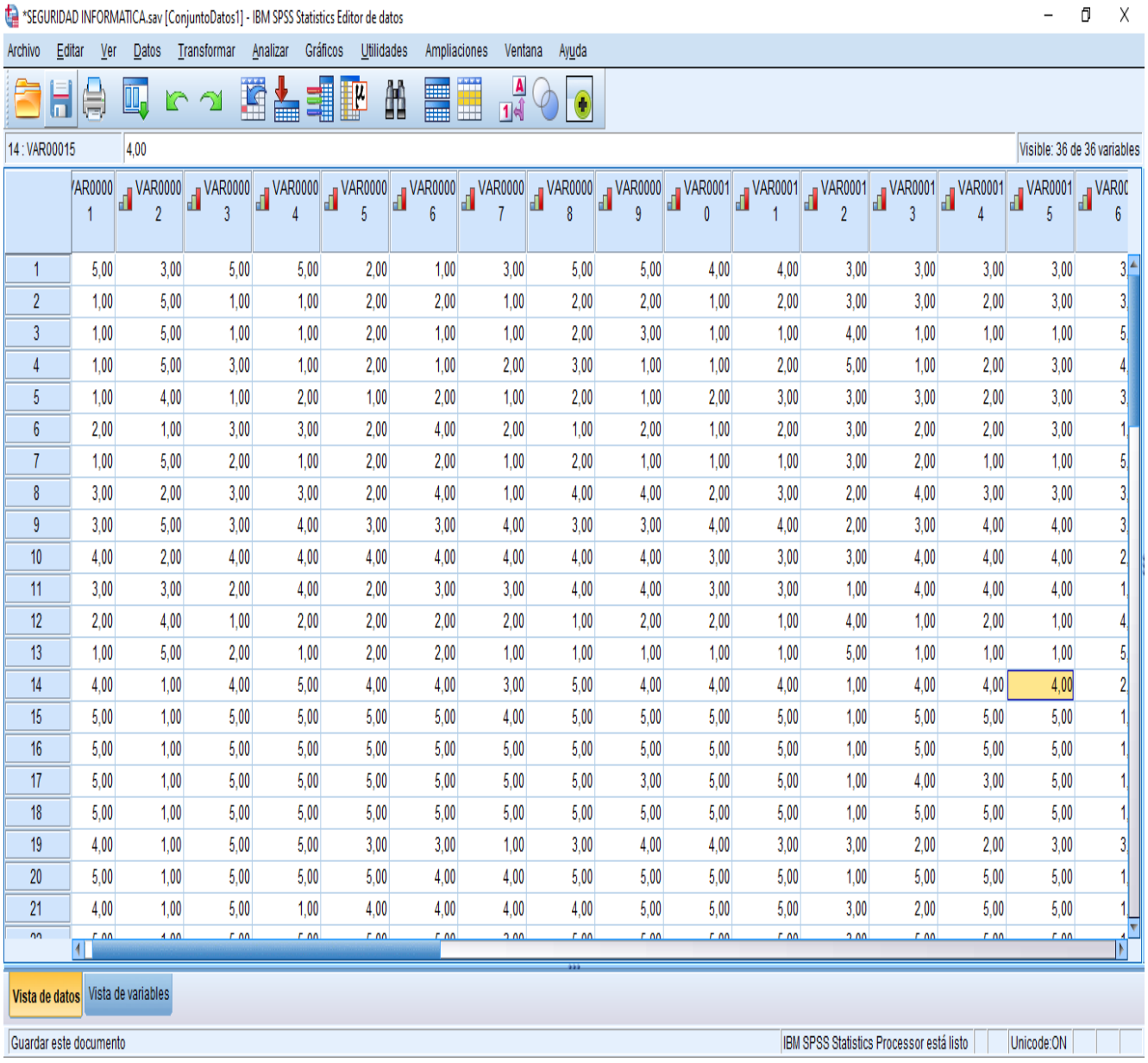
**Anexo 6. Evidencia de recojo de información – Cuestionario virtual**



# Anexo 7. Base de datos de la encuesta de Seguridad informática y riesgo operacional

| V1 SEGURIDAD INFORMATICA | | | | | | | | | | V2 RIESGO OPERACIONAL | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROTECCION DE INFORMACIÓN | | | | ACTIVO FINANCIERO | | | CONFIDENCIALIDAD | | | IDENTIFICACION DE RIESGO | | | | EVALUACION Y PRIORIZACION | | | IMPLEMENTACION DE CONTROLES | | |
| Pregunta 1 | Pregunta 2 | Pregunta 3 | Pregunta 4 | Pregunta 5 | Pregunta 6 | Pregunta 7 | Pregunta 8 | Pregunta 9 | Pregunta 10 | Pregunta 11 | Pregunta 12 | Pregunta 13 | Pregunta 14 | Pregunta 15 | Pregunta 16 | Pregunta 17 | Pregunta 18 | Pregunta 19 | Pregunta 20 |
| 5 | 3 | 5 | 5 | 2 | 1 | 3 | 5 | 5 | 4 | 4 | 3 | 3 | 3 | 3 | 3 | 2 | 4 | 4 | 3 |
| 1 | 5 | 1 | 1 | 2 | 2 | 1 | 2 | 2 | 1 | 2 | 3 | 3 | 2 | 3 | 3 | 2 | 3 | 2 | 2 |
| 1 | 5 | 1 | 1 | 2 | 1 | 1 | 2 | 3 | 1 | 1 | 4 | 1 | 1 | 1 | 5 | 3 | 1 | 1 | 1 |
| 1 | 5 | 3 | 1 | 2 | 1 | 2 | 3 | 1 | 1 | 2 | 5 | 1 | 2 | 3 | 4 | 2 | 1 | 2 | 1 |
| 1 | 4 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 3 | 3 | 3 | 2 | 3 | 3 | 2 | 1 | 2 | 2 |
| 2 | 1 | 3 | 3 | 2 | 4 | 2 | 1 | 2 | 1 | 2 | 3 | 2 | 2 | 3 | 1 | 3 | 1 | 2 | 1 |
| 1 | 5 | 2 | 1 | 2 | 2 | 1 | 2 | 1 | 1 | 1 | 3 | 2 | 1 | 1 | 5 | 1 | 2 | 1 | 1 |
| 3 | 2 | 3 | 3 | 2 | 4 | 1 | 4 | 4 | 2 | 3 | 2 | 4 | 3 | 3 | 3 | 4 | 3 | 4 | 3 |
| 3 | 5 | 3 | 4 | 3 | 3 | 4 | 3 | 3 | 4 | 4 | 2 | 3 | 4 | 4 | 3 | 4 | 1 | 5 | 4 |
| 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 | 2 | 4 | 4 | 5 | 5 |
| 3 | 3 | 2 | 4 | 2 | 3 | 3 | 4 | 4 | 3 | 3 | 1 | 4 | 4 | 4 | 1 | 3 | 3 | 4 | 3 |
| 2 | 4 | 1 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 1 | 4 | 1 | 2 | 1 | 4 | 1 | 2 | 2 | 2 |
| 1 | 5 | 2 | 1 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 1 |
| 4 | 1 | 4 | 5 | 4 | 4 | 3 | 5 | 4 | 4 | 4 | 1 | 4 | 4 | 4 | 2 | 5 | 4 | 4 | 4 |
| 5 | 1 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 5 | 5 | 1 | 4 | 3 | 5 | 1 | 3 | 5 | 5 | 5 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 4 | 4 | 5 | 5 |
| 4 | 1 | 5 | 5 | 3 | 3 | 1 | 3 | 4 | 4 | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 4 |
| 5 | 1 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 4 | 1 | 5 | 1 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 3 | 2 | 5 | 5 | 1 | 5 | 5 | 5 | 4 |
| 5 | 1 | 5 | 5 | 5 | 5 | 3 | 5 | 5 | 5 | 5 | 3 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 4 | 1 | 3 | 3 | 3 | 2 | 3 | 4 | 4 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 3 | 3 | 4 | 2 |
| 5 | 3 | 4 | 5 | 5 | 4 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 3 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 3 | 5 | 1 | 4 | 5 | 4 | 1 | 1 | 5 | 5 | 5 |
| 5 | 1 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 2 | 4 | 4 | 5 | 1 | 4 | 5 | 4 | 5 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 1 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 1 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 1 | 4 | 5 | 5 | 1 | 5 | 4 | 5 | 5 |
| 5 | 1 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 1 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 3 |
| 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 2 | 5 | 5 | 5 | 2 | 5 | 5 | 5 | 5 |
| 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 5 | 1 | 5 | 5 | 5 | 5 | 3 | 5 | 5 | 5 | 5 | 2 | 5 | 5 | 5 | 3 | 2 | 5 | 5 | 3 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 4 | 1 | 4 | 2 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 1 | 4 | 4 | 4 | 1 | 4 | 4 | 4 | 4 |
| 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 5 | 3 | 3 | 3 | 5 | 3 | 3 | 3 | 3 |
| 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 5 | 3 | 3 | 3 | 3 |
| 1 | 3 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 5 | 3 | 3 | 3 | 5 | 3 | 3 | 3 | 3 |
| 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 |
| 1 | 5 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 3 | 3 | 2 | 3 | 5 | 3 | 3 | 3 | 1 |
| 1 | 5 | 1 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 1 |
| 1 | 5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 1 |
| 1 | 5 | 1 | 1 | 3 | 1 | 1 | 1 | 1 | 1 | 3 | 5 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 1 |
| 1 | 5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 5 | 1 | 1 | 1 | 1 |

## Anexo 8. Procesamiento estadístico de la base de datos en el paquete estadístico SPSS V.26



*SEGURIDAD INFORMATICA.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

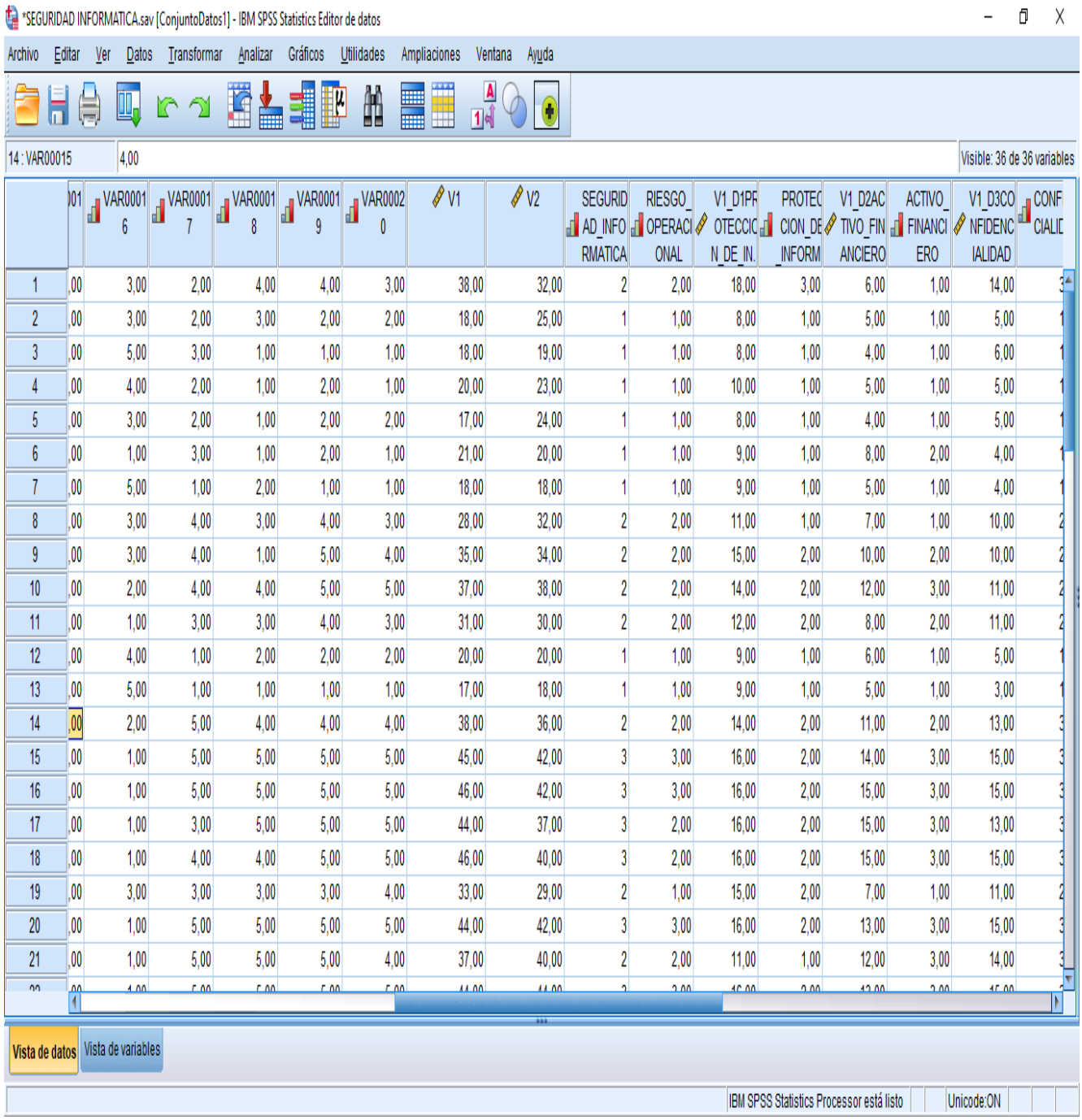
Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

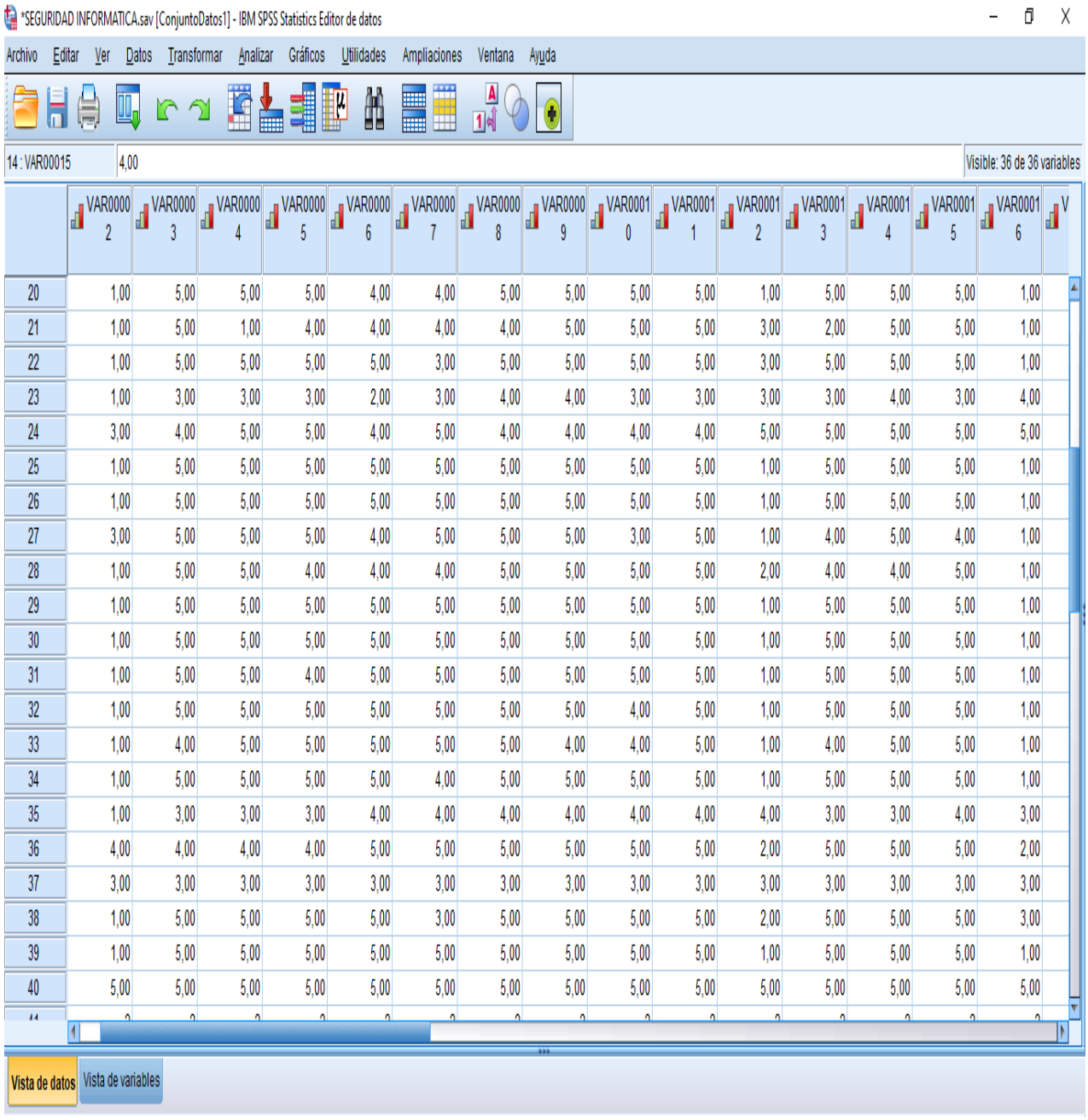
14 : VAR00015 | 4,00 | Visible: 36 de 36 variables

| | VAR00001 | VAR00002 | VAR00003 | VAR00004 | VAR00005 | VAR00006 | VAR00007 | VAR00008 | VAR00009 | VAR00010 | VAR00011 | VAR00012 | VAR00013 | VAR00014 | VAR00015 | VAR00016 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 5,00 | 3,00 | 5,00 | 5,00 | 2,00 | 1,00 | 3,00 | 5,00 | 5,00 | 4,00 | 4,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3 |
| 2 | 1,00 | 5,00 | 1,00 | 1,00 | 2,00 | 2,00 | 1,00 | 2,00 | 2,00 | 1,00 | 2,00 | 3,00 | 3,00 | 2,00 | 3,00 | 3 |
| 3 | 1,00 | 5,00 | 1,00 | 1,00 | 2,00 | 1,00 | 1,00 | 2,00 | 3,00 | 1,00 | 1,00 | 4,00 | 1,00 | 1,00 | 1,00 | 5 |
| 4 | 1,00 | 5,00 | 3,00 | 1,00 | 2,00 | 1,00 | 2,00 | 3,00 | 1,00 | 1,00 | 2,00 | 5,00 | 1,00 | 2,00 | 3,00 | 4 |
| 5 | 1,00 | 4,00 | 1,00 | 2,00 | 1,00 | 2,00 | 1,00 | 2,00 | 1,00 | 2,00 | 3,00 | 3,00 | 3,00 | 2,00 | 3,00 | 3 |
| 6 | 2,00 | 1,00 | 3,00 | 3,00 | 2,00 | 4,00 | 2,00 | 1,00 | 2,00 | 1,00 | 2,00 | 3,00 | 2,00 | 2,00 | 3,00 | 1 |
| 7 | 1,00 | 5,00 | 2,00 | 1,00 | 2,00 | 2,00 | 1,00 | 2,00 | 1,00 | 1,00 | 1,00 | 3,00 | 2,00 | 1,00 | 1,00 | 5 |
| 8 | 3,00 | 2,00 | 3,00 | 3,00 | 2,00 | 4,00 | 1,00 | 4,00 | 4,00 | 2,00 | 3,00 | 2,00 | 4,00 | 3,00 | 3,00 | 3 |
| 9 | 3,00 | 5,00 | 3,00 | 4,00 | 3,00 | 3,00 | 4,00 | 3,00 | 3,00 | 4,00 | 4,00 | 2,00 | 3,00 | 4,00 | 4,00 | 3 |
| 10 | 4,00 | 2,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 3,00 | 3,00 | 3,00 | 4,00 | 4,00 | 4,00 | 2 |
| 11 | 3,00 | 3,00 | 2,00 | 4,00 | 2,00 | 3,00 | 3,00 | 4,00 | 4,00 | 3,00 | 3,00 | 1,00 | 4,00 | 4,00 | 4,00 | 1 |
| 12 | 2,00 | 4,00 | 1,00 | 2,00 | 2,00 | 2,00 | 2,00 | 1,00 | 2,00 | 2,00 | 1,00 | 4,00 | 1,00 | 2,00 | 1,00 | 4 |
| 13 | 1,00 | 5,00 | 2,00 | 1,00 | 2,00 | 2,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 5,00 | 1,00 | 1,00 | 1,00 | 5 |
| 14 | 4,00 | 1,00 | 4,00 | 5,00 | 4,00 | 4,00 | 3,00 | 5,00 | 4,00 | 4,00 | 4,00 | 1,00 | 4,00 | 4,00 | 4,00 | 2 |
| 15 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1 |
| 16 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1 |
| 17 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 3,00 | 5,00 | 5,00 | 1,00 | 4,00 | 3,00 | 5,00 | 1 |
| 18 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1 |
| 19 | 4,00 | 1,00 | 5,00 | 5,00 | 3,00 | 3,00 | 1,00 | 3,00 | 4,00 | 4,00 | 3,00 | 3,00 | 2,00 | 2,00 | 3,00 | 3 |
| 20 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 4,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1 |
| 21 | 4,00 | 1,00 | 5,00 | 1,00 | 4,00 | 4,00 | 4,00 | 4,00 | 5,00 | 5,00 | 5,00 | 3,00 | 2,00 | 5,00 | 5,00 | 1 |

Vista de datos | Vista de variables

Guardar este documento | IBM SPSS Statistics Processor está listo | Unicode:ON


*SEGURIDAD INFORMATICA.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos
Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda
14 : VAR00015
4,00
Visible: 36 de 36 variables
001 VAR00016 VAR00017 VAR00018 VAR00019 VAR00020 V1 V2 SEGURIDAD_INFORMATICA RIESGO_OPERACIONAL V1_D1PROTECCION_DE_IN. PROTECCION_DE_INFORM V1_D2ACTIVO_FINANCIERO ACTIVO_FINANCIERO V1_D3CONFIDENCIALIDAD CONFIDENCIALID
1 ,00 3,00 2,00 4,00 4,00 3,00 38,00 32,00 2 2,00 18,00 3,00 6,00 1,00 14,00 3
2 ,00 3,00 2,00 3,00 2,00 2,00 18,00 25,00 1 1,00 8,00 1,00 5,00 1,00 5,00 1
3 ,00 5,00 3,00 1,00 1,00 1,00 18,00 19,00 1 1,00 8,00 1,00 4,00 1,00 6,00 1
4 ,00 4,00 2,00 1,00 2,00 1,00 20,00 23,00 1 1,00 10,00 1,00 5,00 1,00 5,00 1
5 ,00 3,00 2,00 1,00 2,00 2,00 17,00 24,00 1 1,00 8,00 1,00 4,00 1,00 5,00 1
6 ,00 1,00 3,00 1,00 2,00 1,00 21,00 20,00 1 1,00 9,00 1,00 8,00 2,00 4,00 1
7 ,00 5,00 1,00 2,00 1,00 1,00 18,00 18,00 1 1,00 9,00 1,00 5,00 1,00 4,00 1
8 ,00 3,00 4,00 3,00 4,00 3,00 28,00 32,00 2 2,00 11,00 1,00 7,00 1,00 10,00 2
9 ,00 3,00 4,00 1,00 5,00 4,00 35,00 34,00 2 2,00 15,00 2,00 10,00 2,00 10,00 2
10 ,00 2,00 4,00 4,00 5,00 5,00 37,00 38,00 2 2,00 14,00 2,00 12,00 3,00 11,00 2
11 ,00 1,00 3,00 3,00 4,00 3,00 31,00 30,00 2 2,00 12,00 2,00 8,00 2,00 11,00 2
12 ,00 4,00 1,00 2,00 2,00 2,00 20,00 20,00 1 1,00 9,00 1,00 6,00 1,00 5,00 1
13 ,00 5,00 1,00 1,00 1,00 1,00 17,00 18,00 1 1,00 9,00 1,00 5,00 1,00 3,00 1
14 ,00 2,00 5,00 4,00 4,00 4,00 38,00 36,00 2 2,00 14,00 2,00 11,00 2,00 13,00 3
15 ,00 1,00 5,00 5,00 5,00 5,00 45,00 42,00 3 3,00 16,00 2,00 14,00 3,00 15,00 3
16 ,00 1,00 5,00 5,00 5,00 5,00 46,00 42,00 3 3,00 16,00 2,00 15,00 3,00 15,00 3
17 ,00 1,00 3,00 5,00 5,00 5,00 44,00 37,00 3 2,00 16,00 2,00 15,00 3,00 13,00 3
18 ,00 1,00 4,00 4,00 5,00 5,00 46,00 40,00 3 2,00 16,00 2,00 15,00 3,00 15,00 3
19 ,00 3,00 3,00 3,00 3,00 4,00 33,00 29,00 2 1,00 15,00 2,00 7,00 1,00 11,00 2
20 ,00 1,00 5,00 5,00 5,00 5,00 44,00 42,00 3 3,00 16,00 2,00 13,00 3,00 15,00 3
21 ,00 1,00 5,00 5,00 5,00 4,00 37,00 40,00 2 2,00 11,00 1,00 12,00 3,00 14,00 3
Vista de datos
Vista de variables
IBM SPSS Statistics Processor está listo
Unicode:ON




| | VAR00002 | VAR00003 | VAR00004 | VAR00005 | VAR00006 | VAR00007 | VAR00008 | VAR00009 | VAR00010 | VAR00011 | VAR00012 | VAR00013 | VAR00014 | VAR00015 | V |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 | 1,00 | 5,00 | 5,00 | 5,00 | 4,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 21 | 1,00 | 5,00 | 1,00 | 4,00 | 4,00 | 4,00 | 4,00 | 5,00 | 5,00 | 5,00 | 3,00 | 2,00 | 5,00 | 5,00 | 1,00 | |
| 22 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 3,00 | 5,00 | 5,00 | 5,00 | 5,00 | 3,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 23 | 1,00 | 3,00 | 3,00 | 3,00 | 2,00 | 3,00 | 4,00 | 4,00 | 3,00 | 3,00 | 3,00 | 3,00 | 4,00 | 3,00 | 4,00 | |
| 24 | 3,00 | 4,00 | 5,00 | 5,00 | 4,00 | 5,00 | 4,00 | 4,00 | 4,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | |
| 25 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 26 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 27 | 3,00 | 5,00 | 5,00 | 5,00 | 4,00 | 5,00 | 5,00 | 5,00 | 3,00 | 5,00 | 1,00 | 4,00 | 5,00 | 4,00 | 1,00 | |
| 28 | 1,00 | 5,00 | 5,00 | 4,00 | 4,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 2,00 | 4,00 | 4,00 | 5,00 | 1,00 | |
| 29 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 30 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 31 | 1,00 | 5,00 | 5,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 32 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 4,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 33 | 1,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 4,00 | 4,00 | 5,00 | 1,00 | 4,00 | 5,00 | 5,00 | 1,00 | |
| 34 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 35 | 1,00 | 3,00 | 3,00 | 3,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 3,00 | 3,00 | 4,00 | 3,00 | |
| 36 | 4,00 | 4,00 | 4,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 2,00 | 5,00 | 5,00 | 5,00 | 2,00 | |
| 37 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | |
| 38 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 3,00 | 5,00 | 5,00 | 5,00 | 5,00 | 2,00 | 5,00 | 5,00 | 5,00 | 3,00 | |
| 39 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 40 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | |

*SEGURIDAD INFORMATICA.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

14 : VAR00015 | 4,00 | Visible: 36 de 36 variables

| | VAR00002 | VAR00003 | VAR00004 | VAR00005 | VAR00006 | VAR00007 | VAR00008 | VAR00009 | VAR00010 | VAR00011 | VAR00012 | VAR00013 | VAR00014 | VAR00015 | VAR00016 | V |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 31 | 1,00 | 5,00 | 5,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 32 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 4,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 33 | 1,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 4,00 | 4,00 | 5,00 | 1,00 | 4,00 | 5,00 | 5,00 | 1,00 | |
| 34 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 35 | 1,00 | 3,00 | 3,00 | 3,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 3,00 | 3,00 | 4,00 | 3,00 | |
| 36 | 4,00 | 4,00 | 4,00 | 4,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 2,00 | 5,00 | 5,00 | 5,00 | 2,00 | |
| 37 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | |
| 38 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 3,00 | 5,00 | 5,00 | 5,00 | 5,00 | 2,00 | 5,00 | 5,00 | 5,00 | 3,00 | |
| 39 | 1,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 1,00 | 5,00 | 5,00 | 5,00 | 1,00 | |
| 40 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | 5,00 | |
| 41 | 1,00 | 4,00 | 2,00 | 3,00 | 3,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 1,00 | 4,00 | 4,00 | 4,00 | 1,00 | |
| 42 | 1,00 | 1,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 5,00 | 3,00 | 3,00 | 3,00 | 5,00 | |
| 43 | 3,00 | 3,00 | 3,00 | 2,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 3,00 | 2,00 | 5,00 | |
| 44 | 3,00 | 3,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 5,00 | 3,00 | 3,00 | 3,00 | 5,00 | |
| 45 | 2,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 4,00 | 2,00 | 4,00 | 4,00 | 4,00 | 4,00 | |
| 46 | 5,00 | 3,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 2,00 | 1,00 | 3,00 | 3,00 | 2,00 | 3,00 | 5,00 | |
| 47 | 5,00 | 1,00 | 3,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 5,00 | 1,00 | 1,00 | 1,00 | 5,00 | |
| 48 | 5,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 5,00 | 1,00 | 1,00 | 1,00 | 5,00 | |
| 49 | 5,00 | 1,00 | 1,00 | 3,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 3,00 | 5,00 | 1,00 | 1,00 | 1,00 | 5,00 | |
| 50 | 5,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 5,00 | 1,00 | 1,00 | 1,00 | 5,00 | |
| 51 | | | | | | | | | | | | | | | | |
| 52 | | | | | | | | | | | | | | | | |

Vista de datos | Vista de variables